►B

REGULAMENTO DE EXECUÇÃO (UE) 2016/799 DA COMISSÃO

de 18 de março de 2016

que dá execução ao Regulamento (UE) n.º 165/2014 do Parlamento Europeu e do Conselho que estabelece os requisitos para construção, ensaio, instalação, funcionamento e reparação de tacógrafos e seus componentes

(Texto relevante para efeitos do EEE)

(JO L 139 de 26.5.2016, p. 1)

Retificado por:

►C1 Retificação, JO L 146 de 3.6.2016, p. 31 (2016/799)

►C2 Retificação, JO L 27 de 1.2.2017, p. 169 (2016/799)

▼B

REGULAMENTO DE EXECUÇÃO (UE) 2016/799 DA COMISSÃO

de 18 de março de 2016

que dá execução ao Regulamento (UE) n.º 165/2014 do Parlamento Europeu e do Conselho que estabelece os requisitos para construção, ensaio, instalação, funcionamento e reparação de tacógrafos e seus componentes

(Texto relevante para efeitos do EEE)

Artigo 1.º

Objeto e âmbito de aplicação

1. O presente regulamento estabelece as disposições necessárias para a aplicação uniforme dos seguintes aspetos, relativos aos tacógrafos:

a) registo da posição do veículo em certos pontos durante o período de trabalho diário do condutor;

b) deteção rápida à distância de eventual manipulação ou uso indevido de tacógrafos inteligentes;

c) interface com sistemas de transporte inteligentes;

d) os requisitos administrativos e técnicos para os procedimentos de homologação de tacógrafos, incluindo os mecanismos de segurança.

2. A construção, o ensaio, a instalação, a inspeção, o funcionamento e a reparação de tacógrafos inteligentes e dos respetivos componentes devem cumprir os requisitos técnicos constantes do anexo 1C do presente regulamento.

3. No que respeita à construção, ao ensaio, à instalação, à inspeção, ao funcionamento e à reparação, os tacógrafos, com exceção dos tacógrafos inteligentes, devem continuar a cumprir os requisitos do anexo 1 ou do anexo 1B do Regulamento (CEE) n.º 3821/85 do Conselho ([1]), consoante o que for aplicável.

4. Nos termos do artigo 10.º, alínea d) da Diretiva 96/53/CE, o sistema de deteção rápida à distância deve também transmitir os dados relativos aos pesos, fornecidos por um sistema interno de pesagem a bordo, para efeitos de deteção precoce de fraudes.

Artigo 2.º

Definições

Para efeitos do presente regulamento, aplicam-se as definições estabelecidas no artigo 2.º do Regulamento (UE) n.º 165/2014.

Aplicam-se igualmente as seguintes definições:

1) «tacógrafo digital» ou «tacógrafo da primeira geração»: tacógrafo digital que não seja um tacógrafo inteligente;

2) «módulo GNSS externo»: módulo que contém o recetor GNSS quando a unidade-veículo não é uma unidade única, bem como outros componentes necessários à proteção da comunicação de dados sobre a posição para o resto da unidade-veículo;

([1]) Regulamento (CEE) n.º 3821/85 do Conselho, de 20 de dezembro de 1985, relativo à introdução de um aparelho de controlo no domínio dos transportes rodoviários (JO L 370 de 31.12.1985, p. 8).

▼B

3) «dossier de fabrico»: o dossier completo, em formato eletrónico ou em papel, que contém todas as informações fornecidas pelo fabricante ou pelo seu mandatário à autoridade de homologação para efeitos da homologação de tacógrafos ou de componentes, incluindo os certificados referidos no artigo 12.º, n.º 3, do Regulamento (UE) n.º 165/2014, o resultado dos ensaios definidos no anexo 1C do presente regulamento, assim como desenhos, fotografias e outros documentos pertinentes;

4) «dossier de homologação»: o dossier de fabrico, em formato eletrónico ou em papel, acompanhado de outros documentos adicionados ao dossier de fabrico pela autoridade de homologação no exercício das suas funções, incluindo, no termo do processo de homologação, o certificado de homologação CE do tacógrafo ou de um componente do tacógrafo;

5) «índice do dossier de homologação»: o documento com o conteúdo numerado do dossier de homologação que identifica todas as partes relevantes do presente dossier. O formato desse documento deve distinguir as fases sucessivas no processo de homologação CE, incluindo as datas de revisões e atualizações desse dossier;

6) «sistema de deteção rápida à distância»: o aparelho da unidade-veículo que é utilizado para realizar os controlos rodoviários visados;

7) «tacógrafo inteligente» ou «tacógrafo da segunda geração»: o tacógrafo digital que cumpre o prescrito nos artigos 8.º, 9.º e 10.º do Regulamento (UE) n.º 165/2014, bem como no anexo 1C do presente regulamento;

8) «componente do tacógrafo» ou «componente»: qualquer um dos seguintes elementos: unidade-veículo, sensor de movimentos, cartão tacográfico, folha de registo, módulo GNSS externo e sistema de deteção rápida à distância;

9) «autoridade de homologação»: a autoridade de um Estado-Membro que tem competência para realizar a homologação do tacógrafo ou dos seus componentes, o processo de autorização, a emissão e, se for caso disso, a revogação dos certificados de homologação, agir como ponto de contacto para as autoridades de homologação de outros Estados-Membros e garantir que os fabricantes cumprem as suas obrigações no que diz respeito à conformidade com o prescrito no presente regulamento.

Artigo 3.º

Serviços baseados na localização

1. Os fabricantes devem garantir que os tacógrafos inteligentes são compatíveis com os serviços de posicionamento fornecidos pelos sistemas Galileu e Serviço Europeu Complementar de Navegação Geoestacionária («EGNOS»).

2. Além dos sistemas referidos no n.º 1, os fabricantes podem também optar por garantir a compatibilidade com outros sistemas de navegação por satélite.

▼B

Artigo 4.º

Procedimento para homologação de tacógrafos e componentes dos tacógrafos

1. Os fabricantes ou seus mandatários devem apresentar o pedido de homologação de um modelo de tacógrafo, de qualquer um dos seus componentes ou de grupos de componentes às autoridades de homologação para esse efeito designadas por cada Estado-Membro. O pedido compreende um dossier de fabrico que contém as informações relativas a cada um dos componentes em questão, incluindo, se for caso disso, os certificados de homologação de outros componentes necessários à conclusão do tacógrafo, bem como quaisquer outros documentos pertinentes.

2. Os Estados-Membros devem conceder a homologação aos modelos de tacógrafo, de componente ou de grupo de componentes que estejam em conformidade com os requisitos administrativos e técnicos constantes do artigo 1.º, n.º 2 ou n.º 3, consoante o que for aplicável. Nesse caso, a autoridade de homologação emite ao requerente um certificado de homologação conforme com o modelo estabelecido no anexo II do presente regulamento.

3. A autoridade de homologação pode solicitar informações adicionais ao fabricante (ou ao seu mandatário).

4. O fabricante (ou o seu mandatário) deve disponibilizar às autoridades de homologação, bem como às entidades responsáveis pela emissão dos certificados referidos no artigo 12.º, n.º 3, do Regulamento (UE) n.º 165/2014, os tacógrafos ou componentes de tacógrafos que sejam necessários para permitir a condução satisfatória do procedimento de homologação.

5. Sempre que o fabricante (ou o seu mandatário) visar a homologação de determinados componentes ou grupos de componentes de um tacógrafo, deve fornecer às autoridades de homologação os outros componentes já homologados, bem como outras peças necessárias à construção integral do tacógrafo, a fim de que as autoridades de homologação realizem os ensaios necessários.

Artigo 5.º

Alterações às homologações

1. O fabricante (ou o seu mandatário) deve comunicar imediatamente às autoridades de homologação que concederam a homologação original qualquer alteração do *software*, do equipamento informático ou da natureza dos materiais utilizados no fabrico do tacógrafo que estão registados no dossier de homologação e apresentar um pedido para a alteração da homologação.

2. As autoridades de homologação podem rever ou prorrogar uma homologação existente ou emitir uma nova homologação, de acordo com a natureza e as características das alterações.

Se a autoridade de homologação considerar que as alterações do *software*, do equipamento informático ou da natureza dos materiais utilizados no fabrico são pequenas, deve proceder a uma «revisão». Nesses casos, deve emitir os documentos revistos do dossier de homologação, indicando a natureza das alterações efetuadas e a data da sua homologação. Para cumprimento do presente requisito, será suficiente a versão atualizada do dossier de homologação em forma consolidada, acompanhada de uma descrição pormenorizada das alterações.

▼B

Se a autoridade de homologação considerar que as alterações do *software*, do equipamento informático ou da natureza dos materiais utilizados no fabrico são substanciais, deve proceder a uma «prorrogação». Nesses casos, pode solicitar novos ensaios e informar o fabricante (ou o seu mandatário) em conformidade. Se os novos ensaios forem satisfatórios, a autoridade de homologação deve emitir um certificado de homologação revisto que contém um número relativo à prorrogação concedida. O certificado de homologação deve mencionar o motivo da prorrogação e a correspondente data de emissão.

3. O índice do dossier de homologação deve indicar a data da mais recente prorrogação ou revisão da homologação ou a data da mais recente consolidação da versão atualizada da homologação.

4. Se as alterações exigidas para o tacógrafo homologado ou para os seus componentes homologados conduzirem à emissão de um novo certificado de segurança ou interoperabilidade, será necessária nova homologação.

Artigo 6.º

Entrada em vigor

O presente regulamento entra em vigor no vigésimo dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*.

O presente regulamento é aplicável a partir de 2 de março de 2016.

No entanto, os anexos são aplicáveis a partir de 2 de março de 2019, com exceção do apêndice 16, que é aplicável a partir de 2 de março de 2016.

O presente regulamento é obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros.

▼B

ANEXO IC

Condições de construção, ensaio, instalação e controlo

▼B

3.9.11	Incidente «Erro de comunicação com o módulo GNSS externo»
3.9.12	Incidente «erro nos dados de movimento»
3.9.13	Incidente «Conflito relativo ao movimento do veículo»
3.9.14	Incidente «tentativa de violação da segurança»
3.9.15	Incidente «conflito de tempo»
3.9.16	Falha do «cartão»
3.9.17	Falha do «aparelho de controlo»
3.10	Ensaios incorporados e autoensaios
3.11	Leitura da memória de dados
3.12	Registo e memorização de dados na memória
3.12.1	Dados de identificação do aparelho
3.12.1.1	Dados de identificação da unidade-veículo
3.12.1.2	Dados de identificação do sensor de movimentos
3.12.1.3	Dados de identificação dos sistemas globais de navegação por satélite
3.12.2	Chaves e certificados
3.12.3	Dados relativos à inserção e à retirada de cartões de condutor ou de oficina
3.12.4	Dados relativos à atividade de condutor
3.12.5	Locais e posições em que se iniciam e concluem os períodos diários de trabalho e/ou em que são alcançados os períodos de três horas de condução contínua
3.12.6	Dados do conta-quilómetros
3.12.7	Dados relativos à velocidade
3.12.8	Dados relativos a incidentes
3.12.9	Dados relativos a falhas
3.12.10	Dados relativos à calibração
3.12.11	Dados relativos ao ajustamento do tempo
3.12.12	Dados relativos à atividade de controlo
3.12.13	Dados relativos aos bloqueamentos da empresa
3.12.14	Dados relativos à atividade de descarregamento
3.12.15	Dados relativos às condições especiais
3.12.16	Dados relativos ao cartão tacográfico
3.13	Leitura de cartões tacográficos
3.14	Registo e memorização de dados nos cartões tacográficos
3.14.1	Registo e memorização de dados nos cartões tacográficos de primeira geração
3.14.2	Registo e memorização de dados nos cartões tacográficos da segunda geração
3.15	Visualização
3.15.1	Visualização por defeito
3.15.2	Visualização de alerta

▼B

▼B

4.5.3.1.10	Dados relativos à utilização de veículos
4.5.3.1.11	Locais de início e/ou final dos períodos de trabalho diário
4.5.3.1.12	Dados relativos à sessão de cartão
4.5.3.1.13	Dados relativos à atividade de controlo
4.5.3.1.14	Dados relativos às condições especiais
4.5.3.2	Aplicação tacográfica da segunda geração (não acessível às unidades-veículo de primeira geração)
4.5.3.2.1	Identificação da aplicação
4.5.3.2.2	Chaves e certificados
4.5.3.2.3	Identificação do cartão
4.5.3.2.4	Identificação do titular
4.5.3.2.5	Descarregamento do cartão
4.5.3.2.6	Elementos relativos à carta de condução
4.5.3.2.7	Dados relativos a incidentes
4.5.3.2.8	Dados relativos a falhas
4.5.3.2.9	Dados relativos à atividade de condutor
4.5.3.2.10	Dados relativos à utilização de veículos
4.5.3.2.11	Locais e posições de início e/ou final dos períodos de trabalho diário
4.5.3.2.12	Dados relativos à sessão de cartão
4.5.3.2.13	Dados relativos à atividade de controlo
4.5.3.2.14	Dados relativos às condições especiais
4.5.3.2.15	Dados relativos à utilização de unidades-veículo
4.5.3.2.16	Dados relativos à localização das três horas de condução contínua
4.5.4	Cartão de oficina
4.5.4.1	Aplicação tacográfica (acessível às unidades-veículo das primeira e segunda gerações)
4.5.4.1.1	Identificação da aplicação
4.5.4.1.2	Chaves e certificados
4.5.4.1.3	Identificação do cartão
4.5.4.1.4	Identificação do titular
4.5.4.1.5	Descarregamento do cartão
4.5.4.1.6	Dados relativos à calibração e ao ajustamento do tempo
4.5.4.1.7	Dados relativos a incidentes e a falhas
4.5.4.1.8	Dados relativos à atividade de condutor
4.5.4.1.9	Dados relativos à utilização de veículos
4.5.4.1.10	Dados relativos ao início e/ou ao final dos períodos de trabalho diário
4.5.4.1.11	Dados relativos à sessão de cartão
4.5.4.1.12	Dados relativos à atividade de controlo

▼B

4.5.4.1.13	Dados relativos às condições especiais
4.5.4.2	Aplicação tacográfica de segunda geração (não acessível às unidades-veículo de primeira geração)
4.5.4.2.1	Identificação da aplicação
4.5.4.2.2	Chaves e certificados
4.5.4.2.3	Identificação do cartão
4.5.4.2.4	Identificação do titular
4.5.4.2.5	Descarregamento do cartão
4.5.4.2.6	Dados relativos à calibração e ao ajustamento do tempo
4.5.4.2.7	Dados relativos a incidentes e a falhas
4.5.4.2.8	Dados relativos à atividade de condutor
4.5.4.2.9	Dados relativos à utilização de veículos
4.5.4.2.10	Dados relativos ao início e/ou ao final dos períodos de trabalho diário
4.5.4.2.11	Dados relativos à sessão de cartão
4.5.4.2.12	Dados relativos à atividade de controlo
4.5.4.2.13	Dados relativos à utilização de unidades-veículo
4.5.4.2.14	Dados relativos à localização das três horas de condução contínua
4.5.4.2.15	Dados relativos às condições especiais
4.5.5	Cartão de controlo
4.5.5.1	Aplicação tacográfica (acessível às unidades-veículo das primeira e segunda gerações)
4.5.5.1.1	Identificação da aplicação
4.5.5.1.2	Chaves e certificados
4.5.5.1.3	Identificação do cartão
4.5.5.1.4	Identificação do titular
4.5.5.1.5	Dados relativos à atividade de controlo
4.5.5.2	Aplicação tacográfica G2 (não acessível a unidades-veículo da primeira geração)
4.5.5.2.1	Identificação da aplicação
4.5.5.2.2	Chaves e certificados
4.5.5.2.3	Identificação do cartão
4.5.5.2.4	Identificação do titular
4.5.5.2.5	Dados relativos à atividade de controlo
4.5.6	Cartão de empresa
4.5.6.1	Aplicação tacográfica (acessível às unidades-veículo das primeira e segunda gerações)
4.5.6.1.1	Identificação da aplicação
4.5.6.1.2	Chaves e certificados
4.5.6.1.3	Identificação do cartão

▼B

PREÂMBULO

O sistema tacográfico digital da primeira geração está em funcionamento desde 1 de maio de 2006, podendo ser utilizado até ao final da sua vida nos transportes de âmbito nacional. Em contrapartida, no que respeita aos transportes internacionais, todos os veículos devem ser equipados com os tacógrafos inteligentes da segunda geração de que trata o presente regulamento da Comissão, no prazo de 15 anos após a entrada em vigor do regulamento.

O presente anexo contém os requisitos destinados aos aparelhos de controlo e cartões tacográficos da segunda geração. A partir da data de introdução, devem ser instalados aparelhos de controlo da segunda geração nos veículos matriculados pela primeira vez e devem ser emitidos cartões tacográficos da segunda geração.

A fim de promover a introdução harmoniosa do sistema tacográfico da segunda geração:

▼B

— os cartões tacográficos da segunda geração devem ser concebidos de modo a poderem ser igualmente utilizados nas unidades-veículo da primeira geração;

— não será requerida a substituição de cartões tacográficos da primeira geração que estejam válidos na data de introdução.

Tal permitirá que o condutor mantenha o seu próprio cartão de condutor e o utilize em ambos os sistemas.

No entanto, o aparelho de controlo da segunda geração deverá ser calibrado utilizando unicamente cartões de oficina da segunda geração.

O presente anexo contém todos os requisitos relacionados com a interoperabilidade entre o sistema tacográfico da primeira e da segunda geração.

O apêndice 15 contém mais informações sobre gestão da coexistência entre os dois sistemas.

Lista dos apêndices

1 DEFINIÇÕES

Para efeitos do disposto no presente anexo, entende-se por:

a) «Ativação»

a fase no decurso da qual o tacógrafo se torna plenamente operacional e executa todas as funções, incluindo as de segurança, por recurso a um cartão de oficina;

b) «Autenticação»

função destinada a estabelecer e verificar uma identidade alegada;

c) «Autenticidade»

o facto de determinada informação provir de uma parte cuja identidade pode ser verificada;

d) «Ensaio incorporado (BIT)»

o ensaio realizado a pedido, acionado por efeito do operador ou de um mecanismo externo;

▼B

e) «Dia»

um dia, das 0 horas às 24 horas. Todos os dias se reportam à hora UTC (tempo universal coordenado);

f) «Calibração» de um tacógrafo inteligente

a atualização ou confirmação dos parâmetros do veículo a guardar na memória de dados. Os parâmetros do veículo compreendem a identificação — VIN (número de identificação do veículo), VRN (número de matrícula do veículo) e Estado-Membro de matrícula — e as características do veículo (w, k, l, medida dos pneumáticos, ponto de regulação do dispositivo de limitação da velocidade quando aplicável, hora UTC no momento e valor do conta-quilómetros no momento); durante a calibração de um aparelho de controlo, também devem ser memorizados na memória de dados os tipos e os identificadores de todos os selos relevantes de homologação do tipo, em vigor;

qualquer atualização ou confirmação apenas da hora UTC será considerada um ajustamento de tempo e não uma calibração, desde que não esteja em contradição com o requisito n.º 409;

a calibração de um aparelho de controlo é feita por intermédio de um cartão de oficina;

g) «Número do cartão»

um conjunto de 16 carateres alfanuméricos que identificam inequivocamente um cartão tacográfico dentro de um Estado-Membro. O número do cartão inclui índice de série (quando aplicável), índice de substituição e índice de renovação do cartão;

por conseguinte, o cartão é identificado inequivocamente pelo seu número e pelo código do Estado-Membro emissor;

h) «Índice de série do cartão»

o 14.º caráter alfanumérico do número do cartão, destinado a distinguir os diversos cartões tacográficos atribuídos a uma empresa, a uma oficina ou a uma autoridade de controlo que tenham direito a mais do que um. A empresa, oficina ou autoridade de controlo é identificada inequivocamente pelos primeiros 13 carateres do número do cartão;

i) «Índice de renovação do cartão»

o 16.º caráter alfanumérico do número do cartão tacográfico, que sobe uma unidade cada vez que o cartão é renovado;

j) «Índice de substituição do cartão»:

o 15.º caráter alfanumérico do número do cartão tacográfico, que sobe uma unidade cada vez que o cartão é substituído;

k) «Coeficiente característico do veículo»

característica numérica que dá o valor do sinal de saída emitido pela peça prevista no veículo que faz a ligação deste ao aparelho de controlo (na saída da caixa de velocidades ou nas rodas do veículo, conforme os casos), sempre que o veículo percorrer a distância de 1 quilómetro, medida em condições normais de ensaio, conforme a definição constante do requisito n.º 414. O coeficiente característico é expresso em impulsos por quilómetro (w = … imp/km);

l) «Cartão de empresa»

cartão tacográfico emitido pelas autoridades de um Estado-Membro a uma empresa de transporte rodoviário que necessite de utilizar veículos equipados com tacógrafo, o qual identifica a empresa de transporte e permite visualizar, descarregar e imprimir os dados memorizados no tacógrafo que tenham sido bloqueados por essa empresa de transporte;

▼B

m) «Constante do aparelho de controlo»

a característica numérica que dá o valor do sinal de entrada necessário para obter a indicação e o registo do percurso de uma distância de 1 km; esta constante é expressa em impulsos por quilómetro (k = … imp/km);

n) «Tempo de condução contínua», calculado no aparelho de controlo do seguinte modo (1)

somatório (calculado pelo aparelho de controlo) dos tempos de condução acumulados por um condutor desde o final do seu último período de AVAILABILITY (disponibilidade) ou BREAK/REST (pausa/repouso) ou UNKNOWN (2) (desconhecido) de 45 minutos ou mais [este período pode ter sido cindido em conformidade com o Regulamento (CE) n.º 561/2006 do Parlamento Europeu e do Conselho (3)]. Os cálculos têm em conta, conforme necessário, atividades passadas registadas no cartão do condutor. Se o condutor não tiver inserido o seu cartão, os cálculos baseiam-se nos registos da memória de dados relativos ao período durante o qual não houve inserção e à correspondente faixa horária;

o) «Cartão de controlo»

cartão tacográfico emitido pelas autoridades de um Estado-Membro a uma autoridade nacional responsável pelo controlo, que identifica o organismo e, a título facultativo, o agente de controlo e que permite o acesso aos dados registados na memória ou nos cartões de condutor e, a título facultativo, nos cartões de oficina, para efeitos de leitura, impressão e/ou descarregamento;

deve igualmente dar acesso à função de controlo da calibração de estrada e aos dados existentes do leitor de comunicação da deteção rápida à distância;

p) «Tempo acumulado de pausas», calculado no aparelho de controlo do seguinte modo (1)

as pausas acumuladas no tempo de condução são calculadas como o somatório dos tempos de AVAILABILITY, BREAK/REST ou UNKNOWN (2) de 15 minutos ou mais, desde o final do último período de AVAILABILITY, BREAK/REST ou UNKNOWN (2) de 45 minutos ou mais [este período pode ter sido cindido em conformidade com o Regulamento (CE) n.º 561/2006].

Os cálculos têm em conta, conforme necessário, atividades passadas registadas no cartão do condutor. Os períodos desconhecidos de duração negativa (em que o início é posterior ao final), devidos a sobreposições de tempo entre dois aparelhos de controlo distintos, não são tidos em conta para o cálculo.

(1) Esta forma de calcular o tempo de condução contínua e o tempo acumulado de pausas permite ao aparelho de controlo calcular o aviso de tempo de condução contínua. Não prejudica a interpretação jurídica desses intervalos. Podem utilizar-se formas alternativas de calcular o tempo de condução contínua e o tempo acumulado de pausas para substituir estas definições se elas se tornarem obsoletas devido a atualizações noutra legislação pertinente.

(2) Os períodos UNKNOWN são aqueles em que o cartão do condutor não estava inserido no aparelho de controlo e relativamente aos quais as atividades do condutor não foram introduzidas manualmente.

(3) Regulamento (CE) n.º 561/2006 do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativo à harmonização de determinadas disposições em matéria social no domínio dos transportes rodoviários, que altera os Regulamentos (CEE) n.º 3821/85 e (CEE) n.º 2135/98 do Conselho e revoga o Regulamento (CEE) n.º 3820/85 do Conselho (JO L 102 de 11.4.2006, p. 1).

▼B

Se o condutor não tiver inserido o seu cartão, os cálculos baseiam-se nos registos da memória de dados relativos ao período durante o qual não houve inserção e à correspondente faixa horária;

q) «Memória de dados»

dispositivo eletrónico de memorização de dados, incorporado no aparelho de controlo;

r) «Assinatura digital»

os dados apensos a um bloco de dados (ou transformação criptográfica do mesmo), que permitem ao recetor comprovar a autenticidade e a integridade do bloco de dados;

s) «Descarga»

cópia, juntamente com a assinatura digital, de uma parte ou de um conjunto completo de ficheiros de dados registados na memória da unidade-veículo ou na memória de um cartão tacográfico, desde que este processo não altere nem suprima nenhum dado armazenado;

Os fabricantes de unidades-veículo de tacógrafos inteligentes e os fabricantes de aparelhos projetados e destinados ao descarregamento de ficheiros de dados devem tomar todas as medidas razoáveis para assegurar que o descarregamento desses dados pode ser executado num tempo mínimo para as empresas de transportes ou os condutores.

O descarregamento do ficheiro detalhado da velocidade pode não ser necessário para determinar a conformidade com o Regulamento (CE) n.º 561/2006, mas pode ser utilizado para outros fins, como a investigação de acidentes;

t) «Cartão de condutor»

cartão tacográfico emitido pelas autoridades de um Estado-Membro a um determinado condutor, que identifica o condutor e permite memorizar os dados relativos às suas atividades;

u) «Perímetro efetivo dos pneus das rodas»

média das distâncias percorridas por cada uma das rodas de tração do veículo (rodas motoras) durante uma rotação completa. A medição destas distâncias deve ser feita nas condições normais de ensaio, conforme a definição constante do requisito n.º 414, e é expressa sob a forma: «l = … mm». Os fabricantes dos veículos podem substituir a medição destas distâncias por um cálculo teórico que tenha em conta a distribuição do peso pelos eixos (veículo sem carga e em ordem normal de marcha) ([1]). Os métodos para esse cálculo teórico estão sujeitos a aprovação por uma autoridade nacional competente e só podem ser aplicados antes da ativação do tacógrafo;

v) «Incidente»

operação anormal, detetada pelo tacógrafo inteligente, que pode resultar de uma tentativa de fraude;

w) «Módulo GNSS externo»

módulo que contém o recetor GNSS quando a unidade-veículo não é uma unidade única, bem como outros componentes necessários à proteção da comunicação de dados sobre a posição para o resto da unidade-veículo;

([1]) Regulamento (UE) n. º 1230/2012 da Comissão, de 12 de dezembro de 2012, que dá execução ao Regulamento (CE) n.º 661/2009 do Parlamento Europeu e do Conselho no que respeita aos requisitos de homologação para massas e dimensões dos veículos a motor e seus reboques e altera a Diretiva 2007/46/CE do Parlamento Europeu e do Conselho (JO L 353 de 21.12.2012, p. 31), na sua última redação.

▼B

x) «Falha»

operação anormal, detetada pelo tacógrafo inteligente, que pode resultar de uma deficiência ou avaria do equipamento;

y) «Recetor GNSS»

dispositivo eletrónico que recebe e processa digitalmente os sinais a partir de um ou mais sistemas globais de navegação por satélite (GNSS), a fim de fornecer a posição, a velocidade e informação sobre o tempo;

z) «Instalação»

montagem de um tacógrafo num veículo;

aa) «Interoperabilidade»

capacidade dos sistemas e dos processos industriais que lhes estão subjacentes para trocar dados e partilhar informações;

bb) «Interface»

instalação entre sistemas que fornece os meios de comunicação através dos quais estes podem ligar-se e interagir;

cc) «Posição»

as coordenadas geográficas do veículo num determinado momento;

dd) «Sensor de movimentos»

o componente do tacógrafo que emite um sinal representativo da velocidade do veículo e/ou da distância percorrida;

ee) «Cartão não válido»

cartão no qual foi detetada uma falha, cuja autenticação inicial falhou, cuja data de início da validade não foi ainda alcançada ou cuja data de caducidade foi já ultrapassada;

ff) «Norma aberta»

norma definida num documento de especificação de normas disponível gratuitamente ou a preço simbólico, passível de ser copiada, distribuída ou utilizada gratuitamente ou contra pagamento simbólico;

gg) «Fora de âmbito»

situação em que não é exigível a utilização do aparelho de controlo, nos termos do Regulamento (CE) n.º 561/2006;

hh) «Excesso de velocidade»

a ultrapassagem da velocidade máxima autorizada para o veículo. Define-se como um período superior a 60 segundos durante o qual a velocidade medida do veículo excede o limite relativo à fixação do dispositivo de limitação da velocidade, constante da Diretiva 92/6/CEE do Conselho ([1]), na sua última redação;

ii) «Inspeção periódica»

conjunto de operações destinadas a verificar se o tacógrafo funciona corretamente, se as suas características de regulação correspondem aos parâmetros do veículo e se não lhe foram fixados dispositivos de manipulação;

([1]) Diretiva 92/6/CEE do Conselho, de 10 de fevereiro de 1992, relativa à instalação e utilização de dispositivos de limitação de velocidade para certas categorias de veículos a motor na Comunidade (JO L 57 de 2.3.1992, p. 27).

▼B

jj) «Impressora»

componente do aparelho de controlo que exibe sob forma impressa os dados memorizados;

kk) «Comunicação de deteção rápida à distância»

comunicação entre o sistema de comunicação de deteção rápida à distância e o leitor de comunicação de deteção rápida à distância, durante os controlos de estrada seletivos, com o objetivo de detetar à distância eventuais manipulações ou utilizações indevidas dos aparelhos de controlo;

ll) «Sistema de comunicação à distância»

equipamento da unidade-veículo utilizado para controlos de estrada seletivos;

mm) «Leitor de comunicação de deteção rápida à distância»

sistema utilizado pelos agentes de controlo para os controlos de estrada seletivos;

nn) «Renovação»

a emissão de um novo cartão tacográfico quando o existente atinge o prazo de validade ou acusa defeito e é devolvido à autoridade emissora. A renovação implica sempre a certeza de não coexistirem dois cartões válidos;

oo) «Reparação»

qualquer reparação de um sensor de movimentos, de uma unidade-veículo ou de um cabo que exige que a sua fonte de alimentação energética seja desligada, ou desligada de outros componentes do tacógrafo, ou a abertura desse sensor ou dessa unidade-veículo;

pp) «Substituição do cartão»

emissão de um cartão tacográfico em substituição de um existente que tenha sido declarado extraviado, subtraído ou defeituoso e não tenha sido devolvido à autoridade emissora. A substituição implica sempre o risco de coexistirem dois cartões válidos;

qq) «Certificação de segurança»

processo destinado a certificar, por um organismo de certificação de critérios comuns, se o aparelho (ou o componente) de controlo ou o cartão tacográfico em investigação cumprem os requisitos de segurança definidos nos perfis de proteção em questão;

rr) «Autoensaio»

ensaio realizado cíclica e automaticamente pelo aparelho de controlo, com vista a detetar falhas;

ss) «Medição de tempo»

registo digital permanente da data e do tempo universal coordenado (UTC);

tt) «Ajustamento de tempo»

um ajustamento automático do tempo atual a intervalos regulares e com tolerância máxima de um minuto, ou um ajustamento efetuado durante a calibração;

uu) «Medida do pneumático»

designação das dimensões dos pneumáticos (rodas motoras externas), em conformidade com a Diretiva 92/23/CEE do Conselho ([1]), na sua última redação;

([1]) Diretiva 92/23/CEE do Conselho, de 31 de março de 1992, relativa aos pneumáticos dos veículos a motor e seus reboques bem como à respectiva instalação nesses veículos (JO L 129 de 14.5.1992, p. 95).

▼B

vv) «Identificação do veículo»

números identificativos do veículo: número de matrícula do veículo (VRN), com indicação do Estado-Membro de matrícula, e número de identificação do veículo (VIN) ([1]);

ww) «Semana»

intervalo utilizado pelo aparelho de controlo nos cálculos e que vai das 00h00 UTC de segunda-feira às 24h00 UTC de domingo;

xx) «Cartão de oficina»

cartão tacográfico emitido pelas autoridades de um Estado-Membro a elementos designados de um fabricante ou instalador de tacógrafos, de um fabricante de veículos ou de uma oficina, aprovados por esse Estado-Membro, o qual identifica o titular do cartão e permite o ensaio, a calibração e a ativação de tacógrafos e/ou o descarregamento a partir de tacógrafos;

yy) «Adaptador»

dispositivo que fornece um sinal permanentemente representativo da velocidade do veículo e/ou da distância por ele percorrida, diferente do utilizado para a deteção de movimentos independentes, e que é:

— instalado e utilizado unicamente em veículos das categorias M1 e N1 (conforme a definição constante do anexo II da Diretiva 2007/46/CE do Parlamento Europeu e do Conselho ([2]), na sua última redação) colocado em serviço desde 1 de maio de 2006;

— instalado onde não é mecanicamente possível instalar qualquer outro tipo de sensor de movimentos existente que, por outro lado, cumpre o disposto no presente anexo e nos seus apêndices 1 a 15;

— instalado entre a unidade-veículo e o ponto onde os impulsos velocidade/distância são gerados por sensores integrados ou interfaces alternativas;

— visto de uma unidade-veículo, o comportamento do adaptador é idêntico ao que se verificará se à unidade-veículo estiver ligado um sensor de movimentos que cumpra o disposto no presente anexo e nos seus apêndices 1 a 16;

a utilização de um tal adaptador nos veículos acima referidos deve permitir instalar e utilizar corretamente uma unidade-veículo que cumpra todos os requisitos do presente anexo,

nos veículos em causa, o tacógrafo inteligente inclui cabos, um adaptador e uma unidade-veículo;

([1]) Diretiva 76/114/CEE do Conselho, de 18 de dezembro de 1975, relativa à aproximação das legislações dos Estados-Membros respeitantes às chapas e inscrições regulamentares, bem como à sua localização e modo de fixação no que respeita aos veículos a motor e seus reboques (JO L 24 de 30.1.1976, p. 1).

([2]) Diretiva 2007/46/CE do Parlamento Europeu e do Conselho, de 5 de setembro de 2007, que estabelece um quadro para a homologação dos veículos a motor e seus reboques, e dos sistemas, componentes e unidades técnicas destinados a serem utilizados nesses veículos (Directiva-Quadro) (JO L 263 de 9.10.2007, p. 1).

▼B

zz) Integridade dos dados:

precisão e consistência dos dados memorizados, indicada pela ausência de qualquer alteração nos dados entre duas atualizações de um registo de dados. A integridade implica que os dados sejam uma cópia exata da versão original: por exemplo, não terem sido corrompidos no processo de escrita para — e de leitura a partir de — um cartão tacográfico ou um equipamento dedicado ou durante a transmissão através de qualquer canal de comunicação;

aaa) Privacidade de dados:

medidas técnicas gerais que se tomam para garantir a correta aplicação dos princípios estabelecidos na Diretiva 95/46/CE do Parlamento Europeu e do Conselho ([1]), bem como dos procedimentos previstos na Diretiva 2002/58/CE do Parlamento Europeu e do Conselho ([2]);

bbb) Sistema tacográfico inteligente:

aparelhos de controlo, cartões tacográficos e conjunto de todos os equipamentos que interagem direta ou indiretamente durante a sua construção, a sua instalação, a sua utilização, o seu ensaio e o seu controlo, como cartões, leitor de comunicação à distância e qualquer outro aparelho de descarregamento de dados, análise de dados, calibração, geração, gestão ou produção de elementos de segurança, etc;

ccc) Data de produção:

36 meses após a entrada em vigor das disposições de execução referidas no artigo 11.º do Regulamento (UE) n.º 165/2014 do Parlamento Europeu e do Conselho ([3]).

É a data após a qual os veículos matriculados pela primeira vez:

— *devem estar equipados com um tacógrafo ligado a um serviço de posicionamento baseado num sistema de navegação por satélite*

— *devem poder comunicar dados para controlos de estrada seletivos às autoridades de controlo competentes, enquanto o veículo está em movimento*

— *e podem ser equipados com interfaces normalizadas que permitam a utilização, em modo de funcionamento, dos dados registados ou produzidos por tacógrafos, por um dispositivo externo;*

ddd) Perfil de proteção:

documento utilizado no âmbito do processo de certificação de acordo com critérios comuns, que fornece especificações independentes da aplicação dos requisitos da garantia de segurança da informação;

([1]) Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (JO L 281 de 23.11.1995, p. 31).

([2]) Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (JO L 201 de 31.7.2002, p. 37).

([3]) Regulamento (UE) n.º 165/2014 do Parlamento Europeu e do Conselho, de 4 de fevereiro de 2014, relativo à utilização de tacógrafos nos transportes rodoviários, que revoga o Regulamento (CEE) n.º 3821/85 do Conselho relativo à introdução de um aparelho de controlo no domínio dos transportes rodoviários e que altera o Regulamento (CE) n.º 561/2006 do Parlamento Europeu e do Conselho relativo à harmonização de determinadas disposições em matéria social no domínio dos transportes rodoviários (JO L 60 de 28.2.2014, p. 1).

▼B

eee) Precisão GNSS:

no contexto do registo da posição do sistema global de navegação por satélite (GNSS) com tacógrafos, significa o valor da *Horizontal Dilution of Precision* (HDOP) calculada como os valores mínimos HDOP recolhidos nos sistemas GNSS disponíveis.

2 CARACTERÍSTICAS GERAIS E FUNÇÕES DO APARELHO DE CONTROLO

2.1 **Características gerais**

O aparelho de controlo tem por função registar, memorizar, exibir, imprimir e transmitir os dados relativos às atividades do condutor.

Os veículos equipados com aparelhos de controlo que cumpram o disposto no presente anexo devem ter as funções de visualização da velocidade e de conta-quilómetros incorporadas no aparelho de controlo. Estas funções podem ser incluídas no aparelho de controlo.

1) O aparelho de controlo compreende os cabos de ligação, um sensor de movimentos e uma unidade-veículo.

2) A interface entre os sensores de movimento e as unidades-veículo deve cumprir o prescrito no apêndice 11.

3) A unidade-veículo deve estar ligada ao sistema global de navegação por satélite, conforme especifica o apêndice 12.

4) A unidade-veículo deve comunicar com leitores de comunicações de deteção rápida à distância, conforme especifica o apêndice 14.

5) A unidade-veículo pode incluir uma interface ITS especificada no apêndice 13

O aparelho de controlo pode estar ligado a outros sistemas através de interfaces adicionais e/ou através da interface ITS facultativa.

6) A inclusão de funções ou dispositivos, homologados ou não, no aparelho de controlo, ou a ligação de tais funções ou dispositivos ao aparelho de controlo não deve interferir, real ou potencialmente, com o seu funcionamento correto nem com o disposto no regulamento.

Os utilizadores identificam-se relativamente ao aparelho de controlo por intermédio de cartões tacográficos.

7) O aparelho de controlo proporciona direitos de acesso seletivo aos dados e funções em conformidade com o tipo e/ou a identidade do utilizador.

O aparelho de controlo regista e memoriza dados na sua memória, no sistema de comunicação à distância e nos cartões tacográficos.

Tal é feito em conformidade com a Diretiva 95/46/CE de 24 de outubro de 1995, relativa à proteção das pessoas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados ([1]), com a Diretiva 2002/58/CE, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas ([2]), e com o artigo 7.º do Regulamento (UE) n.º 165/2014.

([1]) JO L 281 de 23.11.1997, p. 31.
([2]) JO L 201 de 31.7.2002, p. 37.

▼B

2.2 **Funções**

8) O aparelho de controlo deve assegurar as seguintes funções:

— controlo da inserção e da retirada de cartões,

— medição da velocidade, da distância e da posição,

— medição do tempo,

— controlo das atividades do condutor,

— controlo da situação de condução,

— entradas efetuadas manualmente pelo condutor:

— introdução do lugar de início e/ou final do período diário de trabalho,

— introdução manual das atividades do condutor,

— introdução de condições especiais,

— gestão dos bloqueamentos da empresa,

— vigilância das atividades de controlo,

— deteção de incidentes e/ou falhas,

— ensaios incorporados e autoensaios,

— leitura de dados memorizados na memória,

— registo e memorização de dados na memória,

— leitura de cartões tacográficos,

— registo e memorização de dados nos cartões tacográficos,

— visualização de dados,

— impressão,

— alertas,

— descarregamento de dados para meios externos,

— comunicação à distância para controlos de estrada seletivos,

— dados de saída para sistemas adicionais,

— calibração,

— controlo de calibração de estrada

— ajustamento do tempo.

2.3 **Modos de funcionamento**

9) O aparelho de controlo deve possuir quatro modos de funcionamento:

— modo operacional,

— modo de controlo,

— modo de calibração,

— modo de empresa.

10) O aparelho de controlo deve passar para os modos de funcionamento indicados no quadro *infra*, consoante os cartões tacográficos válidos inseridos nas correspondentes interfaces. Na determinação do modo de funcionamento, a geração do cartão tacográfico é irrelevante, desde que o cartão inserido esteja válido. O cartão de oficina da primeira geração deve ser sempre considerado como não válido quando inserido numa VU de segunda geração.

▼B

Modo de funcionamento		Ranhura do condutor				
		Ausência de cartão	Cartão de condutor	Cartão de controlo	Cartão de oficina	Cartão de empresa
Ranhura do ajudante	Ausência de cartão	Operacional	Operacional	Controlo	Calibração	Empresa
	Cartão de condutor	Operacional	Operacional	Controlo	Calibração	Empresa
	Cartão de controlo	Controlo	Controlo	Controlo (*)	Operacional	Operacional
	Cartão de oficina	Calibração	Calibração	Operacional	Calibração (*)	Operacional
	Cartão de empresa	Empresa	Empresa	Operacional	Operacional	Empresa (*)

(*) Nestas situações, o aparelho de controlo utiliza unicamente o cartão tacográfico inserido na ranhura do condutor.

11) O aparelho de controlo ignora cartões não válidos inseridos, a menos que seja possível visualizar, imprimir ou descarregar dados constantes de um cartão expirado.

12) Todas as funções enunciadas na secção 2.2 devem estar operacionais em qualquer modo de funcionamento, com as seguintes exceções:

— a função de calibração é acessível unicamente em modo de calibração,

— a função de controlo da calibração de estrada é acessível unicamente em modo de controlo,

— a função de gestão dos bloqueamentos da empresa é acessível unicamente em modo de empresa,

— a função de vigilância das atividades de controlo é operacional unicamente em modo de controlo,

— a função de descarregamento não é acessível em modo operacional (com exceção do previsto no requisito n.º 193), com exceção do descarregamento de um cartão de condutor quando na VU não está inserido outro tipo de cartão.

13) O aparelho de controlo pode transmitir quaisquer dados para o visor, para a impressora ou para interfaces externas, com as seguintes exceções:

— em modo operacional, é apagada uma identificação pessoal (apelido e nome próprio) que não corresponda ao cartão tacográfico inserido e, num número de cartão que não corresponda ao cartão tacográfico inserido, são apagados os carateres discordantes (da esquerda para a direita),

— em modo de empresa, a saída de dados relativos ao condutor (requisitos n.os 102, 105 e 108) só pode concretizar-se quando se tratar de períodos em que não existe bloqueamento ou que não estão bloqueados por outra empresa (identificada pelos primeiros treze algarismos do número do seu cartão),

— se nenhum cartão tiver sido inserido no aparelho de controlo, só pode ser dada saída aos dados do condutor relativamente ao dia corrente e aos oito dias anteriores,

— os dados pessoais provenientes da VU não devem ser transmitidos através da interface ITS da VU, a menos que se verifique o consentimento do condutor a quem se referem os dados,

▼B

— as unidades-veículo têm um período normal de validade do funcionamento de 15 anos, a começar na data de emissão dos respetivos certificados, mas as unidades-veículo podem ser utilizadas por mais 3 meses, somente para descarregamento de dados.

2.4 **Segurança**

O dispositivo de segurança do sistema visa proteger a memória contra acesso e manipulação não autorizados dos dados, bem como detetar tentativas nesse sentido, proteger a integridade e a autenticidade dos dados intercambiados entre o sensor de movimentos e a unidade-veículo, entre o aparelho de controlo e os cartões tacográficos e entre o aparelho de controlo e o módulo GNSS externo, proteger a confidencialidade, a integridade e a autenticidade dos dados intercambiados através da comunicação de deteção rápida à distância para efeitos de controlo e verificar a integridade e a autenticidade dos dados descarregados.

14) A fim de obter a segurança do sistema, os componentes que se seguem devem satisfazer os requisitos de segurança especificados nos respetivos perfis de proteção, exigidos no apêndice 10:

— unidade-veículo,

— cartão tacográfico,

— sensor de movimentos,

— módulo GNSS externo (este perfil é necessário e aplicável somente para a variante GNSS externo).

3 REQUISITOS DE CONSTRUÇÃO E FUNCIONAMENTO DO APARELHO DE CONTROLO

3.1 **Controlo da inserção e da retirada de cartões**

15) O aparelho de controlo controla as interfaces dos cartões, para detetar inserções e retiradas dos cartões.

16) O aparelho de controlo deteta se o cartão inserido é um cartão tacográfico válido e, nessa eventualidade, identifica o tipo e a geração do cartão.

Se no aparelho de controlo tiver já sido inserido um cartão com o mesmo número mas com índice de renovação superior, o cartão será declarado não válido.

Se no aparelho de controlo tiver já sido inserido um cartão com o mesmo número e o mesmo índice de renovação mas com índice de substituição superior, o cartão será declarado não válido.

17) Os cartões tacográficos da primeira geração serão considerados como não válidos pelo aparelho de controlo quando a utilização de cartões tacográficos da primeira geração tiver sido suprimida por uma oficina, em conformidade com o apêndice 15 (req. MIG003).

18) Os cartões de oficina da primeira geração inseridos no aparelho de controlo da segunda geração serão considerados não válidos.

▼B

19) O aparelho de controlo deve ser concebido de modo a que os cartões tacográficos fiquem fixos quando inseridos corretamente nas correspondentes interfaces.

20) A libertação dos cartões tacográficos deve funcionar unicamente com o veículo parado e depois de neles introduzidos os dados pertinentes. Para o efeito de libertação, é necessária ação positiva do utilizador.

3.2 **Medição da velocidade, da posição e da distância**

21) O sensor de movimentos (possivelmente incorporado no adaptador) é a principal fonte para a medição da velocidade e da distância.

22) Esta função mede e fornece continuamente o valor do conta-quilómetros correspondente à distância total percorrida pelo veículo utilizando os impulsos fornecidos pelo sensor de movimentos.

23) Esta função mede e fornece continuamente a velocidade do veículo utilizando os impulsos fornecidos pelo sensor de movimentos.

24) A função de medição da velocidade deve igualmente informar se o veículo está em movimento ou parado. O veículo é considerado em movimento assim que, com base no sensor de movimentos, a função deteta mais de 1 imp/seg durante pelo menos 5 segundos — caso contrário, o veículo é considerado parado.

25) Os dispositivos que exibem a velocidade (velocímetro) e a distância total (conta-quilómetros), instalados em veículos equipados com aparelhos de controlo que cumpram o disposto no presente regulamento, devem cumprir os requisitos relativos a tolerâncias máximas, constantes do presente anexo (secções 3.2.1 e 3.2.2).

26) Para detetar a manipulação dos dados relativos ao movimento, a informação do sensor de movimentos deve ser corroborada por informação de movimentos do veículo derivada do recetor GNSS e, a título facultativo, de outras fontes independentes do sensor de movimentos.

27) Esta função deve medir a posição do veículo, a fim de permitir o registo automático de:

— posições em que o condutor e/ou o ajudante inicia o seu período diário de trabalho;

— posições em que o tempo de condução contínua do condutor atinge um múltiplo de três horas;

— posições em que o condutor e/ou o ajudante termina o seu período diário de trabalho.

3.2.1 *Medição da distância percorrida*

28) A distância percorrida pode ser medida de um dos seguintes modos:

— acumulando quer os movimentos de marcha em frente quer os de marcha atrás ou

— incluindo apenas os movimentos de marcha em frente.

29) O aparelho de controlo deve medir distâncias de 0 a 9 999 999,9 km.

▼B

30) As distâncias medidas devem situar-se dentro das seguintes tolerâncias (distâncias de pelo menos 1 000 m):

— ± 1 % antes da instalação,

— ± 2 % durante a instalação e a inspeção periódica,

— ± 4 % em uso.

31) A medição da distância deve ter uma resolução igual ou superior a 0,1 km.

3.2.2 *Medição da velocidade*

32) O aparelho de controlo deve medir a velocidade de 0 a 220 km/h.

33) Para garantir uma tolerância máxima de ± 6 km/h na velocidade medida durante a utilização, e tendo em conta:

— uma tolerância de ± 2 km/h para variações nos dados introduzidos (variações nos pneumáticos, etc.),

— uma tolerância de ± 1 km/h para medições efetuadas durante a instalação e a inspeção periódica,

o aparelho de controlo, para velocidades entre 20 e 180 km/h e para coeficientes característicos entre 4 000 e 25 000 imp/ /km, deve medir a velocidade com uma tolerância de ± 1 km/h (a velocidade constante).

Nota: A resolução da memorização de dados introduz uma tolerância adicional de ± 0,5 km/h na velocidade memorizada pelo aparelho de controlo.

34) A velocidade deve ser medida corretamente, cumprindo as tolerâncias normais, dentro de 2 segundos após ser consumada uma mudança de velocidade a uma aceleração até 2 m/s^2.

35) A medição da velocidade deve ter resolução igual ou superior a 1 km/h.

3.2.3 *Medição da posição*

36) O aparelho de controlo deve medir a posição absoluta do veículo utilizando o recetor GNSS.

37) A posição absoluta é medida em coordenadas geográficas de latitude e longitude em graus e minutos, com uma resolução de 1/10 de minuto.

3.3 **Medição do tempo**

38) Esta função deve medir permanentemente a data e a hora UTC e fornecê-las sob formato digital.

39) Os valores da data e da hora UTC serão utilizados para datar dados no aparelho de controlo (registos, intercâmbio de dados) e para todas as impressões indicadas no apêndice 4 («Impressão»).

40) Para efeitos de visualização da hora local, deve ser possível modificar o valor exibido em saltos de meia hora. Apenas são permitidas modificações do valor exibido em múltiplos negativos ou positivos de meia hora;

41) A deriva de tempo deve ser efetuada ± 2 segundos por dia, em condições de homologação do tipo, na ausência de qualquer ajustamento do tempo.

▼B

42) A medição do tempo deve ter uma resolução igual ou superior a 1 segundo.

43) A medição do tempo não deve ser afetada por um corte exterior na alimentação energética inferior a 12 meses, em condições de homologação do tipo.

3.4 **Controlo das atividades do condutor**

44) Esta função deve acompanhar permanente e separadamente as atividades de um condutor e de um ajudante.

45) Atividades de condutor: DRIVING (condução), WORK (trabalho), AVAILABILITY (disponibilidade) ou BREAK/REST (pausa/repouso).

46) Deve ser possível ao condutor e/ou ao ajudante selecionar manualmente WORK, AVAILABILITY ou BREAK/REST.

47) Com o veículo em movimento, é selecionada automaticamente a atividade DRIVING para o condutor e a atividade AVAILABILITY para o ajudante.

48) Com o veículo parado, é selecionada automaticamente a atividade WORK para o condutor.

49) A primeira mudança de atividade para REST ou AVAILABILITY que ocorra dentro de 120 segundos após a passagem automática para WORK, devido à paragem do veículo, é considerada como tendo ocorrido no momento da paragem do veículo (podendo, portanto, anular a passagem para WORK).

50) Esta função transmite as mudanças de atividade às funções de registo, com uma resolução de 1 minuto.

51) Se for registada uma atividade DRIVING dentro do minuto imediatamente anterior a um dado intervalo de 1 minuto ou dentro do minuto imediatamente posterior a ele, todo esse intervalo de 1 minuto será considerado DRIVING.

52) Dado um intervalo de 1 minuto que não seja considerado DRIVING nos termos do requisito n.º 51, todo esse intervalo será considerado como do mesmo tipo que a mais longa atividade contínua ocorrida dentro dele (ou a última de várias atividades igualmente longas).

53) Esta função deve também acompanhar permanentemente o tempo de condução contínua e o tempo acumulado de pausas do condutor.

3.5 **Controlo da situação de condução**

54) Esta função deve acompanhar permanente e automaticamente a situação da condução.

55) A situação de condução CREW (tripulação) é selecionada quando dois cartões válidos de condutor são inseridos no aparelho de controlo. Em qualquer outro caso, é selecionada a situação de condução SINGLE (elemento só).

3.6 **Entradas dos condutores**

3.6.1 *Introdução do lugar de início e/ou de final do período diário de trabalho*

56) Esta função permite introduzir os lugares em que se iniciam e/ou concluem os períodos diários de trabalho, segundo o condutor e/ou o ajudante.

▼B

57) Os lugares são definidos como o país e, quando igualmente pertinente, a região, que se introduzem ou confirmam manualmente.

58) No momento em que se retira um cartão de condutor, o aparelho de controlo pede que o condutor (ou ajudante) introduza um «lugar no qual termina o período diário de trabalho».

59) O condutor deve então introduzir o lugar atual do veículo, que será considerado uma entrada temporária.

60) Deve ser possível introduzir lugares de início e/ou final do período diário de trabalho por meio de comandos nos menus. Se se introduzir mais do que uma entrada desse tipo no intervalo de um minuto, será mantido apenas o registo da entrada relativa ao último lugar de início e ao último lugar final introduzidos nesse intervalo.

3.6.2 *Introdução manual das atividades dos condutores e consentimento para interface ITS*

61) Ao ser inserido um cartão de condutor (ou de oficina), e somente nessa situação, o aparelho de controlo permite a introdução manual de atividades. A introdução manual de atividades deve ser executada utilizando a hora local e os valores do fuso horário (UTC com compensação) selecionados para a unidade-veículo.

Aquando da inserção do cartão de condutor ou de oficina, o titular do cartão recebe, a título recapitulativo, as seguintes informações:

— data e hora da sua última retirada do cartão;

— opcionalmente: a hora local compensada, selecionada para a unidade-veículo.

Aquando da primeira inserção de um dado cartão de condutor ou cartão de oficina, de momento desconhecido da unidade-veículo, o titular do cartão é convidado a manifestar o seu consentimento para a saída de dados pessoais relacionados com o tacógrafo através da interface ITS opcional.

Desde que o cartão de condutor (ou de oficina) esteja inserido, o consentimento do condutor (ou da oficina) pode, a qualquer momento, ser ativado ou desativado por meio de comandos no menu.

Deve ser possível introduzir atividades, com as seguintes restrições:

— o tipo de atividade será WORK, AVAILABILITY ou BREAK/REST;

— a hora de início e de final de cada atividade situar-se-á dentro do período entre a última retirada e a atual inserção do cartão;

— não é permitida a sobreposição mútua de atividades.

Deve ser possível introduzir entradas manualmente, se necessário, na primeira inserção de um cartão de condutor (ou de oficina) não utilizado anteriormente.

▼B

O procedimento para introdução manual de atividades deve incluir tantas etapas consecutivas quantas as necessárias para selecionar um tipo, uma hora de início e uma hora de final para cada atividade. Em qualquer momento do período entre a última retirada do cartão e a atual inserção do cartão, o titular do cartão deve ter a opção de não declarar qualquer atividade.

Durante a introdução manual associada à inserção do cartão, e quando aplicável, o titular do cartão deve ter a oportunidade de introduzir:

— um lugar em que um período diário de trabalho anterior terminou, associado à hora pertinente (substituindo assim a entrada feita aquando da última retirada do cartão);

— um lugar em que teve início o atual período diário de trabalho, associado à hora pertinente.

Se for introduzido um lugar, este deve ser registado no cartão tacográfico pertinente.

A introdução manual pode ser interrompida se:

— o cartão for retirado; ou

— o veículo estiver em movimento e o cartão estiver na ranhura do condutor.

São permitidas interrupções adicionais (por exemplo, tempo esgotado após um determinado período de inatividade do utilizador). Se a introdução manual de dados for interrompida, o aparelho de controlo valida os dados completos já introduzidos relativamente ao lugar e à atividade (que tenham lugar ou hora inequívocos ou tenham tipo de atividade, hora de início e hora de final).

Se se inserir um segundo cartão de condutor ou de oficina enquanto está em curso a introdução manual de atividades para um cartão previamente inserido, é permitido terminar a introdução manual de dados para esse cartão anterior antes de se iniciar a introdução manual de dados para o segundo cartão.

O titular do cartão deve ter a opção de inserir dados manualmente de acordo com o seguinte procedimento mínimo:

— introduzir manualmente, por ordem cronológica, as atividades relativas ao período que vai da última retirada até à atual inserção;

— a hora de início da primeira atividade deve ser fixada com a hora de retirada do cartão. Em cada subsequente introdução de dados, a hora de início deve ser pré-fixada a fim de se seguir imediatamente à hora de final da precedente introdução de dados. Para cada atividade, devem ser selecionados o tipo e a hora de final.

▼B

O procedimento termina quando o tempo de final de uma atividade introduzida manualmente coincidir com o tempo de inserção do cartão. O aparelho de controlo permite então, opcionalmente, que o titular do cartão modifique atividades introduzidas manualmente, até à validação por seleção de um comando específico. A partir de então, já não serão permitidas tais modificações.

3.6.3 *Introdução de condições especiais*

62) O aparelho de controlo deve permitir ao condutor introduzir, em tempo real, as duas seguintes condições especiais:

— «OUT OF SCOPE» (fora de âmbito), com início e final;

— «FERRY/TRAIN CROSSING» (travessia de batelão/comboio), com início e final

Uma condição «FERRY/TRAIN CROSSING» não pode ocorrer se tiver sido aberta uma condição «OUT OF SCOPE».

Uma condição «OUT OF SCOPE» que tenha sido aberta deve ser automaticamente fechada pelo aparelho de controlo se se inserir ou retirar um cartão de condutor.

Uma condição «OUT OF SCOPE» que tenha sido aberta inibirá os seguintes incidentes e alertas:

— condução sem cartão adequado;

— alertas associados ao tempo de condução contínua.

O indicador de início de FERRY/TRAIN CROSSING deve ser definido antes de se desligar o motor no batelão/comboio.

Uma condição FERRY/TRAIN CROSSING aberta deve terminar quando ocorrer qualquer uma das seguintes opções:

— o condutor termina manualmente a condição FERRY/ /TRAIN CROSSING;

— o condutor ejeta o seu cartão

Uma condição FERRY/TRAIN CROSSING aberta termina quando deixa de ser válida, com base nas regras estabelecidas no Regulamento (CE) n.º 561/2006.

3.7 **Gestão dos bloqueamentos da empresa**

63) Esta função deve permitir que a gestão dos bloqueamentos efetuados por uma empresa restrinja a si o acesso aos dados em modo de empresa.

64) Os bloqueamentos da empresa compreendem uma data/hora de início (lock-in) e uma data/hora de cessação (lock-out), associadas à identificação da empresa por intermédio do número do seu cartão (no lock-in).

65) Os bloqueamentos só em tempo real podem ser desencadeados (lock-in) ou cessados (lock-out).

66) A cessação do bloqueamento (lock-out) só será possível à empresa que o tiver desencadeado (lock-in) (identificada pelos primeiros treze algarismos do número do respetivo cartão de empresa), ou,

67) O bloqueamento cessará automaticamente (lock-out) se outra empresa desencadear um bloqueamento (lock-in).

▼B

68) No caso de uma empresa desencadear um bloqueamento (lock-in), tendo o bloqueamento anterior sido para a mesma empresa, assume-se que o bloqueamento anterior não foi «cessado» e ainda está «desencadeado».

3.8 **Vigilância das atividades de controlo**

69) Esta função deve vigiar as atividades DISPLAYING (visualização), PRINTING (impressão), VU (unidade-veículo) e DOWNLOADING (descarga) do cartão, bem como as atividades de controlo ROADSIDE CALIBRATION (calibração em estrada), em modo de controlo.

70) Esta função deve vigiar também as atividades OVER SPEEDING CONTROL (controlo de excesso de velocidade), em modo de controlo. Considera-se que houve controlo de excesso de velocidade quando, em modo de controlo, é enviada a mensagem «excesso de velocidade» para a impressora ou para o visor ou quando da memória de dados da VU são descarregados «incidentes e falhas».

3.9 **Deteção de incidentes e/ou falhas**

71) Esta função deve detetar os seguintes incidentes e/ou falhas:

3.9.1 *Incidente «inserção de cartão não válido»*

72) Este incidente produz-se quando é inserido um cartão não válido, quando é inserido um cartão de condutor já substituído e/ou quando expira o prazo de validade de um cartão inserido.

3.9.2 *Incidente «conflito de cartões»*

73) Este incidente produz-se quando se verifica qualquer uma das combinações entre cartões válidos assinaladas com X no quadro seguinte:

Conflito de cartões		Ranhura do condutor				
		Ausência de cartão	Cartão de condutor	Cartão de controlo	Cartão de oficina	Cartão de empresa
Ranhura do ajudante	Ausência de cartão					
	Cartão de condutor				X	
	Cartão de controlo			X	X	X
	Cartão de oficina		X	X	X	X
	Cartão de empresa			X	X	X

3.9.3 *Incidente «sobreposição de tempos»*

74) Este incidente produz-se quando a data/hora da última retirada de um cartão de condutor, lida nesse cartão, é posterior à data/hora atual do aparelho de controlo no qual o cartão está inserido.

3.9.4 *Incidente «condução sem cartão adequado»*

75) Este incidente produz-se quando se verifica qualquer uma das combinações entre cartões tacográficos assinaladas com X no quadro seguinte, quando a atividade do condutor muda para DRIVING ou quando há mudança no modo de funcionamento sendo DRIVING a atividade do condutor:

▼B

Condução sem cartão adequado		Ranhura do condutor				
		Cartão ausente ou não válido	Cartão de condutor	Cartão de controlo	Cartão de oficina	Cartão de empresa
Ranhura do ajudante	Cartão ausente ou não-válido	X		X		X
	Cartão de condutor	X		X	X	X
	Cartão de controlo	X	X	X	X	X
	Cartão de oficina	X	X	X		X
	Cartão de empresa	X	X	X	X	X

3.9.5 *Incidente «inserção de cartão durante a condução»*

76) Este incidente produz-se quando é inserido um cartão tacográfico em qualquer ranhura sendo DRIVING a atividade do condutor.

3.9.6 *Incidente «última sessão de cartão encerrada incorretamente»*

77) Este incidente produz-se quando, na inserção de um cartão, o aparelho de controlo deteta que, apesar do disposto na secção 3.1, a anterior sessão não foi encerrada corretamente (cartão retirado antes de nele terem sido registados todos os dados importantes). Este incidente só se produz com cartões de condutor ou de oficina.

3.9.7 *Incidente «excesso de velocidade»*

78) Este incidente produz-se em situações de excesso de velocidade.

3.9.8 *Incidente «interrupção da alimentação energética»*

79) Este incidente produz-se, fora do modo de calibração ou do modo de controlo, se a alimentação energética do sensor de movimentos e/ou da unidade-veículo for interrompida durante mais de 200 milésimos de segundo. O limiar da interrupção deve ser indicado pelo fabricante. A queda na alimentação energética em consequência da colocação do motor do veículo em marcha não deve acionar este incidente.

3.9.9 *Incidente «Erro de comunicação com o sistema de comunicação à distância»*

80) Este incidente produz-se, **fora do modo de calibração**, quando o sistema de comunicação à distância não reconhece a receção bem-sucedida de dados de comunicação à distância enviados a partir da unidade-veículo por mais de três tentativas.

3.9.10 *Incidente «Ausência de informações sobre a posição do recetor GNSS»*

81) Este incidente produz-se, **fora do modo de calibração**, em caso de ausência de informações sobre a posição inicial do recetor GNSS (interno ou externo) durante mais de três horas de tempo de condução acumulado.

3.9.11 *Incidente «Erro de comunicação com o módulo GNSS externo»*

82) Este incidente produz-se, **fora do modo de calibração**, em caso de interrupção da comunicação entre o módulo GNSS externo e a unidade-veículo durante mais de 20 minutos contínuos, estando o veículo em movimento.

▼B

3.9.12. *Incidente «erro nos dados de movimento»*

83) Este incidente produz-se, **fora do modo de calibração**, em caso de interrupção do fluxo normal de dados entre o sensor de movimentos e a unidade-veículo e/ou em caso de erro na integridade ou na autenticação de dados durante o intercâmbio destes entre o sensor de movimentos e a unidade-veículo.

3.9.13 *Incidente «Conflito relativo ao movimento do veículo»*

84) Este incidente produz-se, **fora do modo de calibração**, se as informações calculadas a partir do detetor de movimento forem contrariadas por informações de movimento calculadas a partir do recetor GNSS interno ou a partir do módulo GNSS externo e, de modo facultativo, por outras fontes independentes, conforme se especifica no apêndice 12. O incidente não se produz durante uma travessia de batelão/comboio, durante uma situação OUT OF SCOPE ou se a informação sobre a posição do recetor GNSS não estiver disponível.

3.9.14 *Incidente «tentativa de violação da segurança»*

85) Este incidente produz-se perante qualquer outro incidente que afete a segurança do sensor de movimentos e/ou da unidade-veículo e/ou do módulo GNSS externo, em conformidade com o apêndice 10, fora do modo de calibração.

3.9.15 *Incidente «conflito de tempo»*

86) Este incidente produz-se, **fora do modo de calibração**, quando a VU deteta uma discrepância de mais de 1 minuto entre o tempo da função de medição do tempo da unidade-veículo e o tempo proveniente do recetor GNSS. O incidente é registado juntamente com o valor do relógio interno da unidade-veículo e surge juntamente com um ajustamento automático do tempo. Após a produção de um incidente de conflito de tempo, a VU não gera outros incidentes de conflito de tempo durante as 12 horas seguintes. O incidente não se produz se o recetor GNSS não tiver detetado qualquer sinal GNSS válido nos últimos 30 dias. No entanto, quando a informação da posição do recetor GNSS estiver disponível novamente, será efetuado o ajustamento automático do tempo.

3.9.16 *Falha do «cartão»*

87) Esta falha ocorre se se verificar algum defeito no cartão tacográfico durante o funcionamento.

3.9.17 *Falha do «aparelho de controlo»*

88) Esta falha ocorre, fora do modo de calibração, perante qualquer das seguintes:

— Falha interna da VU

— Falha da impressora

— Falha do visor

— Falha do descarregamento

— Falha do sensor

— Falha do recetor GNSS ou do módulo GNSS externo

— Falha do sistema de comunicação à distância

▼B

3.10 **Ensaios incorporados e autoensaios**

89) O aparelho de controlo deve detetar automaticamente falhas, por meio de autoensaios e de ensaios incorporados, em conformidade com o quadro seguinte:

Subconjunto a ensaiar	Autoensaio	Ensaio incorporado
Software		Integridade
Memória de dados	Acesso	Acesso, integridade de dados
Interfaces dos cartões	Acesso	Acesso
Teclado		Verificação manual
Impressora	(ao critério do fabricante)	Impressão
Visualizar		Controlo visual
Descarregamento (executado só durante o descarregamento)	Funcionamento correto	
Sensor	Funcionamento correto	Funcionamento correto
Sistema de comunicação à distância	Funcionamento correto	Funcionamento correto
Módulo GNSS	Funcionamento correto	Funcionamento correto

3.11 **Leitura da memória de dados**

90) O aparelho de controlo deve poder ler quaisquer dados memorizados na sua memória.

3.12 **Registo e memorização de dados na memória**

Para efeitos da presente secção,

— Define-se «365 dias» como 365 dias de atividade média do condutor num veículo. A atividade média por dia num veículo é definida como pelo menos 6 condutores ou ajudantes, 6 ciclos de inserção/retirada de cartão e 256 mudanças de atividade. Por conseguinte, «365 dias» inclui pelo menos 2 190 condutores ou ajudantes, 2 190 ciclos de inserção/retirada de cartão e 93 440 mudanças de atividade,

— O número médio de posições por dia é definido como pelo menos 6 posições em que o período diário de trabalho se inicia, 6 posições em que o tempo de condução contínua do condutor atinge um múltiplo de três horas e 6 posições em que o período diário de trabalho termina, de modo que «365 dias» inclua pelo menos 6 570 posições,

— As medidas de tempo são registadas com uma resolução de 1 minuto, salvo indicação diversa,

— Os valores do conta-quilómetros são registados com uma resolução de 1 km,

— As velocidades são registadas com uma resolução de 1 km/h,

— As posições (latitudes e longitudes) são registadas em graus e minutos, com uma resolução de 1/10 de minuto, com a precisão GNSS e o momento de aquisição associados.

▼B

91) Os dados memorizados na memória não devem ser afetados por um corte exterior na alimentação energética inferior a 12 meses, em condições de homologação. Por sua vez, os dados memorizados no sistema externo de comunicação à distância, conforme a definição constante do apêndice 14, não devem ser afetados por um corte na alimentação energética inferior a 28 dias.

92) O aparelho de controlo deve poder registar e memorizar na sua memória, implícita ou explicitamente, os seguintes dados:

3.12.1 *Dados de identificação do aparelho*

3.12.1.1 Dados de identificação da unidade-veículo

93) O aparelho de controlo deve poder memorizar na sua memória os seguintes dados de identificação da unidade-veículo:

— nome do fabricante

— endereço do fabricante

— número da peça

— número de série

— geração da VU

— capacidade de utilização de cartões tacográficos da primeira geração

— número da versão do *software*

— data de instalação da versão do *software*

— ano de fabrico do aparelho

— número de homologação

94) Os dados de identificação da unidade-veículo são registados e memorizados definitivamente pelo seu fabricante, com exceção dos relativos ao *software* e do número de homologação, os quais podem ser modificados na eventualidade de uma reclassificação do *software* e da capacidade de utilização de cartões tacográficos da primeira geração.

3.12.1.2 Dados de identificação do sensor de movimentos

95) O sensor de movimentos deve poder memorizar na sua memória os seguintes dados de identificação:

— nome do fabricante

— número de série

— número de homologação

— identificador incorporado do componente de segurança (por exemplo, número de chip/processador interno)

— identificador do sistema operativo (por exemplo, número da versão do *software*)

96) Os dados de identificação do sensor de movimentos são registados e memorizados definitivamente nele pelo seu fabricante.

97) A unidade-veículo deve poder registar e memorizar na sua memória os seguintes dados relativos aos 20 emparelhamentos mais recentes dos sensores de movimentos (se, no espaço de um dia de calendário, ocorrerem vários emparelhamentos, serão armazenados apenas o primeiro e o último desse dia):

▼B

Para cada um desses emparelhamentos, devem registar-se os seguintes dados:

— Dados de identificação do sensor de movimentos:

— número de série

— número de homologação

— Dados de emparelhamento do sensor de movimentos:

— data do emparelhamento.

3.12.1.3 Dados de identificação dos sistemas globais de navegação por satélite

98) O módulo GNSS externo deve poder memorizar na sua memória os seguintes dados de identificação:

— nome do fabricante

— número de série

— número de homologação

— identificador incorporado do componente de segurança (por exemplo, número de chip/processador interno)

— identificador do sistema operativo (por exemplo, número da versão do *software*)

99) Os dados de identificação são registados e memorizados definitivamente no módulo GNSS externo, pelo seu fabricante.

100) A unidade-veículo deve poder registar e memorizar na sua memória os seguintes dados relativos aos 20 emparelhamentos mais recentes dos módulos GNSS externos (se, no espaço de um dia de calendário, ocorrerem vários emparelhamentos, serão armazenados apenas o primeiro e o último desse dia):

Para cada um desses emparelhamentos, devem registar-se os seguintes dados:

— Dados de identificação do módulo GNSS externo:

— número de série

— número de homologação

— Dados de emparelhamento do módulo GNSS externo:

— data do emparelhamento

3.12.2 *Chaves e certificados*

101) O aparelho de controlo deve poder memorizar várias chaves e certificados criptográficos, conforme especifica o apêndice 11, parte A e parte B.

3.12.3 *Dados relativos à inserção e à retirada de cartões de condutor ou de oficina*

102) Por cada ciclo de inserção e retirada de um cartão de condutor ou de oficina, o aparelho de controlo regista e memoriza na sua memória de dados:

— O apelido e o nome próprio do titular do cartão, conforme registo no mesmo

— O número, o Estado-Membro emissor e o prazo de validade do cartão, conforme registo no mesmo

— A geração do cartão

▼B

— A data e a hora da inserção do cartão

— O valor do conta-quilómetros do veículo no momento da inserção

— A ranhura na qual o cartão foi inserido

— A data e a hora da retirada do cartão

— O valor do conta-quilómetros do veículo no momento da retirada

— Os seguintes elementos relativos ao veículo anteriormente utilizado pelo titular do cartão, conforme registo neste:

  — VRN e Estado-Membro de matrícula

  — Geração da VU (quando disponível)

  — Data e hora da retirada do cartão

— Um indicador de o titular ter efetuado ou não a introdução manual de atividades no momento da inserção do cartão.

103) A memória deve poder guardar estes dados durante pelo menos 365 dias.

104) Quando se esgota a capacidade de memorização, os dados mais antigos são substituídos por dados mais recentes.

3.12.4 *Dados relativos à atividade de condutor*

105) O aparelho de controlo deve registar e memorizar na sua memória de dados qualquer mudança na atividade do condutor ou do ajudante, qualquer mudança na situação da condução e/ou qualquer inserção ou retirada de um cartão de condutor ou de oficina:

— situação da condução (CREW, SINGLE)

— ranhura (DRIVER, CO-DRIVER)

— situação do cartão na ranhura correspondente: INSERTED (inserido), NOT INSERTED (não inserido)

— atividade (DRIVING, AVAILABILITY, WORK, BREAK/ /REST)

— data e hora da mudança.

Por INSERTED entende-se que se encontra inserido na ranhura um cartão válido de condutor ou de oficina. Por NOT INSERTED entende-se o contrário, ou seja, que na ranhura não se encontra inserido nenhum cartão válido de condutor ou de oficina (por exemplo, não foi inserido nenhum cartão ou o inserido é de empresa).

Os dados relativos à atividade introduzidos manualmente por um condutor não são registados na memória.

106) A memória deve poder guardar durante pelo menos 365 dias os dados relativos à atividade do condutor.

107) Quando se esgota a capacidade de memorização, os dados mais antigos são substituídos por dados mais recentes.

▼B

3.12.5 *Locais e posições em que se iniciam e concluem os períodos diários de trabalho e/ou em que são alcançados os períodos de 3 horas de condução contínua*

108) O aparelho de controlo deve registar e memorizar na sua memória os seguintes dados:

— locais e posições em que o condutor e/ou o ajudante inicia o seu período de trabalho diário

— posições em que o tempo de condução contínua do condutor atinge um múltiplo de três horas

— locais e posições em que o condutor e/ou o ajudante conclui o seu período diário de trabalho.

109) Quando a posição do veículo não está disponível a partir do recetor GNSS nessas ocasiões, o aparelho de controlo deve utilizar a última posição disponível, bem como as correspondentes data e hora.

110) Juntamente com cada local ou posição, o aparelho de controlo deve registar e memorizar na sua memória os seguintes dados:

— O número e o Estado-Membro emissor do cartão do condutor ou do ajudante

— A geração do cartão

— A data e a hora da introdução de dados

— O tipo de introdução (início, final ou 3 horas de tempo de condução contínua)

— A precisão relativa ao GNSS, a data e a hora, quando aplicável

— O valor do conta-quilómetros do veículo.

111) A memória deve poder guardar os locais e as posições em que se iniciam e concluem os períodos diários de trabalho e/ou em que são alcançados os períodos de 3 horas de condução contínua durante pelo menos 365 dias.

112) Quando se esgota a capacidade de memorização, os dados mais antigos são substituídos por dados mais recentes.

3.12.6 *Dados do conta-quilómetros*

113) O aparelho de controlo deve registar na sua memória de dados o valor do conta-quilómetros do veículo e a correspondente data, à meia-noite de cada dia.

114) A memória deve poder guardar durante pelo menos 365 dias os valores do conta-quilómetros registados à meia-noite.

115) Quando se esgota a capacidade de memorização, os dados mais antigos são substituídos por dados mais recentes.

3.12.7 *Dados relativos à velocidade*

116) O aparelho de controlo deve registar e memorizar na sua memória de dados a velocidade instantânea do veículo e as correspondentes data e hora, a cada segundo de pelo menos as últimas 24 horas de movimento.

3.12.8 *Dados relativos a incidentes*

Para efeitos da presente secção, os tempos devem ser registados com a resolução de 1 segundo.

117) Relativamente a cada incidente detetado, o aparelho de controlo deve registar e memorizar na sua memória, segundo as regras indicadas, os seguintes dados:

▼B

Incidente	Regras de memorização	Dados a registar por cada incidente
Inserção de cartão não válido	— os 10 incidentes mais recentes	— data e hora do incidente — tipo, número, Estado-Membro emissor e geração do cartão que causa o incidente — número de incidentes similares nesse dia
Conflito de cartões	— os 10 incidentes mais recentes	— data e hora do início do incidente — data e hora do final do incidente — tipo, número, Estado-Membro emissor e geração dos dois cartões que causam o conflito
Condução sem cartão adequado	— o incidente mais longo de cada um dos últimos 10 dias de ocorrência — os 5 incidentes mais longos dos últimos 365 dias	— data e hora do início do incidente — data e hora do final do incidente — tipo, número, Estado-Membro emissor e geração de qualquer cartão inserido no início e/ou no final do incidente — número de incidentes similares nesse dia
Inserção de cartão durante condução	— o último incidente de cada um dos últimos 10 dias de ocorrência	— data e hora do incidente — tipo, número, Estado-Membro emissor e geração — número de incidentes similares nesse dia
Última sessão de cartão encerrada incorretamente	— os 10 incidentes mais recentes	— data e hora de inserção do cartão — tipo, número, Estado-Membro emissor e geração — dados da última sessão, conforme leitura do cartão: — data e hora de inserção do cartão — VRN, Estado-Membro de matrícula e geração da VU
Excesso de velocidade (1)	— o incidente mais grave (ou seja, o caso de velocidade média mais elevada) de cada um dos últimos 10 dias de ocorrência — um dos 5 incidentes mais graves dos últimos 365 dias — o primeiro incidente desde a última calibração	— data e hora do início do incidente — data e hora do final do incidente — velocidade máxima medida durante o incidente — velocidade média (aritmética) medida durante o incidente — tipo, número, Estado-Membro emissor e geração do cartão de condutor (quando aplicável) — número de incidentes similares nesse dia

▼B

Incidente	Regras de memorização	Dados a registar por cada incidente
Interrupção da alimentação energética (2)	— o incidente mais longo de cada um dos últimos 10 dias de ocorrência — os 5 incidentes mais longos dos últimos 365 dias	— data e hora do início do incidente — data e hora do final do incidente — tipo, número, Estado-Membro emissor e geração de qualquer cartão inserido no início e/ou no final do incidente — número de incidentes similares nesse dia
Erro de comunicação com o sistema de comunicação à distância	— o incidente mais longo de cada um dos últimos 10 dias de ocorrência — os 5 incidentes mais longos dos últimos 365 dias	— data e hora do início do incidente — data e hora do final do incidente — tipo, número, Estado-Membro emissor e geração de qualquer cartão inserido no início e/ou no final do incidente — número de incidentes similares nesse dia
Ausência de informações sobre a posição do recetor GNSS	— o incidente mais longo de cada um dos últimos 10 dias de ocorrência — os 5 incidentes mais longos dos últimos 365 dias	— data e hora do início do incidente — data e hora do final do incidente — tipo, número, Estado-Membro emissor e geração de qualquer cartão inserido no início e/ou no final do incidente — número de incidentes similares nesse dia
Erro nos dados de movimento	— o incidente mais longo de cada um dos últimos 10 dias de ocorrência — os 5 incidentes mais longos dos últimos 365 dias	— data e hora do início do incidente — data e hora do final do incidente — tipo, número, Estado-Membro emissor e geração de qualquer cartão inserido no início e/ou no final do incidente — número de incidentes similares nesse dia
Conflito relativo ao movimento do veículo	— o incidente mais longo de cada um dos últimos 10 dias de ocorrência — os 5 incidentes mais longos dos últimos 365 dias	— data e hora do início do incidente — data e hora do final do incidente — tipo, número, Estado-Membro emissor e geração de qualquer cartão inserido no início e/ou no final do incidente — número de incidentes similares nesse dia
Tentativas de violação da segurança	— os 10 incidentes mais recentes por tipo de incidente	— data e hora do início do incidente — data e hora do final do incidente (se pertinente) — tipo, número, Estado-Membro emissor e geração de qualquer cartão inserido no início e/ou no final do incidente — tipo de incidente

▼B

Incidente	Regras de memorização	Dados a registar por cada incidente
Conflito de tempo	— o incidente mais longo de cada um dos últimos 10 dias de ocorrência — os 5 incidentes mais longos dos últimos 365 dias	— data e hora do aparelho de controlo — Data e hora do GNSS — tipo, número, Estado-Membro emissor e geração de qualquer cartão inserido no início e/ou no final do incidente — número de incidentes similares nesse dia

(1) O aparelho de controlo deve igualmente registar e memorizar na sua memória os seguintes dados:

— data e hora do último OVER SPEEDING CONTROL (controlo do excesso de velocidade)

— data e hora do primeiro excesso de velocidade a seguir ao anterior OVER SPEEDING CONTROL

— número de incidentes de excesso de velocidade desde o último OVER SPEEDING CONTROL.

(2) Estes dados só podem ser registados após a reposição da alimentação energética. Os tempos podem ser conhecidos com precisão até ao minuto.

3.12.9 *Dados relativos a falhas*

Para efeitos da presente secção, os tempos devem ser registados com a resolução de 1 segundo.

118) Relativamente a cada falha detetada, o aparelho de controlo deve procurar registar e memorizar na sua memória, segundo as regras indicadas, os seguintes dados:

Falha	Regras de memorização	Dados a registar por cada falha
Falhas do cartão	— as 10 falhas mais recentes de cartão de condutor	— data e hora do início da falha — data e hora do final da falha — data e hora do início da falha, tipo, número, Estado-Membro emissor e geração do cartão
Falhas do aparelho de controlo	— as 10 falhas mais recentes por tipo de falha — a primeira falha ocorrida desde a última calibração	— data e hora do início da falha, data e hora do início da falha — data e hora do final da falha — tipo de falha — tipo, número, Estado-Membro emissor e geração de qualquer cartão inserido no início e/ou no final da falha

3.12.10 *Dados relativos à calibração*

119) O aparelho de controlo deve registar e memorizar na sua memória dados com interesse para:

— parâmetros conhecidos de calibração no momento da ativação

▼B

— a primeira calibração após a ativação

— a primeira calibração no veículo em questão (identificado pelo VIN)

— as 20 calibrações mais recentes (se ocorrerem várias no mesmo dia, é memorizada unicamente a última).

120) Para cada uma das seguintes calibrações, são registados os seguintes dados:

— objetivo da calibração (ativação, primeira instalação, instalação, inspeção periódica)

— nome e endereço da oficina

— número, Estado-Membro emissor e prazo de validade do cartão de oficina

— identificação do veículo

— parâmetros atualizados ou confirmados: dimensão w, k, l, medida do pneumático, ponto de regulação do dispositivo de limitação da velocidade, conta-quilómetros (antigos e novos valores), data e hora (antigos e novos valores)

— tipos e identificadores de todos os selos em vigor.

121) O aparelho de controlo deve também registar e memorizar na sua memória de dados a capacidade de utilização de cartões tacográficos da primeira geração (ainda ativados ou não).

122) O sensor de movimentos deve registar e memorizar na sua memória os seguintes dados relativos à sua instalação:

— primeiro emparelhamento com uma VU (data, hora, número de homologação da VU, número de série da VU)

— último emparelhamento com uma VU (data, hora, número de homologação da VU, número de série da VU).

123) O módulo GNSS externo deve registar e memorizar na sua memória os seguintes dados relativos à instalação do módulo GNSS externo:

— primeiro emparelhamento com uma VU (data, hora, número de homologação da VU, número de série da VU)

— último emparelhamento com uma VU (data, hora, número de homologação da VU, número de série da VU).

3.12.11 *Dados relativos ao ajustamento do tempo*

124) O aparelho de controlo deve registar e memorizar na sua memória dados importantes para os ajustamentos do tempo realizados em modo de calibração fora do âmbito de uma calibração regular (definição f)):

— o mais recente ajustamento do tempo

— os 5 maiores ajustamentos do tempo

125) São registados os seguintes dados por cada um destes ajustamentos do tempo:

— data e hora (antigo valor)

— data e hora (novo valor)

— nome e endereço da oficina

— número, Estado-Membro emissor, geração e prazo de validade do cartão de oficina.

▼B

3.12.12 *Dados relativos à atividade de controlo*

126) O aparelho de controlo deve registar e memorizar na sua memória os seguintes dados relativos às vinte atividades de controlo mais recentes:

— data e hora do controlo

— número, Estado-Membro emissor e geração do cartão de controlo

— tipo do controlo: visualização e/ou impressão e/ou descarregamento da VU e/ou descarregamento do cartão e/ou controlo de calibração de estrada.

127) Em caso de descarregamento, são igualmente registadas as datas dos dias descarregados mais antigo e mais recente.

3.12.13 *Dados relativos aos bloqueamentos da empresa*

128) O aparelho de controlo deve registar e memorizar na sua memória os seguintes dados relativos aos 255 bloqueamentos mais recentes da empresa:

— data e hora de início do bloqueamento (lock-in)

— data e hora de cessação do bloqueamento (lock-out)

— número, Estado-Membro emissor e geração do cartão de empresa

— nome e endereço da empresa.

Devem tratar-se como não bloqueados os dados anteriormente bloqueados por um bloqueamento que, devido ao limite supramencionado, foi apagado da memória.

3.12.14 *Dados relativos à atividade de descarregamento*

129) O aparelho de controlo deve registar e memorizar na sua memória os seguintes dados relativos ao último descarregamento de dados para meios externos em modo de empresa ou de calibração:

— data e hora do descarregamento

— número, Estado-Membro emissor e geração do cartão de empresa ou oficina

— nome da empresa ou da oficina.

3.12.15 *Dados relativos às condições especiais*

130) O aparelho de controlo deve registar na sua memória os seguintes dados relativos a condições especiais:

— data e hora da introdução

— tipo de condição especial.

131) A memória deve poder guardar durante pelo menos 365 dias os dados relativos a condições especiais (partindo do princípio de que, em média, é aberta e encerrada 1 condição por dia). Quando se esgota a capacidade de memorização, os dados mais antigos são substituídos por dados mais recentes.

3.12.16 *Dados relativos ao cartão tacográfico*

132) O aparelho de controlo deve poder memorizar os seguintes dados relativos aos diferentes cartões tacográficos nos quais foram utilizados, na VU:

— o número do cartão tacográfico e o respetivo número de série

— o fabricante do cartão tacográfico

▼B

— o tipo de cartão tacográfico

— a versão do cartão tacográfico.

133) O aparelho de controlo deve poder memorizar pelo menos 88 registos deste tipo.

3.13 **Leitura de cartões tacográficos**

134) O aparelho de controlo deve poder ler nos cartões tacográficos de primeira e segunda geração, consoante os casos, os dados necessários para:

— identificar o tipo e o titular do cartão, o veículo utilizado anteriormente, a data e a hora da última retirada do cartão e a atividade selecionada nesse momento

— verificar se a última sessão do cartão foi corretamente encerrada

— relativamente às semanas anterior e em curso, calcular o tempo de condução contínua do condutor, o tempo acumulado de pausas e o tempo acumulado de condução

— fazer as impressões que se pretendam dos dados registados num cartão de condutor

— descarregar um cartão de condutor para meios externos.

Este requisito aplica-se somente aos cartões tacográficos de primeira geração, caso a sua utilização não tenha sido suprimida por uma oficina.

135) Na eventualidade de um erro de leitura, o aparelho de controlo faz, no máximo, três novas tentativas, após o que, não obtendo êxito, declara o cartão defeituoso e não válido.

3.14 **Registo e memorização de dados nos cartões tacográficos**

3.14.1 *Registo e memorização de dados nos cartões tacográficos de primeira geração*

136) Desde que os cartões tacográficos de primeira geração não tenham sido suprimidos por uma oficina, o aparelho de controlo deve registar e memorizar dados exatamente da mesma forma que faria um aparelho de controlo da primeira geração.

137) O aparelho de controlo deve lançar no cartão de condutor ou de oficina, imediatamente após a sua inserção, os «dados da sessão do cartão».

138) O aparelho de controlo deve atualizar os dados memorizados em cartões válidos de condutor, de oficina, de empresa e/ou de controlo, com todos os dados de interesse para o período durante o qual o cartão está inserido e para o seu titular. Os dados memorizados nestes cartões são especificados no capítulo 4.

139) O aparelho de controlo deve atualizar os dados relativos à atividade e à localização do condutor (conforme especificado nos pontos 4.5.3.1.9 e 4.5.3.1.11), memorizados em cartões válidos de condutor e/ou de oficina, com os dados relativos à atividade e à localização que o titular introduz manualmente.

140) Os incidentes não definidos para o aparelho de controlo da primeira geração não devem ser memorizados nos cartões de condutor e de oficina.

▼B

141) A atualização dos dados de cartões tacográficos deve ser de molde a que, se necessário e tendo em conta a capacidade efetiva de memorização do cartão, os dados mais recentes substituam os mais antigos.

142) Na eventualidade de um erro de escrita, o aparelho de controlo faz, no máximo, três novas tentativas, após o que, não obtendo êxito, declara o cartão defeituoso e não válido.

143) Antes de libertar um cartão de condutor e depois de nele memorizar todos os dados de interesse, o aparelho de controlo restabelece os «dados da sessão do cartão».

3.14.2 *Registo e memorização de dados nos cartões tacográficos da segunda geração*

144) Os cartões tacográficos da segunda geração devem conter 2 aplicações diferentes para cartões, a primeira das quais será exatamente a mesma que a aplicação TACHO dos cartões tacográficos da primeira geração e a segunda a aplicação «TACHO_G2», conforme especificado no capítulo 4 e no apêndice 2.

145) O aparelho de controlo deve lançar no cartão de condutor ou de oficina, imediatamente após a sua inserção, os «dados da sessão do cartão».

146) O aparelho de controlo deve atualizar os dados memorizados nas 2 aplicações de cartões válidos de condutor, de oficina, de empresa e/ou de controlo, com todos os dados de interesse para o período durante o qual o cartão está inserido e para o seu titular. Os dados memorizados nestes cartões são especificados no capítulo 4.

147) O aparelho de controlo deve atualizar os dados relativos aos locais de atividade e às posições do condutor (conforme especificado nos pontos 4.5.3.1.9, 4.5.3.1.11, 4.5.3.2.9 e 4.5.3.2.11), memorizados em cartões válidos de condutor e/ou de oficina, com os dados relativos à atividade e aos locais que o titular introduz manualmente.

148) A atualização dos dados de cartões tacográficos deve ser de molde a que, se necessário e tendo em conta a capacidade efetiva de memorização do cartão, os dados mais recentes substituam os mais antigos.

149) Na eventualidade de um erro de escrita, o aparelho de controlo faz, no máximo, três novas tentativas, após o que, não obtendo êxito, declara o cartão defeituoso e não válido.

150) Antes de libertar um cartão de condutor e depois de memorizar todos os dados de interesse nas duas aplicações do cartão, o aparelho de controlo restabelece os «dados da sessão do cartão».

3.15 **Visualização**

151) Na visualização de mensagens deve haver pelo menos 20 carateres.

152) As dimensões mínimas de um caráter devem ser de 5 mm de altura por 3,5 mm de largura.

153) A visualização deve aceitar os carateres indicados no apêndice 1, capítulo 4, «Conjuntos de carateres». A visualização pode utilizar símbolos simplificados (por exemplo, ausência de acento gráfico, maiúsculas em lugar de minúsculas, etc.).

▼B

154) Na visualização deve ser utilizada iluminação adequada, não ofuscante.

155) As indicações devem ser visíveis de fora do aparelho de controlo.

156) O aparelho de controlo deve poder exibir para visualização:

— data do incumprimento

— dados relativos a alertas

— dados relativos ao acesso ao menu

— outros dados solicitados por um utilizador.

O aparelho de controlo pode exibir elementos informativos adicionais, desde que claramente distinguíveis das informações supra.

157) O visor do aparelho de controlo deve utilizar os pictogramas ou combinações de pictogramas indicados no apêndice 3. Podem utilizar-se pictogramas ou combinações de pictogramas adicionais, desde que claramente distinguíveis dos primeiros.

158) Com o veículo em movimento, o visor deve estar sempre ligado (posição ON).

159) O aparelho de controlo deve incluir um dispositivo manual ou automático para desligar o visor (levá-lo à posição OFF) quando o veículo não está em movimento.

O formato da visualização é especificado no apêndice 5.

3.15.1 *Visualização por defeito*

160) Se não se impuserem outras informações, o aparelho de controlo deve exibir, por defeito, as seguintes:

— hora local (hora UTC, com compensação introduzida pelo condutor)

— modo de funcionamento

— atividade em curso do condutor e atividade em curso do ajudante

— informação relativa ao condutor:

— se a sua atividade em curso for DRIVING: o seu atual tempo de condução contínua e o seu atual tempo acumulado de pausas

— se a sua atividade em curso não for DRIVING: a duração dessa atividade (desde que foi selecionada) e o seu atual tempo acumulado de pausas.

161) A exibição dos dados relativos ao condutor e ao ajudante deve ser clara, direta e inequívoca. Caso a informação relativa a um não possa ser visualizada ao mesmo tempo que a relativa ao outro, o aparelho de controlo deve exibir por defeito a informação relativa ao condutor, permitindo ao utilizador visualizar a informação relativa ao ajudante.

162) Caso a largura do visor não permita exibir por defeito o modo de funcionamento, o aparelho de controlo deve exibir fugazmente o novo modo de funcionamento quando haja mudança deste.

▼B

163) Quando haja inserção de um cartão, o aparelho de controlo deve exibir fugazmente o nome do titular.

164) A abertura de uma condição «OUT OF SCOPE» ou «FERRY/ /TRAIN» deve ser assinalada na visualização por defeito, com recurso aos pictogramas pertinentes (é aceitável que a atividade em curso do condutor não seja visualizada ao mesmo tempo).

3.15.2 *Visualização de alerta*

165) O aparelho de controlo deve exibir informações de alerta, primeiramente com recurso aos pictogramas constantes do apêndice 3, complementados, se necessário, por informação adicional numericamente codificada. Pode também acrescentar-se uma descrição literal do alerta, no idioma de preferência do condutor.

3.15.3 *Acesso ao menu*

166) O aparelho de controlo deve proporcionar os comandos necessários, mediante um menu adequadamente estruturado.

3.15.4 *Outras visualizações*

167) Deve ser possível visualizar seletivamente, conforme se pretenda:

— data e hora UTC e hora local compensada

— conteúdo de qualquer destas seis mensagens, no mesmo formato da mensagem impressa

— tempo de condução contínua e tempo acumulado de pausas do condutor

— tempo de condução contínua e tempo acumulado de pausas do ajudante

— tempo acumulado de condução do condutor nas semanas anterior e em curso

— tempo acumulado de condução do ajudante nas semanas anterior e em curso.

Opcional:

— duração da atividade em curso do ajudante (desde que foi selecionada)

— tempo acumulado de condução do condutor na semana em curso

— tempo acumulado de condução do ajudante no período de trabalho diário em curso

— tempo acumulado de condução do condutor no período de trabalho diário em curso.

168) A visualização do conteúdo das mensagens deve ser sequencial, linha a linha. Se a largura do visor for inferior a 24 carateres, o utilizador deve poder obter a informação completa por um meio adequado (linhas múltiplas, deslocamento, etc.).

As linhas reservadas a informação manuscrita podem ser omitidas na visualização.

▼B

3.16 **Impressão**

169) O aparelho de controlo deve poder imprimir informação contida na sua memória de dados e/ou nos cartões tacográficos, de acordo com as sete impressões seguintes:

— atividades de condutor, da impressão diária dos cartões

— atividades de condutor, da impressão diária da unidade-veículo

— incidentes e falhas, da impressão dos cartões

— incidentes e falhas, da impressão da unidade-veículo

— impressão de dados técnicos

— impressão de excesso de velocidade

— dados históricos do cartão tacográfico para uma determinada VU (ver capítulo 3.12.16).

O formato e o conteúdo destas impressões são pormenorizados no apêndice 4.

No final das impressões, podem ser fornecidos dados adicionais.

Podem também ser fornecidas impressões complementares pelo aparelho de controlo, desde que claramente distinguíveis das sete impressões supramencionadas.

170) As funções «atividades de condutor, da impressão diária dos cartões» e «incidentes e falhas, da impressão dos cartões» só devem ser viabilizadas quando o cartão inserido no aparelho de controlo for de condutor ou de oficina. Antes de iniciar a impressão, o aparelho de controlo atualiza os dados memorizados no cartão em causa.

171) Para concretizar a impressão de «atividades de condutor, da impressão diária dos cartões» e de «incidentes e falhas, da impressão dos cartões», o aparelho de controlo deve:

— selecionar automaticamente o cartão de condutor ou de oficina, se somente um destes cartões tiver sido inserido, ou então

— facultar um comando que selecione o cartão da fonte ou o cartão na ranhura do condutor, se no aparelho de controlo tiverem sido inseridos dois destes cartões.

172) A impressora deve poder imprimir 24 carateres por linha.

173) As dimensões mínimas de um caráter devem ser de 2,1 mm de altura por 1,5 mm de largura.

174) A impressão deve aceitar os carateres indicados no apêndice 1, capítulo 4, «Conjuntos de carateres».

175) As impressoras devem ser projetadas de modo a que as impressões tenham um grau de definição suscetível de evitar ambiguidades de leitura.

176) A impressão deve conservar as dimensões e os registos em condições normais de humidade (10-90 %) e de temperatura.

177) O papel homologado utilizado pelo aparelho de controlo deve exibir a correspondente marca de homologação e a indicação do(s) tipo(s) de aparelho no qual pode ser utilizado.

▼B

178) As impressões devem manter-se claramente legíveis e identificáveis em condições normais de armazenamento (no que diz respeito a intensidade luminosa, humidade e temperatura) durante pelo menos dois anos.

179) As impressões devem estar em conformidade, pelo menos, com as especificações de ensaio definidas no apêndice 9.

180) A estes documentos deve ser igualmente possível acrescentar notas manuscritas, como a assinatura do condutor.

181) Na eventualidade de um incidente «paper out» (falta de papel) durante a impressão, o aparelho de controlo deve geri-lo do seguinte modo: uma vez efetuada a recarga do papel, retomar a impressão desde o início ou prossegui-la, fazendo, nesta última hipótese, uma referência inequívoca à parte anteriormente impressa.

3.17 **Alertas**

182) O aparelho de controlo deve prevenir o condutor quando detetar algum incidente e/ou alguma falha.

183) A sinalização de um incidente de interrupção da alimentação energética pode ser adiada até se restabelecer a alimentação.

184) O aparelho de controlo deve avisar o condutor 15 minutos antes e no momento em que se ultrapassa o tempo máximo de condução contínua permitido.

185) Os sinais de alerta devem ser visuais. Complementarmente, podem ser também emitidos sinais sonoros.

186) Os alertas visuais devem ser claramente reconhecíveis pelo utilizador, situar-se no seu campo de visão e ser claramente legíveis tanto de dia como de noite.

187) Os alertas visuais podem ser incorporados no aparelho de controlo ou ter localização à distância.

188) No último caso, o alerta visual deve comportar um símbolo «T».

189) Os alertas devem ter a duração mínima de 30 segundos, a menos que o condutor acuse a sua emissão premindo uma ou mais teclas específicas do aparelho de controlo. Este primeiro reconhecimento não deve eliminar a visualização da causa do alerta referida no número seguinte.

190) A causa do alerta deve ser visualizada no aparelho de controlo e manter-se visível até o utilizador acusar a sua emissão premindo uma tecla ou um comando específico.

191) Podem ser emitidos alertas adicionais, desde que não provoquem a confusão do condutor em relação a alertas previamente definidos.

3.18 **Descarregamento de dados para meios externos**

192) Caso se pretenda, o aparelho de controlo deve poder descarregar dados da sua memória ou de um cartão de condutor para meios externos de memorização, através do conector de calibração/descarregamento. Antes de iniciar o descarregamento, o aparelho de controlo atualiza os dados memorizados no cartão em causa.

▼B

193) Complementarmente, e como função opcional, o aparelho de controlo deve, em qualquer modo de funcionamento, poder descarregar dados por intermédio de outro meio, para uma empresa autenticada através deste canal. Nesse caso, aplicar-se-ão ao descarregamento direitos de acesso aos dados em modo de empresa.

194) O descarregamento não deve alterar ou apagar dados memorizados.

195) A interface elétrica do conector de calibração/descarregamento é especificada no apêndice 6.

196) Os protocolos relativos ao descarregamento são especificados no apêndice 7.

3.19 **Comunicação à distância para controlos de estrada seletivos**

197) Quando a ignição está ligada, a unidade-veículo deve memorizar a cada 60 segundos, no sistema de comunicação à distância, os dados mais recentes necessários à realização dos controlos de estrada seletivos. Esses dados devem ser encriptados e assinados, conforme se especifica no apêndice 11 e no apêndice 14.

198) Os dados a verificar à distância devem estar disponíveis para os leitores de comunicações à distância por intermédio de comunicação sem fios, conforme se especifica no apêndice 14.

199) Os dados necessários à realização de controlos de estrada seletivos devem estar relacionados com:

— a última tentativa de violação da segurança

— a mais longa interrupção da alimentação energética,

— falha do sensor

— erro nos dados de movimento

— conflito relativo ao movimento do veículo

— condução sem cartão válido

— inserção de cartão durante a condução,

— dados relativos ao ajustamento do tempo

— dados relativos à calibração, incluindo as datas dos dois últimos registos de calibrações memorizados

— número de matrícula do veículo

— velocidade registada pelo tacógrafo.

3.20 **Transmissão de dados para dispositivos externos adicionais**

200) O aparelho de controlo pode igualmente ser equipado com interfaces normalizadas que permitam utilizar, em modo de funcionamento ou calibração, os dados registados ou produzidos por tacógrafos, por um dispositivo externo.

No apêndice 13, especifica-se e normaliza-se uma interface ITS facultativa. Podem coexistir outras interfaces similares, desde que cumpram integralmente os requisitos estabelecidos no apêndice 13 em termos de lista mínima de dados, segurança e consentimento do condutor.

Aos dados ITS disponibilizados através dessa interface aplicam-se os requisitos seguintes:

— trata-se de um conjunto de dados existentes selecionados a partir do dicionário de dados tacográficos (apêndice 1)

▼B

— desses dados selecionados, um subconjunto está marcado como «dados pessoais»

— o subconjunto de «dados pessoais» está disponível somente se estiver ativado o consentimento (verificável) do condutor para que os seus dados pessoais saiam da rede do veículo

— o consentimento do condutor pode ser ativado ou desativado através de comandos no menu, a qualquer momento, desde que o cartão de condutor esteja inserido

— o conjunto e o subconjunto de dados serão transmitidos via protocolo sem fios Bluetooth no raio da cabina do veículo, a um ritmo de atualização de 1 minuto

— o emparelhamento do dispositivo externo com a interface ITS será protegido por um PIN dedicado e aleatório de, pelo menos, 4 dígitos, registado e disponível através do visor de cada unidade-veículo

— em quaisquer circunstâncias, a presença da interface ITS não pode perturbar ou afetar o funcionamento correto e a segurança da unidade-veículo.

Complementarmente, também podem ser transmitidos outros dados ao conjunto de dados existentes selecionados, considerados como a lista mínima, desde que não se considerem como dados pessoais.

O aparelho de controlo deve notificar outros sistemas externos acerca do consentimento do condutor.

Estando ligada a ignição do veículo (ON), estes dados devem ser transmitidos permanentemente.

201) A interface de ligação em série, conforme se especifica no anexo 1(B) do Regulamento (CEE) n.º 3821/85, na sua última redação, pode continuar a equipar tacógrafos para compatibilidade interna. De qualquer modo, o consentimento do condutor continua a ser necessário quando os dados pessoais são transmitidos.

3.21 **Calibração**

202) A função de calibração deve permitir:

— emparelhar automaticamente o sensor de movimentos com a VU

— emparelhar automaticamente o módulo GNSS externo com a VU, se for caso disso

— adaptar digitalmente a constante do aparelho de controlo (k) ao coeficiente característico do veículo (w)

— ajustar o tempo atual no período de validade do cartão de oficina inserido

— ajustar o valor atual do conta-quilómetros

— atualizar os dados de identificação do sensor de movimentos, memorizados na memória

— atualizar, quando aplicável, os dados de identificação do módulo GNSS externo memorizados na memória

▼B

— atualizar os tipos e identificadores de todos os selos em vigor

— atualizar ou confirmar outros parâmetros conhecidos pelo aparelho de controlo: identificação do veículo, w, l, medida do pneumático e instalação do dispositivo de limitação da velocidade, quando aplicável.

203) Além disso, a função de calibração deve permitir suprimir a utilização de cartões tacográficos de primeira geração no aparelho de controlo, desde que se verifiquem as condições especificadas no apêndice 15.

204) O emparelhamento do sensor de movimentos com a VU deve consistir, pelo menos, em:

— atualizar os dados de instalação do sensor de movimentos nele contidos (conforme necessário)

— copiar da memória do sensor de movimentos para a da unidade-veículo os dados de identificação do sensor que forem necessários.

205) O emparelhamento do módulo GNSS externo com a VU deve consistir, pelo menos, em:

— atualizar os dados de instalação do módulo GNSS externo contidos no próprio módulo (conforme necessário)

— copiar do módulo GNSS externo para a memória de dados da VU as informações de identificação necessárias, incluindo o número de série do módulo GNSS externo.

Ao emparelhamento deve seguir-se a verificação das informações da posição GNSS.

206) A função de calibração deve poder admitir os dados que forem necessários, através do conector de calibração/descarregamento, segundo o protocolo definido no apêndice 8. Deve também poder admitir tais dados através de outros meios.

3.22 **Controlo de calibração de estrada**

207) A função de controlo de calibração de estrada deve permitir ler o número de série do sensor de movimentos (eventualmente incorporado no adaptador) e o número de série do módulo GNSS externo (quando aplicável), ligado à unidade-veículo, no momento do pedido.

208) Esta leitura deve ser possível, pelo menos, no visor da unidade-veículo, através de comandos nos menus.

209) A função de controlo de calibração de estrada deve igualmente permitir controlar a seleção do modo de I/O de calibração da linha de sinal I/O especificada no apêndice 6, através da interface K-line. Tal deve ser feito através do ECUAdjustmentSession, conforme especifica o apêndice 8, secção 7, «Controlo dos impulsos de ensaio — Unidade funcional de controlo de entrada/saída».

3.23 **Ajustamento do tempo**

210) A função de ajustamento do tempo deve permitir ajustar automaticamente o momento atual. No aparelho de controlo são utilizadas duas fontes de tempo para ajustamento do tempo: 1) o relógio interno da VU, 2) o recetor de GNSS.

▼B

211) A hora do relógio interno da VU deve ser reajustada automaticamente a intervalos máximos de 12 horas. Se este adiamento tiver expirado e o sinal GNSS não estiver disponível, o acerto da hora deve ser efetuado logo que a VU puder aceder a uma hora válida fornecida pelo recetor GNSS, de acordo com as condições de ignição do veículo. A referência temporal para o acerto automático da hora do relógio interno da VU deve ser determinada pelo recetor GNSS. Se a hora atual se desviar em mais de um (1) minuto da informação de tempo fornecida pelo recetor GNSS produz-se um incidente de conflito de tempo.

212) A função de ajustamento do tempo deve permitir acertar o tempo atual, em modo de calibração.

3.24 **Características de desempenho**

213) A unidade-veículo deve estar plenamente funcional no intervalo de temperatura de – 20 °C a 70 °C, o módulo GNSS externo no intervalo de temperatura de – 20 °C a 70 °C e o sensor de movimentos no intervalo de temperatura de – 40 °C a 135 °C. O conteúdo da memória de dados deve ser preservado até à temperatura de – 40 °C.

214) O tacógrafo deve ser plenamente funcional no intervalo de humidade de 10 % a 90 %.

215) Os selos utilizados no tacógrafo inteligente devem aceitar as mesmas condições aplicáveis aos componentes de tacógrafo a que estão apostos.

216) O aparelho de controlo deve ser protegido contra sobretensão elétrica, inversão da polaridade da sua alimentação energética e curtos-circuitos.

217) Os sensores de movimentos devem:

— reagir a campos magnéticos que perturbem a deteção do movimento do veículo. Nessas circunstâncias, a unidade-veículo regista e memoriza uma falha do sensor (requisito n.º 88) ou,

— dispor de um elemento de deteção que esteja protegido contra campos magnéticos ou lhes seja imune.

218) O aparelho de controlo e o módulo GNSS externo devem cumprir o disposto na regulamentação internacional ONU ECE R10 e ser protegidos contra descargas eletrostáticas e contra transitórios.

3.25 **Materiais**

219) Todas as peças constituintes do aparelho de controlo devem ser em material com estabilidade e resistência mecânica suficientes e com características eletromagnéticas estáveis.

220) Em condições normais de utilização, todas as peças internas do aparelho de controlo devem ser protegidas contra humidade e poeiras.

221) A unidade-veículo e o módulo GNSS externo devem cumprir o grau de proteção IP 40 e o sensor de movimentos deve cumprir o grau de proteção IP 64, conforme a norma IEC 60529:1989, incluindo A1:1999 e A2:2013.

222) O aparelho de controlo deve cumprir as especificações técnicas aplicáveis em matéria de ergonomia.

▼B

223) O aparelho de controlo deve ser protegido contra danos acidentais.

3.26 **Marcações**

224) Se o aparelho de controlo exibir o valor do conta-quilómetros e a velocidade do veículo, o visor deve mostrar os seguintes elementos:

— junto ao número que indica a distância: a unidade de medida da distância, indicada pela abreviatura «km»

— junto ao número que indica a velocidade: a referência «km/h».

O aparelho de controlo pode também ser levado a exibir a velocidade em milhas por hora, caso em que a correspondente unidade de medida será indicada pela abreviatura «mph». O aparelho de controlo pode também ser levado a exibir a distância em milhas, caso em que a correspondente unidade de medida será indicada pela abreviatura «mi».

225) Em cada componente separado do aparelho de controlo deve ser afixada uma placa descritiva com os seguintes elementos:

— nome e endereço do fabricante do aparelho

— número da peça (dado pelo fabricante) e ano de fabrico do aparelho

— número de série do aparelho

— marca de homologação do tipo de aparelho.

226) Se o espaço físico não for suficiente para mostrar todos os pormenores supramencionados, a placa descritiva deve indicar, pelo menos, o nome ou logótipo do fabricante e o número de peça do aparelho.

4 REQUISITOS DE CONSTRUÇÃO E FUNCIONAMENTO DOS CARTÕES TACOGRÁFICOS

4.1 **Dados visíveis**

O anverso do cartão terá o seguinte conteúdo:

227) Os termos «cartão de condutor», «cartão de controlo», «cartão de oficina» ou «cartão de empresa», consoante o tipo de cartão, impressos em maiúsculas na(s) língua(s) oficial(is) do Estado-Membro emissor do cartão.

228) O nome do Estado-Membro que emite o cartão (facultativo).

229) O símbolo distintivo do Estado-Membro que emite o cartão, impresso em negativo num retângulo azul e rodeado de doze estrelas amarelas. Os símbolos distintivos são os seguintes:

B	Bélgica	LV	Letónia
BG	Bulgária	L	Luxemburgo
CZ	República Checa	LT	Lituânia
CY	Chipre	M	Malta
DK	Dinamarca	NL	Países Baixos
D	Alemanha	A	Áustria
EST	Estónia	PL	Polónia

▼B

GR	Grécia	P RO SK SLO	Portugal Roménia Eslováquia Eslovénia
E	Espanha	FIN	Finlândia
F HR H	França Croácia Hungria	S	Suécia
IRL	Irlanda	UK	Reino Unido
I	Itália		

230) Elementos específicos do cartão, com a seguinte numeração:

	Cartão de condutor	Cartão de controlo	Cartão de empresa ou de oficina
1.	Apelido do condutor	Nome do organismo de controlo	Nome da empresa ou da oficina
2.	Nome próprio do condutor	Apelido do controlador (se aplicável)	Apelido do titular do cartão (se aplicável)
3.	Data de nascimento do condutor	Nome próprio do controlador (se aplicável)	Nome próprio do titular do cartão (se aplicável)
4.a	Data do início da validade do cartão		
4.b	Prazo de validade do cartão		
4.c	Nome da autoridade emissora (pode ser impresso no verso)		
4.d	Número distinto do referido na rubrica 5, com utilidade para efeitos administrativos (referência facultativa)		
5. a	Número da carta de condução (à data de emissão do cartão de condutor)	—	—
5. b	Número do cartão		
6.	Fotografia do condutor	Fotografia do controlador (opcional)	Fotografia do instalador (opcional)
7.	Assinatura do titular (opcional)		
8.	Local de residência normal ou endereço postal do titular (facultativo).	Endereço postal do organismo de controlo	Endereço postal da empresa ou da oficina

231) Datas, com o formato «dd/mm/aaaa» ou «dd.mm.aaaa» (dia, mês, ano).

O verso do cartão terá o seguinte conteúdo:

232) Explicação dos elementos numerados que constam do anverso;

▼B

233) Com caráter eventual e mediante o consentimento expresso e por escrito do titular: informação não relacionada com a administração do cartão, sob condição de não prejudicar a utilização do modelo como cartão tacográfico.

234) Os cartões tacográficos devem ser impressos com as seguintes colorações de fundo:

— Cartão de condutor: branco

— Cartão de controlo: azul

— Cartão de oficina: vermelho

— Cartão de empresa: amarelo.

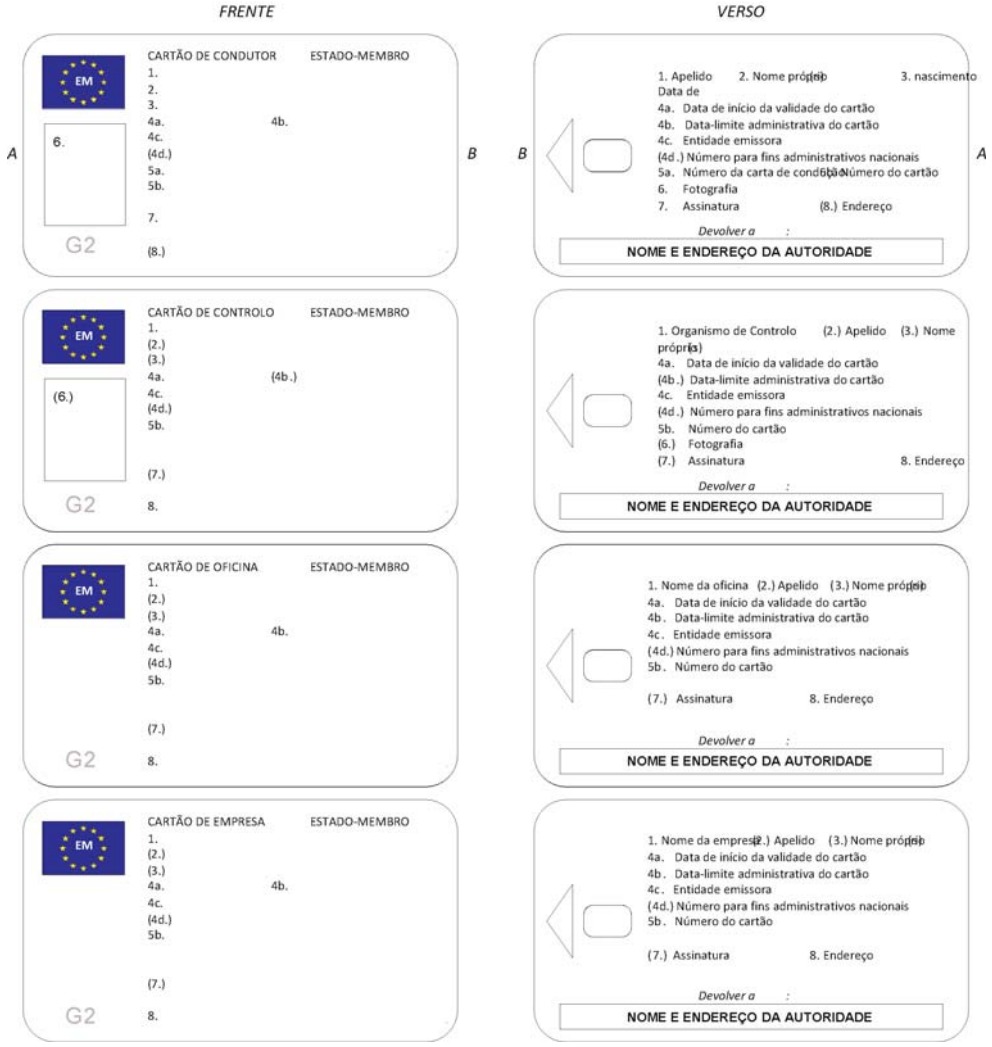
235) Os cartões tacográficos devem ter as seguintes características de proteção contra falsificações:

— fundo de segurança em guilhoché fino e impressão irisada

— na zona da fotografia, sobreposição do fundo de segurança e da fotografia

— pelo menos uma linha de microimpressão bicromática.

MODELO COMUNITÁRIO DE CARTÕES TACOGRÁFICOS



▼B

236) Mediante consulta da Comissão, os Estados-Membros podem acrescentar colorações ou marcações, como símbolos nacionais e elementos de segurança, sem prejuízo do disposto no presente anexo.

237) Os cartões temporários referidos no artigo 26.º, n.º 4, do Regulamento (UE) n.º 165/2014 devem cumprir o disposto neste anexo.

4.2 **Segurança**

A segurança do sistema visa proteger a integridade e a autenticidade dos dados que circulam entre os cartões e o aparelho de controlo e dos dados descarregados dos cartões, permitindo unicamente ao aparelho de controlo determinadas operações de escrita nos cartões, desencriptando dados, excluindo qualquer possibilidade de falsificação dos dados memorizados, prevenindo contrafações e detetando tentativas nesse sentido.

238) Com vista a conseguir a segurança do sistema, os cartões tacográficos devem cumprir o prescrito nos apêndices 10 e 11.

239) Os cartões tacográficos devem ser legíveis por outros aparelhos, como, por exemplo, computadores pessoais.

4.3 **Normas**

240) Os cartões tacográficos devem obedecer às seguintes normas:

— ISO/IEC 7810 Identification cards — Physical characteristics,

— ISO/IEC 7816 Identification cards — Integrated circuit cards:

  — Part 1: Physical characteristics

  — Part 2: Dimensions and position of the contacts (ISO/IEC 7816-2:2007)

  — Part 3: Electrical interface and transmission protocols (ISO/IEC 7816-3:2006)

  — Part 4: Organisation, security and commands for interchange (ISO/IEC 7816-4:2013 + Cor 1:2014)

  — Part 6: Interindustry data elements for interchange (ISO/IEC 7816-6:2004 + Cor 1:2006)

  — Part 8: Commands for security operations (ISO/IEC 7816-8:2004).

— Devem ser feitos ensaios aos cartões tacográficos, em conformidade com a norma ISO/IEC 10373-3: 2010 Identification cards — Test methods — Part 3: Integrated circuit cards with contacts and related interface devices.

4.4 **Especificações ambientais e elétricas**

241) Os cartões tacográficos devem poder funcionar corretamente nas condições climáticas normalmente ocorrentes no território da União Europeia e pelo menos no intervalo térmico de – 25 °C a + 70 °C, com picos ocasionais até + 85 °C, entendendo-se por «ocasionais» ocorrências de duração não superior a 4 horas e em número não superior a 100 ao longo do período de vida útil do cartão.

242) Os cartões tacográficos devem poder funcionar corretamente no intervalo de humidade de 10 % a 90 %.

▼B

243) Os cartões tacográficos devem poder funcionar corretamente durante um período de cinco anos, desde que utilizados em conformidade com as especificações ambientais e elétricas.

244) Durante o seu funcionamento, os cartões devem cumprir o disposto no Regulamento ECE R10, relativo à compatibilidade eletromagnética, e estar protegidos contra descargas eletrostáticas.

4.5 **Armazenamento dos dados**

Para efeitos da presente secção,

— as medidas de tempo são registadas com uma resolução de 1 minuto, salvo indicação diversa

— os valores do conta-quilómetros são registados com uma resolução de 1 km

— as velocidades são registadas com uma resolução de 1 km/h

— as posições (latitudes e longitudes) são registadas em graus e minutos, com uma resolução de 1/10 de minuto.

As funções, os comandos e estruturas lógicas e os requisitos de memorização de dados, aplicáveis aos cartões tacográficos, constam do apêndice 2.

Salvo disposição em contrário, a memorização de dados nos cartões tacográficos deve ser organizada de forma que os novos dados substituem os dados mais antigos memorizados no caso de estar esgotado o tamanho da memória previsto para os registos particulares.

245) Nesta secção, especifica-se a capacidade mínima de memorização para os ficheiros de dados das diversas aplicações. Os cartões tacográficos devem poder indicar ao aparelho de controlo a capacidade efetiva de memorização desses ficheiros.

246) Todos os dados adicionais que podem ser memorizados nos cartões tacográficos, relativos a outras aplicações eventualmente compatíveis com o cartão, devem ser memorizados em conformidade com a Diretiva 95/46/CE e com a Diretiva 2002/58/CE, e em conformidade com o artigo 7.º do Regulamento (UE) n.º 165/2014.

247) Cada ficheiro principal (MF) de qualquer cartão tacográfico deve conter até cinco ficheiros elementares (EF), para gestão de cartões, aplicações e identificações de chip, e dois ficheiros dedicados (DF):

— DF Tachograph, que contém a aplicação acessível a unidades-veículo da primeira geração e que também está presente em cartões tacográficos da primeira geração

— DF Tachograph_G2, que contém a aplicação acessível apenas a unidades-veículo da segunda geração e que está presente apenas em cartões tacográficos da segunda geração.

As informações completas acerca da estrutura dos cartões tacográficos são especificadas no apêndice 2.

4.5.1 *Ficheiros elementares para identificação e gestão de cartões*

4.5.2 *Identificação do cartão IC*

248) Os cartões tacográficos devem poder memorizar os seguintes dados de identificação de cartões inteligentes:

— paragem do relógio

▼B

— número de série do cartão (incluindo referências de fabrico)

— número de homologação do tipo de cartão

— identificação personalizada do cartão (ID)

— identificação incorporada

— identificador do IC.

4.5.2.1 Identificação do chip

249) Os cartões tacográficos devem poder memorizar os seguintes dados de identificação do IC (circuito integrado):

— número de série do IC

— referências de fabrico do IC.

4.5.2.2 DIR (presente somente nos cartões tacográficos da segunda geração)

250) Os cartões tacográficos devem poder memorizar os objetos de dados de identificação da aplicação detalhados no apêndice 2.

4.5.2.3 Informações ATR (condicionadas, presentes somente nos cartões tacográficos da segunda geração)

251) Os cartões tacográficos devem poder memorizar o objeto de dados de informação do aumento do comprimento:

— no caso de o cartão tacográfico aceitar o aumento dos campos de comprimento, o objeto de dados de informação do aumento do comprimento especificado no apêndice 2.

4.5.2.4 Informação do aumento do comprimento (condicionado, presente somente nos cartões tacográficos da segunda geração)

252) Os cartões tacográficos devem poder memorizar os objetos de dados de informação do aumento do comprimento:

— no caso de o cartão tacográfico aceitar o aumento dos campos de comprimento, os objetos de dados de informação do aumento do comprimento especificados no apêndice 2.

4.5.3 *Cartão de condutor*

4.5.3.1 Aplicação tacográfica (acessível às unidades-veículo das primeira e segunda gerações)

4.5.3.1.1 Identificação da aplicação

253) O cartão de condutor deve poder memorizar os seguintes dados relativos à identificação da respetiva aplicação:

— identificação da aplicação tacográfica

— identificação do tipo de cartão tacográfico.

4.5.3.1.2 Chaves e certificados

254) O cartão tacográfico deve poder memorizar várias chaves e certificados criptográficos, conforme especifica o apêndice 11, parte A.

▼B

4.5.3.1.3 Identificação do cartão

255) O cartão de condutor deve poder memorizar os seguintes dados de identificação do cartão:

— número do cartão

— Estado-Membro emissor, autoridade emissora, data de emissão

— datas de início e de cessação do prazo de validade.

4.5.3.1.4 Identificação do titular

256) O cartão de condutor deve poder memorizar os seguintes dados de identificação do respetivo titular:

— apelido

— nome próprio

— data de nascimento

— idioma de preferência.

4.5.3.1.5 Descarregamento do cartão

257) O cartão de condutor deve poder memorizar os seguintes dados relativos ao descarregamento do cartão:

— data e hora relativas ao último descarregamento do cartão (para outras finalidades que não o controlo).

258) O cartão de condutor deve poder guardar 1 registo deste tipo.

4.5.3.1.6 Elementos relativos à carta de condução

259) O cartão de condutor deve poder memorizar os seguintes dados relativos à carta de condução:

— Estado-Membro emissor, autoridade emissora

— número da carta de condução (à data de emissão do cartão).

4.5.3.1.7 Dados relativos a incidentes

Para efeitos da presente secção, os tempos devem ser memorizados com a resolução de 1 segundo.

260) O cartão de condutor deve poder memorizar os dados relativos aos seguintes incidentes detetados pelo aparelho de controlo durante o período de inserção do cartão:

— sobreposição de tempos (se este cartão for a causa do incidente)

— inserção de cartão durante a condução (se este cartão for o protagonista do incidente)

— última sessão de cartão encerrada incorretamente (se este cartão for o protagonista do incidente)

— interrupção da alimentação energética

— erro nos dados de movimento

— tentativas de violação da segurança.

261) O cartão de condutor deve poder memorizar os seguintes dados relativos àqueles incidentes:

— código do incidente

— data e hora do início do incidente (ou da inserção do cartão, caso o incidente estivesse em curso nesse momento)

▼B

— data e hora do final do incidente (ou da retirada do cartão, caso o incidente estivesse em curso nesse momento)

— VRN e Estado-Membro de matrícula do veículo no qual se produziu o incidente.

Nota: No que se refere ao incidente «sobreposição de tempos»:

— a data e a hora de início do incidente devem corresponder à data e à hora de retirada do cartão do veículo anterior

— a data e a hora do final do incidente devem corresponder à data e à hora de inserção do cartão no veículo presente

— os dados relativos ao veículo devem corresponder ao veículo presente, no qual se produziu o incidente.

Nota: No que se refere ao incidente «última sessão de cartão encerrada incorretamente»:

— a data e a hora de início do incidente devem corresponder à data e à hora de inserção do cartão na sessão encerrada incorretamente

— a data e a hora do final do incidente devem corresponder à data e à hora de inserção do cartão na sessão durante a qual o incidente foi detetado (sessão em curso)

— os dados relativos ao veículo devem corresponder ao veículo no qual a sessão não foi encerrada corretamente.

262) O cartão de condutor deve poder memorizar os dados relativos aos 6 incidentes mais recentes de cada um dos 6 tipos (ou seja, os dados relativos a 36 incidentes).

4.5.3.1.8 Dados relativos a falhas

Para efeitos da presente secção, os tempos devem ser registados com a resolução de 1 segundo.

263) O cartão de condutor deve poder memorizar os dados relativos às seguintes falhas detetadas pelo aparelho de controlo durante o período de inserção do cartão:

— falha do cartão (se este for o protagonista da falha)

— falha do aparelho de controlo.

264) O cartão de condutor deve poder memorizar os seguintes dados relativos àquelas falhas:

— código de falha

— data e hora do início da falha (ou da inserção do cartão, caso a falha estivesse em curso nesse momento)

— data e hora do final da falha (ou da retirada do cartão, caso a falha estivesse em curso nesse momento)

— VRN e Estado-Membro de matrícula do veículo no qual se produziu a falha.

265) O cartão de condutor deve poder memorizar os dados relativos às 12 falhas mais recentes de cada um dos tipos (ou seja, os dados relativos a 24 falhas).

▼B

4.5.3.1.9 Dados relativos à atividade de condutor

266) Relativamente a cada dia em que o cartão seja utilizado ou relativamente ao qual o condutor introduza atividades manualmente, o cartão de condutor deve poder memorizar os seguintes dados:

— data

— contador de presença diária (com incrementos de uma unidade por cada um destes dias)

— distância total percorrida pelo condutor nesse dia

— situação do condutor às 00h00

— a cada mudança da atividade do condutor e/ou da situação da condução e/ou a cada inserção ou retirada do cartão do condutor:

— situação da condução (CREW, SINGLE)

— ranhura (DRIVER, CO-DRIVER)

— situação do cartão (INSERTED, NOT INSERTED)

— atividade (DRIVING, AVAILABILITY, WORK, BREAK/REST)

— hora da mudança.

267) A memória do cartão de condutor deve poder guardar os dados relativos à atividade do condutor durante pelo menos 28 dias (define-se atividade média de um condutor como 93 mudanças de atividade por dia).

268) Os dados referidos nos requisitos n.^{os} 261, 264 e 266 devem ser memorizados de modo a permitir recuperar atividades segundo a sua ordem de ocorrência, mesmo na eventualidade de sobreposição de tempos.

4.5.3.1.10 Dados relativos à utilização de veículos

269) Relativamente a cada dia em que o cartão seja utilizado e a cada período de utilização de um determinado veículo nesse dia (um período de utilização inclui a totalidade dos ciclos consecutivos de inserção/retirada do cartão no veículo, considerados do ponto de vista do cartão), o cartão de condutor deve poder memorizar os seguintes dados:

— data e hora da primeira utilização do veículo (ou seja, primeira inserção de cartão durante este período de utilização do veículo, ou 00h00 se o período de utilização estiver a decorrer no momento)

— valor do conta-quilómetros do veículo no momento

— data e hora da última utilização do veículo (ou seja, última retirada de cartão durante este período de utilização do veículo, ou 23h59 se o período de utilização estiver a decorrer no momento)

▼B

— valor do conta-quilómetros do veículo no momento

— VRN e Estado-Membro de matrícula do veículo.

270) O cartão de condutor deve poder memorizar pelo menos 84 registos deste tipo.

4.5.3.1.11 Locais de início e/ou final dos períodos de trabalho diário

271) O cartão de condutor deve poder memorizar os seguintes dados relativos aos locais, introduzidos pelo condutor, em que se iniciam e/ou terminam os períodos de trabalho diário:

— data e hora da introdução (ou data e hora relativas à introdução, se esta for manual)

— tipo de introdução (início ou final, condição da introdução)

— país e região introduzidos

— valor do conta-quilómetros do veículo.

272) A memória do cartão de condutor deve poder guardar pelo menos 42 pares de registos deste tipo.

4.5.3.1.12 Dados relativos à sessão de cartão

273) O cartão de condutor deve poder memorizar os dados relativos ao veículo que abriu a sua sessão em curso:

— data e hora de abertura da sessão (ou seja, da inserção do cartão), com a resolução de 1 segundo

— VRN e Estado-Membro de matrícula.

4.5.3.1.13 Dados relativos à atividade de controlo

274) O cartão de condutor deve poder memorizar os seguintes dados relativos a atividades de controlo:

— data e hora do controlo

— número e Estado-Membro emissor do cartão de controlo

— tipo de controlo: visualização, impressão, descarregamento da VU e/ou descarregamento do cartão (ver nota)

— período descarregado (se o controlo for de descarregamento)

— VRN e Estado-Membro de matrícula do veículo no qual teve lugar o controlo.

Nota: o descarregamento do cartão só será registado se executado por intermédio de um aparelho de controlo.

275) O cartão de condutor deve poder guardar 1 registo deste tipo.

4.5.3.1.14 Dados relativos às condições especiais

276) O cartão de condutor deve poder memorizar os seguintes dados relativos às condições especiais introduzidas durante o período de inserção do cartão (independentemente da ranhura):

— data e hora da introdução dos dados

— tipo de condição especial.

▼B

277) O cartão de condutor deve poder memorizar pelo menos 56 registos deste tipo.

4.5.3.2 Aplicação tacográfica da segunda geração (não acessível às unidades-veículo de primeira geração)

4.5.3.2.1 Identificação da aplicação

278) O cartão de condutor deve poder memorizar os seguintes dados relativos à identificação da respetiva aplicação:

— identificação da aplicação tacográfica

— identificação do tipo de cartão tacográfico.

4.5.3.2.2 Chaves e certificados

279) O cartão tacográfico deve poder memorizar várias chaves e certificados criptográficos, conforme especifica o apêndice 11, parte B.

4.5.3.2.3 Identificação do cartão

280) O cartão de condutor deve poder memorizar os seguintes dados de identificação do cartão:

— número do cartão

— Estado-Membro emissor, autoridade emissora, data de emissão

— datas de início e de cessação do prazo de validade.

4.5.3.2.4 Identificação do titular

281) O cartão de condutor deve poder memorizar os seguintes dados de identificação do respetivo titular:

— apelido do titular

— nome próprio do titular

— data de nascimento

— idioma de preferência.

4.5.3.2.5 Descarregamento do cartão

282) O cartão de condutor deve poder memorizar os seguintes dados relativos ao descarregamento do cartão:

— data e hora relativas ao último descarregamento (para outras finalidades que não o controlo).

283) O cartão de condutor deve poder guardar 1 registo deste tipo.

4.5.3.2.6 Elementos relativos à carta de condução

284) O cartão de condutor deve poder memorizar os seguintes dados relativos à carta de condução:

— Estado-Membro emissor, autoridade emissora

— número da carta de condução (à data de emissão do cartão).

4.5.3.2.7 Dados relativos a incidentes

Para efeitos da presente secção, os tempos devem ser memorizados com a resolução de 1 segundo.

▼B

285) O cartão de condutor deve poder memorizar os dados relativos aos seguintes incidentes detetados pelo aparelho de controlo durante o período de inserção do cartão:

— sobreposição de tempos (se este cartão for a causa do incidente)

— inserção de cartão durante a condução (se este cartão for o protagonista do incidente)

— última sessão de cartão encerrada incorretamente (se este cartão for o protagonista do incidente)

— interrupção da alimentação energética

— erro de comunicação com o sistema de comunicação à distância

— incidente «Ausência de informações sobre a posição do recetor GNSS»

— erro de comunicação com o módulo GNSS externo

— erro nos dados de movimento

— conflito relativo ao movimento do veículo

— tentativas de violação da segurança

— conflito de tempo.

286) O cartão de condutor deve poder memorizar os seguintes dados relativos àqueles incidentes:

— código do incidente

— data e hora do início do incidente (ou da inserção do cartão, caso o incidente estivesse em curso nesse momento)

— data e hora do final do incidente (ou da retirada do cartão, caso o incidente estivesse em curso nesse momento)

— VRN e Estado-Membro de matrícula do veículo no qual se produziu o incidente.

Nota: No que se refere ao incidente «sobreposição de tempos»:

— a data e a hora de início do incidente devem corresponder à data e à hora de retirada do cartão do veículo anterior

— a data e a hora do final do incidente devem corresponder à data e à hora de inserção do cartão no veículo presente

— os dados relativos ao veículo devem corresponder ao veículo presente, no qual se produziu o incidente.

Nota: No que se refere ao incidente «última sessão de cartão encerrada incorretamente»:

— a data e a hora de início do incidente devem corresponder à data e à hora de inserção do cartão na sessão encerrada incorretamente

— a data e a hora do final do incidente devem corresponder à data e à hora de inserção do cartão na sessão durante a qual o incidente foi detetado (sessão em curso)

▼B

— os dados relativos ao veículo devem corresponder ao veículo no qual a sessão não foi encerrada corretamente.

287) O cartão de condutor deve poder memorizar os dados relativos aos 6 incidentes mais recentes de cada um dos tipos (ou seja, os dados relativos a 66 incidentes).

4.5.3.2.8 Dados relativos a falhas

Para efeitos da presente secção, os tempos devem ser registados com a resolução de 1 segundo.

288) O cartão de condutor deve poder memorizar os dados relativos às seguintes falhas detetadas pelo aparelho de controlo durante o período de inserção do cartão:

— falha do cartão (se este for o protagonista da falha)

— falha do aparelho de controlo.

289) O cartão de condutor deve poder memorizar os seguintes dados relativos àquelas falhas:

— código de falha

— data e hora do início da falha (ou da inserção do cartão, caso a falha estivesse em curso nesse momento)

— data e hora do final da falha (ou da retirada do cartão, caso a falha estivesse em curso nesse momento)

— VRN e Estado-Membro de matrícula do veículo no qual se produziu a falha.

290) O cartão de condutor deve poder memorizar os dados relativos às 12 falhas mais recentes de cada um dos tipos (ou seja, os dados relativos a 24 falhas).

4.5.3.2.9 Dados relativos à atividade de condutor

291) Relativamente a cada dia em que o cartão seja utilizado ou relativamente ao qual o condutor introduza atividades manualmente, o cartão de condutor deve poder memorizar os seguintes dados:

— data

— contador de presença diária (com incrementos de uma unidade por cada um destes dias)

— distância total percorrida pelo condutor nesse dia

— situação do condutor às 00h00

— a cada mudança da atividade do condutor e/ou da situação da condução e/ou a cada inserção ou retirada do cartão do condutor:

— situação da condução (CREW, SINGLE)

— ranhura (DRIVER, CO-DRIVER)

— situação do cartão (INSERTED, NOT INSERTED)

— atividade (DRIVING, AVAILABILITY, WORK, BREAK/REST).

▼B

— hora da mudança.

292) A memória do cartão de condutor deve poder guardar os dados relativos à atividade do condutor durante pelo menos 28 dias (define-se atividade média de um condutor como 93 mudanças de atividade por dia).

293) Os dados referidos nos requisitos n.os 286, 289 e 291 devem ser memorizados de modo a permitir recuperar atividades segundo a sua ordem de ocorrência, mesmo na eventualidade de sobreposição de tempos.

4.5.3.2.10 Dados relativos à utilização de veículos

294) Relativamente a cada dia em que se utilize o cartão e a cada período de utilização de um determinado veículo nesse dia (um período de utilização inclui a totalidade dos ciclos consecutivos de inserção/retirada do cartão no veículo, considerados do ponto de vista do cartão), o cartão de condutor deve poder memorizar os seguintes dados:

— data e hora da primeira utilização do veículo (ou seja, primeira inserção de cartão durante este período de utilização do veículo, ou 00h00 se o período de utilização estiver a decorrer no momento)

— valor do conta-quilómetros do veículo aquando da primeira utilização

— data e hora da última utilização do veículo (ou seja, última retirada de cartão durante este período de utilização do veículo, ou 23h59 se o período de utilização estiver a decorrer no momento)

— valor do conta-quilómetros do veículo aquando da última utilização

— VRN e Estado-Membro de matrícula do veículo

— VIN do veículo.

295) O cartão de condutor deve poder memorizar pelo menos 84 registos deste tipo.

4.5.3.2.11 Locais e posições de início e/ou final dos períodos de trabalho diário

296) O cartão de condutor deve poder memorizar os seguintes dados relativos aos locais, introduzidos pelo condutor, em que se iniciam e/ou terminam os períodos de trabalho diário:

— data e hora da introdução (ou data e hora relativas à introdução, se esta for manual)

— tipo de introdução (início ou final, condição da introdução)

— país e região introduzidos

— valor do conta-quilómetros do veículo

— posição do veículo

— precisão GNSS, data e hora no momento de determinação da posição.

297) A memória do cartão de condutor deve poder guardar pelo menos 84 pares de registos deste tipo.

▼B

4.5.3.2.12 Dados relativos à sessão de cartão

298) O cartão de condutor deve poder memorizar os dados relativos ao veículo que abriu a sua sessão em curso:

— data e hora de abertura da sessão (ou seja, da inserção do cartão), com a resolução de 1 segundo

— VRN e Estado-Membro de matrícula.

4.5.3.2.13 Dados relativos à atividade de controlo

299) O cartão de condutor deve poder memorizar os seguintes dados relativos a atividades de controlo:

— data e hora do controlo

— número e Estado-Membro emissor do cartão de controlo

— tipo de controlo: visualização, impressão, descarregamento da VU e/ou descarregamento do cartão (ver nota)

— período descarregado (se o controlo for de descarregamento)

— VRN e Estado-Membro de matrícula do veículo no qual teve lugar o controlo.

Nota: os requisitos de segurança implicam que o descarregamento do cartão só seja registado se executado por intermédio de um aparelho de controlo.

300) O cartão de condutor deve poder guardar 1 registo deste tipo.

4.5.3.2.14 Dados relativos às condições especiais

301) O cartão de condutor deve poder memorizar os seguintes dados relativos às condições especiais introduzidas durante o período de inserção do cartão (independentemente da ranhura):

— data e hora da introdução dos dados

— tipo de condição especial.

302) O cartão de condutor deve poder memorizar pelo menos 56 registos deste tipo.

4.5.3.2.15 Dados relativos à utilização de unidades-veículo

303) O cartão de condutor deve poder memorizar os seguintes dados relativos às diferentes unidades-veículo nas quais foi utilizado o cartão:

— data e hora do início do período de utilização da unidade-veículo (ou seja, a primeira inserção do cartão na unidade-veículo relativa ao período)

— fabricante da VU

— tipo de unidade-veículo

— número da versão do *software* da VU.

304) O cartão de condutor deve poder memorizar pelo menos 84 registos deste tipo.

▼B

4.5.3.2.16 Dados relativos à localização das três horas de condução contínua

305) O cartão de condutor deve poder memorizar os seguintes dados relativos à posição do veículo, em que o tempo de condução contínua do condutor atinge um múltiplo de três horas:

— data e hora em que o tempo de condução contínua do titular do cartão atinge um múltiplo de três horas

— posição do veículo

— precisão GNSS, data e hora no momento de determinação da posição.

306) O cartão de condutor deve poder memorizar pelo menos 252 registos deste tipo.

4.5.4 *Cartão de oficina*

4.5.4.1 Aplicação tacográfica (acessível às unidades-veículo das primeira e segunda gerações)

4.5.4.1.1 Identificação da aplicação

307) O cartão de oficina deve poder memorizar os seguintes dados relativos à identificação da respetiva aplicação:

— identificação da aplicação tacográfica

— identificação do tipo de cartão tacográfico.

4.5.4.1.2 Chaves e certificados

308) O cartão de oficina deve poder memorizar várias chaves e certificados criptográficos, conforme especifica o apêndice 11, parte A.

309) O cartão de oficina deve poder memorizar um número de identificação pessoal (código PIN).

4.5.4.1.3 Identificação do cartão

310) O cartão de oficina deve poder memorizar os seguintes dados relativos à sua identificação:

— número do cartão

— Estado-Membro emissor, autoridade emissora, data de emissão

— datas de início e de cessação do prazo de validade.

4.5.4.1.4 Identificação do titular

311) O cartão de oficina deve poder memorizar os seguintes dados de identificação do respetivo titular:

— nome da oficina

— endereço da oficina

— apelido do titular

— nome próprio do titular

— idioma de preferência.

4.5.4.1.5 Descarregamento do cartão

312) O cartão de oficina deve poder memorizar os dados relativos ao descarregamento do cartão de modo idêntico a um cartão de condutor.

▼B

4.5.4.1.6 Dados relativos à calibração e ao ajustamento do tempo

313) O cartão de oficina deve poder guardar os registos relativos a operações de calibração e/ou de ajustamento do tempo executadas durante o período de inserção do cartão num aparelho de controlo.

314) Cada registo relativo a calibração deve poder guardar os seguintes dados:

— objetivo da calibração (ativação, primeira instalação, instalação, inspeção periódica)

— identificação do veículo

— parâmetros atualizados ou confirmados (dimensões w, k, l, medida do pneumático, ponto de regulação do eventual dispositivo de limitação da velocidade, valor do conta-quilómetros atual e anterior, data e hora atual e anterior)

— identificação do aparelho de controlo (número de peça da VU, número de série da VU, número de série do sensor de movimentos).

315) O cartão de oficina deve poder memorizar pelo menos 88 registos deste tipo.

316) O cartão de oficina deve ser equipado com um contador que indique o número total de calibrações executadas com o cartão.

317) O cartão de oficina deve ser equipado com um contador que indique o número de calibrações executadas desde o seu último descarregamento.

4.5.4.1.7 Dados relativos a incidentes e a falhas

318) O cartão de oficina deve poder memorizar os dados relativos a incidentes e a falhas de modo idêntico a um cartão de condutor.

319) O cartão de oficina deve poder memorizar os dados relativos aos 3 incidentes mais recentes de cada um dos tipos (ou seja, os dados relativos a 18 incidentes) e os dados relativos às 6 falhas mais recentes de cada um dos tipos (ou seja, os dados relativos a 12 falhas).

4.5.4.1.8 Dados relativos à atividade de condutor

320) O cartão de oficina deve poder memorizar os dados relativos à atividade de condutor de modo idêntico a um cartão de condutor.

321) O cartão de oficina deve poder guardar os dados relativos à atividade de condutor durante pelo menos 1 dia de atividade média do condutor.

4.5.4.1.9 Dados relativos à utilização de veículos

322) O cartão de oficina deve poder memorizar os dados relativos à utilização de veículos de modo idêntico a um cartão de condutor.

323) O cartão de oficina deve poder memorizar pelo menos 4 registos deste tipo.

4.5.4.1.10 Dados relativos ao início e/ou ao final dos períodos de trabalho diário

324) O cartão de oficina deve poder memorizar os dados relativos ao início e/ou ao final dos períodos de trabalho diário de modo idêntico a um cartão de condutor.

325) O cartão de oficina deve poder guardar pelo menos 3 pares de registos deste tipo.

▼B

4.5.4.1.11 Dados relativos à sessão de cartão

326) O cartão de oficina deve poder memorizar o registo dos dados relativos à sessão do cartão de modo idêntico a um cartão de condutor.

4.5.4.1.12 Dados relativos à atividade de controlo

327) O cartão de oficina deve poder memorizar os dados relativos à atividade de controlo de modo idêntico a um cartão de condutor.

4.5.4.1.13 Dados relativos às condições especiais

328) O cartão de oficina deve poder memorizar os dados relativos às condições especiais de modo idêntico a um cartão de condutor.

329) O cartão de oficina deve poder memorizar pelo menos 2 registos deste tipo.

4.5.4.2 Aplicação tacográfica de segunda geração (não acessível às unidades-veículo de primeira geração)

4.5.4.2.1 Identificação da aplicação

330) O cartão de oficina deve poder memorizar os seguintes dados relativos à identificação da respetiva aplicação:

— identificação da aplicação tacográfica

— identificação do tipo de cartão tacográfico.

4.5.4.2.2 Chaves e certificados

331) O cartão de oficina deve poder memorizar várias chaves e certificados criptográficos, conforme especifica o apêndice 11, parte B.

332) O cartão de oficina deve poder memorizar um número de identificação pessoal (código PIN).

4.5.4.2.3 Identificação do cartão

333) O cartão de oficina deve poder memorizar os seguintes dados relativos à sua identificação:

— número do cartão

— Estado-Membro emissor, autoridade emissora, data de emissão

— datas de início e de cessação do prazo de validade.

4.5.4.2.4 Identificação do titular

334) O cartão de oficina deve poder memorizar os seguintes dados de identificação do respetivo titular:

— nome da oficina

— endereço da oficina

— apelido do titular

— nome próprio do titular

— idioma de preferência.

4.5.4.2.5 Descarregamento do cartão

335) O cartão de oficina deve poder memorizar os dados relativos ao descarregamento do cartão de modo idêntico a um cartão de condutor.

▼B

4.5.4.2.6 Dados relativos à calibração e ao ajustamento do tempo

336) O cartão de oficina deve poder guardar os registos relativos a operações de calibração e/ou de ajustamento do tempo executadas durante o período de inserção do cartão num aparelho de controlo.

337) Cada registo relativo a calibração deve poder guardar os seguintes dados:

— objetivo da calibração (ativação, primeira instalação, instalação, inspeção periódica)

— identificação do veículo

— parâmetros atualizados ou confirmados (dimensões w, k, l, medida do pneumático, ponto de regulação do eventual dispositivo de limitação da velocidade, valor do conta-quilómetros atual e anterior, data e hora atual e anterior)

— identificação do aparelho de controlo (número de peça da VU, número de série da VU, número de série do sensor de movimentos, número de série do sistema de comunicação à distância e número de série do módulo GNSS externo, quando aplicável)

— tipo de selo e identificador de todos os selos em vigor

— capacidade de utilização de cartões tacográficos da primeira geração por parte da VU (ativada ou não).

338) O cartão de oficina deve poder memorizar pelo menos 88 registos deste tipo.

339) O cartão de oficina deve ser equipado com um contador que indique o número total de calibrações executadas com o cartão.

340) O cartão de oficina deve ser equipado com um contador que indique o número de calibrações executadas desde o seu último descarregamento.

4.5.4.2.7 Dados relativos a incidentes e a falhas

341) O cartão de oficina deve poder memorizar os dados relativos a incidentes e a falhas de modo idêntico a um cartão de condutor.

342) O cartão de oficina deve poder memorizar os dados relativos aos 3 incidentes mais recentes de cada um dos tipos (ou seja, os dados relativos a 33 incidentes) e os dados relativos às 6 falhas mais recentes de cada um dos tipos (ou seja, os dados relativos a 12 falhas).

4.5.4.2.8 Dados relativos à atividade de condutor

343) O cartão de oficina deve poder memorizar os dados relativos à atividade de condutor de modo idêntico a um cartão de condutor.

344) O cartão de oficina deve poder guardar os dados relativos à atividade de condutor durante pelo menos 1 dia de atividade média do condutor.

4.5.4.2.9 Dados relativos à utilização de veículos

345) O cartão de oficina deve poder memorizar os dados relativos à utilização de veículos de modo idêntico a um cartão de condutor.

346) O cartão de oficina deve poder memorizar pelo menos 4 registos deste tipo.

▼B

4.5.4.2.10 Dados relativos ao início e/ou ao final dos períodos de trabalho diário

347) O cartão de oficina deve poder memorizar os dados relativos ao início e/ou ao final dos períodos de trabalho diário de modo idêntico a um cartão de condutor.

348) O cartão de oficina deve poder guardar pelo menos 3 pares de registos deste tipo.

4.5.4.2.11 Dados relativos à sessão de cartão

349) O cartão de oficina deve poder memorizar o registo dos dados relativos à sessão do cartão de modo idêntico a um cartão de condutor.

4.5.4.2.12 Dados relativos à atividade de controlo

350) O cartão de oficina deve poder memorizar os dados relativos à atividade de controlo de modo idêntico a um cartão de condutor.

4.5.4.2.13 Dados relativos à utilização de unidades-veículo

351) O cartão de oficina deve poder memorizar os seguintes dados relativos às diferentes unidades-veículo nas quais foi utilizado o cartão:

— data e hora do início do período de utilização da unidade-veículo (ou seja, a primeira inserção do cartão na unidade-veículo relativa ao período)

— fabricante da VU

— tipo de unidade-veículo

— número da versão do *software* da VU.

352) O cartão de oficina deve poder memorizar pelo menos 4 registos deste tipo.

4.5.4.2.14 Dados relativos à localização das três horas de condução contínua

353) O cartão de oficina deve poder memorizar os seguintes dados relativos à posição do veículo, em que o tempo de condução contínua do condutor atinge um múltiplo de três horas:

— data e hora em que o tempo de condução contínua do titular do cartão atinge um múltiplo de três horas

— posição do veículo

— precisão GNSS, data e hora no momento de determinação da posição.

354) O cartão de oficina deve poder memorizar pelo menos 18 registos deste tipo.

4.5.4.2.15 Dados relativos às condições especiais

355) O cartão de oficina deve poder memorizar os dados relativos às condições especiais de modo idêntico a um cartão de condutor.

356) O cartão de oficina deve poder memorizar pelo menos 2 registos deste tipo.

▼B

4.5.5 *Cartão de controlo*

4.5.5.1 Aplicação tacográfica (acessível às unidades-veículo das primeira e segunda gerações)

4.5.5.1.1 Identificação da aplicação

357) O cartão de controlo deve poder memorizar os seguintes dados de identificação da aplicação:

— identificação da aplicação tacográfica

— identificação do tipo de cartão tacográfico.

4.5.5.1.2 Chaves e certificados

358) O cartão de controlo deve poder memorizar várias chaves e certificados criptográficos, conforme especifica o apêndice 11, parte A.

4.5.5.1.3 Identificação do cartão

359) O cartão de controlo deve poder memorizar os seguintes dados relativos à sua identificação:

— número do cartão

— Estado-Membro emissor, autoridade emissora, data de emissão

— eventuais datas de início e de cessação do prazo de validade.

4.5.5.1.4 Identificação do titular

360) O cartão de controlo deve poder memorizar os seguintes dados de identificação do respetivo titular:

— nome do organismo de controlo

— endereço do organismo de controlo

— apelido do titular

— nome próprio do titular

— idioma de preferência.

4.5.5.1.5 Dados relativos à atividade de controlo

361) O cartão de controlo deve poder memorizar os seguintes dados relativos a atividades de controlo:

— data e hora do controlo

— tipo do controlo (visualização e/ou impressão e/ou descarregamento da VU e/ou descarregamento do cartão e/ou controlo da calibração de estrada)

— período do descarregamento (eventual)

— VRN e Estado-Membro de matrícula do veículo sujeito ao controlo

— número do cartão e Estado-Membro emissor do cartão de condutor sujeito ao controlo.

362) O cartão de controlo deve poder guardar pelo menos 230 registos deste tipo.

▼B

4.5.5.2 Aplicação tacográfica G2 (não acessível a unidades-veículo da primeira geração)

4.5.5.2.1 Identificação da aplicação

363) O cartão de controlo deve poder memorizar os seguintes dados de identificação da aplicação:

— identificação da aplicação tacográfica

— identificação do tipo de cartão tacográfico.

4.5.5.2.2 Chaves e certificados

364) O cartão de controlo deve poder memorizar várias chaves e certificados criptográficos, conforme especifica o apêndice 11, parte B.

4.5.5.2.3 Identificação do cartão

365) O cartão de controlo deve poder memorizar os seguintes dados relativos à sua identificação:

— número do cartão

— Estado-Membro emissor, autoridade emissora, data de emissão

— eventuais datas de início e de cessação do prazo de validade.

4.5.5.2.4 Identificação do titular

366) O cartão de controlo deve poder memorizar os seguintes dados de identificação do respetivo titular:

— nome do organismo de controlo

— endereço do organismo de controlo

— apelido do titular

— nome próprio do titular

— idioma de preferência.

4.5.5.2.5 Dados relativos à atividade de controlo

367) O cartão de controlo deve poder memorizar os seguintes dados relativos a atividades de controlo:

— data e hora do controlo

— tipo de controlo: visualização, impressão, descarregamento da VU e/ou descarregamento do cartão e/ou controlo de calibração de estrada

— período do descarregamento (eventual)

— VRN e Estado-Membro de matrícula do veículo sujeito ao controlo

— número do cartão e Estado-Membro emissor do cartão de condutor sujeito ao controlo.

368) O cartão de controlo deve poder guardar pelo menos 230 registos deste tipo.

▼B

4.5.6 *Cartão de empresa*

4.5.6.1 Aplicação tacográfica (acessível às unidades-veículo das primeira e segunda gerações)

4.5.6.1.1 Identificação da aplicação

369) O cartão de empresa deve poder memorizar os seguintes dados de identificação da aplicação:

— identificação da aplicação tacográfica

— identificação do tipo de cartão tacográfico.

4.5.6.1.2 Chaves e certificados

370) O cartão de empresa deve poder memorizar várias chaves e certificados criptográficos, conforme especifica o apêndice 11, parte A.

4.5.6.1.3 Identificação do cartão

371) O cartão de empresa deve poder memorizar os seguintes dados relativos à sua identificação:

— número do cartão

— Estado-Membro emissor, autoridade emissora, data de emissão

— eventuais datas de início e de cessação do prazo de validade.

4.5.6.1.4 Identificação do titular

372) O cartão de empresa deve poder memorizar os seguintes dados de identificação do respetivo titular:

— nome da empresa

— endereço da empresa.

4.5.6.1.5 Dados relativos à atividade da empresa

373) O cartão de empresa deve poder memorizar os seguintes dados relativos à atividade da empresa:

— data e hora da atividade

— tipo de atividade: início (lock-in) e/ou final (lock-out) de bloqueamento da VU, descarregamento da VU e/ou descarregamento do cartão

— período do descarregamento (eventual)

— VRN e Estado-Membro de matrícula do veículo

— número e Estado-Membro emissor do cartão (em caso de descarregamento do cartão).

374) O cartão de empresa deve poder guardar pelo menos 230 registos deste tipo.

▼B

4.5.6.2 Aplicação tacográfica G2 (não acessível a unidades-veículo da primeira geração)

4.5.6.2.1 Identificação da aplicação

375) O cartão de empresa deve poder memorizar os seguintes dados de identificação da aplicação:

— identificação da aplicação tacográfica

— identificação do tipo de cartão tacográfico.

4.5.6.2.2 Chaves e certificados

376) O cartão de empresa deve poder memorizar várias chaves e certificados criptográficos, conforme especifica o apêndice 11, parte B.

4.5.6.2.3 Identificação do cartão

377) O cartão de empresa deve poder memorizar os seguintes dados relativos à sua identificação:

— número do cartão

— Estado-Membro emissor, autoridade emissora, data de emissão

— eventuais datas de início e de cessação do prazo de validade.

4.5.6.2.4 Identificação do titular

378) O cartão de empresa deve poder memorizar os seguintes dados de identificação do respetivo titular:

— nome da empresa

— endereço da empresa.

4.5.6.2.5 Dados relativos à atividade da empresa

379) O cartão de empresa deve poder memorizar os seguintes dados relativos à atividade da empresa:

— data e hora da atividade

— tipo de atividade: início (lock-in) e/ou final (lock-out) de bloqueamento da VU, descarregamento da VU e/ou descarregamento do cartão

— período do descarregamento (eventual)

— VRN e Estado-Membro de matrícula do veículo

— número e Estado-Membro emissor do cartão (em caso de descarregamento do cartão).

380) O cartão de empresa deve poder guardar pelo menos 230 registos deste tipo.

5 INSTALAÇÃO DE APARELHO DE CONTROLO

5.1 **Instalação**

381) Os aparelhos de controlo novos devem ser entregues não ativados aos instaladores ou fabricantes dos veículos, com todos os parâmetros de calibração, constantes do capítulo 3.21, ajustados aos correspondentes valores por defeito. Nos casos em que não existam valores definidos por defeito, os parâmetros literais devem ser apresentados em séries de «?» e os parâmetros numéricos em séries de «0». A entrega de peças relevantes para a segurança do aparelho de controlo pode ser restringida, se a certificação de segurança o exigir.

▼B

382) Antes da ativação, o aparelho de controlo deve dar acesso à função de calibração, mesmo que não esteja em modo de calibração.

383) Antes da ativação, o aparelho de controlo não deve registar nem memorizar dados referidos nas secções 3.12.3 e 3.12.9 e nas secções 3.12.12 a 3.12.15, inclusive.

384) Durante a instalação, os fabricantes de veículos devem pré-ajustar todos os parâmetros conhecidos.

385) Os fabricantes de veículos ou instaladores devem ativar o aparelho de controlo o mais tardar antes de o veículo ser utilizado para os fins abrangidos pelo Regulamento (CE) n.º 561/2006.

386) A ativação do aparelho de controlo deve ser automaticamente acionada pela primeira inserção de um cartão de oficina em qualquer das suas interfaces.

387) As eventuais operações específicas de emparelhamento entre o sensor de movimentos e a unidade-veículo devem processar-se automaticamente antes ou durante a ativação.

388) Do mesmo modo, as eventuais operações específicas de emparelhamento entre o módulo GNSS externo e a unidade-veículo devem processar-se automaticamente antes ou durante a ativação.

389) Uma vez ativado, o aparelho de controlo deve cumprir plenamente as funções e os direitos de acesso aos dados.

390) Uma vez ativado, o aparelho de controlo deve comunicar ao sistema de comunicação à distância os dados securizados necessários para a realização de controlos de estrada seletivos.

391) As funções de registo e de memorização do aparelho de controlo devem ficar plenamente operacionais após a ativação.

392) À instalação deve seguir-se uma calibração. A primeira calibração pode não incluir necessariamente a introdução do número de matrícula do veículo (VRN), se a oficina aprovada que executa essa calibração não tiver conhecimento do mesmo. Nessas circunstâncias, deve ser possível, ao proprietário do veículo, e apenas neste momento, introduzir o VRN utilizando o seu cartão de empresa antes da utilização do veículo para os fins abrangidos pelo Regulamento (CE) n.º 561/2006 (por exemplo, utilizando comandos através de uma estrutura de menus adequada da interface homem/máquina da unidade-veículo) [1]. A atualização ou confirmação desta introdução de dados apenas será possível utilizando um cartão de oficina.

393) A instalação de um módulo GNSS externo exige o emparelhamento com a unidade-veículo e a posterior verificação das informações de posição GNSS.

394) O aparelho de controlo deve ser instalado no veículo de modo a que o condutor, do seu lugar, possa ter acesso às funções que pretender.

[1] JO L 102 de 11.4.2006, p. 1.

▼B

5.2 **Placa de instalação**

395) Verificada a instalação do aparelho de controlo, deve afixar-se uma placa de instalação claramente visível e facilmente acessível. Se não for possível afixá-la em cima do aparelho, afixa-se no pilar «B» do veículo. Em veículos que não tenham pilar «B», afixa-se a placa na ombreira da porta do lado do condutor do veículo, de modo a ficar claramente visível em qualquer caso.

No final de qualquer inspeção efetuada por um instalador ou oficina homologada, a placa anterior deve ser substituída por uma nova.

396) Na placa devem figurar pelo menos os seguintes elementos:

— nome, endereço e marca do instalador ou oficina homologado

— coeficiente característico do veículo, sob a forma «w = … imp/km»

— constante do aparelho de controlo, sob a forma «k = … imp/km»

— perímetro efetivo dos pneus das rodas, sob a forma «l = … mm»

— medida do pneumático

— data de medição do coeficiente característico do veículo e do perímetro efetivo dos pneus das rodas

— número de identificação do veículo

— presença (ou ausência) de um módulo GNSS externo

— número de série do módulo GNSS externo

— número de série do dispositivo de comunicação à distância

— número de série de todos os selos em vigor

— parte do veículo onde eventualmente está instalado o adaptador

— parte do veículo onde está instalado o sensor de movimentos, se não estiver ligado à caixa de velocidades ou não estiver a ser utilizado um adaptador

— descrição da cor do cabo entre o adaptador e a parte do veículo de onde provêm os impulsos de entrada

— número de série do sensor de movimentos incorporado no adaptador.

397) Apenas no que diz respeito a veículos M1 e N1, equipados com um adaptador em conformidade com o estabelecido no Regulamento (CE) n.º 68/2009 ([1]), e se não for possível incluir toda a informação necessária, conforme descrito no requisito n.º 396, pode utilizar-se uma segunda placa adicional, caso em que tal placa adicional deve conter, pelo menos, os últimos quatro travessões descritos no requisito n.º 396.

([1]) Regulamento (CE) n.º 68/2009 da Comissão, de 23 de janeiro de 2009, que adapta pela nona vez ao progresso técnico o Regulamento (CEE) n.º 3821/85 do Conselho relativo à introdução de um aparelho de controlo no domínio dos transportes rodoviários (JO L 21 de 24.1.2009, p. 3).

▼B

A eventual segunda placa deve ser afixada próximo ou ao lado da primeira placa primária descrita no requisito n.º 396 e deve ter o mesmo nível de proteção. A placa secundária deve também apresentar o nome, o endereço ou a designação comercial do instalador ou a oficina homologada que efetuou a instalação, bem como a data da instalação.

5.3 **Selagem**

398) Devem ser seladas as seguintes peças:

— qualquer ligação que, se estiver desligada, provoque alterações indetetáveis ou perda indetetável de dados (pode, por exemplo, aplicar-se ao encaixe do sensor de movimentos na caixa de velocidades, ao adaptador para veículos M1/N1, à ligação GNSS externa ou à unidade-veículo);

— a placa de instalação, a menos que seja aplicada de tal maneira que não se possa retirar sem destruir as marcações.

399) Os selos supramencionados podem ser removidos:

— em caso de emergência

— para instalar, ajustar ou reparar um dispositivo de limitação da velocidade ou outro dispositivo de segurança rodoviária, sob condição de o aparelho de controlo continuar a funcionar corretamente e ser de novo selado por um instalador ou oficina homologada (em conformidade com o capítulo 6) imediatamente após a fixação do dispositivo de limitação da velocidade ou de outro dispositivo de segurança rodoviária ou no prazo de sete dias noutros casos.

400) Cada vez que os selos forem removidos, deve ser redigida e disponibilizada à autoridade competente uma declaração de motivos.

401) Os selos devem possuir um número de identificação, atribuído pelo seu fabricante. Este número deve ser único e distinto de qualquer outro número de selo atribuído por qualquer outro fabricante de selos.

O número de identificação único é definido como: MM NNNNNN por marcação não removível, sendo MM a identificação única do fabricante (registo da base de dados a gerir pela CE) e NNNNNN o código alfanumérico do selo, único no domínio do fabricante.

402) Os selos devem dispor de um espaço livre onde os instaladores, as oficinas ou os fabricantes de veículos (homologados) possam adicionar uma marca especial nos termos do artigo 22.º, n.º 3 do Regulamento (UE) n.º 165/2014.

Esta marca não deve abranger o número de identificação do selo.

403) Os fabricantes de selos devem estar registados numa base de dados dedicada e disponibilizar publicamente os números dos selos de identificação através de um procedimento a estabelecer pela Comissão Europeia.

404) As oficinas e os fabricantes de veículos (homologados) devem, no âmbito do Regulamento (UE) n.º 165/2014, utilizar somente selos de entre os listados pelos fabricantes na base de dados supramencionada.

▼B

405) Os fabricantes de selos e os respetivos distribuidores devem manter registos completos de rastreabilidade dos selos vendidos a utilizar no âmbito do Regulamento (UE) n.º 165/2014 e devem estar preparados para os produzir para as autoridades nacionais competentes, sempre que necessário.

406) Os números de identificação única dos selos devem estar visíveis na placa de instalação.

6 VERIFICAÇÕES, INSPEÇÕES E REPARAÇÕES

Os requisitos aplicáveis à remoção dos selos, nos termos do artigo 22.º, n.º 5, do Regulamento (UE) n.º 165/2014, figuram no capítulo 5.3 do presente anexo.

6.1 **Homologação de instaladores, oficinas e fabricantes de veículos**

Os Estados-Membros homologam, sujeitam a controlo regular e certificam os organismos responsáveis pelas seguintes operações:

— instalação

— controlos

— inspeções

— reparação.

Os cartões de oficina são emitidos unicamente em nome de instaladores e/ou oficinas homologados para efeitos de ativação e/ou calibração dos aparelhos de controlo, em conformidade com o presente anexo, e, salvo devida justificação:

— que não sejam elegíveis para atribuição de cartão de empresa

— cujas restantes atividades profissionais não representem um risco potencial para a segurança geral do sistema, na aceção do apêndice 10.

6.2 **Verificação de instrumentos novos ou reparados**

407) Cada dispositivo individual, novo ou reparado, deve ser verificado em relação ao seu funcionamento correto e à precisão dos seus registos e leituras, dentro dos limites estabelecidos nos capítulos 3.2.1, 3.2.2, 3.2.3 e 3.3, por meio de selagem (nos termos do capítulo 5.3) e de calibração.

6.3 **Inspeção da instalação**

408) Na fixação a um veículo, o conjunto da instalação (incluindo o aparelho de controlo) deve cumprir o disposto nos capítulos 3.2.1, 3.2.2, 3.2.3 e 3.3 em matéria de tolerâncias máximas.

6.4 **Inspeções periódicas**

409) Devem ser feitas inspeções periódicas aos aparelhos instalados nos veículos nas seguintes circunstâncias: após qualquer reparação dos aparelhos ou qualquer alteração do coeficiente característico do veículo ou do perímetro efetivo dos pneus das rodas; se a hora UTC do aparelho de controlo apresentar desfasamentos superiores a 20 minutos; se o VRN for alterado; e pelo menos uma vez no prazo de dois anos (24 meses) após a última inspeção.

410) Estas inspeções devem incluir as seguintes verificações:

— funcionamento correto do aparelho de controlo, incluindo a função de memorização de dados nos cartões tacográficos e a comunicação com os leitores de comunicação à distância

▼B

— garantia de conformidade com o disposto nos capítulos 3.2.1 e 3.2.2 acerca das tolerâncias máximas admissíveis aquando da instalação

— garantia de conformidade com o disposto nos capítulos 3.2.3 e 3.3

— colocação da marca de homologação de tipo no aparelho de controlo

— presença da placa de instalação, definida no requisito n.º 396, e da placa descritiva, definida no requisito n.º 225

— medida do pneumático e perímetro efetivo dos pneumáticos

— inexistência de dispositivos de manipulação fixados no equipamento

— colocação correta dos selos, bom estado, validade dos números de identificação (fabricante de selos referido na base de dados CE) e correspondência dos respetivos números de identificação com as marcas da placa de instalação (ver requisito n.º 401).

411) Caso se verifique, desde a última inspeção, a ocorrência de um dos incidentes enumerados no capítulo 3.9 (Deteção de incidentes e/ou falhas), que os fabricantes do tacógrafo e/ou as autoridades nacionais considerem suscetíveis de pôr em risco a segurança do equipamento, a oficina deve:

a. fazer uma comparação entre os dados de identificação do sensor de movimentos ligado à caixa de velocidades com os do sensor de movimentos emparelhado registado na unidade-veículo

b. verificar se as informações gravadas na placa de instalação correspondem às informações contidas no registo da unidade-veículo

c. verificar se o número de série e o número de homologação do sensor de movimentos, quando impresso na caixa do sensor de movimentos, corresponde às informações contidas na memória de dados do aparelho de controlo

d. comparar os dados de identificação marcados na placa descritiva do módulo GNSS externo, se houver, com os memorizados na memória de dados da unidade-veículo.

412) As oficinas devem manter, nos seus relatórios de inspeção, registos de quaisquer constatações relativas a selos quebrados ou dispositivos de manipulação. Estes relatórios devem ser mantidos pelas oficinas durante um período mínimo de dois anos e disponibilizados à autoridade competente sempre que esta o solicite.

413) Estas inspeções devem incluir uma calibração e uma substituição preventiva dos selos cuja instalação esteja sob a responsabilidade de oficinas.

6.5 **Determinação dos erros**

414) A determinação dos erros na instalação e durante a utilização efetua-se nas seguintes condições, a considerar como condições normais de ensaio:

— veículos em vazio, em condições normais de marcha

— pressão dos pneus, segundo as indicações do fabricante

▼B

— desgaste dos pneus, segundo os limites autorizados pela legislação nacional

— circulação de veículos:

— o veículo deve avançar movido pelo seu próprio motor, em linha reta sobre uma superfície plana, à velocidade de 50 ± 5 km/h. A distância de medição deve ser de pelo menos 1 000 m.

— sob condição de terem precisão comparável, podem igualmente utilizar-se para o ensaio métodos alternativos, como um banco de ensaios adequado.

6.6 **Reparações**

415) As oficinas devem poder descarregar dados do aparelho de controlo para a empresa de transportes pertinente.

416) Se um mau funcionamento do aparelho de controlo inviabilizar o descarregamento de dados previamente registados, mesmo após reparação efetuada por uma oficina homologada, esta última deve emitir, em nome da empresa de transportes, um certificado relativo à impossibilidade de descarregamento de dados. A oficina deve guardar, durante um período mínimo de dois anos, uma cópia de cada certificado emitido.

7 EMISSÃO DE CARTÕES

Os processos de emissão de cartões estabelecidos pelos Estados-Membros devem cumprir as seguintes condições:

417) O número de um cartão tacográfico, relativo à sua primeira emissão em nome de um requerente, deve ter um índice de série (eventual), um índice de substituição e um índice de renovação ajustado a «0».

418) Os números dos cartões tacográficos não pessoais emitidos em nome de um só organismo de controlo, de uma só oficina ou de uma só empresa de transportes devem ter os mesmos 13 primeiros algarismos, mas diferentes índices de série.

419) Um cartão tacográfico emitido em substituição de outro existente deve ter o mesmo número do cartão substituído, com exceção do índice de substituição, que é sucessivamente acrescido de uma unidade (segundo a ordem 0, …, 9, A, …, Z).

420) Um cartão tacográfico emitido em substituição de outro existente deve ter o mesmo prazo de validade do substituído.

421) Um cartão tacográfico emitido para renovação de outro existente deve ter o mesmo número do cartão renovado, com exceção do índice de substituição, que é ajustado a «0», e do índice de renovação, que é sucessivamente acrescido de uma unidade (segundo a ordem 0, …, 9, A, …, Z).

422) A troca de um cartão tacográfico existente, visando alterar dados administrativos, deve obedecer às regras da renovação se se processar dentro do mesmo Estado-Membro, ou às regras de uma primeira emissão se se processar noutro Estado-Membro.

423) Tratando-se de cartões de oficina ou de controlo, o espaço destinado ao «apelido do titular do cartão» deve ser preenchido com o nome da oficina ou organismo de controlo, ou com o nome do instalador ou do agente de controlo, caso os Estados-Membros assim o decidam.

▼B

424) Os Estados-Membros devem proceder ao intercâmbio eletrónico de dados, a fim de garantir que os cartões de condutor do tacógrafo que emitirem são únicos, em conformidade com o artigo 31.º do Regulamento (UE) n.º 165/2014.

8 HOMOLOGAÇÃO DE TIPO DOS APARELHOS DE CONTROLO E DOS CARTÕES TACOGRÁFICOS

8.1 **Aspetos gerais**

Na aceção do presente capítulo, por «aparelho de controlo» entende-se «o aparelho de controlo ou os seus componentes». Não é necessária homologação de tipo para o(s) cabo(s) que liga(m) o sensor de movimentos à VU, que liga(m) o módulo GNSS externo à VU ou que liga(m) o sistema de comunicação à distância à VU. O papel utilizado no aparelho de controlo é considerado um seu componente.

Qualquer fabricante pode solicitar a homologação de tipo do seu componente com qualquer tipo de sensor de movimentos, módulo GNSS externo e vice-versa, desde que cada componente esteja em conformidade com o prescrito no presente anexo. Em alternativa, os fabricantes podem também solicitar a homologação de tipo do aparelho de controlo.

425) Ao ser apresentado para homologação, o aparelho de controlo deve vir acompanhado de quaisquer dispositivos integrados adicionais.

426) A homologação de tipo do aparelho de controlo e dos cartões tacográficos deve incluir os ensaios de segurança associados, os ensaios de funcionalidade e os ensaios de interoperabilidade. Os resultados positivos de cada um destes ensaios devem constar de correspondentes certificados.

427) As autoridades responsáveis pela homologação de tipo nos Estados-Membros não podem emitir certificados de homologação de tipo se não lhes forem disponibilizados:

— um certificado de segurança

— um certificado de funcionalidade

— um certificado de interoperabilidade

relativos ao aparelho de controlo ou ao cartão tacográfico que são objeto do pedido de homologação de tipo.

428) Qualquer modificação no *software*, no equipamento informático ou na natureza dos materiais utilizados no fabrico do aparelho deve ser notificada à autoridade que concedeu a homologação de tipo do aparelho, antes de este entrar em utilização. Essa autoridade confirma ao fabricante a extensão da homologação de tipo ou pede uma atualização ou confirmação dos certificados de segurança, de funcionalidade e/ou de interoperabilidade.

429) Os procedimentos tendentes à atualização *in situ* do *software* aplicado ao aparelho de controlo devem ser homologados pela autoridade que concedeu a homologação de tipo do aparelho. A atualização do *software* não deve alterar nem apagar dados memorizados no aparelho de controlo e relativos às atividades dos condutores. A atualização do *software* só pode ser feita sob a responsabilidade do fabricante do aparelho.

430) As homologações de tipo das modificações de *software* destinadas a atualizar um aparelho de controlo com prévia homologação de tipo não podem ser recusadas se as modificações se aplicarem apenas a funções não especificadas no presente anexo. Na atualização de *software* de um aparelho de controlo pode ser excluída a introdução de novos conjuntos de carateres, se não for tecnicamente viável.

▼B

8.2 **Certificado de segurança**

431) O certificado de segurança é entregue em conformidade com o disposto no apêndice 10 do presente anexo. Os aparelhos de controlo a certificar são a unidade-veículo, o sensor de movimentos, o módulo GNSS externo e os cartões tacográficos.

432) Caso as autoridades de certificação de segurança se recusem, excecionalmente, a certificar novo equipamento por motivo de obsolescência dos mecanismos de segurança, a homologação de tipo deve continuar a ser concedida apenas nesta circunstância específica e excecional e se não existir solução alternativa que cumpra o regulamento.

433) Nesta circunstância, o Estado-Membro em causa deve, sem demora, informar a Comissão Europeia, a qual, no prazo de doze meses civis a contar da concessão da homologação de tipo, iniciará um procedimento para assegurar a restauração do nível de segurança original.

8.3 **Certificado de funcionalidade**

434) Os candidatos à homologação de tipo devem fornecer às autoridades nacionais competentes todo o material e documentação que estas requererem.

435) Os fabricantes devem fornecer, no prazo de um mês após a apresentação do pedido, as amostras pertinentes dos produtos candidatos a homologação de tipo, bem como a documentação correlata, que os laboratórios nomeados para executar os ensaios de funcionalidade solicitarem. Quaisquer custos resultantes destes pedidos serão assumidos pela entidade requerente. Os laboratórios devem tratar confidencialmente as informações comercialmente sensíveis.

436) Ao fabricante só pode ser concedido um certificado de funcionalidade depois de efetuados com êxito pelo menos os ensaios de funcionalidade especificados no apêndice 9.

437) A autoridade responsável pela homologação de tipo emite o certificado de funcionalidade, do qual constará, além do nome do beneficiário e da identificação do modelo, uma lista dos ensaios executados e dos respetivos resultados.

438) O certificado de funcionalidade de qualquer componente de um aparelho de controlo deve também indicar os números de homologação de todos os outros tipos de componentes de aparelhos de controlo compatíveis que tenham sido homologados e ensaiados para esta certificação.

439) O certificado de funcionalidade de qualquer componente de um aparelho de controlo deve também indicar a norma ISO ou CEN segundo a qual a interface funcional foi certificada.

8.4 **Certificado de interoperabilidade**

440) Os ensaios de interoperabilidade são executados por um laboratório, sob a autoridade e a responsabilidade da Comissão Europeia.

441) O laboratório regista, segundo a ordem cronológica de chegada, os pedidos de ensaio de interoperabilidade apresentados pelos fabricantes.

442) Os pedidos de ensaio só são oficialmente registados quando o laboratório estiver de posse dos seguintes elementos:

— conjunto completo de material e documentação, necessário para os ensaios de interoperabilidade em causa

▼B

— certificado de segurança correspondente

— certificado de funcionalidade correspondente.

A data de registo do pedido é comunicada ao fabricante.

443) Os ensaios de interoperabilidade de aparelhos de controlo ou de cartões tacográficos não podem ser realizados por laboratórios aos quais não tenha sido concedido certificado de segurança e certificado de funcionalidade, exceto nas circunstâncias excecionais referidas no requisito n.º 432.

444) O fabricante que apresenta um pedido de ensaio de interoperabilidade compromete-se a deixar ao laboratório responsável pelo ensaio o conjunto completo de material e documentação que forneceu para a execução do ensaio.

445) Em conformidade com o disposto no apêndice 9 do presente anexo, os ensaios de interoperabilidade são executados, respetivamente, com todos os tipos de aparelhos de controlo e de cartões tacográficos:

— cuja homologação de tipo é ainda válida ou

— cuja homologação de tipo está pendente e que têm certificado de interoperabilidade válido.

446) Os ensaios de interoperabilidade devem abranger todas as gerações de aparelhos de controlo ou cartões tacográficos ainda em utilização.

447) O certificado de interoperabilidade só pode ser passado pelo laboratório ao fabricante depois de executados com êxito todos os ensaios de interoperabilidade requeridos.

448) Se os ensaios de interoperabilidade não forem bem sucedidos relativamente a um ou mais aparelhos de controlo ou cartões tacográficos, o certificado de interoperabilidade não será emitido até o fabricante requerente efetuar as modificações necessárias e obter resultados positivos nos ensaios. O laboratório deve identificar a causa do problema com a ajuda dos fabricantes afetos à falha de interoperabilidade e procurar ajudar o fabricante requerente a encontrar uma solução técnica. No caso de o fabricante ter modificado o seu produto, compete-lhe confirmar junto das autoridades competentes a validade dos certificados de segurança e de funcionalidade.

449) O certificado de interoperabilidade tem uma validade de seis meses, sendo revogado no final deste período se o fabricante não receber o correspondente certificado de homologação de tipo. É transmitido pelo fabricante à autoridade responsável pela homologação de tipo no Estado-Membro emissor do certificado de funcionalidade.

450) Os elementos suscetíveis de originar falhas de interoperabilidade não podem ser utilizados para a obtenção de vantagens ou posições dominantes.

8.5 **Certificado de homologação**

451) A autoridade nacional competente pode emitir o certificado de homologação de tipo logo que disponha dos três certificados requeridos.

▼B

452) O certificado de homologação de tipo de qualquer componente de um aparelho de controlo deve também indicar os números de homologação de tipo de todos os outros aparelhos de controlo interoperáveis homologados.

453) No momento da entrega ao fabricante, o certificado de homologação de tipo é copiado pela autoridade competente para o laboratório responsável pelos ensaios de interoperabilidade.

454) O laboratório competente para os ensaios de interoperabilidade deve gerir um sítio público na Internet do qual constará uma lista atualizada dos modelos de aparelho de controlo ou de cartão tacográfico:

— relativamente aos quais tenham sido registados pedidos de ensaio de interoperabilidade

— que tenham recebido certificado de interoperabilidade (ainda que provisório)

— que tenham recebido certificado de homologação de tipo.

8.6 **Procedimento excecional: primeiros certificados de interoperabilidade para aparelhos de controlo e cartões tacográficos da segunda geração**

455) Durante o período de quatro meses após um conjunto de aparelho de controlo e cartões tacográficos da segunda geração (cartão de condutor, cartão de oficina, cartão de controlo e cartão de empresa) ter sido certificado pela primeira vez como interoperável, deve ser considerado provisório qualquer certificado de interoperabilidade (incluindo esse primeiro) emitido em resposta a pedidos registados ao longo do referido período.

456) Se, no final do referido período, todos os produtos em causa forem mutuamente interoperáveis, os correspondentes certificados de interoperabilidade tornam-se efetivos.

457) Se, ao longo do referido período, forem detetadas falhas de interoperabilidade, o laboratório responsável pelos ensaios de interoperabilidade identifica as causas dos problemas com a ajuda dos fabricantes envolvidos e convida-os a efetuarem as necessárias modificações.

458) Se, no final deste período, subsistirem problemas de interoperabilidade, o laboratório responsável pelos ensaios de interoperabilidade, com a colaboração dos fabricantes envolvidos e das autoridades responsáveis pela homologação de tipo que emitiram os correspondentes certificados de funcionalidade, deve determinar as causas dessas falhas e estabelecer as modificações a introduzir por cada um dos fabricantes envolvidos. A procura de soluções técnicas pode prolongar-se por um máximo de dois meses, após o que, se não for encontrada solução comum, a Comissão, depois de consultar o laboratório responsável pelos ensaios de interoperabilidade, decide qual ou quais os aparelhos de controlo e cartões tacográficos que devem receber certificado definitivo de interoperabilidade, com especificação dos motivos.

459) Os pedidos de ensaio de interoperabilidade, registados pelo laboratório entre o final do período de quatro meses depois de emitido o primeiro certificado provisório de interoperabilidade e a data da decisão da Comissão referida no requisito n.º 455, ficam em suspenso até estarem resolvidos os problemas iniciais de interoperabilidade. Os pedidos são então processados segundo a ordem cronológica do registo.

▼B

Apêndice 1

DICIONÁRIO DE DADOS

ÍNDICE

▼B

2.30. CardRenewalIndex

2.31. CardReplacementIndex

2.32. CardSignCertificate

2.33. CardSlotNumber

2.34. CardSlotsStatus

2.35. CardSlotsStatusRecordArray

2.36. CardStructureVersion

2.37. CardVehicleRecord

2.38. CardVehiclesUsed

2.39. CardVehicleUnitRecord

2.40. CardVehicleUnitsUsed

2.41. Certificado

2.42. CertificateContent

2.43. CertificateHolderAuthorisation

2.44. CertificateRequestID

2.45. CertificationAuthorityKID

2.46. CompanyActivityData

2.47. CompanyActivityType

2.48. CompanyCardApplicationIdentification

2.49. CompanyCardHolderIdentification

2.50. ControlCardApplicationIdentification

2.51. ControlCardControlActivityData

2.52. ControlCardHolderIdentification

2.53. ControlType

2.54. CurrentDateTime

2.55. CurrentDateTimeRecordArray

2.56. DailyPresenceCounter

2.57. Datef

2.58. DateOfDayDownloaded

2.59. DateOfDayDownloadedRecordArray

2.60. Distância

2.61. DriverCardApplicationIdentification

▼B

2.62. DriverCardHolderIdentification

2.63. DSRCSecurityData

2.64. EGFCertificate

2.65. EmbedderIcAssemblerId

2.66. EntryTypeDailyWorkPeriod

2.67. EquipmentType

2.68. EuropeanPublicKey

2.69. EventFaultRecordPurpose

2.70. EventFaultType

2.71. ExtendedSealIdentifier

2.72. ExtendedSerialNumber

2.73. FullCardNumber

2.74. FullCardNumberAndGeneration

2.75. Generation

2.76. GeoCoordinates

2.77. GNSSAccuracy

2.78. GNSSContinuousDriving

2.79. GNSSContinuousDrivingRecord

2.80. GNSSPlaceRecord

2.81. HighResOdometer

2.82. HighResTripDistance

2.83. HolderName

2.84. InternalGNSSReceiver

2.85. K-ConstantOfRecordingEquipment

2.86. KeyIdentifier

2.87. KMWCKey

2.88. Language

2.89. LastCardDownload

2.90. LinkCertificate

2.91. L-TyreCircumference

2.92. MAC

2.93. ManualInputFlag

2.94. ManufacturerCode

2.95. ManufacturerSpecificEventFaultData

2.96. MemberStateCertificate

▼B

2.97. MemberStateCertificateRecordArray

2.98. MemberStatePublicKey

2.99. Name

2.100. NationAlpha

2.101. NationNumeric

2.102. NoOfCalibrationRecords

2.103. NoOfCalibrationsSinceDownload

2.104. NoOfCardPlaceRecords

2.105. NoOfCardVehicleRecords

2.106. NoOfCardVehicleUnitRecords

2.107. NoOfCompanyActivityRecords

2.108. NoOfControlActivityRecords

2.109. NoOfEventsPerType

2.110. NoOfFaultsPerType

2.111. NoOfGNSSCDRecords

2.112. NoOfSpecificConditionRecords

2.113. OdometerShort

2.114. OdometerValueMidnight

2.115. OdometerValueMidnightRecordArray

2.116. OverspeedNumber

2.117. PlaceRecord

2.118. PreviousVehicleInfo

2.119. PublicKey

2.120. RecordType

2.121. RegionAlpha

2.122. RegionNumeric

2.123. RemoteCommunicationModuleSerialNumber

2.124. RSAKeyModulus

2.125. RSAKeyPrivateExponent

2.126. RSAKeyPublicExponent

2.127. RtmData

2.128. SealDataCard

▼B

2.129. SealDataVu

2.130. SealRecord

2.131. SensorApprovalNumber

2.132. SensorExternalGNSSApprovalNumber

2.133. SensorExternalGNSSCoupledRecord

2.134. SensorExternalGNSSIdentification

2.135. SensorExternalGNSSInstallation

2.136. SensorExternalGNSSOSIdentifier

2.137. SensorExternalGNSSSCIdentifier

2.138. SensorGNSSCouplingDate

2.139. SensorGNSSSerialNumber

2.140. SensorIdentification

2.141. SensorInstallation

2.142. SensorInstallationSecData

2.143. SensorOSIdentifier

2.144. SensorPaired

2.145. SensorPairedRecord

2.146. SensorPairingDate

2.147. SensorSCIdentifier

2.148. SensorSerialNumber

2.149. Signature

2.150. SignatureRecordArray

2.151. SimilarEventsNumber

2.152. SpecificConditionRecord

2.153. SpecificConditions

2.154. SpecificConditionType

2.155. Speed

2.156. SpeedAuthorised

2.157. SpeedAverage

2.158. SpeedMax

2.159. TachographPayload

2.160. TachographPayloadEncrypted

▼B

2.161. TDesSessionKey

2.162. TimeReal

2.163. TyreSize

2.164. VehicleIdentificationNumber

2.165. VehicleIdentificationNumberRecordArray

2.166. VehicleRegistrationIdentification

2.167. VehicleRegistrationNumber

2.168. VehicleRegistrationNumberRecordArray

2.169. VuAbility

2.170. VuActivityDailyData

2.171. VuActivityDailyRecordArray

2.172. VuApprovalNumber

2.173. VuCalibrationData

2.174. VuCalibrationRecord

2.175. VuCalibrationRecordArray

2.176. VuCardIWData

2.177. VuCardIWRecord

2.178. VuCardIWRecordArray

2.179. VuCardRecord

2.180. VuCardRecordArray

2.181. VuCertificate

2.182. VuCertificateRecordArray

2.183. VuCompanyLocksData

2.184. VuCompanyLocksRecord

2.185. VuCompanyLocksRecordArray

2.186. VuControlActivityData

2.187. VuControlActivityRecord

2.188. VuControlActivityRecordArray

▼B

2.189. VuDataBlockCounter

2.190. VuDetailedSpeedBlock

2.191. VuDetailedSpeedBlockRecordArray

2.192. VuDetailedSpeedData

2.193. VuDownloadablePeriod

2.194. VuDownloadablePeriodRecordArray

2.195. VuDownloadActivityData

2.196. VuDownloadActivityDataRecordArray

2.197. VuEventData

2.198. VuEventRecord

2.199. VuEventRecordArray

2.200. VuFaultData

2.201. VuFaultRecord

2.202. VuFaultRecordArray

2.203. VuGNSSCDRecord

2.204. VuGNSSCDRecordArray

2.205. VuIdentification

2.206. VuIdentificationRecordArray

2.207. VuITSConsentRecord

2.208. VuITSConsentRecordArray

2.209. VuManufacturerAddress

2.210. VuManufacturerName

2.211. VuManufacturingDate

2.212. VuOverSpeedingControlData

2.213. VuOverSpeedingControlDataRecordArray

2.214. VuOverSpeedingEventData

▼B

2.215. VuOverSpeedingEventRecord

2.216. VuOverSpeedingEventRecordArray

2.217. VuPartNumber

2.218. VuPlaceDailyWorkPeriodData

2.219. VuPlaceDailyWorkPeriodRecord

2.220. VuPlaceDailyWorkPeriodRecordArray

2.221. VuPrivateKey

2.222. VuPublicKey

2.223. VuSerialNumber

2.224. VuSoftInstallationDate

2.225. VuSoftwareIdentification

2.226. VuSoftwareVersion

2.227. VuSpecificConditionData

2.228. VuSpecificConditionRecordArray

2.229. VuTimeAdjustmentData

2.230. VuTimeAdjustmentGNSSRecord

2.231. VuTimeAdjustmentGNSSRecordArray

2.232. VuTimeAdjustmentRecord

2.233. VuTimeAdjustmentRecordArray

2.234. WorkshopCardApplicationIdentification

2.235. WorkshopCardCalibrationData

2.236. WorkshopCardCalibrationRecord

2.237. WorkshopCardHolderIdentification

2.238. WorkshopCardPIN

2.239. W-VehicleCharacteristicConstant

2.240. VuPowerSupplyInterruptionRecord

▼B

1. INTRODUÇÃO

O presente apêndice especifica os formatos, os elementos e as estruturas dos dados a utilizar no aparelho de controlo e nos cartões tacográficos.

1.1. **Metodologia na definição dos tipos de dados**

O presente apêndice utiliza a Abstract Syntax Notation One («notação de sintaxe abstrata um» ou ASN.1) para definir os tipos de dados, permitindo que dados simples e estruturados sejam definidos sem sintaxe específica de transferência (regra de codificação) dependente da aplicação e do ambiente.

As convenções ASN.1 para a nomeação do tipo obedecem à norma ISO/IEC 8824-1, o que implica:

— sempre que possível, o significado do tipo de dado está implícito nos nomes selecionados

— se um tipo de dado consistir numa composição de outros tipos de dados, o nome daquele tipo de dado será ainda uma sequência simples de carateres alfabéticos a começar por uma letra maiúscula, utilizando-se todavia outras maiúsculas no interior do nome a marcar as diversas significações

— os nomes dos tipos de dados estão em geral relacionados com o nome dos tipos de dados a partir dos quais são constituídos, com o equipamento no qual os dados são memorizados e com a função a eles relativa.

Se um tipo ASN.1 estiver já definido como parte de outra norma e for suscetível de utilização no aparelho de controlo, será definido no presente apêndice.

Tendo em conta os diversos tipos de regras de codificação, alguns tipos ASN.1 que constam do presente apêndice são restringidos por identificadores de intervalos (ou gamas) de valores. Na secção 3 e no apêndice 2 definem-se os identificadores de gamas de valores.

1.2. **Referências**

No presente apêndice, utilizam-se as seguintes referências:

ISO 639	Code for the representation of names of languages. First Edition: 1988.

▼B

ISO 3166	Codes for the representation of names of countries and their subdivisions — Part 1: Country codes, 2013
ISO 3779	Road vehicles — Vehicle identification number (VIN) — Content and structure. 2009
ISO/IEC 7816-5	Identification cards — Integrated circuit cards — Part 5: Registration of application providers. Second edition: 2004.
ISO/IEC 7816-6	Identification cards — Integrated circuit cards — Part 6: Interindustry data elements for interchange, 2004 + Technical Corrigendum 1: 2006
ISO/IEC 8824-1	Information technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation. 2008 + Technical Corrigendum 1: 2012 and Technical Corrigendum 2: 2014.
ISO/IEC 8825-2	Information technology — ASN.1 encoding rules: Specification of Packed Encoding Rules (PER). 2008.
ISO/IEC 8859-1	Information technology — 8 bit single-byte coded graphic character sets — Part 1: Latin alphabet No.1. First edition: 1998.
ISO/IEC 8859-7	Information technology — 8 bit single-byte coded graphic character sets — Part 7: Latin/Greek alphabet. 2003.
ISO 16844-3	Road vehicles — Tachograph systems — Motion Sensor Interface. 2004 + Technical Corrigendum 1: 2006..
TR-03110-3	BSI / ANSSI Technical Guideline TR-03110-3, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token — Part 3 Common Specifications, version 2.20, 3. February 2015

2. DEFINIÇÕES DOS TIPOS DE DADOS

Em todos os tipos de dados a seguir definidos, o valor por defeito relativo a um conteúdo «desconhecido» ou «não aplicável» consiste em preencher o elemento de dados com bytes ‘FF’.

Nas aplicações de geração 1 e geração 2 utilizam-se todos os tipos de dados, salvo indicação em contrário.

2.1. **ActivityChangeInfo**

Este tipo de dado permite codificar, numa palavra de dois bytes, uma situação de ranhura às 00h00 e/ou uma situação de condutor às 00h00 e/ou alterações na atividade e/ou alterações na situação da condução e/ou alterações na situação do cartão, quer para o condutor quer para o ajudante. Este tipo de dado está relacionado com os requisitos 105, 266, 291, 320, 321, 343 e 344 do anexo 1C.

```
ActivityChangeInfo ::= OCTET STRING (SIZE(2))
```

Valor atribuído — Alinhamento de octetos: ‘scpaatttttttttt’B (16 bits)

Para registos na memória de dados (ou situação da ranhura):

‘s’B	Ranhura:
	‘0’B: CONDUTOR,
	‘1’B: AJUDANTE,

▼B

‘c’B	Situação da condução:
	‘0’B: ÚNICO,
	‘1’B: TRIPULAÇÃO,
‘p’B	Situação do cartão de condutor (ou de oficina) na ranhura pertinente:
	‘0’B: INSERIDO, está inserido um cartão,
	‘1’B: NÃO INSERIDO, não está inserido nenhum cartão (ou foi retirado um),
‘aa’B	Atividade:
	‘00’B: PAUSA/DESCANSO,
	‘01’B: DISPONIBILIDADE,
	‘10’B: TRABALHO,
	‘11’B: CONDUÇÃO,
‘ttttttttttt’B	Momento da mudança: quantidade de minutos desde as 00h00 no dia em questão.

Para registos (e situação do condutor) no cartão de condutor (ou de oficina):

‘s’B	Ranhura (não pertinente quando ‘p’=1, exceto nota infra):
	‘0’B: CONDUTOR,
	‘1’B: AJUDANTE,
‘c’B	Situação da condução (caso ‘p’=0) ou
	Situação da atividade seguinte (caso ‘p’=1):
	‘0’B: ÚNICO,
	‘0’B: DESCONHECIDO
	‘1’B: TRIPULAÇÃO,
	‘1’B: CONHECIDO (= entrada manual)
‘p’B	Situação do cartão:
	‘0’B: INSERIDO, o cartão está inserido num aparelho de controlo,
	‘1’B: NÃO INSERIDO, o cartão não está inserido (ou foi retirado),
‘aa’B	Atividade (não pertinente quando ‘p’=1 e ‘c’=0, exceto nota infra):
	‘00’B: PAUSA/DESCANSO,
	‘01’B: DISPONIBILIDADE,
	‘10’B: TRABALHO,
	‘11’B: CONDUÇÃO,
‘ttttttttttt’B	Momento da mudança: quantidade de minutos desde as 00h00 no dia em questão.

▼B

Nota relativa ao caso «retirada do cartão»:

Quando o cartão é retirado:

— ‘s’ é pertinente e indica a ranhura da qual o cartão é retirado

— ‘c’ deve ser fixado em 0

— ‘p’ deve ser fixado em 1

— ‘aa’ deve codificar a atividade em curso, selecionada no momento.

Em resultado de uma entrada manual, os bits ‘c’ e ‘aa’ da palavra (memorizada num cartão) podem ser posteriormente reescritos por cima, refletindo a entrada.

2.2. **Endereço**

Um endereço.

```
Address ::= SEQUENCE {
   codePage                          INTEGER (0..255),
   address                           OCTET STRING (SIZE(35))
}
```

codePage especifica um conjunto de carateres definido no capítulo 4

address é um endereço codificado que utiliza o conjunto de carateres especificado.

2.3. **AESKey**

Geração 2:

Uma chave AES com o comprimento de 128, 192 ou 256 bits.

```
AESKey ::= CHOICE {
   aes128Key                         AES128Key,
   aes192Key                         AES192Key,
   aes256Key                         AES256Key
}
```

Valor atribuído: sem mais especificações.

2.4. **AES128Key**

Geração 2:

Uma chave AES128.

```
AES128Key ::= SEQUENCE {
   length                              INTEGER(0..255),
   aes128Key                           OCTET STRING (SIZE(16))
}
```

length indica o comprimento da chave AES128 em octetos.

aes128Key: chave AES com comprimento de 128 bits.

Valor atribuído:

O comprimento deve ter o valor 16.

▼B

2.5. **AES192Key**

Geração 2:

Uma chave AES192.

```
AES192Key ::= SEQUENCE {
   length                              INTEGER(0..255),
   aes192Key                           OCTET STRING (SIZE(24))
}
```

length indica o comprimento da chave AES192 em octetos.

aes192Key: chave AES com um comprimento de 192 bits.

Valor atribuído:

O comprimento deve ter o valor 24.

2.6. **AES256Key**

Geração 2:

Uma chave AES256.

```
AES256Key ::= SEQUENCE {
   length                              INTEGER(0..255),
   aes256Key                           OCTET STRING (SIZE(32))
}
```

length indica o comprimento da chave AES256 em octetos.

aes256Key: chave AES com 256 bits de comprimento.

Valor atribuído:

O comprimento deve ter o valor de 32.

2.7. **BCDString**

BCDString aplica-se na representação de Binary Code Decimal («código binário decimal» ou BCD). Este tipo de dado utiliza-se para representar um algarismo decimal num semiocteto (4 bits). BCDString baseia-se em «CharacterStringType» da norma ISO/IEC 8824-1.

```
BCDString ::= CHARACTER STRING (WITH COMPONENTS {
   identification ( WITH COMPONENTS {
   fixed PRESENT }) })
```

BCDString utiliza uma notação «hstring». O algarismo hexadecimal mais à esquerda deve ser o semiocteto mais significativo do primeiro octeto. Para produzir um múltiplo de octetos, inserem-se os necessários semioctetos de zeros à direita, a partir da posição de semiocteto mais à esquerda no primeiro octeto.

Algarismos autorizados: 0, 1, …, 9.

2.8. **CalibrationPurpose**

Código que explica por que foi registado um conjunto de parâmetros de calibração. Este tipo de dado está relacionado com os requisitos 097 e 098 do anexo 1B e com o requisito 119 do anexo 1C.

```
CalibrationPurpose ::= OCTET STRING (SIZE(1))
```

▼B

Valor atribuído:

Geração 1:

‘00’H	valor reservado
‘01’H	ativação: registo de parâmetros de calibração conhecidos, no momento da ativação da VU
‘02’H	primeira instalação: primeira calibração da VU depois de ativada
‘03’H	instalação: primeira calibração da VU no veículo atual
‘04’H	inspeção periódica.

Geração 2:

Utilizam-se os seguintes elementos de dados, além dos utilizados na geração 1:

‘05’H	introdução do VRN pela empresa
‘06’H	ajustamento do tempo sem calibração
‘07’H a ‘7F’H	RFU,
‘80’H a ‘FF’H	Específico do fabricante.

2.9. **CardActivityDailyRecord**

Informação memorizada num cartão e relativa às atividades de condutor num determinado dia. Este tipo de dado está relacionado com os requisitos 266, 291, 320 e 343 do anexo 1C.

```
CardActivityDailyRecord ::= SEQUENCE {
   activityPreviousRecordLength         INTEGER(0..CardActivityLengthRange),
   activityRecordLength                 INTEGER(0..CardActivityLengthRange),
   activityRecordDate                   TimeReal,
   activityDailyPresenceCounter         DailyPresenceCounter,
   activityDayDistance                  Distance,
   activityChangeInfo                   SET SIZE(1..1440) OF ActivityChangeInfo
}
```

activityPreviousRecordLength é o comprimento total, em bytes, do anterior registo diário. O valor máximo é dado pelo comprimento do OCTET STRING que contém estes registos (ver CardActivityLengthRange, apêndice 2, ponto 4). Se este registo for o registo diário mais antigo, o valor de activityPreviousRecordLength deve ser fixado em 0.

activityRecordLength é o comprimento total, em bytes, deste registo. O valor máximo é dado pelo comprimento do OCTET STRING que contém estes registos.

activityRecordDate é a data do registo.

▼B

activityDailyPresenceCounter é o contador de presenças diárias relativo ao cartão neste dia.

activityDayDistance é a distância total percorrida pelo veículo neste dia.

activityChangeInfo é o conjunto de dados ActivityChangeInfo relativos ao condutor neste dia. Pode conter, no máximo, 1 440 valores (uma mudança de atividade por minuto). Este conjunto inclui sempre a activityChangeInfo que codifica a situação do condutor às 00h00.

2.10. **CardActivityLengthRange**

Número de bytes num cartão de condutor ou de oficina, disponíveis para memorizar registos da atividade de condutor.

```
CardActivityLengthRange ::= INTEGER(0..2^16-1)
```

Valor atribuído: ver apêndice 2.

2.11. **CardApprovalNumber**

Número de homologação do tipo de cartão.

```
CardApprovalNumber ::= IA5String(SIZE(8))
```

Valor atribuído:

O número de homologação deve ser apresentado conforme publicação no respetivo sítio Web da Comissão Europeia, ou seja, incluindo eventuais hífenes. O número de homologação deve estar alinhado à esquerda.

2.12. **CardCertificate**

Geração 1:

Certificado da chave pública de um cartão.

```
CardCertificate ::= Certificate
```

2.13. **CardChipIdentification**

Informação memorizada num cartão e relativa à identificação do circuito integrado (IC) desse cartão (requisito 249 do anexo 1C). O icSerialNumber, juntamente com o icManufacturingReferences, identifica a pastilha do cartão de forma única. O icSerialNumber sozinho não identifica a pastilha do cartão de forma única.

```
CardChipIdentification ::= SEQUENCE {
   icSerialNumber                      OCTET STRING (SIZE(4)),
   icManufacturingReferences           OCTET STRING (SIZE(4))
}
```

icSerialNumber é o número de série do IC.

icManufacturingReferences é o identificador específico do fabricante do IC.

2.14. **CardConsecutiveIndex**

Um índice de série do cartão (definição h)).

```
CardConsecutiveIndex ::= IA5String(SIZE(1))
```

Valor atribuído: (ver anexo 1C, capítulo 7)

Ordem de acréscimo: ‘0, …, 9, A, …, Z, a, …, z’

▼B

2.15. **CardControlActivityDataRecord**

Informação memorizada num cartão de condutor ou de oficina e relativa ao último controlo a que o condutor tiver sido sujeito (requisitos 274, 299, 327 e 350 do anexo 1C).

```
CardControlActivityDataRecord ::= SEQUENCE {
   controlType                          ControlType,
   controlTime                          TimeReal,
   controlCardNumber                    FullCardNumber,
   controlVehicleRegistration           VehicleRegistrationIdentification,
   controlDownloadPeriodBegin           TimeReal,
   controlDownloadPeriodEnd             TimeReal
}
```

controlType é o tipo do controlo.

controlTime é a data e a hora do controlo.

controlCardNumber é o FullCardNumber do técnico que efetuou o controlo.

controlVehicleRegistration é o VRN e o Estado-Membro de matrícula do veículo no qual ocorreu o controlo.

controlDownloadPeriodBegin e **controlDownloadPeriodEnd** é o período descarregado (na eventualidade de descarregamento).

2.16. **CardCurrentUse**

Informação relativa à utilização efetiva do cartão (requisito 273, 298, 326 e 349 do anexo 1C).

```
CardCurrentUse ::= SEQUENCE {
   sessionOpenTime                      TimeReal,
   sessionOpenVehicle                   VehicleRegistrationIdentification
}
```

sessionOpenTime é o momento de inserção do cartão para a utilização em curso. Este elemento é fixado em 0 ao ser retirado o cartão.

sessionOpenVehicle é a identificação do veículo em utilização, fixada ao ser inserido o cartão. Este elemento é fixado em 0 ao ser retirado o cartão.

2.17. **CardDriverActivity**

Informação memorizada num cartão de condutor ou de oficina e relativa às atividades do condutor (requisitos 267, 268, 292, 293, 321 e 344 do anexo 1C).

```
CardDriverActivity ::= SEQUENCE {
   activityPointerOldestDayRecord       INTEGER(0.. CardActivityLengthRange-1),
   activityPointerNewestRecord          INTEGER(0.. CardActivityLengthRange-1),
   activityDailyRecords                 OCTET STRING
                                        (SIZE(CardActivityLengthRange))
}
```

activityPointerOldestDayRecord é a especificação do início do local de memorização (número de bytes desde o princípio da cadeia) do mais antigo registo diário completo na cadeia activityDailyRecords. O valor máximo é dado pelo comprimento da cadeia.

▼B

activityPointerNewestRecord é a especificação do início do local de memorização (número de bytes desde o princípio da cadeia) do mais recente registo diário na cadeia activityDailyRecords. O valor máximo é dado pelo comprimento da cadeia.

activityDailyRecords é o espaço disponível para memorizar os dados de atividade do condutor (estrutura de dados: CardActivityDailyRecord) para cada dia de calendário em que o cartão foi utilizado.

Valor atribuído: esta cadeia de octetos é ciclicamente preenchida com registos de CardActivityDailyRecord. Na primeira utilização, a memorização inicia-se no primeiro byte da cadeia. Cada novo registo é apenso ao final do precedente. Quando a cadeia está preenchida, a memorização prossegue no primeiro byte da cadeia, independentemente de haver descontinuidade dentro de um elemento de dado. Antes de se colocarem novos dados de atividade na cadeia (aumentando o atual activityDailyRecord ou colocando um novo activityDailyRecord) em substituição dos dados de atividade mais antigos, o activityPointerOldestDayRecord tem de ser atualizado, em reflexo da nova localização do mais antigo registo diário completo, e o activityPreviousRecordLength deste (novo) registo diário completo mais antigo deve ser reposto em 0.

2.18. **CardDrivingLicenceInformation**

Informação memorizada num cartão de condutor e relativa aos dados da carta de condução do titular do cartão (requisito 259 e 284 do anexo 1C).

```
CardDrivingLicenceInformation ::= SEQUENCE {
   drivingLicenceIssuingAuthority       Name,
   drivingLicenceIssuingNation          NationNumeric,
   drivingLicenceNumber                 IA5String(SIZE(16))
}
```

drivingLicenceIssuingAuthority é a autoridade responsável pela emissão da carta de condução.

drivingLicenceIssuingNation é a nacionalidade da autoridade que emite a carta de condução.

drivingLicenceNumber é o número da carta de condução.

2.19. **CardEventData**

Informação memorizada num cartão de condutor ou de oficina e relativa aos incidentes associados ao titular do cartão (requisitos 260, 285, 318 e 341 do anexo 1C).

```
CardEventData ::= SEQUENCE SIZE(6) OF {
   cardEventRecords                     SET SIZE(NoOfEventsPerType) OF
                                        CardEventRecord
}
```

CardEventData é uma sequência de registos cardEventRecords (com exceção dos registos relacionados com tentativas de violação da segurança, os quais são reunidos no último conjunto da sequência), por ordem crescente do valor de EventFaultType.

cardEventRecords é um conjunto de registos de incidentes de determinado tipo (ou categoria, no caso de incidentes relativos a tentativas de violação da segurança).

▼B

2.20. **CardEventRecord**

Informação memorizada num cartão de condutor ou de oficina e relativa a um incidente associado ao titular do cartão (requisitos 261, 286, 318 e 341 do anexo 1C).

```
CardEventRecord ::= SEQUENCE {
   eventType                          EventFaultType,
   eventBeginTime                     TimeReal,
   eventEndTime                       TimeReal,
   eventVehicleRegistration           VehicleRegistrationIdentification
}
```

eventType é o tipo de incidente.

eventBeginTime é a data e a hora de início do incidente.

eventEndTime é a data e a hora de cessação do incidente.

eventVehicleRegistration é o VRN e o Estado-Membro de matrícula do veículo no qual ocorreu o incidente.

2.21. **CardFaultData**

Informação memorizada num cartão de condutor ou de oficina e relativa às falhas associadas ao titular do cartão (requisitos 263, 288, 318 e 341 do anexo 1C).

```
CardFaultData ::= SEQUENCE SIZE(2) OF {
   cardFaultRecords                   SET SIZE(NoOfFaultsPerType) OF
                                      CardFaultRecord
}
```

CardFaultData: sequência formada pelo conjunto de registos de falhas do aparelho de controlo ao qual se segue o conjunto de registos de falhas do cartão.

cardFaultRecords: conjunto de registos de falhas de determinada categoria (falhas do aparelho de controlo ou do cartão).

2.22. **CardFaultRecord**

Informação memorizada num cartão de condutor ou de oficina e relativa a uma falha associada ao titular do cartão (requisitos 264, 289, 318 e 341 do anexo 1C).

```
CardFaultRecord ::= SEQUENCE {
   faultType                          EventFaultType,
   faultBeginTime                     TimeReal,
   faultEndTime                       TimeReal,
   faultVehicleRegistration           VehicleRegistrationIdentification
}
```

faultType é o tipo da falha.

faultBeginTime é a data e a hora de início da falha.

faultEndTime é a data e a hora de cessação da falha.

faultVehicleRegistration é o VRN e o Estado-Membro de matrícula do veículo no qual ocorreu a falha.

▼B

2.23. **CardIccIdentification**

Informação memorizada num cartão e relativa à identificação do circuito integrado (IC) (requisito 248 do anexo 1C).

```
CardIccIdentification ::= SEQUENCE {
   clockStop                          OCTET STRING (SIZE(1)),
   cardExtendedSerialNumber           ExtendedSerialNumber,
   cardApprovalNumber                 CardApprovalNumber,
   cardPersonaliserID                 ManufacturerCode,
   embedderIcAssemblerId              EmbedderIcAssemblerId,
   icIdentifier                       OCTET STRING (SIZE(2))
}
```

clockStop é o modo Clockstop (relógio parado), cf. definição no apêndice 2.

cardExtendedSerialNumber é o número de série único do cartão IC conforme especificado pelo tipo de dados ExtendedSerialNumber.

cardApprovalNumber é o número de homologação de tipo do cartão.

cardPersonaliserID é a identificação personalizada do cartão (ID) codificada como ManufacturerCode.

embedderIcAssemblerId fornece informações acerca do fabricante/ /montador do IC.

icIdentifier é o identificador do IC no cartão e do seu fabricante (cf. definição na norma ISO/IEC 7816-6).

2.24. **CardIdentification**

Informação memorizada num cartão e relativa à sua identificação (requisitos 255, 280, 310, 333, 359, 365, 371 e 377 do anexo 1C).

```
CardIdentification ::= SEQUENCE {
   cardIssuingMemberState             NationNumeric,
   cardNumber                         CardNumber,
   cardIssuingAuthorityName           Name,
   cardIssueDate                      TimeReal,
   cardValidityBegin                  TimeReal,
   cardExpiryDate                     TimeReal
}
```

cardIssuingMemberState é o código do Estado-Membro que emite o cartão.

cardNumber é o número do cartão.

cardIssuingAuthorityName é a designação da autoridade que emite o cartão.

cardIssueDate é a data de emissão do cartão ao atual titular.

cardValidityBegin é a data de início da validade do cartão.

cardExpiryDate é a data-limite da validade do cartão.

▼B

2.25. **CardMACertificate**

Geração 2:

Certificado da chave pública do cartão para autenticação mútua com uma VU. A estrutura deste certificado é especificada no apêndice 11.

```
CardMACertificate ::= Certificate
```

2.26. **CardNumber**

Um número de cartão, em conformidade com a definição g).

```
CardNumber ::= CHOICE {
   SEQUENCE {
      driverIdentification              IA5String(SIZE(14)),
      cardReplacementIndex              CardReplacementIndex,
      cardRenewalIndex                  CardRenewalIndex
   },
   SEQUENCE {
      ownerIdentification               IA5String(SIZE(13)),
      cardConsecutiveIndex              CardConsecutiveIndex,
      cardReplacementIndex              CardReplacementIndex,
      cardRenewalIndex                  CardRenewalIndex
   }
}
```

driverIdentification é a identificação única de um condutor num Estado-Membro.

ownerIdentification é a identificação única de uma empresa, de uma oficina ou de um organismo de controlo num Estado-Membro.

cardConsecutiveIndex é o índice de série do cartão.

cardReplacementIndex é o índice de substituição do cartão.

cardRenewalIndex é o índice de renovação do cartão.

A primeira sequência da escolha é adequada para codificar o número de cartão de um condutor; a segunda é adequada para codificar os números de cartão de uma oficina, de um organismo de controlo ou de uma empresa.

2.27. **CardPlaceDailyWorkPeriod**

Informação memorizada num cartão de condutor ou de oficina e relativa aos locais onde se iniciam e/ou terminam os períodos de trabalho diário (requisitos 272, 297, 325 e 348 do anexo 1C).

```
CardPlaceDailyWorkPeriod ::= SEQUENCE {
   placePointerNewestRecord    INTEGER(0 .. NoOfCardPlaceRecords-1),
   placeRecords                SET SIZE(NoOfCardPlaceRecords) OF PlaceRecord
}
```

placePointerNewestRecord é o índice do último registo atualizado do local.

Valor atribuído: o número correspondente ao numerador do registo do local, a começar por ‘0’ na primeira ocorrência dos registos do local na estrutura.

placeRecords é o conjunto dos registos que contêm informação acerca dos locais introduzidos.

▼B

2.28. **CardPrivateKey**

Geração 1:

A chave privada de um cartão.

```
CardPrivateKey ::= RSAKeyPrivateExponent
```

2.29. **CardPublicKey**

A chave pública de um cartão.

```
CardPublicKey ::= PublicKey
```

2.30. **CardRenewalIndex**

O índice de renovação de um cartão, conforme definição i).

```
CardRenewalIndex ::= IA5String(SIZE(1))
```

Valor atribuído: (ver capítulo VII do presente anexo).

‘0’ Primeira emissão.

Ordem de acréscimo: ‘0, …, 9, A, …, Z’

2.31. **CardReplacementIndex**

O índice de substituição de um cartão, conforme definição j).

```
CardReplacementIndex ::= IA5String(SIZE(1))
```

Valor atribuído: (ver capítulo VII do presente anexo).

‘0’ Cartão original.

Ordem de acréscimo: ‘0, …, 9, A, …, Z’

2.32. **CardSignCertificate**

Geração 2:

Certificado da chave pública do cartão para assinatura. A estrutura deste certificado é especificada no apêndice 11.

```
CardSignCertificate ::= Certificate
```

2.33. **CardSlotNumber**

Código que distingue as duas ranhuras de uma unidade-veículo.

```
CardSlotNumber ::= INTEGER {
   driverSlot                          (0),
   co-driverSlot                       (1)
}
```

Valor atribuído: sem mais especificações.

2.34. **CardSlotsStatus**

Código que indica o tipo dos cartões inseridos nas duas ranhuras da unidade-veículo.

```
CardSlotsStatus ::= OCTET STRING (SIZE(1))
```

▼B

Valor atribuído — Alinhamento de octetos: ‘ccccdddd’B

‘cccc’B Identificação do tipo de cartão inserido na ranhura do ajudante

‘dddd’B Identificação do tipo de cartão inserido na ranhura do condutor

com os seguintes códigos de identificação:

‘0000’B nenhum cartão inserido

‘0001’B inserido um cartão de condutor

‘0010’B inserido um cartão de oficina

‘0011’B inserido um cartão de controlo

‘0100’B inserido um cartão de empresa.

2.35. **CardSlotsStatusRecordArray**

Geração 2:

O CardSlotsStatus, mais metadados utilizados no protocolo de descarregamento.

```
CardSlotsStatusRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF CardSlotsStatus
}
```

recordType indica o tipo de registo (CardSlotsStatus). **Valor atribuído**: ver RecordType

recordSize: tamanho do CardSlotsStatus, em bytes.

noOfRecords: número de registos nos registos definidos.

records: conjunto de registos CardSlotsStatus.

2.36. **CardStructureVersion**

Código que indica a versão da estrutura aplicada num cartão tacográfico.

```
CardStructureVersion ::= OCTET STRING (SIZE(2))
```

Valor atribuído: ‘aabb’H:

‘aa’H Índice para alterações da estrutura.

‘00’H para aplicações da geração 1

‘01’H para aplicações da geração 2

‘bb’H Índice para alterações relativas à utilização dos elementos de dados definidos para a estrutura dada pelo byte elevado.

‘00’H para esta versão das aplicações da geração 1

‘00’H para esta versão das aplicações da geração 2

▼B

2.37. **CardVehicleRecord**

Informação memorizada num cartão de condutor ou de oficina e relativa a um período de utilização de um veículo durante um dia (requisitos 269, 294, 322 e 345 do anexo 1C).

Geração 1:

```
CardVehicleRecord ::= SEQUENCE {
   vehicleOdometerBegin                    OdometerShort,
   vehicleOdometerEnd                      OdometerShort,
   vehicleFirstUse                         TimeReal,
   vehicleLastUse                          TimeReal,
   vehicleRegistration                     VehicleRegistrationIdentification,
   vuDataBlockCounter                      VuDataBlockCounter
}
```

vehicleOdometerBegin é o valor do conta-quilómetros do veículo no início do período da sua utilização.

vehicleOdometerEnd é o valor do conta-quilómetros do veículo no final do período da sua utilização.

vehicleFirstUse é a data e a hora do início do período de utilização do veículo.

vehicleLastUse é a data e a hora do final do período de utilização do veículo.

vehicleRegistration é o VRN (número de matrícula) e o Estado-Membro de matrícula do veículo.

vuDataBlockCounter é o valor exibido pelo vuDataBlockCounter (contador do bloco de dados da VU) quando da última extração do período de utilização do veículo.

Geração 2:

```
CardVehicleRecord ::= SEQUENCE {
   vehicleOdometerBegin                    OdometerShort,
   vehicleOdometerEnd                      OdometerShort,
   vehicleFirstUse                         TimeReal,
   vehicleLastUse                          TimeReal,
   vehicleRegistration                     VehicleRegistrationIdentification,
   vuDataBlockCounter                      VuDataBlockCounter,
   vehicleIdentificationNumber             VehicleIdentificationNumber
}
```

Utilizam-se os seguintes elementos de dados, além dos utilizados na geração 1:

VehicleIdentificationNumber é o número de identificação do veículo e diz respeito ao veículo como um todo.

2.38. **CardVehiclesUsed**

Informação memorizada num cartão de condutor ou de oficina e relativa aos veículos utilizados pelo titular do cartão (requisitos 270, 295, 323 e 346 do anexo 1C).

```
CardVehiclesUsed := SEQUENCE {
   vehiclePointerNewestRecord          INTEGER(0..NoOfCardVehicleRecords-1),
   cardVehicleRecords                  SET SIZE(NoOfCardVehicleRecords) OF
                                       CardVehicleRecord
}
```

vehiclePointerNewestRecord é o índice do último registo atualizado do veículo.

▼B

Valor atribuído: o número correspondente ao numerador do registo do veículo, a começar por '0' na primeira ocorrência dos registos do veículo na estrutura.

cardVehicleRecords é o conjunto dos registos que contêm informação acerca dos veículos utilizados.

2.39. **CardVehicleUnitRecord**

Geração 2:

Informação memorizada num cartão de condutor ou de oficina e relativa a uma unidade-veículo que foi utilizada (requisitos 303 e 351 do anexo 1C).

```
CardVehicleUnitRecord ::= SEQUENCE {
   timeStamp                              TimeReal,
   manufacturerCode                       ManufacturerCode,
   deviceID                               INTEGER(0..255),
   vuSoftwareVersion                      VuSoftwareVersion
}
```

timeStamp é o início do período de utilização da unidade-veículo (ou seja, a primeira inserção do cartão na unidade-veículo, relativa ao período).

manufacturerCode identifica o fabricante da unidade-veículo.

deviceID identifica o tipo de unidade-veículo de um fabricante. O valor é específico do fabricante.

vuSoftwareVersion é o número da versão do *software* da unidade-veículo.

2.40. **CardVehicleUnitsUsed**

Geração 2:

Informação memorizada num cartão de condutor ou de oficina e relativa às unidades-veículos utilizadas pelo titular do cartão (requisitos 306 e 352 do anexo 1C).

```
CardVehicleUnitsUsed := SEQUENCE {
   vehicleUnitPointerNewestRecord       INTEGER(0..NoOfCardVehicleUnitRecords-1),
   cardVehicleUnitRecords               SET SIZE(NoOfCardVehicleUnitRecords) OF
                                        CardVehicleUnitRecord
}
```

vehicleUnitPointerNewestRecord é o índice do último registo atualizado da unidade-veículo.

Valor atribuído: o número correspondente ao numerador do registo da unidade-veículo, a começar por '0' na primeira ocorrência dos registos da unidade-veículo na estrutura.

cardVehicleUnitRecords é o conjunto de registos que contêm informação acerca das unidades-veículos utilizadas.

2.41. **Certificado**

O certificado de uma chave pública emitida por uma autoridade de certificação.

Geração 1:

```
Certificate ::= OCTET STRING (SIZE(194))
```

▼B

Valor atribuído: assinatura digital com recuperação parcial de um CertificateContent (conteúdo do certificado) em conformidade com os mecanismos comuns de segurança (apêndice 11): Assinatura (128 bytes) || Alerta de chave pública (58 bytes) || Referência da autoridade de certificação (8 bytes).

Geração 2:

```
Certificate ::= OCTET STRING (SIZE(204..341))
```

Valor atribuído: ver apêndice 11

2.42. **CertificateContent**

Geração 1:

O conteúdo (claro) do certificado de uma chave pública, em conformidade com os mecanismos comuns de segurança (apêndice 11).

```
CertificateContent ::= SEQUENCE {
   certificateProfileIdentifier          INTEGER(0..255),
   certificationAuthorityReference       KeyIdentifier,
   certificateHolderAuthorisation        CertificateHolderAuthorisation,
   certificateEndOfValidity              TimeReal,
   certificateHolderReference            KeyIdentifier,
   publicKey                             PublicKey
}
```

certificateProfileIdentifier é a versão do certificado correspondente.

Valor atribuído: '01h' para esta versão.

certificationAuthorityReference identifica a autoridade de certificação que emite o certificado. Referencia também a chave pública dessa autoridade.

certificateHolderAuthorisation identifica os direitos do titular do certificado.

certificateEndOfValidity é a data-limite administrativa de validade do certificado.

certificateHolderReference identifica o titular do certificado. Referencia também a chave pública do titular.

publicKey é a chave pública certificada por este certificado.

2.43. **CertificateHolderAuthorisation**

Identificação dos direitos do titular de um certificado.

```
CertificateHolderAuthorisation ::= SEQUENCE {
   tachographApplicationID              OCTET STRING(SIZE(6))
   equipmentType                        EquipmentType
}
```

Geração 1:

tachographApplicationID é o identificador de aplicação da aplicação tacográfica.

Valor atribuído: 'FFh' '54h' '41h' '43h' '48h' '4Fh'. Este AID é um identificador de aplicação não registada de proprietário, em conformidade com a norma ISO/IEC 7816-5.

equipmentType é a identificação do tipo de equipamento ao qual se refere o certificado.

Valor atribuído: em conformidade com o tipo de dado EquipmentType: **0** se se tratar do certificado de um Estado-Membro.

▼B

Geração 2:

tachographApplicationID indica os 6 bytes mais significativos do identificador de aplicação (AID) do cartão tacográfico de geração 2. O AID destinado à aplicação do cartão tacográfico é definido no capítulo 6.2.

Valor atribuído: 'FF 53 4D 52 44 54'

equipmentType: identificação do tipo de equipamento, tal como especificado para a geração 2, ao qual se refere o certificado.

Valor atribuído: em conformidade com o tipo de dado EquipmentType.

2.44. **CertificateRequestID**

Identificação única de um pedido de certificado. Pode igualmente utilizar-se como identificador da chave pública de uma unidade-veículo se, no momento da geração do certificado, não se conhecer o número de série da unidade-veículo à qual a chave se destina.

```
CertificateRequestID ::= SEQUENCE{
   requestSerialNumber                  INTEGER(0..2^32-1),
   requestMonthYear                     BCDString(SIZE(2)),
   crIdentifier                         OCTET STRING(SIZE(1)),
   manufacturerCode                     ManufacturerCode
}
```

requestSerialNumber é um número de série do pedido de certificado, único para o fabricante e para o mês *infra*.

requestMonthYear é a identificação do mês e do ano do pedido de certificado.

Valor atribuído: codificação BCD de Month (mês, com dois algarismos) e de Year (ano, com os dois últimos algarismos).

crIdentifier: é um identificador que estabelece a distinção entre um pedido de certificado e um número de série alargado.

Valor atribuído: 'FFh'.

manufacturerCode: é o código numérico do fabricante que pede o certificado.

2.45. **CertificationAuthorityKID**

Identificador da chave pública de uma autoridade de certificação (um Estado-Membro ou a autoridade europeia de certificação).

```
CertificationAuthorityKID ::= SEQUENCE{
   nationNumeric                        NationNumeric,
   nationAlpha                          NationAlpha,
   keySerialNumber                      INTEGER(0..255),
   additionalInfo                       OCTET STRING(SIZE(2)),
   caIdentifier                         OCTET STRING(SIZE(1))
}
```

nationNumeric é o código numérico da autoridade de certificação nacional.

nationAlpha é o código alfanumérico da autoridade de certificação nacional.

▼B

keySerialNumber é um número de série que distingue as diferentes chaves da autoridade de certificação, caso sejam alteradas.

additionalInfo é um campo de dois bytes para codificação adicional (específico da autoridade de certificação).

caIdentifier é um identificador que serve para distinguir um identificador de chave da autoridade de certificação dos outros identificadores de chave.

Valor atribuído: '01h'.

2.46. **CompanyActivityData**

Informação memorizada num cartão de empresa e relativa às atividades executadas com o cartão (requisitos 373 e 379 do anexo 1C).

```
CompanyActivityData ::= SEQUENCE {
   companyPointerNewestRecord        INTEGER(0..NoOfCompanyActivityRecords-1),
   companyActivityRecords            SET SIZE(NoOfCompanyActivityRecords) OF
    companyActivityRecord             SEQUENCE {
     companyActivityType               CompanyActivityType,
     companyActivityTime               TimeReal,
     cardNumberInformation             FullCardNumber,
     vehicleRegistrationInformation    VehicleRegistrationIdentification,
     downloadPeriodBegin               TimeReal,
     downloadPeriodEnd                 TimeReal
    }
}
```

companyPointerNewestRecord é o índice do último companyActivityRecord atualizado.

Valor atribuído: o número correspondente ao numerador do registo da atividade da empresa, a começar por '0' na primeira ocorrência dos registos da atividade da empresa na estrutura.

companyActivityRecords é o conjunto de todos os registos de atividade da empresa.

companyActivityRecord é a sequência de informação relativa à atividade da empresa.

companyActivityType é o tipo em que se integra a atividade da empresa.

companyActivityTime é a data e a hora da atividade da empresa.

cardNumberInformation é o número e o Estado-Membro emissor do cartão eventualmente descarregado.

vehicleRegistrationInformation é o VRN e o Estado-Membro de matrícula do veículo descarregado, bloqueado ou desbloqueado.

downloadPeriodBegin e **downloadPeriodEnd** é o período eventualmente descarregado da VU.

2.47. **CompanyActivityType**

Código que indica uma atividade executada por uma empresa que utiliza o respetivo cartão.

```
CompanyActivityType ::= INTEGER {
   card downloading                  (1),
   VU downloading                    (2),
   VU lock-in                        (3),
   VU lock-out                       (4)
}
```

▼B

2.48. **CompanyCardApplicationIdentification**

Informação memorizada num cartão de empresa e relativa à identificação da aplicação do cartão (requisitos 369 e 375 do anexo 1C).

```
CompanyCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfCompanyActivityRecords          NoOfCompanyActivityRecords
}
```

typeOfTachographCardId especifica o tipo de cartão aplicado.

cardStructureVersion especifica a versão da estrutura aplicada no cartão.

noOfCompanyActivityRecords é o número de registos de atividade da empresa que o cartão pode memorizar.

2.49. **CompanyCardHolderIdentification**

Informação memorizada num cartão de empresa e relativa à identificação do seu titular (requisitos 372 e 378 do anexo 1C).

```
CompanyCardHolderIdentification ::= SEQUENCE {
   companyName                         Name,
   companyAddress                      Address,
   cardHolderPreferredLanguage         Language
}
```

companyName é o nome da empresa titular.

companyAddress é o endereço da empresa titular.

cardHolderPreferredLanguage é o idioma preferencial do titular do cartão.

2.50. **ControlCardApplicationIdentification**

Informação memorizada num cartão de controlo e relativa à identificação da aplicação do cartão (requisitos 357 e 363 do anexo 1C).

```
ControlCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfControlActivityRecords          NoOfControlActivityRecords
}
```

typeOfTachographCardId especifica o tipo de cartão aplicado.

cardStructureVersion especifica a versão da estrutura que é aplicada no cartão.

noOfControlActivityRecords é o número de registos de atividade de controlo que o cartão pode memorizar.

▼B

2.51. **ControlCardControlActivityData**

Informação memorizada num cartão de controlo e relativa à atividade de controlo executada com o cartão (requisitos 361 e 367 do anexo 1C).

```
ControlCardControlActivityData ::= SEQUENCE {
   controlPointerNewestRecord        INTEGER(0.. NoOfControlActivityRecords-1),
   controlActivityRecords            SET SIZE(NoOfControlActivityRecords) OF
    controlActivityRecord             SEQUENCE {
      controlType                      ControlType,
      controlTime                      TimeReal,
      controlledCardNumber             FullCardNumber,
      controlledVehicleRegistration    VehicleRegistrationIdentification,
      controlDownloadPeriodBegin       TimeReal,
      controlDownloadPeriodEnd         TimeReal
    }
}
```

controlPointerNewestRecord é o índice do último registo atualizado da atividade de controlo.

Valor atribuído é o número correspondente ao numerador do registo da atividade de controlo, a começar por '0' na primeira ocorrência dos registos da atividade de controlo na estrutura.

controlActivityRecords é o conjunto de todos os registos de atividade de controlo.

controlActivityRecord é a sequência de informação relativa a um controlo.

controlType é o tipo do controlo.

controlTime é a data e a hora do controlo.

controlledCardNumber é o número e o Estado-Membro emissor do cartão controlado.

controlledVehicleRegistration é o VRN e o Estado-Membro de matrícula do veículo no qual o controlo foi efetuado.

controlDownloadPeriodBegin e **controlDownloadPeriodEnd** é o período descarregado.

2.52. **ControlCardHolderIdentification**

Informação memorizada num cartão de controlo e relativa à identificação do titular do cartão (requisitos 360 e 366 do anexo 1C).

```
ControlCardHolderIdentification ::= SEQUENCE {
   controlBodyName                    Name,
   controlBodyAddress                 Address,
   cardHolderName                     HolderName,
   cardHolderPreferredLanguage        Language
}
```

controlBodyName é o nome do organismo de controlo do titular do cartão.

controlBodyAddress é o endereço do organismo de controlo do titular do cartão.

cardHolderName é o apelido e o nome próprio do titular do cartão de controlo.

▼B

cardHolderPreferredLanguage é o idioma preferencial do titular do cartão.

2.53. **ControlType**

Código que indica as atividades executadas durante um controlo. Este tipo de dado está relacionado com os requisitos 126, 274, 299, 327 e 350 do anexo 1C.

```
ControlType ::= OCTET STRING (SIZE(1))
```

Geração 1:

Valor atribuído — Alinhamento de octetos: 'cvpdxxxx'B (8 bits)

'c'B descarregamento do cartão:

'0'B: cartão não descarregado durante esta atividade de controlo

'1'B: cartão descarregado durante esta atividade de controlo

'v'B descarregamento da VU:

'0'B: VU não descarregada durante esta atividade de controlo

'1'B: VU descarregada durante esta atividade de controlo

'p'B impressão:

'0'B: não efetuada impressão durante esta atividade de controlo

'1'B: efetuada impressão durante esta atividade de controlo

'd'B visualização:

'0'B: não utilizada visualização durante esta atividade de controlo

'1'B: utilizada visualização durante esta atividade de controlo

'xxxx'B Não utilizada.

Geração 2:

Valor atribuído — Alinhamento de octetos: 'cvpdexxx'B (8 bits)

'c'B descarregamento do cartão:

'0'B: cartão não descarregado durante esta atividade de controlo

'1'B: cartão descarregado durante esta atividade de controlo

'v'B descarregamento da VU:

'0'B: VU não descarregada durante esta atividade de controlo

'1'B: VU descarregada durante esta atividade de controlo

'p'B impressão:

'0'B: não efetuada impressão durante esta atividade de controlo

'1'B: efetuada impressão durante esta atividade de controlo

▼B

‘d’B	visualização:
	‘0’B: não utilizada visualização durante esta atividade de controlo
	‘1’B: utilizada visualização durante esta atividade de controlo
‘e’B	Controlo de calibração de estrada:
	‘0’B: parâmetros de calibração não verificados durante esta atividade de controlo
	‘1’B: parâmetros de calibração verificados durante esta atividade de controlo
‘xxx’B	RFU.

2.54. **CurrentDateTime**

Data e hora atuais do aparelho de controlo.

```
CurrentDateTime ::= TimeReal
```

Valor atribuído: sem mais especificações.

2.55. **CurrentDateTimeRecordArray**

Geração 2:

Data e hora atuais, mais metadados utilizados no protocolo de descarregamento.

```
CurrentDateTimeRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF CurrentDateTime
}
```

recordType indica o tipo de registo (CurrentDateTime). **Valor atribuído**: ver RecordType

recordSize: tamanho do CurrentDateTime, em bytes.

noOfRecords: número de registos nos registos definidos.

records: conjunto de registos atuais da data e da hora.

2.56. **DailyPresenceCounter**

Contador, memorizado num cartão de condutor ou de oficina, que vai sofrendo acréscimos unitários por cada dia em que o cartão tenha estado inserido numa VU. Este tipo de dado está relacionado com os requisitos 266, 299, 320 e 343 do anexo 1C.

```
DailyPresenceCounter ::= BCDString(SIZE(2))
```

Valor atribuído: número consecutivo com o valor máximo de 9 999, a recomeçar em 0. No momento da primeira emissão do cartão, o número é fixado em 0.

▼B

2.57. **Datef**

Data expressa num formato numérico que pode ser impresso de imediato.

```
Datef ::= SEQUENCE {
   year        BCDString(SIZE(2)),
   month       BCDString(SIZE(1)),
   day         BCDString(SIZE(1))
}
```

Valor atribuído:

aaaa	Ano
mm	Mês
dd	Dia
‘00000000’H	não indica explicitamente qualquer data.

2.58. **DateOfDayDownloaded**

Geração 2:

Data e hora do descarregamento.

```
DateOfDayDownloaded ::= TimeReal
```

Valor atribuído: sem mais especificações.

2.59. **DateOfDayDownloadedRecordArray**

Geração 2:

Data e hora do descarregamento, mais metadados utilizados no protocolo de descarregamento.

```
DateofDayDownloadedRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       DateOfDayDownloaded
}
```

recordType indica o tipo de registo (DateOfDayDownloaded). **Valor atribuído**: ver RecordType

recordSize: tamanho do CurrentDateTime, em bytes.

noOfRecords: número de registos nos registos definidos.

records: conjunto de data e hora dos registos descarregados.

2.60. **Distância**

Uma distância percorrida (resulta do cálculo da diferença entre dois valores do conta-quilómetros do veículo, em quilómetros).

```
Distance ::= INTEGER(0..2^16-1)
```

Valor atribuído: Binário sem sinal. Valor em km no intervalo operacional de 0 a 9 999 km.

2.61. **DriverCardApplicationIdentification**

Informação memorizada num cartão de condutor e relativa à identificação da aplicação do cartão (requisitos 253 e 278 do anexo 1C).

▼B

Geração 1:

```
DriverCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfEventsPerType                   NoOfEventsPerType,
   noOfFaultsPerType                   NoOfFaultsPerType,
   activityStructureLength             CardActivityLengthRange,
   noOfCardVehicleRecords              NoOfCardVehicleRecords,
   noOfCardPlaceRecords                NoOfCardPlaceRecords
}
```

typeOfTachographCardId especifica o tipo de cartão aplicado.

cardStructureVersion especifica a versão da estrutura aplicada no cartão.

noOfEventsPerType: número de incidentes, por tipo, que o cartão pode registar.

noOfFaultsPerType: número de falhas, por tipo, que o cartão pode registar.

activityStructureLength indica o número de bytes disponíveis para memorizar registos de atividade.

noOfCardVehicleRecords: número de registos de veículo que o cartão pode conter.

noOfCardPlaceRecords: número de locais que o cartão pode registar.

Geração 2:

```
DriverCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   noOfEventsPerType                   NoOfEventsPerType,
   noOfFaultsPerType                   NoOfFaultsPerType,
   activityStructureLength             CardActivityLengthRange,
   noOfCardVehicleRecords              NoOfCardVehicleRecords,
   noOfCardPlaceRecords                NoOfCardPlaceRecords,
   noOfGNSSCDRecords                   NoOfGNSSCDRecords,
   noOfSpecificConditionRecords        NoOfSpecificConditionRecords
}
```

Utilizam-se os seguintes elementos de dados, além dos utilizados na geração 1:

noOfGNSSCDRecords é o número de registos GNSS de condução contínua que o cartão pode memorizar.

noOfSpecificConditionRecords é o número dos registos de condição especial que o cartão pode memorizar.

2.62. **DriverCardHolderIdentification**

Informação memorizada num cartão de condutor e relativa à identificação do titular do cartão (requisitos 256 e 281 do anexo 1C).

```
DriverCardHolderIdentification ::= SEQUENCE {
   cardHolderName                      HolderName,
   cardHolderBirthDate                 Datef,
   cardHolderPreferredLanguage         Language
}
```

▼B

cardHolderName é o apelido e o nome próprio do titular do cartão de condutor.

cardHolderBirthDate é a data de nascimento do titular do cartão de condutor.

cardHolderPreferredLanguage é o idioma preferencial do titular do cartão.

2.63. **DSRCSecurityData**

Geração 2:

As informações de texto simples e o MAC a ser transmitido do tacógrafo para o interrogador remoto (RI), via DSRC (para mais informações, consultar apêndice 11, parte B, capítulo 13).

```
DSRCSecurityData ::= SEQUENCE {
   tagLenthPlainText                    OCTET STRING(SIZE(2)),
   currentDateTime                      CurrentDateTime,
   counter                              INTEGER(0..2^24-1),
   vuSerialNumber                       VuSerialNumber,
   dSRCMKVersionNumber                  INTEGER(SIZE(1)),
   tagLengthMac                         OCTET STRING(SIZE(2)),
   mac                                  MAC
}
```

tagLength faz parte da codificação DER-TLV e deve ser fixado em '81 10' (ver apêndice 11, parte B, capítulo 13).

currentDateTime: data e hora atuais da unidade-veículo.

counter enumera as mensagens RTM.

vuSerialNumber é o número de série da unidade-veículo.

dSRCMKVersionNumber é o número da versão da chave principal DSRC a partir da qual se obtiveram as chaves DSRC específicas da VU.

tagLengthMac: marcador e comprimento do objeto de dados MAC como parte da codificação DER-TLV. O marcador deve ser fixado em '8E' e o comprimento deve codificar o comprimento do MAC em octetos (ver apêndice 11, parte B, capítulo 13).

mac é o MAC calculado sobre a mensagem RTM (ver apêndice 11, parte B, capítulo 13).

2.64. **EGFCertificate**

Geração 2:

Certificado da chave pública do módulo GNSS externo para autenticação mútua com uma VU. A estrutura deste certificado é especificada no apêndice 11.

```
EGFCertificate ::= Certificate
```

▼B

2.65. **EmbedderIcAssemblerId**

Fornece informações sobre o fabricante do IC.

```
EmbedderIcAssemblerId ::= SEQUENCE{
   countryCode                          IA5String(SIZE(2)),
   moduleEmbedder                       BCDString(SIZE(2)),
   manufacturerInformation              OCTET STRING(SIZE(1))
}
```

countryCode é o código de país de duas letras, do fabricante do módulo, em conformidade com a norma ISO 3166.

moduleEmbedder identifica o fabricante do módulo.

manufacturerInformation para utilização interna do fabricante.

2.66. **EntryTypeDailyWorkPeriod**

Código que distingue entre o início e o final de uma entrada relativa ao local de um período de trabalho diário e a condição da entrada.

Geração 1

```
EntryTypeDailyWorkPeriod ::= INTEGER {
   Begin,  related time = card insertion time or time of entry          (0),
   End,    related time = card withdrawal time or time of entry        (1),
   Begin,  related time manually entered (start time)                  (2),
   End,    related time manually entered (end of work period)          (3),
   Begin,  related time assumed by VU                                  (4),
   End,    related time assumed by VU                                  (5)
}
```

Valor atribuído: em conformidade com a norma ISO/IEC 8824-1.

Geração 2

```
EntryTypeDailyWorkPeriod ::= INTEGER {
   Begin,  related time = card insertion time or time of entry          (0),
   End,    related time = card withdrawal time or time of entry        (1),
   Begin,  related time manually entered (start time)                  (2),
   End,    related time manually entered (end of work period)          (3),
   Begin,  related time assumed by VU                                  (4),
   End,    related time assumed by VU                                  (5),
   Begin,  related time based on GNSS data                             (6),
   End     related time based on GNSS data                             (7)
}
```

Valor atribuído: em conformidade com a norma ISO/IEC 8824-1.

2.67. **EquipmentType**

Código que distingue diferentes tipos de equipamento para a aplicação tacográfica.

```
EquipmentType ::= INTEGER(0..255)
```

▼B

Geração 1:

```
--Reserved                          (0),
--Driver Card                       (1),
--Workshop Card                     (2),
--Control Card                      (3),
--Company Card                      (4),
--Manufacturing Card                (5),
--Vehicle Unit                      (6),
--Motion Sensor                     (7),
--RFU                               (8..255)
```

Valor atribuído: em conformidade com a norma ISO/IEC 8824-1.

O valor 0 é reservado para designar um Estado-Membro ou a Europa no campo de certificados CHA.

Geração 2:

Utilizam-se os mesmos valores da geração 1, com as seguintes observações:

```
--GNSS Facility                     (8),
--Remote Communication Module       (9),
--ITS interface module              (10),
--Plaque                            (11), -- may be used in SealRecord
--M1/N1 Adapter                     (12), -- may be used in SealRecord
--European Root CA (ERCA)           (13),
--Member State CA (MSCA)            (14),
--External GNSS connection          (15), -- may be used in SealRecord
--Unused                            (16), -- used in SealDataVu
--RFU                               (17..255)
```

Nota: Os valores da geração 2 para a placa, o adaptador e a conexão GNSS externa, bem como os valores da geração 1 para a unidade-veículo e o sensor de movimentos, podem ser utilizados em SealRecord (se pertinente).

2.68. **EuropeanPublicKey**

Geração 1:

A chave pública europeia.

```
EuropeanPublicKey ::= PublicKey
```

2.69. **EventFaultRecordPurpose**

Código que explica por que foram registados um incidente ou uma falha.

```
EventFaultRecordPurpose ::= OCTET STRING (SIZE(1))
```

Valor atribuído:

'00'H	um dos 10 mais recentes (ou últimos) incidentes ou falhas
'01'H	o incidente mais longo de um dos últimos 10 dias de ocorrência
'02'H	um dos 5 incidentes mais longos dos últimos 365 dias
'03'H	o último incidente de um dos últimos 10 dias de ocorrência
'04'H	o incidente mais grave de um dos últimos 10 dias de ocorrência
'05'H	um dos 5 incidentes mais graves dos últimos 365 dias
'06'H	o primeiro incidente ou falha desde a última calibração
'07'H	um incidente ou falha ativos ou em curso
'08'H to '7F'H	RFU
'80'H to 'FF'H	específico do fabricante

▼B

2.70. **EventFaultType**

Código que qualifica um incidente ou uma falha.

```
EventFaultType ::= OCTET STRING (SIZE(1))
```

Valor atribuído:

Geração 1:

'0x'H	Incidentes gerais
'00'H	Sem pormenores adicionais
'01'H	Inserção de cartão não válido
'02'H	Conflito de cartões
'03'H	Sobreposição de tempos
'04'H	Condução sem cartão adequado
'05'H	Inserção de cartão durante a condução
'06'H	Última sessão de cartão encerrada incorretamente
'07'H	Excesso de velocidade
'08'H	Interrupção da alimentação energética
'09'H	Erro nos dados de movimento
'0A'H	Conflito relativo ao movimento do veículo
'0B' to '0F'H	RFU

'1x'H	Incidentes de tentativa de violação da segurança relativos à VU
'10'H	Sem pormenores adicionais
'11'H	Falha da autenticação do sensor de movimentos
'12'H	Falha da autenticação do cartão tacográfico
'13'H	Mudança não autorizada de sensor de movimentos
'14'H	Erro de integridade na entrada de dados relativos ao cartão
'15'H	Erro de integridade nos dados de utilização memorizados
'16'H	Erro na transferência interna de dados
'17'H	Abertura não autorizada da caixa
'18'H	Sabotagem do equipamento informático
'19'H to '1F'H	RFU

'2x'H	Incidentes de tentativa de violação da segurança relativos ao sensor
'20'H	Sem pormenores adicionais
'21'H	Falha de autenticação
'22'H	Erro de integridade em dados memorizados
'23'H	Erro na transferência interna de dados
'24'H	Abertura não autorizada da caixa
'25'H	Sabotagem do equipamento informático
'26'H to '2F'H	RFU

'3x'H	Falhas do aparelho de controlo
'30'H	Sem pormenores adicionais
'31'H	Falha interna da VU
'32'H	Falha da impressora
'33'H	Falha da visualização
'34'H	Falha do descarregamento
'35'H	Falha do sensor
'36'H to '3F'H	RFU

'4x'H	Falhas do cartão
'40'H	Sem pormenores adicionais
'41'H to '4F'H	RFU

'50'H to '7F'H	RFU

'80'H to 'FF'H	Específico do fabricante.

▼B

Geração 2:

Utilizam-se os mesmos valores da geração 1, com as seguintes observações:

'0B'H	Conflito de tempo (GNSS versus relógio interno da VU)
'0C' to '0F'H	RFU,
'5x'H	Falhas relacionadas com o GNSS
'50'H	Sem pormenores adicionais
'51'H	Falha do recetor GNSS interno
'52'H	Falha do recetor GNSS externo
'53'H	Falha de comunicação GNSS externa
'54'H	Sem dados de posição GNSS
'55'H	Violação de deteção de GNSS
'56'H	Certificado do módulo GNSS externo expirado
'57'H to '5F'H	RFU
'6x'H	Falhas relacionadas com o módulo de comunicação à distância
'60'H	Sem pormenores adicionais
'61'H	Falha do módulo de comunicação à distância
'62'H	Falha de comunicação do módulo de comunicação à distância
'63'H to '6F'H	RFU
'7x'H	Falhas da interface ITS
'70'H	Sem pormenores adicionais
'71'H to '7F'H	RFU.

2.71. **ExtendedSealIdentifier**

Geração 2:

O identificador de selo alargado identifica, com caráter exclusivo, um selo (requisito 401 do anexo 1C).

```
ExtendedSealIdentifier ::= SEQUENCE{
   manufacturerCode                    OCTET STRING (SIZE(2)),
   sealIdentifier                      OCTET STRING (SIZE(6))
}
```

manufacturerCode é um código do fabricante do selo.

sealIdentifier é um identificador destinado ao selo, que é único para o fabricante.

2.72. **ExtendedSerialNumber**

Identificação única de um equipamento. Pode também ser utilizado como identificador da chave pública de um equipamento.

Geração 1:

```
ExtendedSerialNumber ::= SEQUENCE{
   serialNumber                        INTEGER(0..2^32-1),
   monthYear                           BCDString(SIZE(2)),
   type                                OCTET STRING(SIZE(1)),
   manufacturerCode                    ManufacturerCode
}
```

serialNumber é um número de série do equipamento, único para o fabricante, para o tipo de equipamento e para o mês e ano infra.

monthYear é a identificação do mês e do ano de fabrico (ou de atribuição do número de série).

▼B

Valor atribuído: codificação BCD de Month (mês, com dois algarismos) e de Year (ano, com os dois últimos algarismos).

type é um identificador do tipo de equipamento.

Valor atribuído: específico do fabricante, com valor reservado 'FFh'.

manufacturerCode: é o código numérico identificativo de um fabricante do tipo de equipamento homologado.

Geração 2:

```
ExtendedSerialNumber ::= SEQUENCE{
   serialNumber                          INTEGER(0..2^32-1),
   monthYear                             BCDString(SIZE(2)),
   type                                  EquipmentType,
   manufacturerCode                      ManufacturerCode
}
```

serialNumber: ver geração 1

monthYear: ver geração 1

type indica o tipo de equipamento

manufacturerCode: ver geração 1.

2.73. **FullCardNumber**

Código que identifica plenamente um cartão tacográfico.

```
FullCardNumber ::= SEQUENCE {
   cardType                              EquipmentType,
   cardIssuingMemberState                NationNumeric,
   cardNumber                            CardNumber
}
```

cardType é o tipo do cartão tacográfico.

cardIssuingMemberState é o código do Estado-Membro que emitiu o cartão.

cardNumber é o número do cartão.

2.74. **FullCardNumberAndGeneration**

Geração 2:

código que identifica plenamente um cartão tacográfico e a respetiva geração.

```
FullCardNumberAndGeneration ::= SEQUENCE {
   fullCardNumber                        FullCardNumber,
   generation                            Generation
}
```

fullcardNumber identifica o cartão tacográfico.

generation indica a geração do cartão tacográfico utilizado.

▼B

2.75. **Generation**

Geração 2:

indica a geração do tacógrafo utilizado.

```
Generation ::= INTEGER(0..255)
```

Valor atribuído:

'00'H	RFU
'01'H	Geração 1
'02'H	Geração 2
'03'H .. 'FF'H	RFU

2.76. **GeoCoordinates**

Geração 2:

as coordenadas geográficas são codificadas como números inteiros. Estes números inteiros são múltiplos da codificação ±DDMM.M para a latitude e ±DDDMM.M para a longitude. Neste caso, ±DD ou ±DDD indica os graus e MM.M os minutos.

```
GeoCoordinates ::= SEQUENCE {
   latitude                              INTEGER(-90000..90001),
   longitude                             INTEGER(-180000..180001)
}
```

latitude: codificada como um múltiplo (fator 10) da representação ±DDMM.M.

longitude: codificada como um múltiplo (fator 10) da representação ±DDDMM.M.

2.77. **GNSSAccuracy**

Geração 2:

A precisão dos dados de posição GNSS (definição eee)). Esta precisão é codificada como um número inteiro e é um múltiplo (fator 10) do valor X.Y fornecido pela frase GSA NMEA.

```
GNSSAccuracy ::= INTEGER(1..100)
```

2.78. **GNSSContinuousDriving**

Geração 2:

Informação memorizada num cartão de condutor ou de oficina e relativa à posição GNSS do veículo, se o tempo de condução contínua do condutor atingir um múltiplo de três horas (requisitos 306 e 354 do anexo 1C).

```
GNSSContinuousDriving := SEQUENCE {
   gnssCDPointerNewestRecord             INTEGER(0..NoOfGNSSCDRecords -1),
   gnssContinuousDrivingRecords          SET SIZE(NoOfGNSSCDRecords) OF
                                         GNSSContinuousDrivingRecord
}
```

gnssCDPointerNewestRecord é o índice do último registo GNSS atualizado da condução contínua.

▼B

Valor atribuído: o número correspondente ao numerador do registo GNSS da condução contínua, a começar por '0' na primeira ocorrência dos registos GNSS da condução contínua na estrutura.

gnssContinuousDrivingRecords é o conjunto de registos que contêm a data e a hora em que a condução contínua atinge um múltiplo de três horas e informações sobre a posição do veículo.

2.79. **GNSSContinuousDrivingRecord**

Geração 2:

Informação memorizada num cartão de condutor ou de oficina e relativa à posição GNSS do veículo, se o tempo de condução contínua do condutor atingir um múltiplo de três horas (requisitos 305 e 353 do anexo 1C).

```
GNSSContinuousDrivingRecord ::= SEQUENCE {
   timeStamp                              TimeReal,
   gnssPlaceRecord                        GNSSPlaceRecord
}
```

timeStamp é a data e a hora em que o tempo de condução contínua do titular do cartão atinge um múltiplo de três horas.

gnssPlaceRecord contém informação relacionada com a posição do veículo.

2.80. **GNSSPlaceRecord**

Geração 2:

a informação relacionada com a posição GNSS do veículo (requisitos 108, 109, 110, 296, 305, 347 e 353 do anexo 1C).

```
GNSSPlaceRecord ::= SEQUENCE {
   timeStamp                              TimeReal,
   gnssAccuracy                           GNSSAccuracy,
   geoCoordinates                         GeoCoordinates
}
```

timeStamp é a data e a hora em que a posição GNSS do veículo foi determinada.

gnssAccuracy é a precisão dos dados de posição GNSS.

geoCoordinates é a localização registada com a utilização de GNSS.

2.81. **HighResOdometer**

Valor do conta-quilómetros do veículo: cúmulo das distâncias percorridas pelo veículo durante o seu funcionamento.

```
HighResOdometer ::= INTEGER(0..2^32-1)
```

▼B

Valor atribuído: Binário sem sinal. Valor em 1/200 km no intervalo operacional de 0 a 21 055 406 km.

2.82. **HighResTripDistance**

Distância percorrida durante um dia ou parte de um dia.

```
HighResTripDistance ::= INTEGER(0..2^32-1)
```

Valor atribuído: Binário sem sinal. Valor em 1/200 km no intervalo operacional de 0 a 21 055 406 km.

2.83. **HolderName**

Apelido e nome próprio do titular de um cartão.

```
HolderName ::= SEQUENCE {
   holderSurname                    Name,
   holderFirstNames                 Name
}
```

holderSurname é o apelido (nome de família) do titular. Não inclui títulos.

Valor atribuído: Se o cartão não for pessoal, holderSurname contém a mesma informação que companyName, workshopName ou controlBody-Name.

holderFirstNames é o nome próprio e as iniciais do titular.

2.84. **InternalGNSSReceiver**

Geração 2:

Informações sobre se recetor GNSS é interno ou externo à unidade--veículo. True significa que o recetor GNSS é interno à VU. False significa que o recetor GNSS é externo.

```
InternalGNSSReceiver ::= BOOLEAN
```

2.85. **K-ConstantOfRecordingEquipment**

Constante do aparelho de controlo [definição m)].

```
K-ConstantOfRecordingEquipment ::= INTEGER(0..2^16-1)
```

Valor atribuído: Impulsos por quilómetro no intervalo operacional de 0 a 64 255 impulsos/km.

2.86. **KeyIdentifier**

Identificador único de uma chave pública utilizada para referenciar e selecionar a chave. Identifica também o titular da chave.

```
KeyIdentifier ::= CHOICE {
   extendedSerialNumber             ExtendedSerialNumber,
   certificateRequestID             CertificateRequestID,
   certificationAuthorityKID        CertificationAuthorityKID
}
```

▼B

A primeira opção é adequada para referenciar a chave pública de uma unidade-veículo ou de um cartão tacográfico.

A segunda opção é adequada para referenciar a chave pública de uma unidade-veículo (caso o número de série da VU não possa ser conhecido no momento da geração do certificado).

A terceira opção é adequada para referenciar a chave pública de um Estado-Membro.

2.87. **KMWCKey**

Geração 2:

Chave AES e a respetiva versão da chave associada, utilizada para emparelhamento do sensor de movimentos com a VU. Para mais informações, ver apêndice 11.

```
KMWCKey ::= SEQUENCE {
   kMWCKey                                 AESKey,
   keyVersion                              INTEGER (SIZE(1))
}
```

kMWCKey é o comprimento da chave AES concatenada com a chave utilizada para o emparelhamento do sensor de movimentos com a VU.

keyVersion indica a versão de chave da chave AES.

2.88. **Language**

Código identificativo de um idioma.

```
Language ::= IA5String(SIZE(2))
```

Valor atribuído: Código constituído por duas letras minúsculas, em conformidade com a norma ISO 639.

2.89. **LastCardDownload**

Data e hora, memorizadas num cartão de condutor e relativas ao último descarregamento do cartão (para outras finalidades que não o controlo) (requisitos 257 e 282 do anexo 1C). Esta data é atualizável por uma VU ou por qualquer leitor de cartões.

```
LastCardDownload ::= TimeReal
```

Valor atribuído: sem mais especificações.

2.90. **LinkCertificate**

Geração 2:

O certificado de ligação entre pares de chaves European Root CA.

```
LinkCertificate ::= Certificate
```

2.91. **L-TyreCircumference**

Perímetro efetivo dos pneus das rodas [definição u)].

```
L-TyreCircumference ::= INTEGER(0.. 2^16-1)
```

▼B

Valor atribuído: Binário sem sinal, valor em 1/8 mm no intervalo operacional de 0 a 8 031 mm.

2.92. **MAC**

Geração 2:

Uma soma criptográfica de teste, com 8, 12 ou 16 bytes de comprimento, correspondente aos conjuntos de codificação especificados no apêndice 11.

```
MAC ::= CHOICE {
   mac8                                    OCTET STRING (SIZE(8)),
   mac12                                   OCTET STRING (SIZE(12)),
   mac16                                   OCTET STRING (SIZE(12))
}
```

2.93. **ManualInputFlag**

Código que identifica se um titular introduziu manualmente atividades de condutor no momento da inserção do cartão ou não (requisito 081 do anexo 1B e requisito 102 do anexo 1C).

```
ManualInputFlag ::= INTEGER {
   noEntry                                 (0)
   manualEntries                           (1)
}
```

Valor atribuído: sem mais especificações.

2.94. **ManufacturerCode**

Código identificativo de um fabricante do tipo de equipamento homologado.

```
ManufacturerCode ::= INTEGER(0..255)
```

O laboratório competente para ensaios de interoperabilidade deve manter e publicar a lista de códigos de fabricantes no seu sítio Web (requisito 454 do anexo 1C).

Os ManufacturerCodes são provisoriamente atribuídos a criadores de tacógrafos quando do pedido de ensaios de interoperabilidade ao laboratório competente.

2.95. **ManufacturerSpecificEventFaultData**

Geração 2:

Os códigos de erro específicos do fabricante simplificam a análise de erros e a manutenção das unidades-veículo.

```
ManufacturerSpecificEventFaultData ::= SEQUENCE {
   manufacturerCode                        ManufacturerCode,
   manufacturerSpecificErrorCode           OCTET STRING(SIZE(3))
}
```

ManufacturerCode identifica o fabricante da unidade-veículo.

manufacturerSpecificErrorCode é um código de erro específico para o fabricante.

▼B

2.96. **MemberStateCertificate**

O certificado da chave pública de um Estado-Membro, emitido pela autoridade europeia de certificação.

```
MemberStateCertificate ::= Certificate
```

2.97. **MemberStateCertificateRecordArray**

Geração 2:

O certificado do Estado-Membro, mais metadados utilizados no protocolo de descarregamento.

```
MemberStateCertificateRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       MemberStateCertificate
}
```

recordType indica o tipo de registo (MemberStateCertificate). **Valor atribuído**: ver RecordType

recordSize: tamanho do MemberStateCertificate, em bytes.

noOfRecords: número de registos nos registos definidos. O valor deve ser fixado em 1, dado que os certificados podem ter comprimentos diferentes.

records: conjunto de certificados do Estado-Membro.

2.98. **MemberStatePublicKey**

Geração 1:

Chave pública de um Estado-Membro.

```
MemberStatePublicKey ::= PublicKey
```

2.99. **Name**

Um nome.

```
Name ::= SEQUENCE {
   codePage                            INTEGER (0..255),
   name                                OCTET STRING (SIZE(35))
}
```

codePage especifica um conjunto de carateres definido no capítulo 4

name é um nome codificado que utiliza o conjunto de carateres especificado.

2.100. **NationAlpha**

A referência alfabética a um país deve estar em conformidade com os códigos distintivos utilizados em veículos no tráfego internacional (Convenção das Nações Unidas sobre Trânsito Viário, Viena, 1968).

```
NationAlpha ::= IA5String(SIZE(3))
```

Os códigos NationAlpha e NationNumeric devem constar de uma lista publicada no sítio Web do laboratório nomeado para a realização do ensaio de interoperabilidade, conforme estabelecido no requisito 440 do anexo 1C.

▼B

2.101. **NationNumeric**

Referência numérica a um país.

```
NationNumeric ::= INTEGER(0 .. 255)
```

Valor atribuído: ver tipo de dados 2.100 (NationAlpha).

Só deve ser efetuada uma alteração ou atualização da especificação NationAlpha ou NationNumeric descrita no parágrafo supra após o laboratório nomeado receber os pontos de vista de fabricantes de unidades-veículo homologadas para tacógrafos digitais e tacógrafos inteligentes.

2.102. **NoOfCalibrationRecords**

Número de registos de calibração que um cartão de oficina pode memorizar.

Geração 1:

```
NoOfCalibrationRecords ::= INTEGER(0..255)
```

Valor atribuído: ver apêndice 2.

Geração 2:

$$\text{NoOfCalibrationRecords ::= INTEGER}(0..2^{16}-1)$$

Valor atribuído: ver apêndice 2.

2.103. **NoOfCalibrationsSinceDownload**

Contador que indica o número de calibrações efetuadas com um cartão de oficina desde o seu último descarregamento (requisitos 317 e 340 do anexo 1C).

$$\text{NoOfCalibrationsSinceDownload ::= INTEGER}(0..2^{16}-1)$$

Valor atribuído: sem outras especificações.

2.104. **NoOfCardPlaceRecords**

Número de registos de local que um cartão de condutor ou de oficina pode memorizar.

Geração 1:

```
NoOfCardPlaceRecords ::= INTEGER(0..255)
```

Valor atribuído: ver apêndice 2.

Geração 2:

$$\text{NoOfCardPlaceRecords ::= INTEGER}(0..2^{16}-1)$$

Valor atribuído: ver apêndice 2.

▼B

2.105. **NoOfCardVehicleRecords**

Número de registos de utilização de veículos que um cartão de condutor ou de oficina pode memorizar.

```
NoOfCardVehicleRecords ::= INTEGER(0.. 2^16-1)
```

Valor atribuído: ver apêndice 2.

2.106. **NoOfCardVehicleUnitRecords**

Geração 2:

Número de registos de utilização de unidades-veículo que um cartão de condutor ou de oficina pode memorizar.

```
NoOfCardVehicleUnitRecords ::= INTEGER(0.. 2^16-1)
```

Valor atribuído: ver apêndice 2.

2.107. **NoOfCompanyActivityRecords**

Número de registos de atividade de empresa que um cartão de empresa pode memorizar.

```
NoOfCompanyActivityRecords ::= INTEGER(0.. 2^16-1)
```

Valor atribuído: ver apêndice 2.

2.108. **NoOfControlActivityRecords**

Número de registos de atividade de controlo que um cartão de controlo pode memorizar.

```
NoOfControlActivityRecords ::= INTEGER(0.. 2^16-1)
```

Valor atribuído: ver apêndice 2.

2.109. **NoOfEventsPerType**

Número de incidentes, por tipo, que um cartão pode memorizar.

```
NoOfEventsPerType ::= INTEGER(0..255)
```

Valor atribuído: ver apêndice 2.

2.110. **NoOfFaultsPerType**

Número de falhas, por tipo, que um cartão pode memorizar.

```
NoOfFaultsPerType ::= INTEGER(0..255)
```

Valor atribuído: ver apêndice 2.

▼B

2.111. **NoOfGNSSCDRecords**

Geração 2:

Número de registos GNSS de condução contínua que o cartão pode memorizar.

```
NoOfGNSSCDRecords ::= INTEGER(0..2^16-1)
```

Valor atribuído: ver apêndice 2.

2.112. **NoOfSpecificConditionRecords**

Geração 2:

Número de registos de condição especial que o cartão pode memorizar.

```
NoOfSpecificConditionRecords ::= INTEGER(0..2^16-1)
```

Valor atribuído: ver apêndice 2.

2.113. **OdometerShort**

Valor do conta-quilómetros do veículo sob forma sincopada (abreviada).

```
OdometerShort ::= INTEGER(0..2^24-1)
```

Valor atribuído: Binário sem sinal. Valor em km no intervalo operacional de 0 a 9 999 999 km.

2.114. **OdometerValueMidnight**

O valor do conta-quilómetros do veículo à meia-noite de um determinado dia (requisito 090 do anexo 1B e requisito 113 do anexo 1C).

```
OdometerValueMidnight ::= OdometerShort
```

Valor atribuído: sem mais especificações.

2.115. **OdometerValueMidnightRecordArray**

Geração 2:

O OdometerValueMidnight, mais metadados utilizados no protocolo de descarregamento.

```
OdometerValueMidnightRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       OdometerValueMidnight
}
```

recordType indica o tipo de registo (OdometerValueMidnight). **Valor atribuído**: ver RecordType

recordSize: tamanho do OdometerValueMidnight, em bytes.

noOfRecords: número de registos nos registos definidos.

records: conjunto dos registos OdometerValueMidnight.

▼B

2.116. **OverspeedNumber**

Número de incidentes de velocidade excessiva desde o último controlo de excesso de velocidade.

```
OverspeedNumber ::= INTEGER(0..255)
```

Valor atribuído: 0 significa que, desde o último controlo de excesso de velocidade, não ocorreu nenhum incidente de excesso de velocidade, 1 significa que ocorreu um incidente de excesso de velocidade, …, 255 significa que ocorreram 255 ou mais incidentes.

2.117. **PlaceRecord**

Informação relativa a um local onde se inicia ou termina um período de trabalho diário (requisitos 108, 271, 296, 324 e 347 do anexo 1C).

Geração 1:

```
PlaceRecord ::= SEQUENCE {
   entryTime                        TimeReal,
   entryTypeDailyWorkPeriod         EntryTypeDailyWorkPeriod,
   dailyWorkPeriodCountry           NationNumeric,
   dailyWorkPeriodRegion            RegionNumeric,
   vehicleOdometerValue             OdometerShort
}
```

entryTime é uma data e hora relativa à entrada.

entryTypeDailyWorkPeriod é o tipo de entrada.

dailyWorkPeriodCountry é o país introduzido.

dailyWorkPeriodRegion é a região introduzida.

vehicleOdometerValue é o valor do conta-quilómetros no momento da introdução do local.

Geração 2:

```
PlaceRecord ::= SEQUENCE {
   entryTime                        TimeReal,
   entryTypeDailyWorkPeriod         EntryTypeDailyWorkPeriod,
   dailyWorkPeriodCountry           NationNumeric,
   dailyWorkPeriodRegion            RegionNumeric,
   vehicleOdometerValue             OdometerShort,
   entryGNSSPlaceRecord             GNSSPlaceRecord
}
```

Utilizam-se os seguintes elementos de dados, além dos utilizados na geração 1:

entryGNSSPlaceRecord: localização e hora registadas.

▼B

2.118. **PreviousVehicleInfo**

Informação relativa ao veículo previamente utilizado por um condutor no momento em que insere o seu cartão numa unidade-veículo (requisito 081 do anexo 1B e requisito 102 do anexo 1C).

Geração 1:

```
PreviousVehicleInfo ::= SEQUENCE {
   vehicleRegistrationIdentification      VehicleRegistrationIdentification,
   cardWithdrawalTime                     TimeReal
}
```

vehicleRegistrationIdentification é o VRN e o Estado-Membro de matrícula do veículo.

cardWithdrawalTime: data e hora a que o cartão foi retirado.

Geração 2:

```
PreviousVehicleInfo ::= SEQUENCE {
   vehicleRegistrationIdentification      VehicleRegistrationIdentification,
   cardWithdrawalTime                     TimeReal,
   vuGeneration                           Generation
}
```

Utiliza-se o seguinte elemento de dados, além dos utilizados na geração 1:

vuGeneration identifica a geração da unidade-veículo.

2.119. **PublicKey**

Geração 1:

Uma chave pública RSA.

```
PublicKey ::= SEQUENCE {
   rsaKeyModulus                          RSAKeyModulus,
   rsaKeyPublicExponent                   RSAKeyPublicExponent
}
```

rsaKeyModulus é o módulo do par de chaves.

rsaKeyPublicExponent é o expoente público do par de chaves.

2.120. **RecordType**

Geração 2:

Referência a um tipo de registo. Utiliza-se este tipo de dados em RecordArrays.

```
RecordType ::= OCTET STRING(SIZE(1))
```

▼B

Valor atribuído:

'01'H	ActivityChangeInfo
'02'H	CardSlotsStatus
'03'H	CurrentDateTime
'04'H	MemberStateCertificate
'05'H	OdometerValueMidnight
'06'H	DateOfDayDownloaded
'07'H	SensorPaired
'08'H	Signature
'09'H	SpecificConditionRecord
'0A'H	VehicleIdentificationNumber
'0B'H	VehicleRegistrationNumber
'0C'H	VuCalibrationRecord
'0D'H	VuCardIWRecord
'0E'H	VuCardRecord
'0F'H	VuCertificate
'10'H	VuCompanyLocksRecord
'11'H	VuControlActivityRecord
'12'H	VuDetailedSpeedBlock
'13'H	VuDownloadablePeriod
'14'H	VuDownloadActivityData
'15'H	VuEventRecord
'16'H	VuGNSSCDRecord
'17'H	VuITSConsentRecord
'18'H	VuFaultRecord
'19'H	VuIdentification
'1A'H	VuOverSpeedingControlData
'1B'H	VuOverSpeedingEventRecord
'1C'H	VuPlaceDailyWorkPeriodRecord
'1D'H	VuTimeAdjustmentGNSSRecord
'1E'H	VuTimeAdjustmentRecord
'1F'H	VuPowerSupplyInterruptionRecord,
'20'H	SensorPairedRecord,
'21'H	SensorExternalGNSSCoupledRecord,
'22'H to '7F'H	RFU
'80'H to 'FF'H	Específico do fabricante.

2.121. **RegionAlpha**

Referência alfabética a uma região, dentro de um país especificado.

```
RegionAlpha ::= IA5STRING(SIZE(3))
```

Geração 1:

Valor atribuído:

' '	No information available,
Spain:	
'AN '	Andalucía,
'AR '	Aragón,
'AST'	Asturias,
'C '	Cantabria,
'CAT'	Cataluña,
'CL '	Castilla-León,
'CM '	Castilla-La-Mancha,
'CV'	Valencia,
'EXT'	Extremadura,
'G '	Galicia,
'IB '	Baleares,
'IC '	Canarias,
'LR '	La Rioja,
'M '	Madrid,
'MU '	Murcia,
'NA '	Navarra,
'PV '	País Vasco

▼B

Geração 2:

Os códigos RegionAlpha devem constar de uma lista publicada no sítio Web do laboratório nomeado para a realização do ensaio de interoperabilidade.

2.122. **RegionNumeric**

Referência numérica a uma região, dentro de um país especificado.

```
RegionNumeric ::= OCTET STRING (SIZE(1))
```

Geração 1:

Valor atribuído:

```
'00'H        No information available,
Spain:
'01'H        Andalucía,
'02'H        Aragón,
'03'H        Asturias,
'04'H        Cantabria,
'05'H        Cataluña,
'06'H        Castilla-León,
'07'H        Castilla-La-Mancha,
'08'H        Valencia,
'09'H        Extremadura,
'0A'H        Galicia,
'0B'H        Baleares,
'0C'H        Canarias,
'0D'H        La Rioja,
'0E'H        Madrid,
'0F'H        Murcia,
'10'H        Navarra,
'11'H        País Vasco
```

Geração 2:

Os códigos RegionNumeric devem constar de uma lista publicada no sítio Web do laboratório nomeado para a realização do ensaio de interoperabilidade.

2.123. **RemoteCommunicationModuleSerialNumber**

Geração 2:

O número de série do dispositivo de comunicação à distância.

```
RemoteCommunicationModuleSerialNumber ::= ExtendedSerialNumber
```

2.124. **RSAKeyModulus**

Geração 1:

O módulo de um par de chaves RSA.

```
RSAKeyModulus ::= OCTET STRING (SIZE(128))
```

Valor atribuído: não especificado.

2.125. **RSAKeyPrivateExponent**

Geração 1:

O expoente privado de um par de chaves RSA.

```
RSAKeyPrivateExponent ::= OCTET STRING (SIZE(128))
```

Valor atribuído: não especificado.

▼B

2.126. **RSAKeyPublicExponent**

Geração 1:

O expoente público de um par de chaves RSA.

```
RSAKeyPublicExponent ::= OCTET STRING (SIZE(8))
```

Valor atribuído: não especificado.

2.127. **RtmData**

Geração 2:

Relativamente à definição deste tipo de dados, ver apêndice 14.

2.128. **SealDataCard**

Geração 2:

Este tipo de dado memoriza informações sobre os selos que estão ligados aos diferentes componentes do veículo e destina-se a memorização num cartão. Este tipo de dado está relacionado com o requisito 337 do anexo 1C.

```
SealDataCard ::= SEQUENCE {
   noOfSealRecords                    INTEGER(1..5),
   sealRecords                        SET SIZE(noOfSealRecords) OF SealRecord
}
```

noOfSealRecords é o número de registos em sealRecords.

sealRecords é um conjunto de registos dos selos.

2.129. **SealDataVu**

Geração 2:

Este tipo de dado memoriza informações sobre os selos que estão ligados aos diferentes componentes do veículo e destina-se a memorização numa unidade-veículo.

```
SealDataVu ::= SEQUENCE SIZE(5) OF {
   sealRecords                        SealRecord
}
```

sealRecords é um conjunto de registos dos selos. Se houver menos de cinco selos disponíveis, o valor de EquipmentType em todos os sealRecords não utilizados deverá ser fixado em 16, isto é, não utilizado.

2.130. **SealRecord**

Geração 2:

Este tipo de dado memoriza informações sobre um selo que está ligado a um componente. Este tipo de dado está relacionado com o requisito 337 do anexo 1C.

```
SealRecord ::= SEQUENCE {
   equipmentType                      EquipmentType,
   extendedSealIdentifier             ExtendedSealIdentifier
}
```

equipmentType identifica o tipo de equipamento a que o selo está ligado.

extendedSealIdentifier é o identificador do selo ligado ao equipamento.

▼B

2.131. **SensorApprovalNumber**

Número de homologação de tipo do sensor.

Geração 1:

```
SensorApprovalNumber ::= IA5String(SIZE(8))
```

Valor atribuído: não especificado.

Geração 2:

```
SensorApprovalNumber ::= IA5String(SIZE(16))
```

Valor atribuído:

O número de homologação deve ser apresentado conforme publicação no respetivo sítio Web da Comissão Europeia, ou seja, incluindo hífenes, se existirem. O número de homologação deve estar alinhado à esquerda.

2.132. **SensorExternalGNSSApprovalNumber**

Geração 2:

número de homologação de tipo do módulo GNSS externo.

```
SensorExternalGNSSApprovalNumber ::= IA5String(SIZE(16))
```

Valor atribuído:

O número de homologação deve ser apresentado conforme publicação no respetivo sítio Web da Comissão Europeia, ou seja, incluindo hífenes, se existirem. O número de homologação deve estar alinhado à esquerda.

2.133. **SensorExternalGNSSCoupledRecord**

Geração 2:

Informação memorizada numa unidade-veículo e relativa à identificação do módulo GNSS externo acoplado a ela (requisito 100 do anexo 1C).

```
SensorExternalGNSSCoupledRecord ::= SEQUENCE {
   sensorSerialNumber                  SensorGNSSSerialNumber,
   sensorApprovalNumber                SensorExternalGNSSApprovalNumber,
   sensorCouplingDate                  SensorGNSSCouplingDate
}
```

sensorSerialNumber é o número de série do módulo GNSS externo acoplado à unidade-veículo.

sensorApprovalNumber é o número de homologação deste módulo GNSS externo.

sensorCouplingDate é uma data de acoplamento deste módulo GNSS externo à unidade-veículo.

2.134. **SensorExternalGNSSIdentification**

Geração 2:

Informação relativa à identificação do módulo GNSS externo (requisito 98 do anexo 1C).

▼B

```
SensorExternalGNSSIdentification ::= SEQUENCE {
   sensorSerialNumber                    SensorGNSSSerialNumber,
   sensorApprovalNumber                  SensorExternalGNSSApprovalNumber,
   sensorSCIdentifier                    SensorExternalGNSSSCIdentifier,
   sensorOSIdentifier                    SensorExternalGNSSOSIdentifier
}
```

sensorSerialNumber é o número de série alargado do módulo GNSS externo.

sensorApprovalNumber é o número de homologação do módulo GNSS externo.

sensorSCIdentifier é o identificador do componente de segurança do módulo GNSS externo.

sensorOSIdentifier é o identificador do sistema operacional do módulo GNSS externo.

2.135. **SensorExternalGNSSInstallation**

Geração 2:

Informação memorizada num módulo GNSS externo e relativa à instalação do sensor GNSS externo (requisito 123 do anexo 1C).

```
SensorExternalGNSSInstallation ::= SEQUENCE {
   sensorCouplingDateFirst               SensorGNSSCouplingDate,
   firstVuApprovalNumber                 VuApprovalNumber,
   firstVuSerialNumber                   VuSerialNumber,
   sensorCouplingDateCurrent             SensorGNSSCouplingDate,
   currentVuApprovalNumber               VuApprovalNumber,
   currentVUSerialNumber                 VuSerialNumber
}
```

sensorCouplingDateFirst é a data do primeiro acoplamento do módulo GNSS externo à unidade-veículo.

firstVuApprovalNumber é o número de homologação da primeira unidade-veículo acoplada ao módulo GNSS externo.

firstVuSerialNumber é o número de série da primeira unidade-veículo emparelhada com o módulo GNSS externo.

sensorCouplingDateCurrent é a data do acoplamento atual do módulo GNSS externo à unidade-veículo.

currentVuApprovalNumber é o número de homologação da unidade-veículo acoplada atualmente ao módulo GNSS externo.

currentVUSerialNumber é o número de série da unidade-veículo acoplada atualmente ao módulo GNSS externo.

▼B

2.136. **SensorExternalGNSSOSIdentifier**

Geração 2:

Identificador do sistema operacional do módulo GNSS externo.

```
SensorOSIdentifier ::= IA5String(SIZE(2))
```

Valor atribuído: específico do fabricante.

2.137. **SensorExternalGNSSSCIdentifier**

Geração 2:

Este tipo utiliza-se, por exemplo, para identificar o módulo criptográfico do módulo GNSS externo.

Identificador do componente de segurança do módulo GNSS externo.

```
SensorExternalGNSSSCIdentifier ::= IA5String(SIZE(8))
```

Valor atribuído: específico do fabricante do componente.

2.138. **SensorGNSSCouplingDate**

Geração 2:

Data de um acoplamento do módulo GNSS externo a uma unidade-veículo.

```
SensorGNSSCouplingDate ::= TimeReal
```

Valor atribuído: não especificado.

2.139. **SensorGNSSSerialNumber**

Geração 2:

Este tipo utiliza-se para memorizar o número de série do recetor GNSS, quer esteja dentro da VU ou fora da VU.

Número de série do recetor GNSS.

```
SensorGNSSSerialNumber ::= ExtendedSerialNumber
```

2.140. **SensorIdentification**

Informação memorizada num sensor de movimentos e relativa à identificação do mesmo (requisito 077 do anexo 1B e requisito 95 do anexo 1C).

```
SensorIdentification ::= SEQUENCE {
   sensorSerialNumber                SensorSerialNumber,
   sensorApprovalNumber              SensorApprovalNumber,
   sensorSCIdentifier                SensorSCIdentifier,
   sensorOSIdentifier                SensorOSIdentifier
}
```

sensorSerialNumber é o número de série alargado do sensor de movimentos (inclui número da peça e código do fabricante).

sensorApprovalNumber é o número de homologação do sensor de movimentos.

sensorSCIdentifier é o identificador do componente de segurança do sensor de movimentos.

▼B

sensorOSIdentifier é o identificador do sistema operacional do sensor de movimentos.

2.141. **SensorInstallation**

Informação memorizada num sensor de movimentos e relativa à instalação do mesmo (requisito 099 do anexo 1B e requisito 122 do anexo 1C).

```
SensorInstallation ::= SEQUENCE {
   sensorPairingDateFirst                SensorPairingDate,
   firstVuApprovalNumber                 VuApprovalNumber,
   firstVuSerialNumber                   VuSerialNumber,
   sensorPairingDateCurrent              SensorPairingDate,
   currentVuApprovalNumber               VuApprovalNumber,
   currentVUSerialNumber                 VuSerialNumber
}
```

sensorPairingDateFirst é a data do primeiro emparelhamento do sensor de movimentos com uma VU.

firstVuApprovalNumber é o número de homologação da primeira unidade-veículo emparelhada com o sensor de movimentos.

firstVuSerialNumber é o número de série da primeira unidade-veículo emparelhada com o sensor de movimentos.

sensorPairingDateCurrent é a data do atual emparelhamento do sensor de movimentos com a VU.

currentVuApprovalNumber é o número de homologação da unidade-veículo atualmente emparelhada com o sensor de movimentos.

currentVUSerialNumber é o número de série da unidade-veículo atualmente emparelhada com o sensor de movimentos.

2.142. **SensorInstallationSecData**

Informação memorizada num cartão de oficina e relativa aos dados de segurança necessários para emparelhar sensores de movimentos com unidades-veículo (requisitos 308 e 331 do anexo 1C).

Geração 1:

```
SensorInstallationSecData ::= TdesSessionKey
```

Valor atribuído: em conformidade com a norma ISO 16844-3.

Geração 2:

Conforme descrito no apêndice 11, um cartão de oficina deve memorizar até três chaves para emparelhamento do sensor de movimentos com a VU. Estas chaves têm diferentes versões principais.

```
SensorInstallationSecData ::= SEQUENCE {
   kMWCKey1                              KMWCKey,
   kMWCKey2                              KMWCKey OPTIONAL,
   kMWCKey3                              KMWCKey OPTIONAL
}
```

▼B

2.143. **SensorOSIdentifier**

Identificador do sistema operacional do sensor de movimentos.

```
SensorOSIdentifier ::= IA5String(SIZE(2))
```

Valor atribuído: específico do fabricante.

2.144. **SensorPaired**

Geração 1:

Informação memorizada numa unidade-veículo e relativa à identificação do sensor de movimentos emparelhado com ela (requisito 079 do anexo 1B).

```
SensorPaired ::= SEQUENCE {
   sensorSerialNumber                  SensorSerialNumber,
   sensorApprovalNumber                SensorApprovalNumber,
   sensorPairingDateFirst              SensorPairingDate
}
```

sensorSerialNumber é o número de série do sensor de movimentos atualmente emparelhado com a unidade-veículo.

sensorApprovalNumber é o número de homologação do sensor de movimentos atualmente emparelhado com a unidade-veículo.

sensorPairingDateFirst é a data em que o sensor de movimentos atualmente emparelhado com a unidade-veículo foi emparelhado pela primeira vez com uma VU.

2.145. **SensorPairedRecord**

Geração 2:

Informação memorizada numa unidade-veículo e relativa à identificação do sensor de movimentos emparelhado com ela (requisito 079 do anexo 1C).

```
SensorPairedRecord ::= SEQUENCE {
   sensorSerialNumber                  SensorSerialNumber,
   sensorApprovalNumber                SensorApprovalNumber,
   sensorPairingDate                   SensorPairingDate
}
```

sensorSerialNumber: número de série de um sensor de movimentos emparelhado com a unidade-veículo.

sensorApprovalNumber: número de homologação deste sensor de movimentos.

sensorPairingDate: data do emparelhamento deste sensor de movimentos com a unidade-veículo.

2.146. **SensorPairingDate**

Data do emparelhamento do sensor de movimentos com uma VU.

```
SensorPairingDate ::= TimeReal
```

Valor atribuído: não especificado.

▼B

2.147. **SensorSCIdentifier**

Identificador do componente de segurança do sensor de movimentos.

```
SensorSCIdentifier ::= IA5String(SIZE(8))
```

Valor atribuído: específico do fabricante do componente.

2.148. **SensorSerialNumber**

Número de série do sensor de movimentos.

```
SensorSerialNumber ::= ExtendedSerialNumber
```

2.149. **Signature**

Uma assinatura digital.

Geração 1:

```
Signature ::= OCTET STRING (SIZE(128))
```

Valor atribuído: em conformidade com o apêndice 11 (Mecanismos comuns de segurança).

Geração 2:

```
Signature ::= OCTET STRING (SIZE(64..132))
```

Valor atribuído: em conformidade com o apêndice 11 (Mecanismos comuns de segurança).

2.150. **SignatureRecordArray**

Geração 2:

Um conjunto de assinaturas, mais metadados utilizados no protocolo de descarregamento.

```
SignatureRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF Signature
}
```

recordType indica o tipo de registo (Signature). **Valor atribuído**: ver RecordType

recordSize: tamanho de Signature, em bytes.

noOfRecords: número de registos nos registos definidos. O valor deve ser fixado em 1, dado que as assinaturas podem ter diferentes comprimentos.

records: conjunto de assinaturas.

2.151. **SimilarEventsNumber**

O número de eventos semelhantes para um determinado dia (requisito 094 do anexo 1B e requisito 117 do anexo 1C).

```
SimilarEventsNumber ::= INTEGER(0..255)
```

Valor atribuído: 0 não se utiliza, 1 significa que, no dia em questão, apenas um incidente deste tipo foi memorizado, 2 significa que ocorreram dois incidentes deste tipo (memorizado apenas um), …, 255 significa que ocorreram 255 ou mais incidentes deste tipo no dia em questão.

▼B

2.152. **SpecificConditionRecord**

Informação memorizada num cartão de condutor ou de oficina ou numa unidade-veículo e relativa a uma condição especial (requisitos 130, 276, 301, 328 e 355 do anexo 1C).

```
SpecificConditionRecord ::= SEQUENCE {
   entryTime                          TimeReal,
   specificConditionType              SpecificConditionType
}
```

entryTime: data e hora da entrada.

specificConditionType: código que identifica a condição especial.

2.153. **SpecificConditions**

Informação memorizada num cartão de condutor ou de oficina ou numa unidade-veículo e relativa a uma condição especial (requisitos 131, 277, 302, 329 e 356 do anexo 1C).

Geração 2:

```
SpecificConditions := SEQUENCE {
   conditionPointerNewestRecord         INTEGER(0..NoOfSpecificConditionRecords-1),
   specificConditionRecords             SET SIZE(NoOfSpecificConditionRecords) OF
                                        SpecificConditionRecord
}
```

conditionPointerNewestRecord é o índice do último registo atualizado de condição especial.

Valor atribuído: o número correspondente ao numerador do registo da condição especial, a começar por '0' na primeira ocorrência dos registos da condição especial na estrutura.

specificConditionRecords é o conjunto de registos que contém informações sobre as condições especiais gravadas.

2.154. **SpecificConditionType**

Código que identifica uma condição especial (requisitos 050b, 105a, 212a e 230a do anexo 1B e requisito 62 do anexo 1C).

```
SpecificConditionType ::= INTEGER(0..255)
```

Geração 1:

Valor atribuído:

'00'H	RFU
'01'H	Fora de âmbito — Início
'02'H	Fora de âmbito — Final
'03'H	Travessia de batelão/comboio
'04'H .. 'FF'H	RFU

Geração 2:

Valor atribuído:

'00'H	RFU
'01'H	Fora de âmbito — Início
'02'H	Fora de âmbito — Final
'03'H	Travessia de batelão/comboio — Início
'04'H	Travessia de batelão/comboio — Final
'05'H .. 'FF'H	RFU

▼B

2.155. **Speed**

Velocidade do veículo (km/h).

```
Speed ::= INTEGER(0..255)
```

Valor atribuído: quilómetros por hora no intervalo operacional de 0 a 220 km/h.

2.156. **SpeedAuthorised**

Velocidade máxima autorizada para o veículo [definição hh)].

```
SpeedAuthorised ::= Speed
```

2.157. **SpeedAverage**

Velocidade média num intervalo de duração previamente definido (km/h).

```
SpeedAverage ::= Speed
```

2.158. **SpeedMax**

Velocidade máxima num intervalo de duração previamente definido.

```
SpeedMax ::= Speed
```

2.159. **TachographPayload**

Geração 2:

Relativamente à definição deste tipo de dados, ver apêndice 14.

2.160. **TachographPayloadEncrypted**

Geração 2:

A carga útil do tacógrafo encriptada DER-TLV, ou seja, os dados enviados encriptados na mensagem RTM. Relativamente ao mecanismo de encriptação ver apêndice 11, parte B, capítulo 13.

```
TachographPayloadEncrypted ::= SEQUENCE {
   tag                                  OCTET STRING(SIZE(1)),
   length                               OCTET STRING(SIZE(1..2)),
   paddingContentIndicatorByte          OCTET STRING(SIZE(1)),
   encryptedData                        OCTET STRING(SIZE(16..192))
}
```

tag faz parte da codificação DER-TLV e deve ser fixado em '87' (ver apêndice 11, parte B, capítulo 13).

length faz parte da codificação DER-TLV e deve codificar o comprimento da sequência paddingContentIndicatorByte e de encryptedData.

paddingContentIndicatorByte deve ser fixado em '00'.

encryptedData é encriptado tachographPayload conforme especificado no apêndice 11, parte B, capítulo 13. O comprimento destes dados em octetos será sempre um múltiplo de 16.

2.161. **TDesSessionKey**

Geração 1:

Uma chave tripla de sessão DES.

```
TDesSessionKey ::= SEQUENCE {
   tDesKeyA                             OCTET STRING (SIZE(8)),
   tDesKeyB                             OCTET STRING (SIZE(8))
}
```

Valor atribuído: sem mais especificações.

▼B

2.162. **TimeReal**

Código para um campo combinado de data e hora, em que a data e a hora são expressas como segundos depois das 00h00m00s TMG de 1.1.1970.

```
TimeReal{INTEGER:TimeRealRange} ::= INTEGER(0..TimeRealRange)
```

Valor atribuído — Alinhamento de octetos: número de segundos a partir da meia-noite TMG de 1.1.1970.

O valor máximo de data/hora situa-se no ano de 2106.

2.163. **TyreSize**

Designação das dimensões dos pneus.

```
TyreSize ::= IA5String(SIZE(15))
```

Valor atribuído: em conformidade com a Diretiva 92/23/CEE de 31.3.92 (JO L 129, p. 95).

2.164. **VehicleIdentificationNumber**

Número de identificação do veículo (VIN), referente ao veículo como um todo. Normalmente, número de série do chassi.

```
VehicleIdentificationNumber ::= IA5String(SIZE(17))
```

Valor atribuído: conforme definição na norma ISO 3779.

2.165. **VehicleIdentificationNumberRecordArray**

Geração 2:

O número de identificação do veículo, mais metadados utilizados no protocolo de descarregamento.

```
VehicleIdentificationNumberRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VehicleIdentificationNumber
}
```

recordType indica o tipo de registo (VehicleIdentificationNumber). **Valor atribuído**: ver RecordType

recordSize: tamanho do VehicleIdentificationNumber, em bytes.

noOfRecords: número de registos nos registos definidos.

records: conjunto de números de identificação de veículos.

2.166. **VehicleRegistrationIdentification**

Identificação de um veículo, única para a Europa (VRN e Estado-Membro).

```
VehicleRegistrationIdentification ::= SEQUENCE {
   vehicleRegistrationNation           NationNumeric,
   vehicleRegistrationNumber           VehicleRegistrationNumber
}
```

vehicleRegistrationNation é o país no qual o veículo está matriculado.

▼B

vehicleRegistrationNumber é o número de matrícula do veículo (VRN).

2.167. **VehicleRegistrationNumber**

Número de matrícula do veículo (VRN), atribuído pela autoridade competente nesta matéria.

```
VehicleRegistrationNumber ::= SEQUENCE {
   codePage                              INTEGER (0..255),
   vehicleRegNumber                      OCTET STRING (SIZE(13))
}
```

codePage especifica um conjunto de carateres definido no capítulo 4.

vehicleRegNumber é um VRN codificado que utiliza o conjunto de carateres especificado.

Valor atribuído: específico do país.

2.168. **VehicleRegistrationNumberRecordArray**

Geração 2:

O número de matrícula do veículo, mais metadados utilizados no protocolo de descarregamento.

```
VehicleRegistrationNumberRecordArray ::= SEQUENCE {
   recordType                            RecordType,
   recordSize                            INTEGER(1..65535),
   noOfRecords                           INTEGER(0..65535),
   records                               SET SIZE(noOfRecords) OF
                                         VehicleRegistrationNumber
}
```

recordType indica o tipo de registo (VehicleRegistrationNumber). **Valor atribuído**: ver RecordType

recordSize: tamanho do VehicleRegistrationNumber, em bytes.

noOfRecords: número de registos nos registos definidos.

records: conjunto de números de matrícula dos veículos.

2.169. **VuAbility**

Geração 2:

As informações memorizadas numa VU sobre a sua capacidade para utilizar ou não cartões tacográficos da geração 1 (requisito 121 do anexo 1C).

```
VuAbility ::= OCTET STRING (SIZE(1))
```

Valor atribuído — Alinhamento de octetos: ‘xxxxxxxa’B (8 bits)

Para a capacidade de suporte da geração 1:

‘a’B	Capacidade para aceitar cartões tacográficos da geração 1:
	‘0’B: geração 1 é compatível,
	‘1’B: geração 1 não é compatível,
‘xxxxxxx’B	RFU

▼B

2.170. **VuActivityDailyData**

Geração 1:

Informação memorizada numa VU e relativa a mudanças na atividade e/ou na situação da condução e/ou na situação do cartão num determinado dia (requisito 084 do anexo 1B e requisito 105, 106 e 107 do anexo 1C) e na situação das ranhuras às 00h00 desse dia.

```
VuActivityDailyData ::= SEQUENCE {
   noOfActivityChanges                  INTEGER SIZE(0..1440),
   activityChangeInfos                  SET SIZE(noOfActivityChanges) OF
                                        ActivityChangeInfo
}
```

noOfActivityChanges: número de palavras ActivityChangeInfo no conjunto activityChangeInfos.

activityChangeInfos: conjunto de palavras ActivityChangeInfo memorizadas na VU relativamente ao dia em questão. Inclui sempre duas palavras ActivityChangeInfo que dão a situação das duas ranhuras às 00h00 desse dia.

2.171. **VuActivityDailyRecordArray**

Geração 2:

Informação memorizada numa VU e relativa a mudanças na atividade e/ou na situação da condução e/ou na situação do cartão num determinado dia (requisito 105, 106 e 107 do anexo 1C) e na situação das ranhuras às 00h00 desse dia.

```
VuActivityDailyRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF ActivityChangeInfo
}
```

recordType indica o tipo de registo (ActivityChangeInfo). **Valor atribuído**: ver RecordType

recordSize: tamanho de ActivityChangeInfo, em bytes.

noOfRecords: número de registos nos registos definidos.

records: conjunto de palavras ActivityChangeInfo memorizadas na VU relativamente ao dia em questão. Inclui sempre duas palavras ActivityChangeInfo que dão a situação das duas ranhuras às 00h00 desse dia.

2.172. **VuApprovalNumber**

Número de homologação de tipo da unidade-veículo.

Geração 1:

```
VuApprovalNumber ::= IA5String(SIZE(8))
```

Valor atribuído: não especificado.

Geração 2:

```
VuApprovalNumber ::= IA5String(SIZE(16))
```

▼B

Valor atribuído:

O número de homologação deve ser apresentado conforme publicação no respetivo sítio Web da Comissão Europeia (por exemplo, incluindo eventuais hífenes). Deve estar alinhado à esquerda.

2.173. **VuCalibrationData**

Geração 1:

Informação memorizada numa VU e relativa às calibrações do aparelho de controlo (requisito 098 do anexo 1B).

```
VuCalibrationData ::= SEQUENCE {
   noOfVuCalibrationRecords              INTEGER(0..255),
   vuCalibrationRecords                  SET SIZE(noOfVuCalibrationRecords) OF
                                         VuCalibrationRecord
}
```

noOfVuCalibrationRecords é o número de registos contidos no conjunto vuCalibrationRecords.

vuCalibrationRecords é o conjunto de registos de calibração.

2.174. **VuCalibrationRecord**

Informação memorizada numa unidade-veículo e relativa à calibração do aparelho de controlo (requisito 098 do anexo 1B e requisitos 119 e 120 do anexo 1C).

Geração 1:

```
VuCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                    CalibrationPurpose,
   workshopName                          Name,
   workshopAddress                       Address,
   workshopCardNumber                    FullCardNumber,
   workshopCardExpiryDate                TimeReal,
   vehicleIdentificationNumber           VehicleIdentificationNumber,
   vehicleRegistrationIdentification     VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant        W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment         K-ConstantOfRecordingEquipment,
   lTyreCircumference                    L-TyreCircumference,
   tyreSize                              TyreSize,
   authorisedSpeed                       SpeedAuthorised,
   oldOdometerValue                      OdometerShort,
   newOdometerValue                      OdometerShort,
   oldTimeValue                          TimeReal,
   newTimeValue                          TimeReal,
   nextCalibrationDate                   TimeReal
}
```

calibrationPurpose é o objetivo da calibração.

workshopName, workshopAddress: nome e endereço da oficina.

workshopCardNumber identifica o cartão de oficina utilizado durante a calibração.

workshopCardExpiryDate: prazo de validade do cartão.

vehicleIdentificationNumber: VIN.

▼B

vehicleRegistrationIdentification contém o VRN e o Estado-Membro de matrícula.

wVehicleCharacteristicConstant: coeficiente característico do veículo.

kConstantOfRecordingEquipment: constante do aparelho de controlo.

lTyreCircumference: perímetro efetivo dos pneus das rodas.

tyreSize: designação das dimensões dos pneus montados no veículo

authorisedSpeed: velocidade autorizada para o veículo.

oldOdometerValue, newOdometerValue: valores antigo e novo do conta-quilómetros.

oldTimeValue, newTimeValue: valores antigo e novo da data e da hora.

nextCalibrationDate: data da próxima calibração do tipo especificado em CalibrationPurpose, a efetuar pela autoridade responsável pela inspeção.

Geração 2:

```
VuCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                    CalibrationPurpose,
   workshopName                          Name,
   workshopAddress                       Address,
   workshopCardNumber                    FullCardNumber,
   workshopCardExpiryDate                TimeReal,
   vehicleIdentificationNumber           VehicleIdentificationNumber,
   vehicleRegistrationIdentification     VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant        W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment         K-ConstantOfRecordingEquipment,
   lTyreCircumference                    L-TyreCircumference,
   tyreSize                              TyreSize,
   authorisedSpeed                       SpeedAuthorised,
   oldOdometerValue                      OdometerShort,
   newOdometerValue                      OdometerShort,
   oldTimeValue                          TimeReal,
   newTimeValue                          TimeReal,
   nextCalibrationDate                   TimeReal,
   sealDataVu                            SealDataVu
}
```

Utiliza-se o seguinte elemento de dados, além dos utilizados na geração 1:

sealDataVu: fornece informações sobre os selos ligados a diferentes componentes do veículo.

2.175. **VuCalibrationRecordArray**

Geração 2:

Informação memorizada numa VU e relativa às calibrações do aparelho de controlo (requisitos 119 e 120 do anexo 1C).

▼B

```
VuCalibrationRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuCalibrationRecord
}
```

recordType indica o tipo de registo (VuCalibrationRecord). **Valor atribuído**: ver RecordType

recordSize: tamanho do VuCalibrationRecord, em bytes.

noOfRecords: número de registos nos registos definidos.

records: conjunto de registos de calibração.

2.176. **VuCardIWData**

Geração 1:

Informação memorizada numa unidade-veículo e relativa aos ciclos de inserção e retirada de cartões de condutor ou de oficina nessa unidade-veículo (requisito 081 do anexo 1B e requisito 103 do anexo 1C).

```
VuCardIWData ::= SEQUENCE {
   noOfIWRecords                       INTEGER(0..2^16-1),
   vuCardIWRecords                     SET SIZE(noOfIWRecords) OF VuCardIWRecord
}
```

noOfIWRecords: número de registos no conjunto vuCardIWRecords.

vuCardIWRecords: conjunto de registos relativos aos ciclos de inserção e retirada de cartões.

2.177. **VuCardIWRecord**

Informação memorizada numa unidade-veículo e relativa a um ciclo de inserção e retirada de um cartão de condutor ou de oficina nessa VU (requisito 081 do anexo 1B e requisito 102 do anexo 1C).

Geração 1:

```
VuCardIWRecord ::= SEQUENCE {
   cardHolderName                      HolderName,
   fullCardNumber                      FullCardNumber,
   cardExpiryDate                      TimeReal,
   cardInsertionTime                   TimeReal,
   vehicleOdometerValueAtInsertion     OdometerShort,
   cardSlotNumber                      CardSlotNumber,
   cardWithdrawalTime                  TimeReal,
   vehicleOdometerValueAtWithdrawal    OdometerShort,
   previousVehicleInfo                 PreviousVehicleInfo,
   manualInputFlag                     ManualInputFlag
}
```

cardHolderName: apelido e nome próprio do titular do cartão de condutor ou de oficina, memorizados no mesmo.

fullCardNumber: tipo, Estado-Membro emissor e número do cartão, nele memorizados.

▼B

cardExpiryDate: prazo de validade do cartão, nele memorizado.

cardInsertionTime: data e hora a que o cartão foi inserido.

vehicleOdometerValueAtInsertion: valor no conta-quilómetros do veículo no momento da inserção do cartão.

cardSlotNumber: ranhura na qual o cartão é inserido.

cardWithdrawalTime: data e hora a que o cartão foi retirado.

vehicleOdometerValueAtWithdrawal: valor no conta-quilómetros do veículo no momento da retirada do cartão.

previousVehicleInfo contém informação, memorizada no cartão, acerca do anterior veículo utilizado pelo condutor.

manualInputFlag: marcador que identifica se o titular do cartão introduziu manualmente atividades de condutor no momento da inserção do cartão.

Geração 2:

```
VuCardIWRecord ::= SEQUENCE {
   cardHolderName                          HolderName,
   fullCardNumberAndGeneration             FullCardNumberAndGeneration,
   cardExpiryDate                          TimeReal,
   cardInsertionTime                       TimeReal,
   vehicleOdometerValueAtInsertion         OdometerShort,
   cardSlotNumber                          CardSlotNumber,
   cardWithdrawalTime                      TimeReal,
   vehicleOdometerValueAtWithdrawal        OdometerShort,
   previousVehicleInfo                     PreviousVehicleInfo,
   manualInputFlag                         ManualInputFlag
}
```

Em vez de fullCardNumber, a estrutura de dados da geração 2 recorre à sequência do elemento de dados.

fullCardNumberAndGeneration: tipo, Estado-Membro emissor, número e geração do cartão, nele memorizados.

2.178. **VuCardIWRecordArray**

Geração 2:

Informação memorizada numa unidade-veículo e relativa aos ciclos de inserção e retirada de cartões de condutor ou de oficina nessa VU (requisito 103 do anexo 1C).

```
VuCardIWRecordArray ::= SEQUENCE {
   recordType                              RecordType,
   recordSize                              INTEGER(1..65535),
   noOfRecords                             INTEGER(0..65535),
   records                                 SET SIZE(noOfRecords) OF VuCardIWRecord
}
```

recordType indica o tipo de registo (VuCardIWRecord). **Valor atribuído**: ver RecordType

recordSize: tamanho do VuCardIWRecord, em bytes.

▼B

noOfRecords: número de registos nos registos definidos.

records: conjunto de registos relativos aos ciclos de inserção e retirada de cartões.

2.179. **VuCardRecord**

Geração 2:

Informações memorizadas numa unidade-veículo sobre um cartão tacográfico utilizado (requisito 132 do anexo 1C).

```
VuCardRecord ::= SEQUENCE {
   cardExtendedSerialNumber            ExtendedSerialNumber,
   cardPersonaliserID                  OCTET STRING(SIZE(1)),
   typeofTachographCardID              EquipmentType,
   cardStructureVersion                CardStructureVersion,
   cardNumber                          CardNumber
}
```

cardExtendedSerialNumber lido no ficheiro EF_ICC sob o MF do cartão.

cardPersonaliserID lido no ficheiro EF_ICC sob o MF do cartão.

typeOfTachographCardId lido no ficheiro EF_Application_Identification sob o DF_Tachograph_G2

cardStructureVersion lido no ficheiro EF_Application_Identification sob o DF_Tachograph_G2.

cardNumber lido no ficheiro EF_Identification sob o DF_Tachograph_G2.

2.180. **VuCardRecordArray**

Geração 2:

Informações memorizadas numa unidade-veículo sobre os cartões tacográficos utilizados nesta VU. Estas informações destinam-se à análise de problemas com cartões na VU (requisito 132 do anexo 1C).

```
VuCardRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuCardRecord
}
```

recordType indica o tipo de registo (VuCardRecord). **Valor atribuído**: ver RecordType

recordSize: tamanho do VuCardRecord, em bytes.

noOfRecords: número de registos nos registos definidos.

records: conjunto de registos relacionados com os cartões tacográficos utilizados na VU.

▼B

2.181. **VuCertificate**

Certificado da chave pública de uma unidade-veículo.

```
VuCertificate ::= Certificate
```

2.182. **VuCertificateRecordArray**

Geração 2:

O certificado da VU, mais metadados utilizados no protocolo de descarregamento.

```
VuCertificateRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuCertificate
}
```

recordType indica o tipo de registo (VuCertificate). **Valor atribuído**: ver RecordType

recordSize: tamanho do VuCertificate, em bytes.

noOfRecords: número de registos nos registos definidos. O valor deve ser fixado em 1, dado que os certificados podem ter diferentes comprimentos.

records: conjunto de certificados da VU.

2.183. **VuCompanyLocksData**

Geração 1:

Informação memorizada numa unidade-veículo e relativa aos bloqueios de uma empresa (requisito 104 do anexo 1B).

```
VuCompanyLocksData ::= SEQUENCE {
   noOfLocks                           INTEGER(0..255),
   vuCompanyLocksRecords               SET SIZE(noOfLocks) OF VuCompanyLocksRecord
}
```

noOfLocks é o número de bloqueios que constam de VuCompanyLocksRecords.

vuCompanyLocksRecords é o conjunto de registos de bloqueios da empresa.

2.184. **VuCompanyLocksRecord**

Informação memorizada numa unidade-veículo e relativa aos bloqueios de uma empresa (requisito 104 do anexo 1B e requisito 128 do anexo 1C).

Geração 1:

```
VuCompanyLocksRecord ::= SEQUENCE {
   lockInTime                          TimeReal,
   lockOutTime                         TimeReal,
   companyName                         Name,
   companyAddress                      Address,
   companyCardNumber                   FullCardNumber
}
```

▼B

lockInTime, lockOutTime: data e hora de início do bloqueio e de cessação do bloqueio.

companyName, companyAddress: nome e endereço da empresa relacionada com o início do bloqueio.

companyCardNumber identifica o cartão utilizado no início do bloqueio.

Geração 2:

```
VuCompanyLocksRecord ::= SEQUENCE {
   lockInTime                          TimeReal,
   lockOutTime                         TimeReal,
   companyName                         Name,
   companyAddress                      Address,
   companyCardNumberAndGeneration      FullCardNumberAndGeneration
}
```

Em vez de companyCardNumber, a estrutura de dados da geração 2 recorre à sequência do elemento de dados.

companyCardNumberAndGeneration identifica o cartão (incluindo a sua geração) utilizado no início do bloqueio.

2.185. **VuCompanyLocksRecordArray**

Geração 2:

Informação memorizada numa unidade-veículo e relativa aos bloqueios de uma empresa (requisito 128 do anexo 1C).

```
VuCompanyLocksRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuCompanyLocksRecord
}
```

recordType indica o tipo de registo (VuCompanyLocksRecord). **Valor atribuído**: ver RecordType

recordSize: tamanho do VuCompanyLocksRecord, em bytes.

noOfRecords: número de registos nos registos definidos. Valor 0, ..., 255.

records: conjunto de registos de bloqueios da empresa.

2.186. **VuControlActivityData**

Geração 1:

Informação memorizada numa unidade-veículo e relativa aos controlos executados por meio da mesma (requisito 102 do anexo 1B).

```
VuControlActivityData ::= SEQUENCE {
   noOfControls                        INTEGER(0..20),
   vuControlActivityRecords            SET SIZE(noOfControls) OF
                                       VuControlActivityRecord
}
```

▼B

noOfControls é o número de controlos que constam de vuControlActivityRecords.

vuControlActivityRecords: conjunto de registos da atividade de controlo.

2.187. **VuControlActivityRecord**

Informação memorizada numa unidade-veículo e relativa aos controlos executados por meio da mesma (requisito 102 do anexo 1B e requisito 126 do anexo 1C).

Geração 1:

```
VuControlActivityRecord ::= SEQUENCE {
   controlType                          ControlType,
   controlTime                          TimeReal,
   controlCardNumber                    FullCardNumber,
   downloadPeriodBeginTime              TimeReal,
   downloadPeriodEndTime                TimeReal
}
```

controlType: tipo do controlo.

controlTime: data e hora do controlo.

controlCardNumber identifica o cartão de controlo utilizado para o controlo.

downloadPeriodBeginTime: hora de início do período de eventual descarregamento.

downloadPeriodEndTime: hora de final do período de eventual descarregamento.

Geração 2:

```
VuControlActivityRecord ::= SEQUENCE {
   controlType                          ControlType,
   controlTime                          TimeReal,
   controlCardNumberAndGeneration       FullCardNumberAndGeneration,
   downloadPeriodBeginTime              TimeReal,
   downloadPeriodEndTime                TimeReal
}
```

Em vez de controlCardNumber, a estrutura de dados da geração 2 recorre à sequência do elemento de dados.

controlCardNumberAndGeneration identifica o cartão de controlo (incluindo a sua geração) utilizado para o controlo.

2.188. **VuControlActivityRecordArray**

Geração 2:

Informação memorizada numa unidade-veículo e relativa aos controlos executados por meio da mesma (requisito 126 do anexo 1C).

▼B

```
VuControlActivityRecordArray ::= SEQUENCE {
   recordType                              RecordType,
   recordSize                              INTEGER(1..65535),
   noOfRecords                             INTEGER(0..65535),
   records                                 SET SIZE(noOfRecords) OF
                                           VuControlActivityRecord
}
```

recordType indica o tipo de registo (VuControlActivityRecord). **Valor atribuído**: ver RecordType

recordSize: tamanho do VuControlActivityRecord, em bytes.

noOfRecords: número de registos nos registos definidos.

records: conjunto de registos da atividade de controlo da VU.

2.189. **VuDataBlockCounter**

Contador memorizado num cartão e que identifica sequencialmente os ciclos de inserção e retirada desse cartão em unidades-veículo.

```
VuDataBlockCounter ::= BCDString(SIZE(2))
```

Valor atribuído: número consecutivo, com o valor máximo de 9 999 e a recomeçar em 0.

2.190. **VuDetailedSpeedBlock**

Informação memorizada numa unidade-veículo e relativa à velocidade detalhada do veículo num minuto durante o qual o mesmo esteve em movimento (requisito 093 do anexo 1B e requisito 116 do anexo 1C).

```
VuDetailedSpeedBlock ::= SEQUENCE {
   speedBlockBeginDate    TimeReal,
   speedsPerSecond        SEQUENCE SIZE(60) OF Speed
}
```

speedBlockBeginDate: data e hora do primeiro valor da velocidade no bloco.

speedsPerSecond: sequência cronológica de velocidades medidas em cada segundo, durante o minuto que começa em speedBlockBeginDate (inclusive).

2.191. **VuDetailedSpeedBlockRecordArray**

Geração 2:

Informação memorizada numa unidade-veículo e relativa à velocidade detalhada do veículo.

```
VuDetailedSpeedBlockRecordArray ::= SEQUENCE {
   recordType                              RecordType,
   recordSize                              INTEGER(1..65535),
   noOfRecords                             INTEGER(0..65535),
   records                                 SET SIZE(noOfRecords) OF
                                           VuDetailedSpeedBlock
}
```

recordType indica o tipo de registo (VuDetailedSpeedBlock). **Valor atribuído**: ver RecordType

▼B

recordSize: tamanho do VuDetailedSpeedBlock, em bytes.

noOfRecords: número de registos nos registos definidos.

records: conjunto de blocos de velocidade detalhada.

2.192. **VuDetailedSpeedData**

Geração 1:

Informação memorizada numa unidade-veículo e relativa à velocidade detalhada do veículo.

```
VuDetailedSpeedData ::= SEQUENCE {
   noOfSpeedBlocks                    INTEGER(0..2^16-1),
   vuDetailedSpeedBlocks              SET SIZE(noOfSpeedBlocks) OF
                                      VuDetailedSpeedBlock
}
```

noOfSpeedBlocks: número de blocos de velocidade no conjunto vuDetailedSpeedBlocks.

vuDetailedSpeedBlocks: conjunto de blocos de velocidade detalhada.

2.193. **VuDownloadablePeriod**

Datas mais antiga e mais recente relativamente às quais uma unidade-veículo detém dados referentes às atividades dos condutores (requisitos 081, 084 ou 087 do anexo 1B e requisitos 102, 105 e 108 do anexo 1C).

```
VuDownloadablePeriod ::= SEQUENCE {
   minDownloadableTime                TimeReal
   maxDownloadableTime                TimeReal
}
```

minDownloadableTime é a mais antiga data e hora de inserção do cartão, de mudança de atividade ou de entrada de um local, memorizada na VU.

maxDownloadableTime é a mais recente data e hora de retirada do cartão, de mudança de atividade ou de entrada de um local, memorizada na VU.

2.194. **VuDownloadablePeriodRecordArray**

Geração 2:

O VUDownloadablePeriod, mais metadados utilizados no protocolo de descarregamento.

```
VuDownloadablePeriodRecordArray ::= SEQUENCE {
   recordType                         RecordType,
   recordSize                         INTEGER(1..65535),
   noOfRecords                        INTEGER(0..65535),
   records                            SET SIZE(noOfRecords) OF
                                      VuDownloadablePeriod
}
```

recordType indica o tipo de registo (VuDownloadablePeriod). **Valor atribuído**: ver RecordType

▼B

recordSize: tamanho do VuDownloadablePeriod, em bytes.

noOfRecords: número de registos nos registos definidos.

records: conjunto dos registos VuDownloadablePeriod.

2.195. **VuDownloadActivityData**

Informação memorizada numa unidade-veículo e relativa ao seu último descarregamento (requisito 105 do anexo 1B e requisito 129 do anexo 1C).

Geração 1:

```
VuDownloadActivityData ::= SEQUENCE {
   downloadingTime                    TimeReal,
   fullCardNumber                     FullCardNumber,
   companyOrWorkshopName              Name
}
```

downloadingTime: data e hora do descarregamento.

fullCardNumber identifica o cartão utilizado para autorizar o descarregamento.

companyOrWorkshopName: nome da empresa ou da oficina.

Geração 2:

```
VuDownloadActivityData ::= SEQUENCE {
   downloadingTime                    TimeReal,
   fullCardNumberAndGeneration        FullCardNumberAndGeneration,
   companyOrWorkshopName              Name
}
```

Em vez de fullCardNumber, a estrutura de dados da geração 2 recorre à sequência do elemento de dados.

fullCardNumberAndGeneration identifica o cartão (incluindo a sua geração) utilizado para autorizar o descarregamento.

2.196. **VuDownloadActivityDataRecordArray**

Geração 2:

Informações relacionadas com o último descarregamento da VU (requisito 129 do anexo 1C).

```
VuDownloadActivityDataRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuDownloadActivityData
}
```

recordType indica o tipo de registo (VuDownloadActivityData). **Valor atribuído**: ver RecordType

recordSize: tamanho do VuDownloadActivityData, em bytes.

noOfRecords: número de registos nos registos definidos.

▼B

records: conjunto de registos de descarregamento dos dados da atividade.

2.197. **VuEventData**

Geração 1:

Informação memorizada numa unidade-veículo e relativa aos incidentes (requisito 094 do anexo 1B, com exceção do incidente de excesso de velocidade).

```
VuEventData ::= SEQUENCE {
   noOfVuEvents                          INTEGER(0..255),
   vuEventRecords                        SET SIZE(noOfVuEvents) OF VuEventRecord
}
```

noOfVuEvents: número de incidentes que constam do conjunto vuEventRecords.

vuEventRecords: conjunto de registos de incidentes.

2.198. **VuEventRecord**

Informação memorizada numa unidade-veículo e relativa a um incidente (requisito 094 do anexo 1B e requisito 117 do anexo 1C, com exceção do incidente de excesso de velocidade).

Geração 1:

```
VuEventRecord ::= SEQUENCE {
   eventType                             EventFaultType,
   eventRecordPurpose                    EventFaultRecordPurpose,
   eventBeginTime                        TimeReal,
   eventEndTime                          TimeReal,
   cardNumberDriverSlotBegin             FullCardNumber,
   cardNumberCodriverSlotBegin           FullCardNumber,
   cardNumberDriverSlotEnd               FullCardNumber,
   cardNumberCodriverSlotEnd             FullCardNumber,
   similarEventsNumber                   SimilarEventsNumber
}
```

eventType: tipo de incidente.

eventRecordPurpose: objetivo pelo qual este incidente foi registado.

eventBeginTime: data e hora de início do incidente.

eventEndTime: data e hora de cessação do incidente.

cardNumberDriverSlotBegin identifica o cartão que se encontrava inserido na ranhura do condutor no momento em que o incidente teve início.

cardNumberCodriverSlotBegin identifica o cartão que se encontrava inserido na ranhura do ajudante no momento em que o incidente teve início.

cardNumberDriverSlotEnd identifica o cartão que se encontrava inserido na ranhura do condutor no momento em que terminou o incidente.

cardNumberCodriverSlotEnd identifica o cartão que se encontrava inserido na ranhura do ajudante no momento em que terminou o incidente.

similarEventsNumber: número de incidentes similares no dia em questão.

Esta sequência pode ser utilizada para quaisquer incidentes, com exceção dos incidentes de excesso de velocidade.

▼B

Geração 2:

```
VuEventRecord ::= SEQUENCE {
   eventType                              EventFaultType,
   eventRecordPurpose                     EventFaultRecordPurpose,
   eventBeginTime                         TimeReal,
   eventEndTime                           TimeReal,
   cardNumberAndGenDriverSlotBegin        FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin      FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd          FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd        FullCardNumberAndGeneration,
   similarEventsNumber                    SimilarEventsNumber,
   manufacturerSpecificEventFaultData   ManufacturerSpecificEventFaultData
}
```

Utilizam-se os seguintes elementos de dados, além dos utilizados na geração 1:

manufacturerSpecificEventFaultData contém informações adicionais, específicas do fabricante sobre o incidente.

Em vez de cardNumberDriverSlotBegin, cardNumberCodriverSlotBegin, cardNumberDriverSlotEnd e cardNumberCodriverSlotEnd, a estrutura de dados da geração 2 recorre aos seguintes elementos de dados:

cardNumberAndGenDriverSlotBegin identifica o cartão (incluindo a sua geração) que se encontrava inserido na ranhura do condutor no momento em que o incidente teve início.

cardNumberAndGenCodriverSlotBegin identifica o cartão (incluindo a sua geração) que se encontrava inserido na ranhura do ajudante no momento em que o incidente teve início.

cardNumberAndGenDriverSlotEnd identifica o cartão (incluindo a sua geração) que se encontrava inserido na ranhura do condutor no momento em que o incidente terminou.

cardNumberAndGenCodriverSlotEnd identifica o cartão (incluindo a sua geração) que se encontrava inserido na ranhura do ajudante no momento em que o incidente terminou.

Se o incidente for um conflito de tempo, eventBeginTime e eventEndTime interpretam-se da seguinte forma:

eventBeginTime: data e hora do aparelho de controlo.

eventEndTime: data e hora do GNSS.

2.199. **VuEventRecordArray**

Geração 2:

Informação memorizada numa unidade-veículo e relativa aos incidentes (requisito 117 do anexo 1C, com exceção do incidente de excesso de velocidade).

```
VuEventRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuEventRecord
}
```

recordType indica o tipo de registo (VuEventRecord). **Valor atribuído**: ver RecordType

▼B

recordSize: tamanho do VuEventRecord, em bytes.

noOfRecords: número de registos nos registos definidos.

records: conjunto de registos de incidentes.

2.200. **VuFaultData**

Geração 1:

Informação memorizada numa unidade-veículo e relativa às falhas (requisito 096 do anexo 1B).

```
VuFaultData ::= SEQUENCE {
   noOfVuFaults                         INTEGER(0..255),
   vuFaultRecords                       SET SIZE(noOfVuFaults) OF VuFaultRecord
}
```

noOfVuFaults: número de falhas que constam do conjunto vuFaultRecords.

vuFaultRecords: conjunto de registos de falhas.

2.201. **VuFaultRecord**

Informação memorizada numa unidade-veículo e relativa a uma falha (requisito 096 do anexo 1B e requisito 118 do anexo 1C).

Geração 1:

```
VuFaultRecord ::= SEQUENCE {
   faultType                            EventFaultType,
   faultRecordPurpose                   EventFaultRecordPurpose,
   faultBeginTime                       TimeReal,
   faultEndTime                         TimeReal,
   cardNumberDriverSlotBegin            FullCardNumber,
   cardNumberCodriverSlotBegin          FullCardNumber,
   cardNumberDriverSlotEnd              FullCardNumber,
   cardNumberCodriverSlotEnd            FullCardNumber
}
```

faultType: tipo de falha no aparelho de controlo.

faultRecordPurpose: objetivo pelo qual esta falha foi registada.

faultBeginTime: data e hora de início da falha.

faultEndTime: data e hora de cessação da falha.

cardNumberDriverSlotBegin identifica o cartão que se encontrava inserido na ranhura do condutor no momento em que a falha teve início.

cardNumberCodriverSlotBegin identifica o cartão que se encontrava inserido na ranhura do ajudante no momento em que a falha teve início.

cardNumberDriverSlotEnd identifica o cartão que se encontrava inserido na ranhura do condutor no momento em que a falha terminou.

cardNumberCodriverSlotEnd identifica o cartão que se encontrava inserido na ranhura do ajudante no momento em que a falha terminou.

▼B

Geração 2:

```
VuFaultRecord ::= SEQUENCE {
   faultType                              EventFaultType,
   faultRecordPurpose                     EventFaultRecordPurpose,
   faultBeginTime                         TimeReal,
   faultEndTime                           TimeReal,
   cardNumberAndGenDriverSlotBegin        FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin      FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd          FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd        FullCardNumberAndGeneration,
   manufacturerSpecificEventFaultData   ManufacturerSpecificEventFaultData
}
```

Utiliza-se o seguinte elemento de dados, além dos utilizados na geração 1:

manufacturerSpecificEventFaultData contém informações adicionais, específicas do fabricante sobre a falha.

Em vez de cardNumberDriverSlotBegin, cardNumberCodriverSlotBegin, cardNumberDriverSlotEnd e cardNumberCodriverSlotEnd, a estrutura de dados da geração 2 recorre aos seguintes elementos de dados:

cardNumberAndGenDriverSlotBegin identifica o cartão (incluindo a sua geração) que se encontrava inserido na ranhura do condutor no momento em que a falha teve início.

cardNumberAndGenCodriverSlotBegin identifica o cartão (incluindo a sua geração) que se encontrava inserido na ranhura do ajudante no momento em que a falha teve início.

cardNumberAndGenDriverSlotEnd identifica o cartão (incluindo a sua geração), que se encontrava inserido na ranhura do condutor no momento em que a falha terminou.

cardNumberAndGenCodriverSlotEnd identifica o cartão (incluindo a sua geração) que se encontrava inserido na ranhura do ajudante no momento em que a falha terminou.

2.202. **VuFaultRecordArray**

Geração 2:

Informação memorizada numa unidade-veículo e relativa às falhas (requisito 118 do anexo 1C).

```
VuFaultRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuFaultRecord
}
```

recordType indica o tipo de registo (VuFaultRecord). **Valor atribuído**: ver RecordType

recordSize: tamanho do VuFaultRecord, em bytes.

noOfRecords: número de registos nos registos definidos.

records: conjunto de registos da falhas.

▼B

2.203. **VuGNSSCDRecord**

Geração 2:

Informação memorizada numa unidade-veículo e relativa à posição GNSS do veículo, se o tempo de condução contínua do condutor atingir um múltiplo de três horas (requisitos 108 e 110 do anexo 1C).

```
VuGNSSCDRecord ::= SEQUENCE {
   timeStamp                              TimeReal,
   cardNumberAndGenDriverSlot             FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlot           FullCardNumberAndGeneration,
   gnssPlaceRecord                        GNSSPlaceRecord
}
```

timeStamp: data e hora em que o tempo de condução contínua do titular do cartão atinge um múltiplo de três horas.

cardNumberAndGenDriverSlot identifica o cartão (incluindo a sua geração) que se encontrava inserido na ranhura do condutor.

cardNumberAndGenCodriverSlot identifica o cartão (incluindo a sua geração) que se encontrava inserido na ranhura do ajudante.

gnssPlaceRecord contém informação relacionada com a posição do veículo.

2.204. **VuGNSSCDRecordArray**

Geração 2:

Informação memorizada numa unidade-veículo e relativa à posição GNSS do veículo, se o tempo de condução contínua do condutor atingir um múltiplo de três horas (requisitos 108 e 110 do anexo 1C).

```
VuGNSSCDRecordArray  ::= SEQUENCE {
   recordType                             RecordType,
   recordSize                             INTEGER(1..65535),
   noOfRecords                            INTEGER(0..65535),
   records                                SET SIZE(noOfRecords) OF VuGNSSCDRecord
}
```

recordType indica o tipo de registo (VuGNSSCDRecord). **Valor atribuído**: ver RecordType

recordSize: tamanho do VuGNSSCDRecord, em bytes.

noOfRecords: número de registos nos registos definidos.

records: conjunto de registos GNSS da condução contínua.

2.205. **VuIdentification**

Informação memorizada numa unidade-veículo e relativa à identificação da mesma (requisito 075 do anexo 1B e requisitos 93 e 121 do anexo 1C).

▼B

Geração 1:

```
VuIdentification ::= SEQUENCE {
   vuManufacturerName                    VuManufacturerName,
   vuManufacturerAddress                 VuManufacturerAddress,
   vuPartNumber                          VuPartNumber,
   vuSerialNumber                        VuSerialNumber,
   vuSoftwareIdentification              VuSoftwareIdentification,
   vuManufacturingDate                   VuManufacturingDate,
   vuApprovalNumber                      VuApprovalNumber
}
```

vuManufacturerName: nome do fabricante da unidade-veículo.

vuManufacturerAddress: endereço do fabricante da unidade-veículo.

vuPartNumber: número de peça da unidade-veículo.

vuSerialNumber: número de série da unidade-veículo.

vuSoftwareIdentification identifica o *software* implantado na unidade-veículo.

vuManufacturingDate: data de fabrico da unidade-veículo.

vuApprovalNumber: número de homologação de tipo da unidade-veículo.

Geração 2:

```
VuIdentification ::= SEQUENCE {
   vuManufacturerName                    VuManufacturerName,
   vuManufacturerAddress                 VuManufacturerAddress,
   vuPartNumber                          VuPartNumber,
   vuSerialNumber                        VuSerialNumber,
   vuSoftwareIdentification              VuSoftwareIdentification,
   vuManufacturingDate                   VuManufacturingDate,
   vuApprovalNumber                      VuApprovalNumber,
   vuGeneration                          Generation,
   vuAbility                             VuAbility
}
```

Utilizam-se os seguintes elementos de dados, além dos utilizados na geração 1:

vuGeneration identifica a geração da unidade-veículo.

vuAbility fornece informações sobre se a VU aceita cartões tacográficos da geração 1 ou não.

2.206. **VuIdentificationRecordArray**

Geração 2:

A VuIdentification, mais metadados utilizados no protocolo de descarregamento.

▼B

```
VuIdentificationRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuIdentification
}
```

recordType indica o tipo de registo (VuIdentification). **Valor atribuído**: ver RecordType

recordSize: tamanho do VuIdentification, em bytes.

noOfRecords: número de registos nos registos definidos.

records: conjunto de registos VuIdentification.

2.207. **VuITSConsentRecord**

Geração 2:

Informações memorizadas numa unidade-veículo e relativas ao consentimento de um condutor para a utilização de sistemas de transporte inteligentes.

```
VuITSConsentRecord ::= SEQUENCE {
   cardNumberAndGen                    FullCardNumberAndGeneration,
   consent                             BOOLEAN
}
```

cardNumberAndGen identifica o cartão, incluindo a sua geração. O cartão deve ser de condutor ou de oficina.

consent: marcador que indica se o condutor deu o seu consentimento para a utilização de sistemas de transporte inteligentes neste veículo/unidade-veículo.

Valor atribuído:

TRUE	indica o consentimento do condutor para a utilização de sistemas de transporte inteligentes.
FALSE	indica a recusa do condutor em utilizar sistemas de transporte inteligentes.

2.208. **VuITSConsentRecordArray**

Geração 2:

Informações memorizadas numa unidade-veículo e relativas ao consentimento do condutor para a utilização de sistemas de transporte inteligentes (requisito 200 do anexo 1C).

```
VuITSConsentRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF VuITSConsentRecord
}
```

recordType indica o tipo de registo (VuITSConsentRecord). **Valor atribuído**: ver RecordType

recordSize: tamanho do VuITSConsentRecord, em bytes.

noOfRecords: número de registos nos registos definidos.

records: conjunto de registos de consentimento de ITS.

▼B

2.209. **VuManufacturerAddress**

Endereço do fabricante da unidade-veículo.

```
VuManufacturerAddress ::= Address
```

Valor atribuído: não especificado.

2.210. **VuManufacturerName**

Nome do fabricante da unidade-veículo.

```
VuManufacturerName ::= Name
```

Valor atribuído: não especificado.

2.211. **VuManufacturingDate**

Data de fabrico da unidade-veículo.

```
VuManufacturingDate ::= TimeReal
```

Valor atribuído: não especificado.

2.212. **VuOverSpeedingControlData**

Informação memorizada numa unidade-veículo e relativa a incidentes de excesso de velocidade desde o último controlo (requisito 095 do anexo 1B e requisito 117 do anexo 1C).

```
VuOverSpeedingControlData ::= SEQUENCE {
   lastOverspeedControlTime             TimeReal,
   firstOverspeedSince                  TimeReal,
   numberOfOverspeedSince               OverspeedNumber
}
```

lastOverspeedControlTime: data e hora do último controlo do excesso de velocidade.

firstOverspeedSince: data e hora do primeiro excesso de velocidade desde aquele controlo.

numberOfOverspeedSince: número de incidentes de excesso de velocidade desde o último controlo do excesso de velocidade.

2.213. **VuOverSpeedingControlDataRecordArray**

Geração 2:

O VuOverSpeedingControlData, mais metadados utilizados no protocolo de descarregamento.

```
VuOverSpeedingControlDataRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        VuOverSpeedingControlData
}
```

▼B

recordType indica o tipo de registo (VuOverSpeedingControlData). **Valor atribuído**: ver RecordType

recordSize: tamanho do VuOverSpeedingControlData, em bytes.

noOfRecords: número de registos nos registos definidos.

records: conjunto dos registos de dados do controlo do excesso de velocidade.

2.214. **VuOverSpeedingEventData**

Geração 1:

Informação memorizada numa unidade-veículo e relativa a incidentes de excesso de velocidade (requisito 094 do anexo 1B).

```
VuOverSpeedingEventData ::= SEQUENCE {
   noOfVuOverSpeedingEvents              INTEGER(0..255),
   vuOverSpeedingEventRecords            SET SIZE(noOfVuOverSpeedingEvents) OF
                                         VuOverSpeedingEventRecord
}
```

noOfVuOverSpeedingEvents: número de incidentes que constam do conjunto vuOverSpeedingEventRecords.

vuOverSpeedingEventRecords: conjunto de registos de incidentes de excesso de velocidade.

2.215. **VuOverSpeedingEventRecord**

▼C2

Geração 1:

Informação memorizada numa unidade-veículo e relativa a incidentes de excesso de velocidade (requisito 094 do anexo 1B e requisito 117 do anexo 1C).

```
VuOverSpeedingEventRecord::= SEQUENCE {
   eventType                             EventFaultType,
   eventRecordPurpose                    EventFaultRecordPurpose,
   eventBeginTime                        TimeReal,
   eventEndTime                          TimeReal,
   maxSpeedValue                         SpeedMax,
   averageSpeedValue                     SpeedAverage,
   cardNumberDriverSlotBegin             FullCardNumber,
   similarEventsNumber                   SimilarEventsNumber
}
```

eventType: tipo de incidente.

eventRecordPurpose: objetivo pelo qual este incidente foi registado.

eventBeginTime: data e hora de início do incidente.

eventEndTime: data e hora de cessação do incidente.

maxSpeedValue: velocidade máxima medida durante o incidente.

averageSpeedValue: média aritmética da velocidade medida durante o incidente.

▼C2

cardNumberDriverSlotBegin: identifica o cartão que se encontrava inserido na ranhura do condutor no momento em que o incidente teve início.

similarEventsNumber: número de incidentes similares no dia em questão.

Geração 2:

Informação memorizada numa unidade-veículo e relativa a incidentes de excesso de velocidade (requisito 094 do anexo 1B e requisito 117 do anexo 1C).

```
VuOverSpeedingEventRecord::= SEQUENCE {
   eventType                              EventFaultType,
   eventRecordPurpose                     EventFaultRecordPurpose,
   eventBeginTime                         TimeReal,
   eventEndTime                           TimeReal,
   maxSpeedValue                          SpeedMax,
   averageSpeedValue                      SpeedAverage,
   cardNumberAndGenDriverSlotBegin        FullCardNumberAndGeneration,
   similarEventsNumber                    SimilarEventsNumber
}
```

Em vez de cardNumberDriverSlotBegin, a estrutura de dados da geração 2 recorre ao seguinte elemento de dados:

cardNumberAndGenDriverSlotBegin: identifica o cartão, incluindo a respetiva geração, que está inserido na ranhura do condutor no início do incidente.

▼B

2.216. **VuOverSpeedingEventRecordArray**

Geração 2:

Informação memorizada numa unidade-veículo e relativa a incidentes de excesso de velocidade (requisito 117 do anexo 1C).

```
VuOverSpeedingEventRecordArray ::= SEQUENCE {
   recordType                             RecordType,
   recordSize                             INTEGER(1..65535),
   noOfRecords                            INTEGER(0..65535),
   records                                SET SIZE(noOfRecords) OF
                                          VuOverSpeedingEventRecord
}
```

recordType indica o tipo de registo (VuOverSpeedingEventRecord).
Valor atribuído: ver RecordType

recordSize: tamanho do VuOverSpeedingEventRecord, em bytes.

noOfRecords: número de registos nos registos definidos.

records: conjunto de registos de incidentes de excesso de velocidade.

2.217. **VuPartNumber**

Número de peça da unidade-veículo.

```
VuPartNumber ::= IA5String(SIZE(16))
```

Valor atribuído: específico do fabricante da VU.

▼B

2.218. **VuPlaceDailyWorkPeriodData**

Geração 1:

Informação memorizada numa unidade-veículo e relativa aos locais onde os condutores iniciam ou terminam um período de trabalho diário (requisito 087 do anexo 1B e requisitos 108 e 110 do anexo 1C).

```
VuPlaceDailyWorkPeriodData ::= SEQUENCE {
   noOfPlaceRecords                    INTEGER(0..255),
   vuPlaceDailyWorkPeriodRecords       SET SIZE(noOfPlaceRecords) OF
                                       VuPlaceDailyWorkPeriodRecord
}
```

noOfPlaceRecords é o número de registos que constam do conjunto vuPlaceDailyWorkPeriodRecords.

vuPlaceDailyWorkPeriodRecords: conjunto de registos relativos à localização.

2.219. **VuPlaceDailyWorkPeriodRecord**

Geração 1:

Informação memorizada numa unidade-veículo e relativa a um local onde um condutor inicia ou termina um período de trabalho diário (requisito 087 do anexo 1B e requisitos 108 e 110 do anexo 1C).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
   fullCardNumber                      FullCardNumber,
   placeRecord                         PlaceRecord
}
```

fullCardNumber: tipo, Estado-Membro emissor e número do cartão do condutor.

placeRecord contém a informação relativa ao local introduzido.

Geração 2:

Informação memorizada numa unidade-veículo e relativa a um local onde um condutor inicia ou termina um período de trabalho diário (requisito 087 do anexo 1B e requisitos 108 e 110 do anexo 1C).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {
   fullCardNumberAndGeneration         FullCardNumberAndGeneration,
   placeRecord                         PlaceRecord
}
```

Em vez de fullCardNumber, a estrutura de dados da geração 2 recorre ao seguinte elemento de dados:

fullCardNumberAndGeneration: tipo, Estado-Membro emissor, número e geração do cartão, nele memorizados.

▼B

2.220. **VuPlaceDailyWorkPeriodRecordArray**

Geração 2:

Informação memorizada numa unidade-veículo e relativa aos locais onde os condutores iniciam ou terminam um período de trabalho diário (requisitos 108 e 110 do anexo 1C).

```
VuPlaceDailyWorkPeriodRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuPlaceDailyWorkPeriodRecord
}
```

recordType indica o tipo de registo (VuPlaceDailyWorkPeriodRecord).
Valor atribuído: ver RecordType

recordSize: tamanho do VuPlaceDailyWorkPeriodRecord, em bytes.

noOfRecords: número de registos nos registos definidos.

records: conjunto de registos relativos à localização.

2.221. **VuPrivateKey**

Geração 1:

A chave privada de uma unidade-veículo.

```
VuPrivateKey ::= RSAKeyPrivateExponent
```

2.222. **VuPublicKey**

Geração 1:

A chave pública de uma unidade-veículo.

```
VuPublicKey ::= PublicKey
```

2.223. **VuSerialNumber**

O número de série da unidade-veículo (requisito 075 do anexo 1B e requisito 93 do anexo 1C).

```
VuSerialNumber ::= ExtendedSerialNumber
```

2.224. **VuSoftInstallationDate**

Data de instalação da versão de *software* na unidade-veículo.

```
VuSoftInstallationDate ::= TimeReal
```

Valor atribuído: não especificado.

▼B

2.225. **VuSoftwareIdentification**

Informação memorizada numa unidade-veículo e relativa ao *software* nela instalado.

```
VuSoftwareIdentification ::= SEQUENCE {
   vuSoftwareVersion                    VuSoftwareVersion,
   vuSoftInstallationDate               VuSoftInstallationDate
}
```

vuSoftwareVersion: número da versão do *software* da unidade-veículo.

vuSoftInstallationDate: data de instalação da versão de *software*.

2.226. **VuSoftwareVersion**

Número da versão de *software* da unidade-veículo.

```
VuSoftwareVersion ::= IA5String(SIZE(4))
```

Valor atribuído: não especificado.

2.227. **VuSpecificConditionData**

Geração 1:

Informação memorizada numa unidade-veículo e relativa às condições especiais.

```
VuSpecificConditionData ::= SEQUENCE {
   noOfSpecificConditionRecords         INTEGER(0..2^16-1)
   specificConditionRecords             SET SIZE (noOfSpecificConditionRecords) OF
                                        SpecificConditionRecord
}
```

noOfSpecificConditionRecords: número de registos que constam do conjunto specificConditionRecords.

specificConditionRecords: conjunto de registos relativos às condições especiais.

2.228. **VuSpecificConditionRecordArray**

Geração 2:

Informação memorizada numa unidade-veículo e relativa às condições especiais (requisito 130 do anexo 1C).

```
VuSpecificConditionRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        SpecificConditionRecord
}
```

recordType indica o tipo de registo (SpecificConditionRecord). **Valor atribuído**: ver RecordType

recordSize: tamanho do SpecificConditionRecord, em bytes.

noOfRecords: número de registos nos registos definidos.

records: conjunto de registos relativos às condições especiais.

▼B

2.229. **VuTimeAdjustmentData**

Geração 1:

Informação memorizada numa unidade-veículo e relativa aos ajustamentos do tempo executados fora do âmbito de uma calibração regular (requisito 101 do anexo 1B).

```
VuTimeAdjustmentData ::= SEQUENCE {
   noOfVuTimeAdjRecords                    INTEGER(0..6),
   vuTimeAdjustmentRecords                 SET SIZE(noOfVuTimeAdjRecords) OF
                                           VuTimeAdjustmentRecord
}
```

noOfVuTimeAdjRecords: número de registos em vuTimeAdjustmentRecords**.**

vuTimeAdjustmentRecords: conjunto de registos de ajustamento do tempo.

2.230. **VuTimeAdjustmentGNSSRecord**

Geração 2:

Informações memorizadas numa unidade-veículo e relativas a um ajustamento do tempo com base nos dados do tempo do GNSS (requisitos 124 e 125 do anexo 1C).

```
VuTimeAdjustmentGNSSRecord ::= SEQUENCE {
   oldTimeValue                            TimeReal,
   newTimeValue                            TimeReal
}
```

oldTimeValue e **newTimeValue**: valores antigo e novo da data e da hora.

2.231. **VuTimeAdjustmentGNSSRecordArray**

Geração 2:

Informações memorizadas numa unidade-veículo e relativas a um ajustamento do tempo com base nos dados do tempo provenientes de GNSS (requisitos 124 e 125 do anexo 1C).

```
VuTimeAdjustmentGNSSRecordArray ::= SEQUENCE {
   recordType                              RecordType,
   recordSize                              INTEGER(1..65535),
   noOfRecords                             INTEGER(0..65535),
   records                                 SET SIZE(noOfRecords) OF
                                           VuTimeAdjustmentGNSSRecord
}
```

recordType indica o tipo de registo (VuTimeAdjustmentGNSSRecord).
Valor atribuído: ver RecordType

recordSize: tamanho do VuTimeAdjustmentGNSSRecord, em bytes.

noOfRecords: número de registos nos registos definidos.

records: conjunto de registos GNSS de ajustamento do tempo.

▼B

2.232. **VuTimeAdjustmentRecord**

Informação memorizada numa unidade-veículo e relativa a um ajustamento do tempo executado fora do âmbito de uma calibração regular (requisito 101 do anexo 1B e requisitos 124 e 125 do anexo 1C).

Geração 1:

```
VuTimeAdjustmentRecord ::= SEQUENCE {
   oldTimeValue                         TimeReal,
   newTimeValue                         TimeReal,
   workshopName                         Name,
   workshopAddress                      Address,
   workshopCardNumber                   FullCardNumber
}
```

oldTimeValue e **newTimeValue**: valores antigo e novo da data e da hora.

workshopName e **workshopAddress**: nome e endereço da oficina.

workshopCardNumber identifica o cartão de oficina utilizado para efetuar o ajustamento do tempo.

Geração 2:

```
VuTimeAdjustmentRecord ::= SEQUENCE {
   oldTimeValue                         TimeReal,
   newTimeValue                         TimeReal,
   workshopName                         Name,
   workshopAddress                      Address,
   workshopCardNumberAndGeneration      FullCardNumberAndGeneration
}
```

Em vez de workshopCardNumber, a estrutura de dados da geração 2 recorre à sequência do elemento de dados.

workshopCardNumberAndGeneration identifica o cartão de oficina (incluindo a sua geração) utilizado para executar o ajustamento do tempo.

2.233. **VuTimeAdjustmentRecordArray**

Geração 2:

Informação memorizada numa unidade-veículo e relativa aos ajustamentos do tempo executados fora do âmbito de uma calibração regular (requisitos 124 e 125 do anexo 1C).

```
VuTimeAdjustmentRecordArray ::= SEQUENCE {
   recordType                           RecordType,
   recordSize                           INTEGER(1..65535),
   noOfRecords                          INTEGER(0..65535),
   records                              SET SIZE(noOfRecords) OF
                                        VuTimeAdjustmentRecord
}
```

recordType indica o tipo de registo (VuTimeAdjustmentRecord). **Valor atribuído**: ver RecordType

recordSize: tamanho do VuTimeAdjustmentRecord, em bytes.

▼B

noOfRecords: número de registos nos registos definidos.

records: conjunto de registos do ajustamento do tempo.

2.234. **WorkshopCardApplicationIdentification**

Informação memorizada num cartão de oficina e relativa à identificação da aplicação do cartão (requisitos 307 e 330 do anexo 1C).

Geração 1:

```
WorkshopCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId               EquipmentType,
   cardStructureVersion                 CardStructureVersion,
   noOfEventsPerType                    NoOfEventsPerType,
   noOfFaultsPerType                    NoOfFaultsPerType,
   activityStructureLength              CardActivityLengthRange,
   noOfCardVehicleRecords               NoOfCardVehicleRecords,
   noOfCardPlaceRecords                 NoOfCardPlaceRecords,
   noOfCalibrationRecords               NoOfCalibrationRecords
}
```

typeOfTachographCardId especifica o tipo de cartão aplicado.

cardStructureVersion especifica a versão da estrutura aplicada no cartão.

noOfEventsPerType: número de incidentes, por tipo, que o cartão pode registar.

noOfFaultsPerType: número de falhas, por tipo, que o cartão pode registar.

activityStructureLength indica o número de bytes disponíveis para memorizar registos de atividade.

noOfCardVehicleRecords: número de registos de veículo que o cartão pode conter.

noOfCardPlaceRecords: número de locais que o cartão pode registar.

noOfCalibrationRecords: número de registos de calibração que o cartão pode memorizar.

Geração 2:

```
WorkshopCardApplicationIdentification ::= SEQUENCE {
   typeOfTachographCardId               EquipmentType,
   cardStructureVersion                 CardStructureVersion,
   noOfEventsPerType                    NoOfEventsPerType,
   noOfFaultsPerType                    NoOfFaultsPerType,
   activityStructureLength              CardActivityLengthRange,
   noOfCardVehicleRecords               NoOfCardVehicleRecords,
   noOfCardPlaceRecords                 NoOfCardPlaceRecords,
   noOfCalibrationRecords               NoOfCalibrationRecords,
   noOfGNSSCDRecords                    NoOfGNSSCDRecords,
   noOfSpecificConditionRecords         NoOfSpecificConditionRecords
}
```

Utilizam-se os seguintes elementos de dados, além dos utilizados na geração 1:

noOfGNSSCDRecords: número de registos GNSS de condução contínua que o cartão pode memorizar.

▼B

noOfSpecificConditionRecords: número dos registos de condição especial que o cartão pode memorizar.

2.235. **WorkshopCardCalibrationData**

Informação memorizada num cartão de oficina e relativa à atividade dessa oficina, executada com o cartão (requisitos 314, 316, 337 e 339 do anexo 1C).

```
WorkshopCardCalibrationData ::= SEQUENCE {
   calibrationTotalNumber              INTEGER(0 .. 2^16-1),
   calibrationPointerNewestRecord      INTEGER(0 .. NoOfCalibrationRecords-1),
   calibrationRecords                  SET SIZE(NoOfCalibrationRecords) OF
                                       WorkshopCardCalibrationRecord
}
```

calibrationTotalNumber: número total de calibrações efetuadas com o cartão.

calibrationPointerNewestRecord: índice do último registo atualizado de calibração.

Valor atribuído: número correspondente ao numerador do registo de calibração, a começar por '0' à primeira ocorrência de registos de calibração na estrutura.

calibrationRecords: conjunto de registos que contêm informação relativa a calibração e/ou a ajustamento do tempo.

2.236. **WorkshopCardCalibrationRecord**

Informação memorizada num cartão de oficina e relativa a uma calibração efetuada com esse cartão (requisitos 314 e 337 do anexo 1C).

Geração 1:

```
WorkshopCardCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                  CalibrationPurpose,
   vehicleIdentificationNumber         VehicleIdentificationNumber,
   vehicleRegistration                 VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant      W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment       K-ConstantOfRecordingEquipment,
   lTyreCircumference                  L-TyreCircumference,
   tyreSize                            TyreSize,
   authorisedSpeed                     SpeedAuthorised,
   oldOdometerValue                    OdometerShort,
   newOdometerValue                    OdometerShort,
   oldTimeValue                        TimeReal,
   newTimeValue                        TimeReal,
   nextCalibrationDate                 TimeReal,
   vuPartNumber                        VuPartNumber,
   vuSerialNumber                      VuSerialNumber,
   sensorSerialNumber                  SensorSerialNumber
}
```

calibrationPurpose: objetivo da calibração.

vehicleIdentificationNumber: VIN.

vehicleRegistration contém o VRN e o Estado-Membro de matrícula.

wVehicleCharacteristicConstant: coeficiente característico do veículo.

▼B

kConstantOfRecordingEquipment: constante do aparelho de controlo.

lTyreCircumference: perímetro efetivo dos pneus das rodas.

tyreSize: designação das dimensões dos pneus montados no veículo.

authorisedSpeed: velocidade máxima autorizada para o veículo.

oldOdometerValue, newOdometerValue: valores antigo e novo do conta-quilómetros.

oldTimeValue, newTimeValue: valores antigo e novo da data e da hora.

nextCalibrationDate: data da próxima calibração do tipo especificado em CalibrationPurpose, a efetuar pela autoridade responsável pela inspeção.

vuPartNumber, **vuSerialNumber** e **sensorSerialNumber**: elementos de dados relativos à identificação do aparelho de controlo.

Geração 2:

```
WorkshopCardCalibrationRecord ::= SEQUENCE {
   calibrationPurpose                  CalibrationPurpose,
   vehicleIdentificationNumber         VehicleIdentificationNumber,
   vehicleRegistration                 VehicleRegistrationIdentification,
   wVehicleCharacteristicConstant      W-VehicleCharacteristicConstant,
   kConstantOfRecordingEquipment       K-ConstantOfRecordingEquipment,
   lTyreCircumference                  L-TyreCircumference,
   tyreSize                            TyreSize,
   authorisedSpeed                     SpeedAuthorised,
   oldOdometerValue                    OdometerShort,
   newOdometerValue                    OdometerShort,
   oldTimeValue                        TimeReal,
   newTimeValue                        TimeReal,
   nextCalibrationDate                 TimeReal,
   vuPartNumber                        VuPartNumber,
   vuSerialNumber                      VuSerialNumber,
   sensorSerialNumber                  SensorSerialNumber,
   sensorGNSSSerialNumber              SensorGNSSSerialNumber,
   rcmSerialNumber                     RemoteCommunicationModuleSerialNumber,
   sealDataCard                        SealDataCard
}
```

Utilizam-se os seguintes elementos de dados, além dos utilizados na geração 1:

sensorGNSSSerialNumber identifica um módulo GNSS externo.

rcmSerialNumber identifica um módulo de comunicação à distância.

sealDataCard fornece informações sobre os selos que estão ligados a diferentes componentes do veículo.

▼B

2.237. **WorkshopCardHolderIdentification**

Informação memorizada num cartão de oficina e relativa à identificação do titular do cartão (requisitos 311 e 334 do anexo 1C).

```
WorkshopCardHolderIdentification ::= SEQUENCE {
   workshopName                        Name,
   workshopAddress                     Address,
   cardHolderName                      HolderName,
   cardHolderPreferredLanguage         Language
}
```

workshopName é o nome da oficina do titular do cartão.

workshopAddress é o endereço da oficina do titular do cartão.

cardHolderName é o apelido e o nome próprio do titular (p. ex., o nome do mecânico).

cardHolderPreferredLanguage é o idioma preferencial do titular do cartão.

2.238. **WorkshopCardPIN**

Número de identificação pessoal do cartão de oficina (requisitos 309 e 332 do anexo 1C).

```
WorkshopCardPIN ::= IA5String(SIZE(8))
```

Valor atribuído: O PIN conhecido pelo titular do cartão, preenchido à direita com bytes 'FF' até um máximo de 8 bytes.

2.239. **W-VehicleCharacteristicConstant**

Coeficiente característico do veículo [definição k)].

```
W-VehicleCharacteristicConstant ::= INTEGER(0..2^16-1))
```

Valor atribuído: Impulsos por quilómetro no intervalo operacional de 0 a 64 255 impulsos/km.

2.240. **VuPowerSupplyInterruptionRecord**

Geração 2:

Informação memorizada numa unidade-veículo e relativa a incidentes de interrupção da alimentação elétrica (requisito 117 do anexo 1C).

```
VuPowerSupplyInterruptionRecord ::= SEQUENCE {
   eventType                           EventFaultType,
   eventRecordPurpose                  EventFaultRecordPurpose,
   eventBeginTime                      TimeReal,
   eventEndTime                        TimeReal,
   cardNumberAndGenDriverSlotBegin     FullCardNumberAndGeneration,
   cardNumberAndGenDriverSlotEnd       FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotBegin   FullCardNumberAndGeneration,
   cardNumberAndGenCodriverSlotEnd     FullCardNumberAndGeneration,
   similarEventsNumber                 SimilarEventsNumber
}
```

eventType: tipo do incidente.

eventRecordPurpose: objetivo pelo qual este incidente foi registado.

eventBeginTime: data e hora de início do incidente.

▼B

eventEndTime: data e hora de cessação do incidente.

cardNumberAndGenDriverSlotBegin identifica o cartão (incluindo a sua geração) inserido na ranhura do condutor, no início do incidente.

cardNumberAndGenDriverSlotEnd identifica o cartão (incluindo a sua geração) inserido na ranhura do condutor, no final do incidente.

cardNumberAndGenCodriverSlotBegin identifica o cartão (incluindo a sua geração) inserido na ranhura do ajudante, no início do incidente.

cardNumberAndGenCodriverSlotEnd identifica o cartão (incluindo a sua geração) inserido na ranhura do ajudante, no final do incidente.

similarEventsNumber: número de incidentes similares no dia em questão.

2.241. **VuPowerSupplyInterruptionRecordArray**

Geração 2:

Informação memorizada numa unidade-veículo e relativa a incidentes de interrupção da alimentação elétrica (requisito 117 do anexo 1C).

```
VuPowerSupplyInterruptionRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       VuPowerSupplyInterruptionRecord
}
```

recordType indica o tipo de registo (VuPowerSupplyInterruptionRecord). **Valor atribuído**: ver RecordType

recordSize: tamanho do VuPowerSupplyInterruptionRecord, em bytes.

noOfRecords: número de registos nos registos definidos.

records: conjunto de registos de incidentes de interrupção da alimentação elétrica.

2.242. **VuSensorExternalGNSSCoupledRecordArray**

Geração 2:

Conjunto de SensorExternalGNSSCoupledRecord, mais metadados utilizados no protocolo de descarregamento.

```
VuSensorExternalGNSSCoupledRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF
                                       SensorExternalGNSSCoupledRecord
}
```

recordType indica o tipo de registo (SensorExternalGNSSCoupledRecord). **Valor atribuído**: ver RecordType

▼B

recordSize: tamanho do SensorExternalGNSSCoupledRecord, em bytes.

noOfRecords: número de registos nos registos definidos.

records: conjunto de registos de Sensor External GNSS Coupled.

2.243. **VuSensorPairedRecordArray**

Geração 2:

Conjunto de SensorPairedRecord, mais metadados utilizados no protocolo de descarregamento.

```
VuSensorPairedRecordArray ::= SEQUENCE {
   recordType                          RecordType,
   recordSize                          INTEGER(1..65535),
   noOfRecords                         INTEGER(0..65535),
   records                             SET SIZE(noOfRecords) OF SensorPairedRecord
}
```

recordType indica o tipo de registo (SensorPairedRecord). **Valor atribuído**: ver RecordType

recordSize: tamanho do SensorPairedRecord, em bytes.

noOfRecords: número de registos nos registos definidos.

records: conjunto de registos do sensor emparelhado.

3. DEFINIÇÕES DOS VALORES E DOS INTERVALOS DE DIMENSÃO

Definição dos valores variáveis utilizados nas definições da secção 2 deste apêndice.

```
TimeRealRange ::= 2^32-1
```

4. CONJUNTOS DE CARATERES

IA5Strings utiliza os carateres ASCII definidos na norma ISO/IEC 8824-1. Por uma questão de legibilidade e de mais fácil referência, indica-se abaixo a atribuição de valor. Na eventualidade de discrepância, a norma ISO/IEC 8824-1 prevalece sobre esta nota informativa.

```
  ! " # $ % & ' ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ?
@ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [ \ ] ^ _
` a b c d e f g h i j k l m n o p q r s t u v w x y z { | } ~
```

Outras «character strings» ou cadeias de carateres (Address, Name, VehicleRegistrationNumber) utilizam, adicionalmente, os carateres da gama de códigos de carateres decimais de 161-255 dos seguintes conjuntos de carateres normalizados de 8 bits, especificados pelo número de página de código (Code Page): Conjunto de carateres normalizado	Página de código (decimal)
ISO/IEC 8859-1 Latim-1 Europa Ocidental	1
ISO/IEC 8859-2 Latim-2 Europa Central	2
ISO/IEC 8859-3 Latim-3 Europa Meridional	3
ISO/IEC 8859-5 Latim/Cirílico	5
ISO/IEC 8859-7 Latim/Grego	7
ISO/IEC 8859-9 Latim-5 Turco	9

▼B

Outras «character strings» ou cadeias de carateres (Address, Name, VehicleRegistrationNumber) utilizam, adicionalmente, os carateres da gama de códigos de carateres decimais de 161-255 dos seguintes conjuntos de carateres normalizados de 8 bits, especificados pelo número de página de código (Code Page): Conjunto de carateres normalizado	Página de código (decimal)
ISO/IEC 8859-13 Latim-7 Báltico	13
ISO/IEC 8859-15 Latim-9	15
ISO/IEC 8859-16 Latim-10 Sudeste da Europa	16
KOI8-R Latim/Cirílico	80
KOI8-U Latim/Cirílico	85

5. CODIFICAÇÃO

Se a sua codificação for feita segundo as regras ASN.1, os tipos de dados definidos devem ser codificados em conformidade com a norma ISO/IEC 8825-2, variante alinhada.

6. IDENTIFICADORES DE OBJETO E IDENTIFICADORES DE APLICAÇÃO

6.1. **Identificadores de objeto**

Os identificadores de objeto (OID) que constam do presente capítulo têm importância apenas para a geração 2. São especificados na orientação técnica TR-03110-3 e repetidos aqui por uma questão de exaustividade. Estão contidos na subárvore de bsi-de:

```
bsi-de OBJECT IDENTIFIER ::= {
   itu-t(0) identified-organization(4) etsi(0)
   reserved(127) etsi-identified-organization(0) 7
}
```

Identificadores de protocolo de autenticação da VU

```
id-TA         OBJECT IDENTIFIER ::= {bsi-de protocols(2) smartcard(2) 2}

id-TA-ECDSA                OBJECT IDENTIFIER ::= {id-TA 2}

id-TA-ECDSA-SHA-256 OBJECT IDENTIFIER ::= {id-TA-ECDSA 3}

id-TA-ECDSA-SHA-384 OBJECT IDENTIFIER ::= {id-TA-ECDSA 4}

id-TA-ECDSA-SHA-512 OBJECT IDENTIFIER ::= {id-TA-ECDSA 5}
```

Exemplo: Supondo que a autenticação da VU deve ser efetuada com SHA-384, o identificador do objeto a utilizar é (na notação ASN.1) `bsi-de protocols(2) smartcard(2) 2 2 4`. O valor deste identificador do objeto na notação de ponto é `0.4.0.127.0.7.2.2.2.2.4`.

	Notação de ponto	Notação de byte
id-TA-ECDSA-SHA-256	0.4.0.127.0.7.2.2.2.2.3	‘04 00 7F 00 07 02 02 02 02 03’
id-TA-ECDSA-SHA-384	0.4.0.127.0.7.2.2.2.2.4	‘04 00 7F 00 07 02 02 02 02 04’
id-TA-ECDSA-SHA-512	0.4.0.127.0.7.2.2.2.2.5	‘04 00 7F 00 07 02 02 02 02 05’

▼B

Identificadores de protocolo de autenticação da pastilha

```
id-CA         OBJECT IDENTIFIER ::= {bsi-de protocols(2) smartcard(2) 3}

id-CA-ECDH                        OBJECT IDENTIFIER ::= {id-CA 2}

id-CA-ECDH-AES-CBC-CMAC-128       OBJECT IDENTIFIER ::= {id-CA-ECDH 2}

id-CA-ECDH-AES-CBC-CMAC-192       OBJECT IDENTIFIER ::= {id-CA-ECDH 3}

id-CA-ECDH-AES-CBC-CMAC-256       OBJECT IDENTIFIER ::= {id-CA-ECDH 4}
```

Exemplo: Supondo que a autenticação da pastilha deve ser efetuada utilizando o algoritmo ECDH, tal resulta num comprimento de chave de sessão AES de 128 bits. Esta chave de sessão será posteriormente utilizada no modo CBC de funcionamento para garantir a confidencialidade de dados e com o algoritmo CMAC para garantir a autenticidade dos dados. Por conseguinte, o identificador do objeto a utilizar é (na notação ASN.1) `bsi-de protocols(2) smartcard(2) 3 2 2`. O valor deste identificador do objeto na notação de ponto é`0.4.0.127.0.7.2.2.3.2.2`.

	Notação de ponto	Notação de byte
id-CA-ECDH-AES-CBC-CMAC-128	0.4.0.127.0.7.2.2.3.2.2	‘04 00 7F 00 07 02 02 03 02 02’
id-CA-ECDH-AES-CBC-CMAC-192	0.4.0.127.0.7.2.2.3.2.3	‘04 00 7F 00 07 02 02 03 02 03’
id-CA-ECDH-AES-CBC-CMAC-256	0.4.0.127.0.7.2.2.3.2.4	‘04 00 7F 00 07 02 02 03 02 04’

6.2. **Identificadores da aplicação**

Geração 2:

O identificador de aplicação (AID) para o módulo GNSS externo (geração 2) é dado por ‘FF 44 54 45 47 4D’. Este é um AID de proprietário, em conformidade com a norma ISO/IEC 7816-4.

Nota: Os últimos 5 bytes codificam DTEGM para o módulo GNSS externo dos tacógrafos inteligentes.

O identificador de aplicação para a aplicação do cartão tacográfico da geração 2 é dado por ‘FF 53 4D 52 44 54’. Este é um AID de proprietário, em conformidade com a norma ISO/IEC 7816-4.

▼B

Apêndice 2

ESPECIFICAÇÕES APLICÁVEIS AOS CARTÕES TACOGRÁFICOS

ÍNDICE

▼B

1. INTRODUÇÃO

1.1. **Abreviaturas**

Para efeitos do presente apêndice, aplicam-se as seguintes abreviaturas:

AC	Condições de acesso
AES	Norma avançada de cifragem
AID	Identificador de aplicação
ALW	Sempre
APDU	Unidade de dados do protocolo de uma aplicação (estrutura de um comando)
ATR	Answer To Reset
AUT	Autenticado
C6, C7	Contactos n.^{os} 6 e 7 do cartão conforme norma ISO/IEC 7816-2
CC	Ciclos do relógio
CHV	Informação sobre a verificação do titular do cartão
CLA	Byte de classe de um comando APDU

▼B

DSRC	Comunicações dedicadas de curto alcance
DF	Ficheiro dedicado; um DF pode conter outros ficheiros (EF ou DF)
ECC	Criptografia de curva elíptica
EF	Ficheiro elementar
etu	Unidade elementar de tempo
G1	Geração 1
G2	Geração 2
IC	Circuito integrado
ICC	Cartão com circuito integrado
ID	Identificador
IFD	Dispositivo de interface
IFS	Dimensão do campo de informação
IFSC	Dimensão do campo de informação para o cartão
IFSD	Dispositivo de dimensão do campo de informação (para o terminal)
INS	Byte de instrução de um comando APDU
Lc	Comprimento dos dados de entrada de um comando APDU
Le	Comprimento dos dados esperados (dados de saída para um comando)
MF	Ficheiro principal (DF raiz)
NAD	Endereço de nó utilizado no protocolo T=1
NEV	Nunca
P1-P2	Bytes de parâmetro
PIN	Número de identificação pessoal
PRO SM	Protegido com envio seguro de mensagens
PTS	Seleção de transmissão de um protocolo
RFU	Reservado para utilização futura
RST	Reinicialização (do cartão)
SFID	Identificador EF curto
SM	Envio seguro de mensagens
SW1-SW2	Bytes de estatuto ou de situação
TS	Caráter inicial de ATR
VPP	Tensão de programação
VU	Unidade-veículo
XXh	Valor XX em notação hexadecimal
‘XXh’	Valor XX em notação hexadecimal
||	Símbolo de concatenação 03||04=0304

▼B

1.2. **Referências**

No presente apêndice, são utilizadas as seguintes referências:

ISO/IEC 7816-2 Identification cards — Integrated circuit cards — Part 2: Dimensions and location of the contacts. ISO/IEC 7816-2:2007.

ISO/IEC 7816-3 Identification cards — Integrated circuit cards — Part 3: Electrical interface and transmission protocols. ISO/IEC 7816-3:2006.

ISO/IEC 7816-4 Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange. ISO/IEC 7816-4:2013 + Cor 1: 2014.

ISO/IEC 7816-6 Identification cards — Integrated circuit cards — Part 6: Interindustry data elements for interchange. ISO/IEC 7816-6:2004 + Cor 1: 2006.

ISO/IEC 7816-8 Identification cards — Integrated circuit cards — Part 8: Commands for security operations. ISO/IEC 7816-8:2004.

ISO/IEC 9797-2 Information technology — Security techniques — Message Authentication Codes (MACs) — Part 2: Mechanisms using a dedicated hash-function. ISO/IEC 9797-2:2011

2. CARACTERÍSTICAS ELÉTRICAS E FÍSICAS

TCS_01 Salvo especificação diversa, os sinais eletrónicos devem cumprir o prescrito na norma ISO/IEC 7816-3.

TCS_02 A localização e as dimensões dos contactos do cartão devem cumprir o prescrito na norma ISO/IEC 7816-2.

2.1. **Tensão de alimentação e consumo elétrico**

TCS_03 O cartão deve funcionar em conformidade com os limites de consumo especificados na norma ISO/IEC 7816-3.

TCS_04 O cartão deve funcionar com Vcc = 3V (+/- 0,3V) ou com Vcc = 5V (+/- 0,5V).

A seleção da tensão deve cumprir o prescrito na norma ISO/IEC 7816-3.

2.2. **Tensão de programação V_{pp}**

TCS_05 O cartão não deve carecer de tensão de programação no pino C6. Espera-se que o pino C6 não esteja ligado a um IFD. O contacto C6 pode ser ligado a V_{cc} no cartão mas não à terra. Esta tensão em caso nenhum deve ser interpretada.

2.3. **Geração e frequência do relógio**

TCS_06 O cartão deve funcionar num alcance de frequência de 1 a 5 MHz, podendo aceitar frequências mais elevadas. No âmbito de uma sessão de cartão, a frequência do relógio pode variar ± 2 %. A frequência do relógio é gerada pela unidade-veículo e não propriamente pelo cartão. O ciclo de funcionamento pode variar entre 40 % e 60 %.

TCS_07 Nas condições contidas no ficheiro de cartão EF ICC, o relógio exterior pode ser parado. O primeiro byte do corpo do ficheiro EF ICC codifica as condições do modo Clock-stop («paragem do relógio»):

▼B

Reduzido	Elevado		
Bit 3	Bit 2	Bit 1	
0	0	1	Clockstop permitido, sem nível preferido
0	1	1	Clockstop permitido, preferido nível elevado
1	0	1	Clockstop permitido, preferido nível reduzido
0	0	0	Clockstop não permitido
0	1	0	Clockstop permitido somente no nível elevado
1	0	0	Clockstop permitido somente no nível reduzido

Os bits 4 a 8 não são utilizados.

2.4. **Contacto I/O**

TCS_08 O contacto I/O C7 é utilizado para receber dados do IFD e transmitir-lhos. Durante o funcionamento apenas o cartão ou o IFD estarão em modo de transmissão. Se ambas as unidades estiverem em modo de transmissão, não ocorrerá qualquer dano no cartão. Salvo se estiver a transmitir, o cartão deve introduzir o modo de receção.

2.5. **Estados do cartão**

TCS_09 Enquanto lhe for aplicada a tensão de alimentação, o cartão trabalha em dois estados:

Estado de funcionamento durante a execução de comandos ou ações de interface com a unidade digital,

Estado inativo em todas as outras ocasiões; neste estado, o cartão reterá todos os dados.

3. EQUIPAMENTO INFORMÁTICO E COMUNICAÇÃO

3.1. **Introdução**

Esta secção refere as condições mínimas de funcionalidade requeridas pelos cartões tacográficos e pelas VU, para garantir funcionamento e interoperabilidade corretos.

Os cartões tacográficos cumprem o mais rigorosamente possível as normas ISO/IEC aplicáveis (com destaque para a ISO/IEC 7816). Os comandos e protocolos são, no entanto, referidos na íntegra, para especificar algumas utilizações restritas ou diferenças eventuais. Salvo indicação em contrário, os comandos especificados cumprem integralmente as normas referidas.

3.2. **Protocolo de transmissão**

TCS_10 O protocolo de transmissão deve cumprir a norma ISO/IEC 7816-3 para T = 0 e T = 1. Em particular, a VU deve reconhecer extensões de tempo de espera enviadas pelo cartão.

3.2.1 *Protocolos*

TCS_11 O cartão deve proporcionar quer o protocolo **T=0** quer o protocolo **T=1**. Além disso, é compatível com outros protocolos orientados para o contacto.

TCS_12 **T=0** é o protocolo por defeito, pelo que é necessário um comando **PTS** para o passar a **T=1**.

▼B

TCS_13 Em ambos os protocolos haverá dispositivos de suporte a **«convenção direta»**: a «convenção direta» é, pois, obrigatória para o cartão.

TCS_14 O byte presente no **cartão que indica a dimensão do campo de informação** deve ser apresentado na ATR em carateres TA3. Este valor será, pelo menos, 'F0h' (= 240 bytes).

Aos protocolos aplicam-se as seguintes restrições:

TCS_15 **T=0**

— O dispositivo de interface deve ser compatível com uma resposta em I/O depois da elevação do sinal em RST a partir de 400 cc.

— O dispositivo de interface deve poder ler carateres separados por 12 etu.

— O dispositivo de interface deve ler um caráter errado e a sua repetição quando separados por 13 etu. Se for detetado um caráter errado, o sinal de erro em I/O pode ocorrer entre 1 etu e 2 etu. O dispositivo deve aceitar um atraso de 1 etu.

— O dispositivo de interface deve aceitar uma ATR de 33 bytes (TS+32).

— Se na ATR estiver presente TC1, o Extra Guard Time deve estar presente para carateres enviados pelo dispositivo de interface, embora os carateres enviados pelo cartão possam estar ainda separados por 12 etu. O mesmo se verifica relativamente ao caráter ACK enviado pelo cartão depois de um caráter P3 emitido pelo dispositivo de interface.

— O dispositivo de interface deve ter em conta um caráter NUL emitido pelo cartão.

— O dispositivo de interface deve aceitar o modo complementar para ACK.

— O comando GET RESPONSE (obter resposta) não pode ser utilizado em modo de encadeamento para obter um dado com comprimento suscetível de exceder 255 bytes.

TCS_16 **T=1**

— Byte NAD: não utilizado (NAD deve ser colocado no valor '00').

— S-block ABORT: não utilizado.

— S-block VPP state error: não utilizado.

— O comprimento total de encadeamento para um campo de dados não deve exceder 255 bytes (a garantir pelo IFD).

— O dispositivo de dimensão do campo de informação (IFSD) deve ser indicado pelo IFD imediatamente a seguir à ATR: o IFD transmite o pedido de S-Block IFS a seguir à ATR, e o cartão devolve S-Block IFS. O valor recomendado para o IFSD é de 254 bytes.

— O cartão não pede reajustamento da IFS.

▼B

3.2.2 *ATR*

TCS_17 O dispositivo verifica os bytes da ATR, em conformidade com a norma ISO/IEC 7816-3. Não é feita qualquer verificação aos carateres históricos da ATR.

Exemplo de biprotocolo ATR de base, em conformidade com a norma ISO/IEC 7816-3

▼C2

Carater	Valor	Observações
TS	«3Bh»	Indica convenção direta.
T0	«85h»	TD1 presente; 5 bytes históricos presentes.
TD1	«80h»	TD2 presente; utilizar T = 0
TD2	«11h»	TA3 presente; utilizar T = 1
TA3	«XXh» (pelo menos «VF0h»)	Dimensão do campo de informação para o cartão (IFSC)
TH1 a TH5	«XXh»	Carateres históricos
TCK	«XXh»	Carater de controlo (OR exclusivo)

▼B

TCS_18 Depois de Answer To Reset [resposta à reinicialização] (ATR), o ficheiro principal (MF) é implicitamente selecionado, tornando-se o diretório em curso.

3.2.3 *PTS*

TCS_19 O protocolo por defeito é T=0. Para obter o protocolo T=1, o dispositivo deve enviar ao cartão uma PTS (também conhecida como PPS).

TCS_20 Como ambos os protocolos T=0 e T=1 são obrigatórios para o cartão, a PTS de base para a mudança de protocolo é também obrigatória para o cartão.

Tal como indica a norma ISO/IEC 7816-3, a PTS pode ser utilizada para passar a bauds mais elevados do que o de defeito, eventualmente proposto pelo cartão na ATR [byte TA(1)].

Bauds mais elevados são opcionais para o cartão.

TCS_21 Se somente o baud de defeito for aceite (ou se o baud selecionado não for aceite), o cartão responderá corretamente à PTS, em conformidade com ISO/IEC 7816-3, omitindo o byte PPS1.

Exemplos de PTS de base para seleção de protocolo:

▼C2

Carater	Valor	Observações
PPSS	«FFh»	Carater de iniciação.
PPS0	«00h» ou «01h»	PPS1 a PPS3 não estão presentes; «00h» para selecionar T0, «01h» para selecionar T1.
PK	«XXh»	Carater de controlo: «XXh» = «FFh» se PPS0 = «00h», «XXh» = «FEh» se PPS0 = «01h».

▼B

3.3. **Regras de acesso**

TCS_22 Uma regra de acesso define os controlos de acesso correspondentes para um modo de acesso, ou seja, comando. Se os presentes controlos de acesso forem cumpridos, é processado o comando correspondente.

TCS_23 No cartão tacográfico utilizam-se os controlos de acesso a seguir indicados:

Abreviatura	Significado
ALW	A ação é sempre possível e pode ser executada sem qualquer restrição. A APDU de comando e resposta é enviada em texto simples, ou seja, sem envio seguro de mensagens.
NEV	A ação nunca é possível.
PLAIN-C	A APDU de comando é enviada em texto simples, ou seja, sem envio seguro de mensagens.
PWD	A ação só pode ser executada se o PIN do cartão da oficina tiver sido verificado com êxito, ou seja, se estiver definido o estado de segurança interna «PIN_Verified» do cartão. O comando deve ser enviado sem envio seguro de mensagens.
EXT-AUT-G1	A ação só pode ser executada se o comando EXTERNAL AUTHENTICATE para a autenticação da geração 1 (ver também apêndice 11, parte A) tiver sido executado com êxito.
SM-MAC-G1	A APDU (comando e resposta) deve ser aplicada com o envio seguro de mensagens da geração 1 no modo apenas de autenticação (ver apêndice 11, parte A).
SM-C-MAC-G1	A APDU de comando deve ser aplicada com o envio seguro de mensagens da geração 1 no modo só de autenticação (ver apêndice 11, parte A).
SM-R-ENC-G1	A APDU de resposta deve ser aplicada com o envio seguro de mensagens da geração 1 no modo de encriptação (ver apêndice 11, parte A), ou seja, nenhum código de autenticação de mensagem é devolvido.
SM-R-ENC--MAC-G1	A APDU de resposta deve ser aplicada com o envio seguro de mensagens da geração 1 no modo encriptar depois autenticar (ver apêndice 11, parte A).
SM-MAC-G2	A APDU (comando e resposta) deve ser aplicada com o envio seguro de mensagens da geração 2 no modo apenas de autenticação (ver apêndice 11, parte B).
SM-C-MAC-G2	A APDU de comando deve ser aplicada com o envio seguro de mensagens da geração 2 no modo só de autenticação (ver apêndice 11, parte B).
SM-R-ENC--MAC-G2	A APDU de resposta deve ser aplicada com o envio seguro de mensagens da geração 2 no modo encriptar depois autenticar (ver apêndice 11, parte B).

TCS_24 Estes controlos de acesso podem ser ligados das seguintes formas:

E: Todos os controlos de acesso devem ser cumpridos

OU: Deve ser cumprido, pelo menos, um controlo de acesso

As regras de acesso ao sistema de ficheiros, ou seja, os comandos SELECT, READ BINARY e UPDATE BINARY, são especificadas no capítulo 4. As regras de acesso aos comandos restantes são especificadas nos quadros seguintes.

▼B

TCS_25 Na aplicação DF Tachograph G1 utilizam-se as seguintes regras de acesso:

Comando	Cartão de condutor	Cartão de oficina	Cartão de controlo	Cartão de empresa
EXTERNAL AUTHENTICATE				
— Para autenticação da geração 1	ALW	ALW	ALW	ALW
— Para autenticação da geração 2	ALW	PWD	ALW	ALW
Internal Authenticate	ALW	PWD	ALW	ALW
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Não aplicável	Não aplicável	Não aplicável	Não aplicável
PSO: Compute Digital Signature	ALW OR SM-MAC--G2	ALW OR SM-MAC--G2	Não aplicável	Não aplicável
PSO: Hash	Não aplicável	Não aplicável	ALW	Não aplicável
PSO: Hash of File	ALW OR SM-MAC--G2	ALW OR SM-MAC--G2	Não aplicável	Não aplicável
PSO: VERIFY CERTIFICATE	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Não aplicável	Não aplicável	ALW	Não aplicável
Verify	Não aplicável	ALW	Não aplicável	Não aplicável

TCS_26 Na aplicação DF Tachograph G2 utilizam-se as seguintes regras de acesso:

Comando	Cartão de condutor	Cartão de oficina	Cartão de controlo	Cartão de empresa
External Authenticate				
— Para autenticação da geração 1	Não aplicável	Não aplicável	Não aplicável	Não aplicável
— Para autenticação da geração 2	ALW	PWD	ALW	ALW
Internal Authenticate	Não aplicável	Não aplicável	Não aplicável	Não aplicável

▼B

Comando	Cartão de condutor	Cartão de oficina	Cartão de controlo	Cartão de empresa
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Não aplicável	ALW	ALW	Não aplicável
PSO: Compute Digital Signature	ALW OR SM-MAC--G2	ALW OR SM-MAC--G2	Não aplicável	Não aplicável
PSO: Hash	Não aplicável	Não aplicável	ALW	Não aplicável
PSO: Hash of File	ALW OR SM-MAC--G2	ALW OR SM-MAC--G2	Não aplicável	Não aplicável
PSO: Verify Certificate	ALW	ALW	ALW	ALW
PSO: Verify Digital Signature	Não aplicável	Não aplicável	ALW	Não aplicável
Verify	Não aplicável	ALW	Não aplicável	Não aplicável

TCS_27 No MF utilizam-se as seguintes regras de acesso:

Comando	Cartão de condutor	Cartão de oficina	Cartão de controlo	Cartão de empresa
External Authenticate				
— Para autenticação da geração 1	Não aplicável	Não aplicável	Não aplicável	Não aplicável
— Para autenticação da geração 2	ALW	PWD	ALW	ALW
Internal Authenticate	Não aplicável	Não aplicável	Não aplicável	Não aplicável
General Authenticate	ALW	ALW	ALW	ALW
Get Challenge	ALW	ALW	ALW	ALW
MSE:SET AT	ALW	ALW	ALW	ALW
MSE:SET DST	ALW	ALW	ALW	ALW
Process DSRC Message	Não aplicável	Não aplicável	Não aplicável	Não aplicável

▼B

Comando	Cartão de condutor	Cartão de oficina	Cartão de controlo	Cartão de empresa
PSO: Compute Digital Signature	Não aplicável	Não aplicável	Não aplicável	Não aplicável
PSO: Hash	Não aplicável	Não aplicável	Não aplicável	Não aplicável
PSO: Hash of File	Não aplicável	Não aplicável	Não aplicável	Não aplicável
PSO: Verify Certificate	ALW	ALW	ALW	ALW
Verify	Não aplicável	ALW	Não aplicável	Não aplicável

TCS_28 Um cartão tacográfico pode ou não aceitar um comando com nível de segurança superior ao especificado nos controlos de acesso. Ou seja, se o controlo de acesso for ALW (ou PLAIN-C), o cartão pode aceitar um comando com envio seguro de mensagens (encriptação e/ou modo de autenticação). Se o controlo de acesso exigir o envio seguro de mensagens com modo de autenticação, o cartão tacográfico pode aceitar um comando com envio seguro de mensagens da mesma geração no modo de autenticação e encriptação.

Nota: As descrições do comando fornecem informações adicionais acerca do suporte dos comandos para os diferentes tipos de cartões tacográficos e diferentes DF.

3.4. **Descrição de comandos e códigos de erro**

Os comandos e a organização dos ficheiros são deduzidos da norma ISO/IEC 7816-4, à qual obedecem.

A presente secção incide nos pares comando-resposta de APDU *infra*. Nas descrições do comando correspondentes, especificam-se as variantes de comando compatíveis com uma aplicação das gerações 1 ou 2.

Comando	INS
SELECT	‘A4h’
READ BINARY	‘B0h’, ‘B1h’
UPDATE BINARY	‘D6h’, ‘D7h’
GET CHALLENGE	‘84h’
VERIFY	‘20h’
GET RESPONSE	‘C0h’
PERFORM SECURITY OPERATION	‘2Ah’

▼B

Comando	INS
— VERIFY CERTIFICATE	
— COMPUTE DIGITAL SIGNATURE	
— VERIFY DIGITAL SIGNATURE	
— HASH	
— PERFORM HASH OF FILE	
— PROCESS DSRC MESSAGE	
INTERNAL AUTHENTICATE	‘88h’
EXTERNAL AUTHENTICATE	‘82h’
MANAGE SECURITY ENVIRONMENT	‘22h’
— SET DIGITAL SIGNATURE TEMPLATE	
— SET AUTHENTICATION TEMPLATE	
GENERAL AUTHENTICATE	‘86h’

TCS_29 As palavras de estatuto ou situação SW1 e SW2 são emitidas nas mensagens de resposta e denotam o estado de processamento do comando.

SW1	SW2	Significado
90	00	Processamento normal
61	XX	Processamento normal. XX = número de bytes de resposta disponíveis
62	81	Processamento de alerta. Possível corrupção de parte dos dados devolvidos
63	00	Falha de autenticação (alerta)
63	CX	CHV (PIN) errado. Contador de tentativas remanescentes fornecido por ‘X’
64	00	Erro de execução — Estado de memória não viva inalterado. Erro de integridade
65	00	Erro de execução — Estado de memória não viva alterado
65	81	Erro de execução — Estado de memória não viva alterado — Falha de memória
66	88	Erro de segurança: soma criptográfica de teste errada (durante envio seguro de mensagens) ou certificado errado (durante a verificação do certificado) ou criptograma errado (durante autenticação externa) ou assinatura errada (durante a verificação de assinatura)
67	00	Comprimento errado (Lc ou Le errados)

▼B

SW1	SW2	Significado
68	82	Envio seguro de mensagens não aeite
68	83	Último comando esperado da cadeia
69	00	Comando proibido (não há resposta disponível em T=0)
69	82	Estatuto de segurança não satisfeito
69	83	Método de autenticação bloqueado
69	85	Condições de utilização não satisfeitas
69	86	Comando não permitido (nenhum EF em curso)
69	87	Inexistentes os objetos de dados esperados do envio seguro de mensagens
69	88	Incorretos os objetos de dados do envio seguro de mensagens
6A	80	Parâmetros incorretos no campo de dados
6A	82	Ficheiro não encontrado
6A	86	Parâmetros P1-P2 errados
6A	88	Dados referenciados não encontrados
6B	00	Parâmetros errados (deslocamento fora de EF)
6C	XX	Comprimento errado; SW2 indica o comprimento exato. Sem devolução de campo de dados
6D	00	Código de instrução não aceite ou inválido
6E	00	Classe não aceite
6F	00	Outros erros de verificação

TCS_30 Se num comando APDU estiver preenchida mais do que uma condição de erro, o cartão pode devolver qualquer uma das palavras de estatuto adequadas.

3.5. **Descrição dos comandos**

O presente capítulo incide nos comandos obrigatórios para os cartões tacográficos.

O apêndice 11 (Mecanismos comuns de segurança para os tacógrafos da geração 1 e da geração 2) indica elementos adicionais, com importância para as operações criptográficas em causa.

Todos os comandos são descritos independentemente do protocolo utilizado (T=0 ou T=1). Os bytes de APDU CLA, INS, P1, P2, Lc e Le são sempre indicados. Se Lc ou Le não forem necessários para o comando descrito, surgem em branco os respetivos valor, comprimento e descrição.

TCS_31 Sendo pedidos ambos os bytes de comprimento (Lc e Le), o comando descrito tem de ser dividido em duas partes se o IFD utilizar o protocolo T=0: o IFD envia o comando tal como descrito com P3=Lc+dados e, em seguida, envia um comando GET RESPONSE (ver ponto 3.5.6) com P3=Le.

TCS_32 Sendo pedidos ambos os bytes de comprimento e Le=0 (envio seguro de mensagens):

▼B

— ao utilizar o protocolo T=1, o cartão responde a Le=0 enviando todos os dados de saída disponíveis;

— ao utilizar o protocolo T=0, o IFD envia o primeiro comando com P3=Lc+dados e o cartão responde (a este Le=0 implícito) pelos bytes de estatuto '**61La**', onde La é o número de bytes de resposta disponíveis. O IFD gera então um comando GET RESPONSE com P3=La para ler os dados.

TCS_33 Como recurso opcional, um cartão tacográfico pode aceitar o aumento dos campos de comprimento em conformidade com a norma ISO/IEC 7816-4. Um cartão tacográfico que aceite o aumento dos campos de comprimento deve:

— Indicar o suporte do aumento do campo de comprimento na ATR;

— Fornecer as dimensões da margem de segurança aceites por meio da informação do aumento do comprimento na EF ATR/INFO (ver TCS_146);

— Indicar se aceita o aumento dos campos de comprimento para T=1 e/ou T=0 no aumento do comprimento EF (ver TCS_147);

— Aceitar o aumento dos campos de comprimento para a aplicação tacográfica das gerações 1 e 2.

Notas:

Todos os comandos são especificados para campos de comprimento curto. A utilização de APDU de aumento do comprimento decorre da norma ISO/IEC 7816-4.

De um modo geral, os comandos são especificados para o modo normal, ou seja, sem envio seguro de mensagens, tal como a camada do envio seguro de mensagens é especificada no apêndice 11. A partir das regras de acesso para um comando, é evidente se o comando deve aceitar o envio seguro de mensagens ou não e se o comando deve aceitar o envio seguro de mensagens da geração 1 e/ou da geração 2. Algumas variantes do comando são descritas com envio seguro de mensagens para ilustrar a utilização do envio seguro de mensagens.

TCS_34 A VU executa o protocolo total de autenticação mútua do cartão da VU da geração 2 para uma sessão, incluindo a verificação do certificado (quando necessário) quer no DF Tachograph, no DF Tachograph_G2 ou no MF.

3.5.1 *SELECT*

Este comando cumpre a norma ISO/IEC 7816-4, mas tem uma utilização restrita, em comparação com o comando definido na norma.

O comando SELECT é utilizado para:

— selecionar uma aplicação DF (tem de se utilizar seleção por nome)

— selecionar um ficheiro elementar correspondente ao ID do ficheiro apresentado

3.5.1.1 Seleção por nome (AID)

Este comando permite selecionar um DF de aplicação no cartão.

TCS_35 Este comando pode ser executado a partir de qualquer ponto na estrutura do ficheiro (depois da ATR ou em qualquer momento).

▼B

TCS_36 A seleção de uma aplicação reinicializa o ambiente de segurança vigente. Depois de se selecionar a aplicação, não volta a ser selecionada nenhuma chave pública vigente. É igualmente perdida a condição de acesso EXT-AUT-G1. Se o comando tiver sido executado sem o envio seguro de mensagens, as antigas chaves de sessão do envio seguro de mensagens deixam de estar disponíveis.

TCS_37 **Mensagem de comando**

Byte	Comprimento	Valor	Descrição
CLA	1	‘00h’	
INS	1	‘A4h’	
P1	1	‘04h’	Seleção por nome (AID)
P2	1	‘0Ch’	Nenhuma resposta esperada
Lc	1	‘NNh’	Número de bytes enviados ao cartão (comprimento da AID): ‘06h’ para a aplicação tacográfica
#6-#(5+NN)	NN	‘XX..XXh’	AID: ‘FF 54 41 43 48 4F’ para a aplicação tacográfica da geração 1 AID: ‘FF 53 4D 52 44 54’ para a aplicação tacográfica da geração 2

Não é necessária resposta ao comando SELECT (Le ausente em T=1 ou não é pedida resposta em T=0).

TCS_38 **Mensagem de resposta (não é pedida resposta)**

Byte	Comprimento	Valor	Descrição
SW	2	‘XXXXh’	Palavras de estatuto (SW1, SW2)

— Se o comando for bem sucedido, o cartão devolve ‘**9000**’.

— Se a aplicação correspondente ao AID não for encontrada, o estado de processamento devolvido é ‘**6A82**’.

— Em T=1, se o byte Le estiver presente, o estado devolvido é **‘6700’**.

— Em T=0, se for pedida uma resposta depois do comando SELECT, o estado devolvido é **‘6900’**.

— Se a aplicação selecionada for considerada corrompida (o erro de integridade é detetado nos atributos do ficheiro), o estado de processamento devolvido é ‘**6400**’ ou ‘**6581**’.

3.5.1.2 Seleção de um ficheiro elementar utilizando o seu identificador de ficheiro

TCS_39 **Mensagem de comando**

TCS_40 Conforme especificado no apêndice 11, parte B, um cartão tacográfico deve aceitar o envio seguro de mensagens da geração 2 para esta variante de comando.

Byte	Comprimento	Valor	Descrição
CLA	1	‘00h’	
INS	1	‘A4h’	
P1	1	‘02h’	Seleção de um EF sob o DF em curso

▼B

Byte	Comprimento	Valor	Descrição
P2	1	‘0Ch’	Nenhuma resposta esperada
Lc	1	‘02h’	Número de bytes enviados ao cartão
#6-#7	2	‘XXXXh’	Identificador de ficheiro

Não é necessária resposta ao comando SELECT (Le ausente em T=1 ou não é pedida resposta em T=0).

TCS_41 **Mensagem de resposta (não é pedida resposta)**

Byte	Comprimento	Valor	Descrição
SW	2	‘XXXXh’	Palavras de estatuto (SW1, SW2)

— Se o comando for bem sucedido, o cartão devolve ‘**9000**’.

— Se o ficheiro correspondente ao identificador de ficheiro não for encontrado, o estado de processamento devolvido é ‘**6A82**’.

— Em T=1, se o byte Le estiver presente, o estado devolvido é **‘6700’**.

— Em T=0, se for pedida uma resposta depois do comando SELECT, o estado devolvido é **‘6900’**.

— Se o ficheiro selecionado for considerado corrompido (o erro de integridade é detetado nos atributos do ficheiro), o estado de processamento devolvido é ‘**6400**’ ou ‘**6581**’.

3.5.2 *READ BINARY*

Este comando cumpre a norma ISO/IEC 7816-4, mas tem uma utilização restrita, em comparação com o comando definido na norma.

O comando READ BINARY é utilizado para ler dados de ficheiros transparentes.

A resposta do cartão consiste em devolver os dados lidos, opcionalmente encapsulados numa estrutura de envio seguro de mensagens.

3.5.2.1 Comando com deslocamento em P1-P2

Este comando permite ao IFD ler dados do EF selecionado de momento, sem envio seguro de mensagens.

Nota: Este comando sem envio seguro de mensagens pode ser utilizado apenas para ler um ficheiro que aceite o controlo de acesso ALW para o modo de acesso Read.

TCS_42 **Mensagem de comando**

Byte	Comprimento	Valor	Descrição
CLA	1	‘00h’	
INS	1	‘B0h’	Read Binary
P1	1	‘XXh’	Deslocamento em bytes desde o início do ficheiro: Byte mais significativo

▼B

Byte	Comprimento	Valor	Descrição
P2	1	‘XXh’	Deslocamento em bytes desde o início do ficheiro: Byte menos significativo
Le	1	‘XXh’	Comprimento dos dados esperados. Número de bytes a ler

Nota: O bit 8 de P1 deve ser fixado em 0.

TCS_43 **Mensagem de resposta**

Byte	Comprimento	Valor	Descrição
#1-#X	X	‘XX..XXh’	Dados lidos
SW	2	‘XXXXh’	Palavras de estatuto (SW1, SW2)

— Se o comando for bem sucedido, o cartão devolve ‘**9000**’.

— Se não for selecionado nenhum EF, o estado de processamento devolvido é **‘6986’**.

— Se o controlo de acesso do ficheiro selecionado não for satisfeito, o comando é interrompido com ‘**6982**’.

— Se o deslocamento não for compatível com a dimensão do EF (deslocamento > dimensão EF), o estado de processamento devolvido é **‘6B00’**.

— Se a dimensão dos dados a ler não for compatível com a dimensão do EF (deslocamento + Le > dimensão EF), o estado de processamento devolvido é ‘**6700**’ ou ‘**6Cxx**’, onde ‘xx’ indica o comprimento exato.

— Se for detetado um erro de integridade nos atributos do ficheiro, o cartão considera o ficheiro corrompido e irrecuperável e o estado de processamento devolvido é **‘6400’** ou ‘**6581**’.

— Se for detetado um erro de integridade nos dados memorizados, o cartão devolve os dados pedidos e o estado de processamento devolvido é **‘6281’**.

3.5.2.1.1 Comando com envio seguro de mensagens (exemplos)

Este comando permite ao IFD ler dados do EF selecionado de momento, com envio seguro de mensagens, a fim de verificar a integridade dos dados recebidos e proteger a sua confidencialidade caso seja aplicado o controlo de acesso SM-R-ENC-MAC-G1 (geração 1) ou SM-R-ENC-MAC-G2 (geração 2).

TCS_44 **Mensagem de comando**

Byte	Comprimento	Valor	Descrição
CLA	1	‘0Ch’	Pedido envio seguro de mensagens
INS	1	‘B0h’	Read Binary
P1	1	‘XXh’	P1 (deslocamento em bytes desde o início do ficheiro): Byte mais significativo
P2	1	‘XXh’	P2 (deslocamento em bytes desde o início do ficheiro): Byte menos significativo

▼B

Byte	Comprimento	Valor	Descrição
Lc	1	‘XXh’	Comprimento dos dados de entrada para envio seguro de mensagens
#6	1	‘97h’	T_{LE}: Marcador para a especificação do comprimento esperado
#7	1	‘01h’	L_{LE}: Comprimento do comprimento esperado
#8	1	‘NNh’	Especificação do comprimento esperado (Le original): Número de bytes a ler
#9	1	‘8Eh’	T_{CC}: Marcador para soma criptográfica de teste
#10	1	‘XXh’	L_{CC}: Comprimento da soma criptográfica de teste *infra* ‘04h’ para envio seguro de mensagens da geração 1 (ver apêndice 11, parte A) ‘08h’, ‘0Ch’ ou ‘10h’, dependendo do comprimento da chave AES para o envio seguro de mensagens da geração 2 (ver apêndice 11, parte B)
#11-#(10+L)	L	‘XX..XXh’	Soma criptográfica de teste
Le	1	‘00h’	Conforme a norma ISO/IEC 7816-4

TCS_45 **Mensagem de resposta se não for necessário SM-R--ENC-MAC-G1 (geração 1) ou SM-R-ENC-MAC-G2 (geração 2) e se o formato de entrada do envio seguro de mensagens estiver correto:**

Byte	Comprimento	Valor	Descrição
#1	1	‘99h’	Marcador do estado de processamento (SW1-SW2) — opcional para o envio seguro de mensagens da geração 1
#2	1	‘02h’	Comprimento do estado de processamento
#3 — #4	2	‘XX XXh’	Estado de processamento da APDU de resposta desprotegida
#5	1	‘81h’	T_{PV}: Marcador para dados de valor simples
#6	L	‘NNh’ or ‘81 NNh’	L_{PV}: comprimento dos dados devolvidos (= Le original). L é 2 bytes se L_{PV}>127 bytes
#(6+L)--#(5+L+NN)	NN	‘XX..XXh’	Valor de dado simples
#(6+L+NN)	1	‘8Eh’	T_{CC}: Marcador para soma criptográfica de teste
#(7+L+NN)	1	‘XXh’	L_{CC}: Comprimento da soma criptográfica de teste *infra* ‘04h’ para envio seguro de mensagens da geração 1 (ver apêndice 11, parte A) ‘08h’, ‘0Ch’ ou ‘10h’, dependendo do comprimento da chave AES para o envio seguro de mensagens da geração 2 (ver apêndice 11, parte B)
#(8+L+NN)--#(7+M+L+N-N)	M	‘XX..XXh’	Soma criptográfica de teste
SW	2	‘XXXXh’	Palavras de estatuto (SW1, SW2)

▼B

TCS_46 **Mensagem de resposta se for necessário SM-R-ENC--MAC-G1 (geração 1) ou SM-R-ENC-MAC-G2 (geração 2) e se o formato de entrada do envio seguro de mensagens estiver correto:**

Byte	Comprimento	Valor	Descrição
#1	1	‘87h’	$T_{PI\ CG}$: Marcador para dados encriptados (criptograma)
#2	L	‘MMh’ ou ‘81 MMh’	$L_{PI\ CG}$: comprimento dos dados encriptados devolvidos (diferente do Le original do comando devido a preenchimento). L é 2 bytes se $L_{PI\ CG} > 127$ bytes.
#(2+L)--#(1+L+MM)	MM	‘01XX..XXh’	Dados encriptados: Indicador de preenchimento e criptograma
#(2+L+MM)	1	‘99h’	Marcador do estado de processamento (SW1-SW2) — opcional para o envio seguro de mensagens da geração 1
#(3+L+MM)	1	‘02h’	Comprimento do estado de processamento
#(4+L+MM) — #(5+L+MM)	2	‘XX XXh’	Estado de processamento da APDU de resposta desprotegida
#(6+L+MM)	1	‘8Eh’	T_{CC}: Marcador para soma criptográfica de teste
#(7+L+MM)	1	‘XXh’	L_{CC}: Comprimento da soma criptográfica de teste *infra* ‘04h’ para envio seguro de mensagens da geração 1 (ver apêndice 11, parte A) ‘08h’, ‘0Ch’ ou ‘10h’, dependendo do comprimento da chave AES para o envio seguro de mensagens da geração 2 (ver apêndice 11, parte B)
#(8+L+MM)--#(7+N+L+M-M)	N	‘XX..XXh’	Soma criptográfica de teste
SW	2	‘XXXXh’	Palavras de estatuto (SW1, SW2)

O comando READ BINARY pode devolver estados de processamento regulares enumerados no TCS_43 sob o marcador ‘99h’, conforme descrito no TCS_59, utilizando a estrutura de resposta do envio seguro de mensagens.

Podem ocorrer alguns erros especificamente relacionados com o envio seguro de mensagens. Em tal caso, o estado de processamento é simplesmente devolvido, sem ser envolvida nenhuma estrutura de envio seguro de mensagens:

TCS_47 **Mensagem de resposta se o formato de entrada do envio seguro de mensagens estiver incorreto**

Byte	Comprimento	Valor	Descrição
SW	2	‘XXXXh’	Palavras de estatuto (SW1, SW2)

— Se não estiver disponível nenhuma chave de sessão em curso, o estado de processamento **‘6A88’** é devolvido, o que acontece se a chave de sessão não tiver ainda sido gerada ou se a sua validade tiver expirado (neste caso, o IFD deve voltar a desencadear um processo de autenticação mútua para criar uma nova chave de sessão).

▼B

— Se no formato de envio seguro de mensagens faltarem alguns objetos de dados esperados (cf. especificação supra), o estado de processamento **'6987'** é devolvido: este erro ocorre se faltar um marcador esperado ou se o corpo do comando não for construído adequadamente.

— Se alguns objetos de dado estiverem incorretos, o estado de processamento devolvido é **'6988'**: este erro ocorre se todos os marcadores necessários estiverem presentes mas alguns comprimentos forem diferentes dos esperados.

— Se falhar a verificação da soma criptográfica de teste, o estado de processamento devolvido é **'6688'**.

3.5.2.2 Comando com identificador EF (Elementary File) curto

Esta variante de comando permite ao IFD selecionar um EF por meio de um identificador EF curto e ler dados deste EF.

TCS_48 Um cartão tacográfico deve aceitar esta variante de comando para todos os ficheiros elementares que contenham um determinado identificador EF curto. Os presentes identificadores EF curtos são especificados no capítulo 4.

TCS_49 **Mensagem de comando**

Byte	Comprimento	Valor	Descrição
CLA	1	'00h'	
INS	1	'B0h'	Read Binary
P1	1	'XXh'	O bit 8 é fixado em 1 Os bits 7 e 6 são fixados em 00 O bit 5-1 codifica o identificador EF curto do EF correspondente
P2	1	'XXh'	Codifica um deslocamento de 0 a 255 bytes no EF referenciado por P1
Le	1	'XXh'	Comprimento dos dados esperados. Número de bytes a ler

Nota: Os identificadores EF curtos utilizados para a aplicação tacográfica da geração 2 são especificados no capítulo 4.

Se P1 codificar um identificador EF curto e o comando for bem sucedido, o EF identificado passa a ser o EF selecionado no momento (EF atual).

TCS_50 **Mensagem de resposta**

Byte	Comprimento	Valor	Descrição
#1-#L	L	'XX..XXh'	Dados lidos
SW	2	'XXXXh'	Palavras de estatuto (SW1, SW2)

— Se o comando for bem sucedido, o cartão devolve '**9000**'.

— Se o ficheiro correspondente ao identificador EF curto não for encontrado, o estado de processamento devolvido é **'6A82'**.

— Se o controlo de acesso do ficheiro selecionado não for satisfeito, o comando é interrompido com '**6982**'.

▼B

— Se o deslocamento não for compatível com a dimensão do EF (deslocamento > dimensão EF), o estado de processamento devolvido é **'6B00'**.

— Se a dimensão dos dados a ler não for compatível com a dimensão do EF (deslocamento + Le > dimensão EF), o estado de processamento devolvido é '**6700**' ou '**6Cxx**' onde 'xx' indica o comprimento exato.

— Se for detetado um erro de integridade nos atributos do ficheiro, o cartão considera o ficheiro corrompido e irrecuperável e o estado de processamento devolvido é **'6400'** ou '**6581.**'

— Se for detetado um erro de integridade nos dados memorizados, o cartão devolve os dados pedidos e o estado de processamento devolvido é **'6281'**.

3.5.2.3 Comando com byte de instrução ímpar

Esta variante de comando permite ao IFD ler dados de um EF com 32 768 bytes ou mais.

TCS_51 Um cartão tacográfico que aceite EF com 32 768 bytes ou mais deve aceitar esta variante de comando para esses EF. Um cartão tacográfico pode ou não aceitar esta variante de comando para outros EF, com exceção do EF Sensor_Installation_Data (ver TCS_156 e TCS_160).

TCS_52 **Mensagem de comando**

Byte	Comprimento	Valor	Descrição
CLA	1	'00h'	
INS	1	'B1h'	Read Binary
P1	1	'00h'	EF atual
P2	1	'00h'	
Lc	1	'NNh'	Comprimento Lc do deslocamento do objeto de dados
#6-#(5+NN)	NN	'XX..XXh'	Objeto de dados do deslocamento: Marcador '54h' Comprimento '01h' ou '02h' Valor deslocamento
Le	1	'XXh'	Número de bytes a ler

O IFD deve codificar o comprimento do objeto de dados do deslocamento com um número mínimo possível de octetos, ou seja, ao utilizar o byte de comprimento '01h', o IFD deve codificar um deslocamento de 0 a 255 e, ao utilizar o byte de comprimento '02h', um deslocamento de '256' até '65 535' bytes.

TCS_53 **Mensagem de resposta**

Byte	Comprimento	Valor	Descrição
#1-#L	L	'XX..XXh'	Dados lidos encapsulados num objeto de dados discricionário com marcador '53h'.
SW	2	'XXXXh'	Palavras de estatuto (SW1, SW2)

▼B

— Se o comando for bem sucedido, o cartão devolve '**9000**'.

— Se não for selecionado nenhum EF, o estado de processamento devolvido é '**6986**'.

— Se o controlo de acesso do ficheiro selecionado não for satisfeito, o comando é interrompido com '**6982**'.

— Se o deslocamento não for compatível com a dimensão do EF (deslocamento > dimensão EF), o estado de processamento devolvido é '**6B00**'.

— Se a dimensão dos dados a ler não for compatível com a dimensão do EF (deslocamento + Le > dimensão EF), o estado de processamento devolvido é '**6700**' ou '**6Cxx**', onde 'xx' indica o comprimento exato.

— Se for detetado um erro de integridade nos atributos do ficheiro, o cartão considera o ficheiro corrompido e irrecuperável e o estado de processamento devolvido é '**6400**' ou '**6581**'.

— Se for detetado um erro de integridade nos dados memorizados, o cartão devolve os dados pedidos e o estado de processamento devolvido é '**6281**'.

3.5.2.3.1 Comando com envio seguro de mensagens (exemplo)

O exemplo que se segue ilustra a utilização do envio seguro de mensagens caso se aplique o controlo de acesso SM-MAC-G2.

TCS_54 Mensagem de comando

Byte	Comprimento	Valor	Descrição
CLA	1	'0Ch'	Pedido envio seguro de mensagens
INS	1	'B1h'	Read Binary
P1	1	'00h'	EF atual
P2	1	'00h'	
Lc	1	'XXh'	Comprimento do campo de dados securizado
#6	1	'B3h'	Marcador para dados de valor simples codificados em BER-TLV
#7	1	'NNh'	L_{PV}: comprimento dos dados transmitidos
#(8)-#(7+NN)	NN	'XX..XXh'	Dados simples codificados em BER-TLV, ou seja, o objeto de dados do deslocamento com marcador '54'
#(8+NN)	1	'97h'	T_{LE}: Marcador para a especificação do comprimento esperado.
#(9+NN)	1	'01h'	L_{LE}: Comprimento do comprimento esperado
#(10+NN)	1	'XXh'	Especificação do comprimento esperado (Le original): Número de bytes a ler
#(11+NN)	1	'8Eh'	T_{CC}: Marcador para soma criptográfica de teste
#(12+NN)	1	'XXh'	L_{CC}: Comprimento da soma criptográfica de teste infra '08h', '0Ch' ou '10h', dependendo do comprimento da chave AES para o envio seguro de mensagens da geração 2 (ver apêndice 11, parte B)
#(13+NN)--#(12+M+NN)	M	'XX..XXh'	Soma criptográfica de teste
Le	1	'00h'	Conforme a norma ISO/IEC 7816-4

▼B

TCS_55 Mensagem de resposta se o comando for bem sucedido

Byte	Comprimento	Valor	Descrição
#1	1	‘B3h’	Dados simples codificados em BER-TLV
#2	L	‘NNh’ or ‘81 NNh’	L_{PV}: comprimento dos dados devolvidos (= Le original). L é 2 bytes se L_{PV}>127 bytes
#(2+L)--#(1+L+NN)	NN	‘XX..XXh’	Valor de dado simples codificado em BER-TLV, ou seja, dados lidos encapsulados num objeto de dados discricionário com marcador ‘53h’
#(2+L+NN)	1	‘99h’	Estado de processamento da APDU de resposta desprotegida
#(3+L+NN)	1	‘02h’	Comprimento do estado de processamento
#(4+L+NN) — #(5+L+NN)	2	‘XX XXh’	Estado de processamento da APDU de resposta desprotegida
#(6+L+NN)	1	‘8Eh’	T_{CC}: Marcador para soma criptográfica de teste
#(7+L+NN)	1	‘XXh’	L_{CC}: Comprimento da soma criptográfica de teste *infra* ‘08h’, ‘0Ch’ ou ‘10h’, dependendo do comprimento da chave AES para o envio seguro de mensagens da geração 2 (ver apêndice 11, parte B)
#(8+L+NN)--#(7+M+L+NN)	M	‘XX..XXh’	Soma criptográfica de teste
SW	2	‘XXXXh’	Palavras de estatuto (SW1, SW2)

3.5.3 *UPDATE BINARY*

Este comando cumpre a norma ISO/IEC 7816-4, mas tem utilização restrita, em comparação com o comando definido na norma.

A mensagem de comando UPDATE BINARY inicia a atualização (apagar + escrever) dos bits já presentes num binário EF com os bits dados no comando APDU.

3.5.3.1 Comando com deslocamento em P1-P2

Este comando permite ao IFD escrever dados no EF selecionado de momento, sem o cartão verificar a integridade dos dados recebidos.

Nota: Este comando sem envio seguro de mensagens pode ser utilizado apenas para atualizar um ficheiro que aceite o controlo de acesso ALW para o modo de acesso Update.

TCS_56 **Mensagem de comando**

Byte	Comprimento	Valor	Descrição
CLA	1	‘00h’	
INS	1	‘D6h’	UPDATE BINARY
P1	1	‘XXh’	Deslocamento em bytes desde o início do ficheiro: Byte mais significativo
P2	1	‘XXh’	Deslocamento em bytes desde o início do ficheiro: Byte menos significativo

▼B

Byte	Comprimento	Valor	Descrição
Lc	1	‘NNh’	Comprimento Lc dos dados a atualizar. Número de bytes a escrever
#6-#(5+NN)	NN	‘XX..XXh’	Dados a escrever

Nota: O bit 8 de P1 deve ser fixado em 0.

TCS_57 **Mensagem de resposta**

Byte	Comprimento	Valor	Descrição
SW	2	‘XXXXh’	Palavras de estatuto (SW1, SW2)

— Se o comando for bem sucedido, o cartão devolve ‘**9000**’.

— Se não for selecionado nenhum EF, o estado de processamento devolvido é **‘6986’**.

— Se o controlo de acesso do ficheiro selecionado não for satisfeito, o comando é interrompido com ‘**6982**’.

— Se o deslocamento não for compatível com a dimensão do EF (deslocamento > dimensão EF), o estado de processamento devolvido é **‘6B00’**.

— Se a dimensão dos dados a escrever não for compatível com a dimensão do EF (deslocamento + Lc > dimensão EF), o estado de processamento devolvido é **‘6700’**.

— Se for detetado um erro de integridade nos atributos do ficheiro, o cartão considera o ficheiro corrompido e irrecuperável e o estado de processamento devolvido é **‘6400’** ou **‘6500’**.

— Se a escrita não tiver êxito, o estado de processamento devolvido é **‘6581’**.

3.5.3.1.1 Comando com envio seguro de mensagens (exemplos)

Este comando permite ao IFD escrever dados no EF selecionado de momento, com o cartão a verificar a integridade dos dados recebidos. Como não é exigida confidencialidade, os dados não são encriptados.

TCS_58 **Mensagem de comando**

Byte	Comprimento	Valor	Descrição
CLA	1	‘0Ch’	Pedido envio seguro de mensagens
INS	1	‘D6h’	Update Binary
P1	1	‘XXh’	Deslocamento em bytes desde o início do ficheiro: Byte mais significativo
P2	1	‘XXh’	Deslocamento em bytes desde o início do ficheiro: Byte menos significativo
Lc	1	‘XXh’	Comprimento do campo de dados securizado
#6	1	‘81h’	T_{PV}: Marcador para dados de valor simples
#7	L	‘NNh’ or ‘81 NNh’	L_{PV}: comprimento dos dados transmitidos. L é 2 bytes se L_{PV} > 127 bytes

▼B

Byte	Comprimento	Valor	Descrição
#(7+L)--#(6+L+NN)	NN	'XX..XXh'	Valor de dado simples (dados a escrever)
#(7+L+NN)	1	'8Eh'	T_{CC}: Marcador para soma criptográfica de teste
#(8+L+NN)	1	'XXh'	L_{CC}: Comprimento da soma criptográfica de teste *infra* '04h' para o envio seguro de mensagens da geração 1 (ver apêndice 11, parte A) '08h', '0Ch' ou '10h', dependendo do comprimento da chave AES para o envio seguro de mensagens da geração 2 (ver apêndice 11, parte B)
#(9+L+NN)--#(8+M+L+NN)	M	'XX..XXh'	Soma criptográfica de teste
Le	1	'00h'	Conforme a norma ISO/IEC 7816-4

TCS_59 **Mensagem de resposta se o formato de entrada do envio seguro de mensagens estiver correto:**

Byte	Comprimento	Valor	Descrição
#1	1	'99h'	T_{SW}: Marcador para palavras de estatuto (a proteger por CC)
#2	1	'02h'	L_{SW}: comprimento das palavras de estatuto devolvidas
#3-#4	2	'XXXXh'	Estado de processamento da APDU de resposta desprotegida
#5	1	'8Eh'	T_{CC}: Marcador para soma criptográfica de teste
#6	1	'XXh'	L_{CC}: Comprimento da soma criptográfica de teste *infra* '04h' para envio seguro de mensagens da geração 1 (ver apêndice 11, parte A) '08h', '0Ch' ou '10h', dependendo do comprimento da chave AES para o envio seguro de mensagens da geração 2 (ver apêndice 11, parte B)
#7-#(6+L)	L	'XX..XXh'	Soma criptográfica de teste
SW	2	'XXXXh'	Palavras de estatuto (SW1, SW2)

Os estados de processamento «regular», descritos relativamente ao comando UPDATE BINARY sem envio seguro de mensagens (ver ponto 3.5.3.1), podem ser devolvidos utilizando as estruturas de mensagem de resposta acima descritas.

Podem ocorrer alguns erros especificamente relacionados com o envio seguro de mensagens. Em tal caso, o estado de processamento é simplesmente devolvido, sem envolvimento de nenhuma estrutura de envio seguro de mensagens:

TCS_60 **Mensagem de resposta se houver erro no envio seguro de mensagens**

Byte	Comprimento	Valor	Descrição
SW	2	'XXXXh'	Palavras de estatuto (SW1, SW2)

▼B

— Se não estiver disponível nenhuma chave de sessão em curso, o estado de processamento **'6A88'** é devolvido.

— Se no formato de envio seguro de mensagens faltarem alguns objetos de dados esperados (cf. especificação supra), o estado de processamento **'6987'** é devolvido: este erro ocorre se faltar um marcador esperado ou se o corpo do comando não for construído adequadamente.

— Se alguns objetos de dados estiverem incorretos, o estado de processamento devolvido é **'6988'**: este erro ocorre se todos os marcadores necessários estiverem presentes mas alguns comprimentos forem diferentes dos esperados.

— Se falhar a verificação da soma criptográfica de teste, o estado de processamento devolvido é **'6688'**.

3.5.3.2 Comando com identificador EF curto

Esta variante de comando permite ao IFD selecionar um EF por meio de um identificador EF curto e escrever dados deste EF.

TCS_61 Um cartão tacográfico deve aceitar esta variante de comando para todos os ficheiros elementares que contenham um determinado identificador EF curto. Os presentes identificadores EF curtos são especificados no capítulo 4.

TCS_62 **Mensagem de comando**

Byte	Comprimento	Valor	Descrição
CLA	1	'00h'	
INS	1	'D6h'	Update Binary
P1	1	'XXh'	O bit 8 é fixado em 1 Os bits 7 e 6 são fixados em 00 O bit 5-1 codifica o identificador EF curto do EF correspondente
P2	1	'XXh'	Codifica um deslocamento de 0 a 255 bytes no EF referenciado por P1
Lc	1	'NNh'	Comprimento Lc dos dados a atualizar. Número de bytes a escrever
#6-#(5+NN)	NN	'XX..XXh'	Dados a escrever

TCS_63 **Mensagem de resposta**

Byte	Comprimento	Valor	Descrição
SW	2	'XXXXh'	Palavras de estatuto (SW1, SW2)

Nota: Os identificadores EF curtos utilizados para a aplicação tacográfica da geração 2 são especificados no capítulo 4.

Se P1 codificar um identificador EF curto e o comando for bem sucedido, o EF identificado passa a ser o EF selecionado no momento (EF atual).

▼B

— Se o comando for bem sucedido, o cartão devolve '**9000**'.

— Se o ficheiro correspondente ao identificador EF curto não for encontrado, o estado de processamento devolvido é **'6A82'**.

— Se o controlo de acesso do ficheiro selecionado não for satisfeito, o comando é interrompido com '**6982**'.

— Se o deslocamento não for compatível com a dimensão do EF (deslocamento > dimensão EF), o estado de processamento devolvido é **'6B00'**.

— Se a dimensão dos dados a escrever não for compatível com a dimensão do EF (deslocamento + Lc > dimensão EF), o estado de processamento devolvido é **'6700'**.

— Se for detetado um erro de integridade nos atributos do ficheiro, o cartão considera o ficheiro corrompido e irrecuperável e o estado de processamento devolvido é **'6400'** ou '**6581**'.

— Se a escrita não tiver êxito, o estado de processamento devolvido é **'6581'**.

3.5.3.3 Comando com byte de instrução ímpar

Esta variante de comando permite ao IFD escrever dados num EF com 32 768 bytes ou mais.

TCS_64 Um cartão tacográfico que aceite EF com 32 768 bytes ou mais deve aceitar esta variante de comando para esses EF. Um cartão tacográfico pode ou não aceitar esta variante de comando para outros EF.

TCS_65 **Mensagem de comando**

Byte	Comprimento	Valor	Descrição
CLA	1	'00h'	
INS	1	'D7h'	Update Binary
P1	1	'00h'	EF atual
P2	1	'00h'	
Lc	1	'NNh'	Comprimento Lc de dados no campo de dados de comando
#6-#(5+NN)	NN	'XX..XXh'	Objeto de dados do deslocamento com marcador '54h' || Objeto de dados discricionário com marcador '53h' que encapsula os dados a escrever

O IFD codifica o comprimento do objeto de dados do deslocamento e do objeto de dados discricionário com um número mínimo possível de octetos, ou seja, ao utilizar o byte de comprimento '01h', o IFD codifica um deslocamento/ comprimento de 0 a 255 e, ao utilizar o byte de comprimento '02h', um deslocamento/ comprimento de '256' até '65 535' bytes.

TCS_66 **Mensagem de resposta**

Byte	Comprimento	Valor	Descrição
SW	2	'XXXXh'	Palavras de estatuto (SW1, SW2)

▼B

— Se o comando for bem sucedido, o cartão devolve '**9000**'.

— Se não for selecionado nenhum EF, o estado de processamento devolvido é **'6986'**.

— Se o controlo de acesso do ficheiro selecionado não for satisfeito, o comando é interrompido com '**6982**'.

— Se o deslocamento não for compatível com a dimensão do EF (deslocamento > dimensão EF), o estado de processamento devolvido é **'6B00'**.

— Se a dimensão dos dados a escrever não for compatível com a dimensão do EF (deslocamento + Lc > dimensão EF), o estado de processamento devolvido é '**6700'**.

— Se for detetado um erro de integridade nos atributos do ficheiro, o cartão considera o ficheiro corrompido e irrecuperável e o estado de processamento devolvido é **'6400'** ou **'6500'**.

— Se a escrita não tiver êxito, o estado de processamento devolvido é **'6581'**.

3.5.3.3.1 Comando com envio seguro de mensagens (exemplo)

O exemplo a seguir ilustra a utilização do envio seguro de mensagens caso se aplique o controlo de acesso SM-MAC-G2.

TCS_67 Mensagem de comando

Byte	Comprimento	Valor	Descrição
CLA	1	'0Ch'	Pedido envio seguro de mensagens
INS	1	'D7h'	Update Binary
P1	1	'00h'	EF atual
P2	1	'00h'	
Lc	1	'XXh'	Comprimento do campo de dados securizado
#6	1	'B3h'	Marcador para dados de valor simples codificados em BER-TLV
#7	L	'NNh' or '81 NNh'	L_{PV}: comprimento dos dados transmitidos. L é 2 bytes se L_{PV} > 127 bytes.
#(7+L)--#(6+L+NN)	NN	'XX..XXh'	Dados simples codificados em BER-TLV, ou seja, objeto de dados do deslocamento com marcador '54h' || Objeto de dados discricionário com marcador '53h' que encapsula os dados a escrever
#(7+L+NN)	1	'8Eh'	T_{CC}: Marcador para soma criptográfica de teste
#(8+L+NN)	1	'XXh'	L_{CC}: Comprimento da soma criptográfica de teste *infra* '08h', '0Ch' ou '10h', dependendo do comprimento da chave AES para o envio seguro de mensagens da geração 2 (ver apêndice 11, parte B)
#(9+L+NN)--#(8+M+L+NN)	M	'XX..XXh'	Soma criptográfica de teste
Le	1	'00h'	Conforme a norma ISO/IEC 7816-4

▼B

TCS_68 Mensagem de resposta se o comando for bem sucedido

Byte	Comprimento	Valor	Descrição
#1	1	‘99h’	T_{SW}: Marcador para palavras de estatuto (a proteger por CC)
#2	1	‘02h’	L_{SW}: comprimento das palavras de estatuto devolvidas
#3-#4	2	‘XXXXh’	Estado de processamento da APDU de resposta desprotegida
#5	1	‘8Eh’	T_{CC}: Marcador para soma criptográfica de teste
#6	1	‘XXh’	L_{CC}: Comprimento da soma criptográfica de teste *infra* ‘08h’, ‘0Ch’ ou ‘10h’, dependendo do comprimento da chave AES para o envio seguro de mensagens da geração 2 (ver apêndice 11, parte B)
#7-#(6+L)	L	‘XX..XXh’	Soma criptográfica de teste
SW	2	‘XXXXh’	Palavras de estatuto (SW1, SW2)

3.5.4 *GET CHALLENGE*

Este comando cumpre a norma ISO/IEC 7816-4, mas tem utilização restrita, em comparação com o comando definido na norma.

O comando GET CHALLENGE pede ao cartão que emita um desafio, a fim de o utilizar num procedimento de segurança no âmbito do qual são enviados ao cartão um criptograma ou alguns dados cifrados.

TCS_69 O desafio emitido pelo cartão só é válido para o comando seguinte enviado ao cartão e que utiliza desafio.

TCS_70 **Mensagem de comando**

Byte	Comprimento	Valor	Descrição
CLA	1	‘00h’	
INS	1	‘84h’	INS
P1	1	‘00h’	P1
P2	1	‘00h’	P2
Le	1	‘08h’	Le (comprimento do desafio esperado)

TCS_71 **Mensagem de resposta**

Byte	Comprimento	Valor	Descrição
#1-#8	8	‘XX..XXh’	Desafio
SW	2	‘XXXXh’	Palavras de estatuto (SW1, SW2)

— Se o comando for bem sucedido, o cartão devolve ‘**9000**’.

— Se Le for diferente de ‘08h’, o estado de processamento é **‘6700’**.

— Se os parâmetros P1-P2 forem incorretos, o estado de processamento é **‘6A86’**.

▼B

3.5.5 *VERIFY*

Este comando cumpre a norma ISO/IEC 7816-4, mas tem utilização restrita, em comparação com o comando definido na norma.

Basta o cartão da oficina para aceitar este comando.

Outros tipos de cartões tacográficos podem ou não executar este comando, mas para esses cartões não é personalizada qualquer referência CHV. Portanto, não podem executar este comando com êxito. No caso de outros tipos de cartões tacográficos além dos cartões dos centros de ensaio, o comportamento, ou seja, o código de erro devolvido, fica fora do âmbito desta especificação se o comando for enviado.

O comando Verify inicia a comparação, no cartão, entre os dados CHV (PIN) enviados do comando e a CHV de referência memorizada no cartão.

TCS_72 O PIN introduzido pelo utilizador deve ser codificado ASCI e preenchido à direita com bytes 'FFh' até um comprimento de 8 bytes pelo IFD (ver também o tipo de dados WorkshopCardPIN no apêndice 1).

TCS_73 As aplicações tacográficas das gerações 1 e 2 utilizam o mesmo CHV de referência.

TCS_74 O cartão tacográfico verifica se o comando está corretamente codificado. Em caso negativo, o cartão não compara os valores CHV, não diminui o contador de tentativas remanescentes da CHV nem reinicializa o estatuto de segurança «PIN_Verified», mas interrompe-se o comando. Um comando é corretamente codificado se os bytes CLA, INS, P1, P2 e Lc tiverem os valores especificados, Le estiver ausente e o campo de dados de comando tiver o comprimento correto.

TCS_75 Se o comando for bem sucedido, reinicializa-se o contador de tentativas remanescentes da CHV. O valor inicial do contador de tentativas remanescentes da CHV é 5. Se o comando for bem sucedido, o cartão define o estatuto da segurança interna «PIN_Verified». O cartão reinicializa este estatuto de segurança se for reinicializado ou se o código CHV transmitido no comando não coincidir com a CHV de referência memorizada.

Nota: A utilização da mesma CHV de referência e de um estatuto de segurança global impede que um funcionário da oficina reintroduza o PIN após a seleção de outro DF da aplicação tacográfica.

TCS_76 Uma comparação mal sucedida é registada no cartão, ou seja, o contador de tentativas remanescentes da CHV é diminuído de um valor, a fim de limitar a quantidade de novas tentativas de utilização da CHV de referência.

TCS_77 **Mensagem de comando**

Byte	Comprimento	Valor	Descrição
CLA	1	'00h'	
INS	1	'20h'	INS
P1	1	'00h'	P1

▼B

Byte	Comprimento	Valor	Descrição
P2	1	‘00h’	P2 (a CHV verificada é implicitamente conhecida)
Lc	1	‘08h’	Comprimento do código CHV transmitido
#6-#13	8	‘XX..XXh’	CHV

TCS_78 **Mensagem de resposta**

Byte	Comprimento	Valor	Descrição
SW	2	‘XXXXh’	Palavras de estatuto (SW1, SW2)

— Se o comando for bem sucedido, o cartão devolve ‘**9000**’.

— Se a CHV de referência não for encontrada, o estado de processamento devolvido é **‘6A88’.**

— Se a CHV estiver bloqueada (o contador de tentativas remanescentes da CHV é nulo), o estado de processamento devolvido é **‘6983’**. Uma vez nesse estado, a CHV não poderá voltar a ser apresentada com êxito.

— Se a comparação não for bem sucedida, o contador de tentativas remanescentes decresce e é devolvido o estatuto **‘63CX’** (X>0 e X igual ao contador de tentativas remanescentes da CHV.

— Se a CHV de referência for considerada corrompida, o estado de processamento devolvido é **‘6400’** ou **‘6581’**.

— Se Lc for diferente de ‘08h’, o estado de processamento é ‘**6700**’.

3.5.6 *GET RESPONSE*

Este comando cumpre a norma ISO/IEC 7816-4.

Este comando (necessário e disponível somente para o protocolo T=0) é utilizado para transmitir dados do cartão ao dispositivo de interface (caso em que um comando tivesse incluído tanto Lc como Le).

O comando GET RESPONSE tem de ser emitido imediatamente após o comando que prepara os dados, sob pena de estes se perderem. Uma vez executado o comando GET RESPONSE (a menos que ocorram os erros ‘**61xx**’ ou ‘**6Cxx**’ — ver *infra*), os dados preparados anteriormente deixam de estar disponíveis.

TCS_79 **Mensagem de comando**

Byte	Comprimento	Valor	Descrição
CLA	1	‘00h’	
INS	1	‘C0h’	
P1	1	‘00h’	
P2	1	‘00h’	
Le	1	‘XXh’	Número esperado de bytes

▼B

TCS_80 **Mensagem de resposta**

Byte	Comprimento	Valor	Descrição
#1-#X	X	'XX..XXh'	Dados
SW	2	'XXXXh'	Palavras de estatuto (SW1, SW2)

— Se o comando for bem sucedido, o cartão devolve '**9000**'.

— Se não tiverem sido preparados dados pelo cartão, o estado de processamento devolvido é **'6900'** ou **'6F00'**.

— Se Le exceder o número de bytes disponíveis ou for nulo, o estado de processamento devolvido é **'6Cxx'**, onde 'xx' indica o número exato de bytes disponíveis. Nesse caso, os dados preparados estão ainda disponíveis para um comando GET RESPONSE subsequente.

— Se Le não for nulo e for menor do que o número de bytes disponíveis, os dados requeridos são enviados normalmente pelo cartão e o estado de processamento devolvido é **'61xx'**, onde 'xx' indica um número de bytes extra ainda disponíveis para um comando GET RESPONSE subsequente.

— Se o comando não for aceite (protocolo T=1), o cartão devolve **'6D00'**.

3.5.7 *PSO: VERIFY CERTIFICATE*

Este comando cumpre a norma ISO/IEC 7816-8, mas tem utilização restrita, em comparação com o comando definido na norma.

O comando VERIFY CERTIFICATE é utilizado pelo cartão para obter uma chave pública do exterior e verificar a sua validade.

3.5.7.1 Comando da geração 1 — par de resposta

TCS_81 Esta variante de comando é aceite apenas por uma aplicação tacográfica da geração 1.

TCS_82 Quando um comando VERIFY CERTIFICATE é bem sucedido, a chave pública é memorizada para futura utilização no ambiente de segurança. Esta chave é explicitamente estabelecida para utilização em comandos relativos à segurança (INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE ou VERIFY CERTIFICATE) pelo comando MSE (ver ponto 3.5.11), recorrendo ao seu identificador de chave.

TCS_83 Em qualquer caso, o comando VERIFY CERTIFICATE utiliza a chave pública previamente selecionada pelo comando MSE para abrir o certificado. Esta chave pública deve ser a de um Estado-Membro ou da Europa.

TCS_84 **Mensagem de comando**

Byte	Comprimento	Valor	Descrição
CLA	1	'00h'	
INS	1	'2Ah'	Executar operação de segurança
P1	1	'00h'	P1

▼B

Byte	Comprimento	Valor	Descrição
P2	1	‘AEh’	P2: dados codificados não BER-TLV (concatenação de elementos dos dados)
Lc	1	‘C2h’	Lc: Comprimento do certificado, 194 bytes
#6-#199	194	‘XX..XXh’	Certificado: concatenação de elementos dos dados (cf. apêndice 11)

TCS_85 **Mensagem de resposta**

Byte	Comprimento	Valor	Descrição
SW	2	‘XXXXh’	Palavras de estatuto (SW1, SW2)

— Se o comando for bem sucedido, o cartão devolve ‘**9000**’.

— Se a verificação do certificado falhar, o estado de processamento devolvido é **‘6688’**. O processo de verificação e desmontagem do certificado para G1 e G2 é descrito no apêndice 11.

— Se nenhuma chave pública estiver presente no ambiente de segurança, é devolvido **‘6A88’**.

— Se a chave pública selecionada (utilizada para desmontar o certificado) for considerada corrompida, o estado de processamento devolvido é **‘6400’** ou **‘6581’**.

— Apenas geração 1: Se a chave pública selecionada (utilizada para desmontar o certificado) tiver um CHA.LSB (`CertificateHolderAuthorisation.equipmentType`) diferente de ‘00’ (ou seja, não for a de um Estado-Membro ou da Europa), o estado de processamento devolvido é **‘6985’**.

3.5.7.2 Comando da geração 2 — par de resposta

Dependendo da dimensão da curva, os certificados ECC podem ser tão extensos que se torna impossível transmiti-los numa APDU única. Neste caso, de acordo com a norma ISO/IEC 7816-4, deve aplicar-se o encadeamento do comando e o certificado transmitido em dois PSO consecutivos: APDU de verificação do certificado.

A estrutura do certificado e os parâmetros de domínio são definidos no apêndice 11.

TCS_86 O comando pode ser executado no MF, no DF Tachograph e no DF Tachograph_G2 (ver também TCS_33).

TCS_87 **Mensagem de comando**

Byte	Comprimento	Valor	Descrição
CLA	1	‘X0h’	Byte CLA que indica encadeamento de comando: ‘00h’ o único ou o último comando da cadeia ‘10h’ não é o último comando de uma cadeia
INS	1	‘2Ah’	Executar operação de segurança
P1	1	‘00h’	
P2	1	‘BEh’	Verificar certificado autodescritivo

▼B

Byte	Comprimento	Valor	Descrição
Lc	1	'XXh'	Comprimento do campo de dados de comando, ver TCS_88 e TCS_89
#6-#5+L	L	'XX..XXh'	Dados codificados DER-TLV: Objeto de dados do corpo do certificado ECC como primeiro objeto de dados concatenado com o objeto de dados de assinatura do certificado ECC como segundo objeto de dados ou uma parte dessa concatenação. O marcador '7F21' e o comprimento correspondente não devem ser transmitidos. A ordem desses objetos de dados é fixa.

TCS_88 Às APDU de comprimento curto aplicam-se as disposições seguintes: O IFD utiliza o número mínimo necessário de APDU para transmitir a carga útil do comando e transmitir o número máximo de bytes na primeira APDU de comando, de acordo com o valor da dimensão do campo de informação do byte do cartão (ver TCS_14). Se o IFD tiver um comportamento diferente, o comportamento do cartão está fora de alcance.

TCS_89 Às APDU de aumento do comprimento aplicam-se as disposições seguintes: Se o certificado não couber numa única APDU, o cartão aceita o encadeamento de comando. O IFD utiliza o número mínimo necessário de APDU para transmitir a carga útil do comando e transmitir o número máximo de bytes na primeira APDU de comando. Se o IFD tiver um comportamento diferente, o comportamento do cartão está fora de alcance.

Nota: Segundo o apêndice 11, o cartão memoriza o certificado ou os conteúdos relevantes do certificado e atualiza o respetivo currentAuthenticatedTime.

A estrutura da mensagem de resposta e as palavras de estatuto são as definidas em TCS_85.

TCS_90 Além dos códigos de erro listados em TCS_85, o cartão pode devolver os seguintes códigos de erro:

— Se a chave pública selecionada (utilizada para desmontar o certificado) tiver um CHA.LSB (CertificateHolderAuthorisation.equipmentType) que não se adeque à verificação do certificado, o estado de processamento devolvido é '**6985**', de acordo com o apêndice 11.

— Se o currentAuthenticatedTime do cartão for posterior à data de validade do certificado, o estado de processamento devolvido é '**6985**'.

— Se for esperado o último comando da cadeia, o cartão devolve '**6883**'.

— Se forem enviados parâmetros incorretos no campo de dados de comando, o cartão devolve '**6A80**' (utilizado igualmente no caso de os objetos de dados não serem enviados na ordem especificada).

▼B

3.5.8 *INTERNAL AUTHENTICATE*

Este comando cumpre a norma ISO/IEC 7816-4.

TCS_91 No DF Tachograph geração 1, todos os cartões tacográficos são compatíveis com este comando. O comando pode ou não estar acessível no MF e/ou no DF Tachograph_G2. Em caso afirmativo, o comando interrompe-se com um código de erro adequado como a chave privada do cartão (Card.SK), já que o protocolo de autenticação da geração 1 está acessível apenas no DF_Tachograph geração 1.

É por intermédio do comando INTERNAL AUTHENTICATE que o IFD pode autenticar o cartão. O processo de autenticação, descrito no apêndice 11, inclui as seguintes declarações:

TCS_92 O comando INTERNAL AUTHENTICATE utiliza a chave privada do cartão (implicitamente selecionada) para assinar dados de autenticação, incluindo K1 (primeiro elemento para acordo de chave de sessão) e RND1, e utiliza a chave pública selecionada no momento (através do último comando MSE) para encriptar a assinatura e formar o testemunho de autenticação (mais pormenores no apêndice 11).

TCS_93 **Mensagem de comando**

Byte	Comprimento	Valor	Descrição
CLA	1	‘00h’	CLA
INS	1	‘88h’	INS
P1	1	‘00h’	P1
P2	1	‘00h’	P2
Lc	1	‘10h’	Comprimento dos dados enviados ao cartão
#6 — #13	8	‘XX..XXh’	Desafio utilizado para autenticar o cartão
#14 -#21	8	‘XX..XXh’	VU.CHR (ver apêndice 11)
Le	1	‘80h’	Comprimento dos dados esperados do cartão

TCS_94 **Mensagem de resposta**

Byte	Comprimento	Valor	Descrição
#1-#128	128	‘XX..XXh’	Testemunho de autenticação do cartão (ver apêndice 11)
SW	2	‘XXXXh’	Palavras de estatuto (SW1, SW2)

— Se o comando for bem sucedido, o cartão devolve ‘**9000**’.

— Se nenhuma chave pública estiver presente no ambiente de segurança, o estado de processamento devolvido é **‘6A88’**.

— Se nenhuma chave privada estiver presente no ambiente de segurança, o estado de processamento devolvido é **‘6A88’**.

— Se VU.CHR não corresponder ao identificador de chave pública em curso, o estado de processamento devolvido é **‘6A88’**.

▼B

— Se a chave privada selecionada for considerada corrompida, o estado de processamento devolvido é **'6400'** ou **'6581'**.

TCS_95 Se o comando INTERNAL AUTHENTICATE for bem sucedido, a chave de sessão em curso, a existir, é apagada e deixa de estar disponível. Para dispor de uma nova chave de sessão, tem de se executar com êxito o comando EXTERNAL AUTHENTICATE para o mecanismo de autenticação da geração 1.

3.5.9 *EXTERNAL AUTHENTICATE*

Este comando cumpre a norma ISO/IEC 7816-4.

É por intermédio do comando EXTERNAL AUTHENTICATE que o cartão pode autenticar o IFD. O processo de autenticação para os tacógrafos G1 e G2 (autenticação VU) é descrito no apêndice 11.

TCS_96 A variante de comando para o mecanismo de autenticação mútua da geração 1 é compatível apenas com aplicações tacográficas da geração 1.

TCS_97 A variante de comando destinada a autenticação mútua do cartão VU da segunda geração pode ser executada no MF, no DF Tachograph e no DF Tachograph_G2 (ver igualmente TCS_34).

TCS_98 **Mensagem de comando**

Byte	Comprimento	Valor	Descrição
CLA	1	'00h'	CLA
INS	1	'82h'	INS
P1	1	'00h'	Chaves e algoritmos implicitamente conhecidos
P2	1	'00h'	
Lc	1	'XXh'	Lc (comprimento dos dados enviados ao cartão)
#6-#(5+L)	L	'XX..XXh'	Autenticação da geração 1: Criptograma (ver apêndice 11, parte A) Autenticação da geração 2: Assinatura gerada pelo IFD (ver apêndice 11, parte B)

TCS_99 **Mensagem de resposta**

Byte	Comprimento	Valor	Descrição
SW	2	'XXXXh'	Palavras de estatuto (SW1, SW2)

— Se o comando for bem sucedido, o cartão devolve '**9000**'.

— Se o CHA da chave pública estabelecida não for a concatenação do AID da aplicação tacográfica e de um tipo de equipamento VU, o estado de processamento devolvido é **'6F00'**.

— Se o comando não for imediatamente precedido por um comando GET CHALLENGE, o estado de processamento devolvido é **'6985'**.

▼B

A aplicação tacográfica da geração 1 pode devolver outros códigos de erro a seguir indicados:

— Se nenhuma chave pública estiver presente no ambiente de segurança, é devolvido **'6A88'**.

— Se nenhuma chave privada estiver presente no ambiente de segurança, o estado de processamento devolvido é **'6A88'**.

— Se a verificação do criptograma estiver errada, o estado de processamento devolvido é **'6688'**.

— Se a chave privada selecionada for considerada corrompida, o estado de processamento devolvido é **'6400'** ou **'6581'**.

A variante de comando para a autenticação da geração 2 pode devolver ainda o seguinte código de erro:

— Se a verificação da assinatura falhar, o cartão devolve '**6300**'.

3.5.10 *GENERAL AUTHENTICATE*

Este comando, que cumpre a norma ISO/IEC 7816-4, é utilizado para o protocolo de autenticação da pastilha (chip) da geração 2 especificada no apêndice 11, parte B.

TCS_100 O comando pode ser executado no MF, no DF Tachograph e no DF Tachograph_G2 (ver também TCS_34).

TCS_101 **Mensagem de comando**

Byte	Comprimento	Valor	Descrição
CLA	1	'00h'	
INS	1	'86h'	
P1	1	'00h'	Chaves e protocolo implicitamente conhecidos
P2	1	'00h'	
Lc	1	'NNh'	Lc: comprimento do campo de dados subsequente
#6-#(5+L)	L	'7Ch' + L_{7C} + '80h' + L_{80} + 'XX..XXh'	Valor da chave pública efémera codificada DER-TLV (ver apêndice 11) A VU envia os objetos de dados por esta ordem.

TCS_102 **Mensagem de resposta**

Byte	Comprimento	Valor	Descrição
#1-#L	L	'7Ch' + L_{7C} + '81h' + '08h' + 'XX..XXh' + '82h' + L_{82} + 'XX..XXh'	Dados de autenticação dinâmica codificados DER-TLV: nonce e testemunho de autenticação (ver apêndice 11)
SW	2	'XXXXh'	Palavras de estatuto (SW1, SW2)

— Se o comando for bem sucedido, o cartão devolve '**9000**'.

— O cartão devolve '**6A80**' para indicar parâmetros incorretos no campo de dados.

▼B

— O cartão devolve '**6982**' se o comando EXTERNAL AUTHENTICATE não tiver sido executado com êxito

A resposta '7Ch' objeto de dados de autenticação dinâmica:

— deve esta presente se a operação for bem sucedida, ou seja, as palavras de estatuto são '**9000**';

— deve estar ausente no caso de um erro de execução ou erro de verificação, ou seja, se as palavras de estatuto estiverem no intervalo '**6400**'-'**6FFF**', e

— pode estar ausente em caso de alerta, ou seja, se as palavras de estatuto estiverem no intervalo '**6200**'--'**63FF**'.

3.5.11 *MANAGE SECURITY ENVIRONMENT*

Utiliza-se este comando para estabelecer uma chave pública com fins de autenticação.

3.5.11.1 Comando da geração 1 — par de resposta

Este comando cumpre a norma ISO/IEC 7816-4. A comparar com a norma, a sua utilização é restrita.

TCS_103 Este comando é aceite apenas por uma aplicação tacográfica da geração 1.

TCS_104 A chave referenciada no campo de dados MSE mantém-se como chave pública em curso até ao próximo comando MSE correto, até ser selecionado um DF ou até o cartão ser reinicializado.

TCS_105 Se a chave referenciada não estiver (já) presente no cartão, o ambiente de segurança mantém-se inalterado.

TCS_106 **Mensagem de comando**

Byte	Comprimento	Valor	Descrição
CLA	1	'00h'	CLA
INS	1	'22h'	INS
P1	1	'C1h'	P1: chave referenciada válida para todas as operações criptográficas
P2	1	'B6h'	P2 (dados referenciados relativos à assinatura digital)
Lc	1	'0Ah'	Lc: comprimento do campo de dados subsequente
#6	1	'83h'	Marcador para referenciar uma chave pública em casos assimétricos
#7	1	'08h'	Comprimento da referência da chave (identificador da chave)
#8-#15	8	'XX..XXh'	Identificador de chave, conforme especifica o apêndice 11

TCS_107 **Mensagem de resposta**

Byte	Comprimento	Valor	Descrição
SW	2	'XXXXh'	Palavras de estatuto (SW1, SW2)

▼B

— Se o comando for bem sucedido, o cartão devolve '**9000**'.

— Se a chave referenciada não estiver presente no cartão, o estado de processamento devolvido é **'6A88'**.

— Se no formato de envio seguro de mensagens faltarem alguns objetos de dados esperados, o estado de processamento **'6987'** é devolvido. O que pode ocorrer se faltar o marcador '83h'.

— Se alguns objetos de dados estiverem incorretos, o estado de processamento devolvido é **'6988'**. O que pode ocorrer se o comprimento do identificador de chave não for '08h'.

— Se a chave selecionada for considerada corrompida, o estado de processamento devolvido é **'6400'** ou **'6581'**.

3.5.11.2 Comando da geração 2 — pares de resposta

Para a autenticação da geração 2 o cartão tacográfico é compatível com as versões *infra* do comando MSE:SET, que cumprem a norma ISO/IEC 7816-4. Estas versões de comando não são compatíveis com a autenticação da geração 1.

3.5.11.2.1 MSE:SET AT para autenticação da pastilha (chip)

Utiliza-se o comando MSE:SET AT a seguir indicado para selecionar os parâmetros da autenticação da pastilha que são executados por um comando GENERAL AUTHENTICATE subsequente.

TCS_108 O comando pode ser executado no MF, no DF Tachograph e no DF Tachograph_G2 (ver também TCS_34).

TCS_109 **Mensagem de comando MSE:SET AT para autenticação da pastilha**

Byte	Comprimento	Valor	Descrição
CLA	1	'00h'	
INS	1	'22h'	
P1	1	'41h'	Definir para autenticação interna
P2	1	'A4h'	Autenticação
Lc	1	'NNh'	Lc: comprimento do campo de dados subsequente
#6-#(5+L)	L	'80h' + '0Ah' + 'XX..XXh'	Referência do mecanismo criptográfico codificado DER-TLV: Identificador de objeto de autenticação da pastilha (apenas valor, o marcador '06h' é omitido). Ver apêndice 1 acerca dos valores dos identificadores de objeto; deve ser utilizada a notação de byte. Ver apêndice 11 a título de orientação sobre como selecionar um destes identificadores de objeto.

3.5.11.2.2 MSE:SET AT para autenticação VU

Utiliza-se o comando MSE:SET AT a seguir indicado para selecionar os parâmetros e as chaves da autenticação VU que são executados por um comando EXTERNAL AUTHENTICATE subsequente.

▼B

TCS_110 O comando pode ser executado no MF, no DF Tachograph e no DF Tachograph_G2 (ver também TCS_34).

TCS_111 **Mensagem de comando MSE:SET AT para autenticação VU**

Byte	Comprimento	Valor	Descrição
CLA	1	‘00h’	
INS	1	‘22h’	
P1	1	‘81h’	Definir para autenticação externa
P2	1	‘A4h’	Autenticação
Lc	1	‘NNh’	Lc: comprimento do campo de dados subsequente
#6-#(5+L)	L	‘80h’ + ‘0Ah’ + ‘XX..XXh’	Referência do mecanismo criptográfico codificado DER--TLV: Identificador de objeto de autenticação VU (apenas valor, o marcador ‘06h’ é omitido). Ver apêndice 1 acerca dos valores dos identificadores de objeto; deve ser utilizada a notação de byte. Ver apêndice 11 a título de orientação sobre como selecionar um destes identificadores de objeto.
		‘83h’ + ‘08h’ + ‘XX..XXh’	Referência codificada DER-TLV da chave pública VU pela referência do titular do certificado mencionada no respetivo certificado.
		‘91h’ + L_{91} + ‘XX..XXh’	Representação comprimida codificada DER-TLV da chave pública efémera da VU que será utilizada durante a autenticação da pastilha (ver apêndice 11)

3.5.11.2.3 MSE:SET DST

Utiliza-se o comando MSE:SET DST para definir uma chave pública:

— quer para a verificação de uma assinatura fornecida num comando PSO: VERIFY DIGITAL SIGNATURE subsequente

— quer para a verificação da assinatura de um certificado fornecido num comando PSO: VERIFY CERTIFICATE subsequente.

TCS_112 O comando pode ser executado no MF, no DF Tachograph e no DF Tachograph_G2 (ver também TCS_33).

TCS_113 **Mensagem de comando MSE:SET DST**

Byte	Comprimento	Valor	Descrição
CLA	1	‘00h’	
INS	1	‘22h’	
P1	1	‘81h’	Definir para verificação
P2	1	‘B6h’	Assinatura digital

▼B

Lc	1	‘NNh’	Lc: comprimento do campo de dados subsequente
#6-#(5+L)	L	‘83h’ + ‘08h’ + ‘XX...XXh’	Referência codificada DER-TLV de uma chave pública, ou seja, a referência do titular do certificado no certificado da chave pública (ver apêndice 11)

A estrutura da mensagem de resposta e as palavras de estatuto de todas as versões de comando são dadas por:

TCS_114 **Mensagem de resposta**

Byte	Comprimento	Valor	Descrição
SW	2	‘XXXXh’	Palavras de estatuto (SW1, SW2)

— Se o comando for bem sucedido, o cartão devolve ‘**9000**’. O protocolo foi selecionado e inicializado.

— **‘6A80’** indica parâmetros incorretos no campo de dados de comando.

— **‘6A88’** indica que os dados referenciados (ou seja, uma chave referenciada) não estão disponíveis.

3.5.12 *PSO: HASH*

Utiliza-se este comando para transferir, para o cartão, o resultado de um cálculo HASH sobre alguns dados. Serve para a verificação de assinaturas digitais. O valor de HASH é memorizado temporariamente para o comando PSO: VERIFY DIGITAL SIGNATURE subsequente.

Este comando cumpre a norma ISO/IEC 7816-8. A comparar com a norma, a sua utilização é restrita.

Para aceitar este comando em DF Tachograph e DF Tachograph_G2 é necessário apenas o cartão de controlo.

Outros tipos de cartões tacográficos podem ou não executar este comando. O comando pode estar acessível ou não no MF.

A aplicação do cartão de controlo da geração 1 aceita apenas SHA-1.

TCS_115 O valor HASH memorizado temporariamente será apagado se for calculado um novo valor HASH por meio do comando PSO: HASH, se for selecionado um DF ou se o cartão tacográfico for reinicializado.

TCS_116 **Mensagem de comando**

Byte	Comprimento	Valor	Descrição
CLA	1	‘00h’	CLA
INS	1	‘2Ah’	Executar operação de segurança
P1	1	‘90h’	Devolver HASH CODE

▼B

Byte	Comprimento	Valor	Descrição
P2	1	‘A0h’	Marcador: o campo de dados contém DO com interesse para a função hash
Lc	1	‘XXh’	Comprimento Lc do campo de dados subsequente
#6	1	‘90h’	Marcador para HASH CODE
#7	1	‘XXh’	Comprimento L do HASH CODE: ‘14h’ na aplicação da geração 1 (ver apêndice 11, parte A) ‘20h’, ‘30h’ ou ‘40h’ na aplicação da geração 2 (ver apêndice 11, parte B)
#8-#(7+L)	L	‘XX..XXh’	HASH CODE

TCS_117 **Mensagem de resposta**

Byte	Comprimento	Valor	Descrição
SW	2	‘XXXXh’	Palavras de estatuto (SW1, SW2)

— Se o comando for bem sucedido, o cartão devolve ‘**9000**’.

— Se faltarem alguns objetos de dados esperados (cf. especificação *supra*), o estado de processamento **‘6987’** é devolvido. O que pode ocorrer se faltar um dos marcadores ‘90h’.

— Se alguns objetos de dados estiverem incorretos, o estado de processamento devolvido é **‘6988’**. Este erro ocorre se o marcador necessário estiver presente mas com comprimento diferente de ‘14h’ para SHA-1, ‘20h’ para SHA-256, ‘30h’ para SHA-384, ‘40h’ para SHA--512 (aplicação da geração 2).

3.5.13 *PERFORM HASH of FILE*

Este comando não cumpre a norma ISO/IEC 7816-8. Por conseguinte, o seu byte CLA indica que existe uma utilização privada do PERFORM SECURITY OPERATION / HASH.

Para aceitar este comando em DF Tachograph e DF Tachograph_G2 são necessários apenas o cartão de condutor e o cartão da oficina.

Outros tipos de cartões tacográficos podem ou não executar este comando. Se uma empresa ou cartão de controlo o executar, o comando será executado conforme se especifica neste capítulo.

O comando pode ou não estar acessível no MF. Em caso afirmativo, é executado conforme se especifica neste capítulo, ou seja, não permite o cálculo de um valor HASH, mas interrompe-se com um código de erro adequado.

TCS_118 O comando PERFORM HASH OF FILE utiliza-se para controlar a área de dados do EF transparente selecionado no momento.

TCS_119 Um cartão tacográfico aceita este comando apenas para os EF enumerados no capítulo 4 em DF_Tachograph e DF_Tachograph_G2, com a seguinte exceção: um cartão tacográfico não é compatível com o comando para o EF Sensor_Installation_Data do DF Tachograph_G2.

▼B

TCS_120 O resultado da operação HASH é memorizado temporariamente no cartão, podendo ser utilizado para obter uma assinatura digital do ficheiro, por intermédio do comando PSO: COMPUTE DIGITAL SIGNATURE.

TCS_121 O valor HASH OF FILE memorizado temporariamente será apagado se for calculado um novo valor HASH OF FILE por meio do comando PSO: HASH OF FILE, se for selecionado um DF ou se o cartão tacográfico for reinicializado.

TCS_122 A aplicação tacográfica da geração 1 é compatível com SHA-1.

TCS_123 A aplicação tacográfica da geração 2 é compatível com SHA-1 e SHA-2 (256, 384 e 512 bits).

TCS_124 **Mensagem de comando**

Byte	Comprimento	Valor	Descrição
CLA	1	‘80h’	CLA
INS	1	‘2Ah’	Executar operação de segurança
P1	1	‘90h’	Marcador: HASH
P2	1	‘XXh’	P2: Indica o algoritmo a utilizar para a função HASH dos dados do ficheiro transparente selecionado no momento: ‘00h’ para SHA-1 ‘01h’ para SHA-256 ‘02h’ para SHA-384 ‘03h’ para SHA-512

TCS_125 **Mensagem de resposta**

Byte	Comprimento	Valor	Descrição
SW	2	‘XXXXh’	Palavras de estatuto (SW1, SW2)

— Se o comando for bem sucedido, o cartão devolve ‘**9000**’.

— Se o EF atual não permitir este comando (EF Sensor_Installation_Data no DF Tachograph_G2), o estado de processamento **‘6985’** é devolvido.

— Se o EF selecionado for considerado corrompido (erros de integridade nos atributos do ficheiro ou nos dados memorizados), o estado de processamento devolvido é ‘**6400**’ ou **‘6581’**.

— Se o ficheiro selecionado não for transparente ou se não houver EF no momento, o estado de processamento devolvido é ‘**6986**’.

3.5.14 *PSO: COMPUTE DIGITAL SIGNATURE*

Utiliza-se este comando para calcular a assinatura digital do código HASH previamente calculado (ver PERFORM HASH OF FILE, ponto3.5.13).

Para aceitar este comando em DF Tachograph e DF Tachograph_G2 são necessários apenas o cartão de condutor e o cartão da oficina.

▼B

Outros tipos de cartões tacográficos podem ou não executar este comando, mas não terão chave de assinatura. Por conseguinte, estes cartões não podem executar o comando com êxito, mas interrompem-se com um código de erro adequado.

O comando pode estar ou não acessível no MF. Em caso afirmativo, interrompe-se com um código de erro adequado.

Este comando cumpre a norma ISO/IEC 7816-8. A comparar com a norma, a sua utilização é restrita.

TCS_126 Este comando não calcula uma assinatura digital de código HASH previamente calculado com o comando PSO: HASH.

TCS_127 A chave privada do cartão é utilizada para calcular a assinatura digital e é implicitamente conhecida pelo cartão.

TCS_128 A aplicação tacográfica da geração 1 executa uma assinatura digital por um método de preenchimento que cumpre PKCS1 (ver apêndice 11 para mais pormenores).

TCS_129 A aplicação tacográfica da geração 2 calcula uma assinatura digital baseada na curva elíptica (ver apêndice 11 para mais pormenores).

TCS_130 **Mensagem de comando**

Byte	Comprimento	Valor	Descrição
CLA	1	‘00h’	CLA
INS	1	‘2Ah’	Executar operação de segurança
P1	1	‘9Eh’	Assinatura digital a devolver
P2	1	‘9Ah’	Marcador: o campo de dados contém dados a assinar. Como nenhum campo de dados é incluído, assume-se que os dados estão já presentes no cartão (HASH OF FILE)
Le	1	‘NNh’	Comprimento da assinatura esperada

TCS_131 **Mensagem de resposta**

Byte	Comprimento	Valor	Descrição
#1-#L	L	‘XX..XXh’	Assinatura do HASH previamente calculado
SW	2	‘XXXXh’	Palavras de estatuto (SW1, SW2)

— Se o comando for bem sucedido, o cartão devolve ‘**9000**’.

— Se a chave privada implicitamente selecionada for considerada corrompida, o estado de processamento devolvido é ‘**6400**’ ou **‘6581’**.

— Se o HASH calculado num comando PERFORM HASH OF FILE anterior não estiver disponível, o estado de processamento devolvido é **‘6985’**.

▼B

3.5.15 *PSO: VERIFY DIGITAL SIGNATURE*

Utiliza-se este comando para verificar a assinatura digital, fornecida sob a forma de entrada, cujo HASH é conhecido pelo cartão. O algoritmo da assinatura é implicitamente conhecido pelo cartão.

Este comando cumpre a norma ISO/IEC 7816-8. A comparar com a norma, a sua utilização é restrita.

Para aceitar este comando em DF Tachograph e DF Tachograph_G2 é necessário apenas o cartão de controlo.

Outros tipos de cartões tacográficos podem executar ou não este comando. O comando pode estar acessível ou não no MF.

TCS_132 O comando VERIFY DIGITAL SIGNATURE utiliza sempre a chave pública selecionada pelo anterior comando MANAGE SECURITY ENVIRONMENT MSE: SET DST e o anterior HASH CODE introduzido por um comando PSO: HASH.

TCS_133 **Mensagem de comando**

Byte	Comprimento	Valor	Descrição
CLA	1	‘00h’	CLA
INS	1	‘2Ah’	Executar operação de segurança
P1	1	‘00h’	
P2	1	‘A8h’	Marcador: campo de dados contém DO com interesse para verificação
Lc	1	‘83h’	Comprimento Lc do campo de dados subsequente
6	1	‘9Eh’	Marcador para assinatura digital
#7-#8	2	‘81 XXh’	Comprimento da assinatura digital: 128 bytes codificados em conformidade com o apêndice 11, parte A, para a aplicação tacográfica da geração 1 Dependendo da curva selecionada para a aplicação tacográfica da geração 2 (ver apêndice 11, parte B)
#9-#(8+L)	L	‘XX..XXh’	Conteúdo da assinatura digital

TCS_134 **Mensagem de resposta**

Byte	Comprimento	Valor	Descrição
SW	2	‘XXXXh’	Palavras de estatuto (SW1, SW2)

— Se o comando for bem sucedido, o cartão devolve ‘**9000**’.

— Se a verificação da assinatura falhar, o estado de processamento devolvido é **‘6688’**. O processo de verificação é descrito no apêndice 11.

— Se nenhuma chave pública for selecionada, o estado de processamento devolvido é **‘6A88’**.

— Se faltarem alguns objetos de dados esperados (cf. especificação supra), o estado de processamento **‘6987’** é devolvido. O que pode ocorrer se faltar um dos marcadores exigidos.

▼B

— Se não estiver disponível nenhum HASH CODE para processar o comando (em resultado de um anterior comando PSO: HASH), o estado de processamento devolvido é **'6985'**.

— Se alguns objetos de dados estiverem incorretos, o estado de processamento devolvido é **'6988'**. O que pode ocorrer se o comprimento de um dos objetos de dados exigidos for incorreto.

— Se a chave pública selecionada for considerada corrompida, o estado de processamento devolvido é **'6400'** ou **'6581'**.

3.5.16 *PROCESS DSRC MESSAGE*

Utiliza-se este comando para verificar a integridade e a autenticidade da mensagem DSRC e para decifrar os dados comunicados a partir de uma VU a uma autoridade de controlo ou a uma oficina, através da ligação DSRC. O cartão deriva a chave de encriptação e a chave MAC utilizada para proteger a mensagem DSRC, conforme descrito no apêndice 11, parte B, capítulo 13.

Para aceitar este comando em DF Tachograph_G2 são necessários apenas o cartão de controlo e o cartão da oficina.

Outros tipos de cartões tacográficos podem executar ou não este comando, mas não terão uma chave de segurança DSRC. Por conseguinte, estes cartões não podem executar o comando com êxito, mas interrompem-se com um código de erro adequado.

O comando pode estar acessível ou não no MF e/ou no DF Tachograph. Em caso afirmativo, interrompe-se com um código de erro adequado.

TCS_135 A chave de segurança DSRC é acessível apenas no DF Tachograph_G2, ou seja, o cartão de controlo e de oficina é compatível com uma execução bem sucedida do comando apenas no DF Tachograph_G2.

TCS_136 O comando apenas decifra os dados DSRC e verifica a soma criptográfica de teste, mas não interpreta os dados de entrada.

TCS_137 A ordem dos objetos de dados no campo de dados de comando é fixada por esta especificação.

TCS_138 **Mensagem de comando**

Byte	Comprimento	Valor	Descrição
CLA	1	'80h'	CLA de uso privado
INS	1	'2Ah'	Executar operação de segurança
P1	1	'80h'	Dados da resposta: valor simples
P2	1	'B0h'	Dados do comando: valor simples codificado em BER-TLV e que inclui SM DO
Lc	1	'NNh'	Comprimento Lc do campo de dados subsequente

▼B

Byte	Comprimento	Valor	Descrição
#6-#(5+L)	L	'87h' + L_{87} + 'XX..XXh'	Byte indicador de preenchimento do conteúdo codificado DER-TLV seguido por carga útil do tacógrafo encriptada. Para o byte indicador de preenchimento do conteúdo utiliza-se o valor '00h' ('nenhuma indicação adicional', de acordo com a norma ISO/IEC 7816-4:2013, quadro 52). Relativamente ao mecanismo de criptografia ver apêndice 11, parte B, capítulo 13. Os valores permitidos para o comprimento L_{87} são os múltiplos do comprimento de bloco AES mais 1 para o byte indicador de preenchimento do conteúdo, ou seja, de 17 a 193 bytes, inclusive. *Nota:* Ver ISO/IEC 7816-4:2013, quadro 49, para o objeto de dados SM com marcador '87h'.
		'81h' + '10h'	Modelo de referência do controlo codificado DER-TLV para a confidencialidade que encadeia a concatenação dos elementos de dados seguintes (ver apêndice 1 DSRCSecurityData e apêndice 11, parte B, capítulo 13): — validação cronológica de 4 bytes — contador de 3 bytes — número de série da VU de 8 bytes — versão da chave de segurança DSRC de 1 byte *Nota:* Ver ISO/IEC 7816-4:2013, quadro 49, para o objeto de dados SM com marcador '81h'.
		'8Eh' + L_{8E} + 'XX..XXh'	MAC codificado DER-TLV através da mensagem DSRC. Relativamente ao algoritmo e ao cálculo MAC, ver apêndice 11, parte B, capítulo 13. *Nota:* Ver ISO/IEC 7816-4:2013, quadro 49, para o objeto de dados SM com marcador '8Eh'.

TCS_139 **Mensagem de resposta**

Byte	Comprimento	Valor	Descrição
#1-#L	L	'XX..XXh'	Ausente (no caso de um erro) ou dados decifrados (preenchimento removido)
SW	2	'XXXXh'	Palavras de estatuto (SW1, SW2)

— Se o comando for bem sucedido, o cartão devolve '**9000**'.

— **'6A80'** indica parâmetros incorretos no campo de dados de comando (utilizado igualmente no caso de os objetos de dados não serem enviados na ordem especificada).

— **'6A88'** indica que os dados referenciados não estão disponíveis, ou seja, a chave de segurança DSRC referenciada não está disponível.

— **'6900'** indica que a verificação da soma criptográfica de teste ou a desencriptação dos dados falhou.

4. ESTRUTURA DOS CARTÕES TACOGRÁFICOS

Esta secção especifica as estruturas de ficheiro dos cartões tacográficos para memorização de dados acessíveis.

▼B

Não especifica estruturas internas dependentes do fabricante do cartão, como, por exemplo, cabeçalhos do ficheiro, nem a memorização ou o manuseamento de elementos de dados necessários unicamente para utilização interna, como EuropeanPublicKey,CardPrivateKey,TdesSessionKey ouWorkshopCardPin.

TCS_140 Um cartão tacográfico da geração 2 acolhe o ficheiro principal MF e uma aplicação tacográfica da geração 1 e da geração 2 do mesmo tipo (por exemplo, aplicações para cartão de condutor).

TCS_141 Um cartão tacográfico aceita, pelo menos, o número mínimo de registos especificados para as aplicações correspondentes e não aceita mais registos do que o número máximo de registos especificados para as aplicações correspondentes.

Neste capítulo especificam-se os números máximos e mínimos de registos para as diferentes aplicações.

Relativamente ao controlo de acesso utilizado nas regras de acesso ao longo deste capítulo, consultar o capítulo 3.3. De um modo geral, o modo de acesso «read» denota o comando READ BINARY com byte INS par e, se aceite, ímpar, à exceção do EF Sensor_Installation_Data no cartão da oficina (ver TCS_156 e TCS_160). O modo de acesso «update» denota o comando UPDATE BINARY com byte INS par e, se aceite, ímpar, e o modo de acesso «select» o comando SELECT.

4.1. Ficheiro principal MF

TCS_142 Uma vez personalizado, o ficheiro principal MF terá permanentemente as seguintes estrutura de ficheiro e regras de acesso do ficheiro:

Nota: Ao SFID do identificador EF curto é atribuído um número decimal: por exemplo, o valor 30 corresponde a 11110 em binário.

			Access rules	
File	**File ID**	**SFID**	**Read / Select**	**Update**
MF	'3F00h'			
├─ EF ICC	'0002h'		ALW	NEV
├─ EF IC	'0005h'		ALW	NEV
├─ EF DIR	'2F00h'	30	ALW	NEV
├─ EF ATR/INFO (conditional)	'2F01h'	29	ALW	NEV
├─ EF Extended_Length (conditional)	'0006h'	28	ALW	NEV
├─ DF Tachograph	'0500h'		SC1	
└─ DF Tachograph_G2			SC1	

Neste quadro, utiliza-se a seguinte abreviatura para o controlo de acesso:

SC1 ALW OR SM-MAC-G2

TCS_143 Todas as estruturas de EF são transparentes.

TCS_144 O ficheiro principal MF tem a seguinte estrutura de dados:

▼B

File / Data element	No of Records	Size (bytes) Min	Size (bytes) Max	Default Values
MF		*63*	*164*	
└─EF ICC		*25*	*25*	
└─CardIccIdentification		*25*	*25*	
├─clockStop		1	1	{00}
├─cardExtendedSerialNumber		8	8	{00..00}
├─cardApprovalNumber		8	8	{20..20}
├─cardPersonaliserID		1	1	{00}
├─embedderIcAssemblerId		5	5	{00..00}
└─icIdentifier		2	2	{00 00}
└─EF IC		*8*	*8*	
└─CardChipIdentification		*8*	*8*	
├─icSerialNumber		4	4	{00..00}
└─icManufacturingReferences		4	4	{00..00}
└─EF DIR		*20*	*20*	
└─See TCS_145		*20*	*20*	{00..00}
└─EF ATR/INFO		*7*	*128*	
└─See TCS_146		*7*	*128*	{00..00}
└─EF EXTENDED_LENGTH		*3*	*3*	
└─See TCS_147		*3*	*3*	{00..00}
└─DF Tachograph				
└─DF Tachograph_G2				

TCS_145 O ficheiro elementar EF DIR contém os seguintes objetos de dados relacionados com a aplicação: '61 08 4F 06 FF 54 41 43 48 4F 61 08 4F 06 FF 53 4D 52 44 54'

TCS_146 O ficheiro elementar EF ATR/INFO estará presente se o cartão tacográfico indicar no seu ATR que aceita o aumento dos campos de comprimento. Neste caso, o EF ATR/INFO conterá o aumento do objeto de dados da informação de comprimento (DO'7F66'), conforme a norma ISO/IEC 7816-4:2013 (cláusula 12.7.1).

TCS_147 O ficheiro elementar EF Extended_Length está presente se o cartão tacográfico indicar no seu ATR que aceita o aumento dos campos de comprimento. Neste caso, o EF contém o seguinte objeto de dados: '02 01 xx', onde o valor 'xx' indica se o aumento dos campos de comprimento é aceite para o protocolo T = 1 e/ou T = 0.

O valor '01' indica suporte do aumento do campo de comprimento para o protocolo T = 1.

O valor '10' indica suporte do aumento do campo de comprimento para o protocolo T = 0.

O valor '11' indica suporte do aumento do campo de comprimento para o protocolo T = 1 e o T = 0.

4.2. Aplicações para cartão de condutor

4.2.1 *Aplicação para cartão de condutor da geração 1*

TCS_148 Uma vez personalizada, a aplicação para cartão de condutor da geração 1 terá permanentemente as seguintes estrutura de ficheiro e regras de acesso do ficheiro:

File	File ID	Access rules: Read	Access rules: Select	Access rules: Update
└─DF Tachograph	'0500h'		SC1	
├─EF Application_Identification	'0501h'	SC2	SC1	NEV
├─EF Card_Certificate	'C100h'	SC2	SC1	NEV
├─EF CA_Certificate	'C108h'	SC2	SC1	NEV
├─EF Identification	'0520h'	SC2	SC1	NEV
├─EF Card_Download	'050Eh'	SC2	SC1	SC1
├─EF Driving_Licence_Info	'0521h'	SC2	SC1	NEV
├─EF Events_Data	'0502h'	SC2	SC1	SC3
├─EF Faults_Data	'0503h'	SC2	SC1	SC3
├─EF Driver_Activity_Data	'0504h'	SC2	SC1	SC3
├─EF Vehicles_Used	'0505h'	SC2	SC1	SC3
├─EF Places	'0506h'	SC2	SC1	SC3
├─EF Current_Usage	'0507h'	SC2	SC1	SC3
├─EF Control_Activity_Data	'0508h'	SC2	SC1	SC3
└─EF Specific_Conditions	'0522h'	SC2	SC1	SC3

▼B

Neste quadro utilizam-se as seguintes abreviaturas para o controlo de acesso:

SC1 ALW OR SM-MAC-G2

SC2 ALW OR SM-MAC-G1 OR SM-MAC-G2

SC3 SM-MAC-G1 OR SM-MAC-G2

TCS_149 Todas as estruturas de EF são transparentes.

TCS_150 A aplicação para cartão de condutor da geração 1 tem a seguinte estrutura de dados:

File / Data element	No of Records	Size (bytes) Min	Size (bytes) Max	Default Values
DF Tachograph		*11378*	*24926*	
EF Application_Identification		*10*	*10*	
DriverCardApplicationIdentification		*10*	*10*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		1	1	{00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*143*	*143*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
DriverCardHolderIdentification		*78*	*78*	
cardHolderName		*72*	*72*	
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderBirthDate		4	4	{00..00}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*4*	*4*	
LastCardDownload		4	4	
EF Driving_Licence_Info		*53*	*53*	
CardDrivingLicenceInformation		*53*	*53*	
drivingLicenceIssuingAuthority		36	36	{00, 20..20}
drivingLicenceIssuingNation		1	1	{00}
drivingLicenceNumber		16	16	{20..20}
EF Events_Data		*864*	*1728*	
CardEventData		*864*	*1728*	
cardEventRecords	6	*144*	*288*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*576*	*1152*	
CardFaultData		*576*	*1152*	
cardFaultRecords	2	*288*	*576*	
CardFaultRecord	n_2	*24*	*24*	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				

▼B

vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*5548*	*13780*	
CardDriverActivity		*5548*	*13780*	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n_6	5544	13776	{00..00}
EF Vehicles_Used		*2606*	*6202*	
CardVehiclesUsed		*2606*	*6202*	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		*2604*	*6200*	
CardVehicleRecord	n_3	*31*	*31*	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
EF Places		*841*	*1121*	
CardPlaceDailyWorkPeriod		*841*	*1121*	
placePointerNewestRecord		1	1	{00}
placeRecords		*840*	*1120*	
PlaceRecord	n_4	*10*	*10*	
entryTime		4	4	{00..00}
entryTypeDailyWorkPeriod		1	1	{00}
dailyWorkPeriodCountry		1	1	{00}
dailyWorkPeriodRegion		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		*19*	*19*	
CardCurrentUse		*19*	*19*	
sessionOpenTime		4	4	{00..00}
sessionOpenVehicle				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
CardControlActivityDataRecord		*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		*280*	*280*	
SpecificConditionRecord	56	*5*	*5*	
entryTime		4	4	{00..00}
SpecificConditionType		1	1	{00}

▼B

TCS_151 Os valores seguintes, que servem para fornecer as dimensões no quadro anterior, são os valores mínimos e máximos do número de registos que a estrutura de dados do cartão de condutor deve utilizar para a aplicação da geração 1:

		Min	Max
n_1	NoOfEventsPerType	6	12
n_2	NoOfFaultsPerType	12	24
n_3	NoOfCardVehicleRecords	84	200
n_4	NoOfCardPlaceRecords	84	112
n_6	CardActivityLengthRange	5 544 bytes (28 dias * 93 mudanças de atividade)	13 776 Bytes (28 dias * 240 mudanças de atividade)

4.2.2 *Aplicação para cartão de condutor da geração 2*

TCS_152 Uma vez personalizada, a aplicação para cartão de condutor da geração 2 terá permanentemente as seguintes estrutura de ficheiro e regras de acesso do ficheiro.

Nota: Ao SFID do identificador EF curto é atribuído um número decimal: por exemplo, o valor 30 corresponde a 11110 em binário.

			Access rules	
File	**File ID**	**SFID**	**Read / Select**	**Update**
└─ DF Tachograph_G2			SC1	
├─ EF Application_Identification	'0501h'	1	SC1	NEV
├─ EF CardMA_Certificate	'C100h'	2	SC1	NEV
├─ EF CardSignCertificate	'C101h'	3	SC1	NEV
├─ EF CA_Certificate	'C108h'	4	SC1	NEV
├─ EF Link_Certificate	'C109h'	5	SC1	NEV
├─ EF Identification	'0520h'	6	SC1	NEV
├─ EF Card_Download	'050Eh'	7	SC1	SC1
├─ EF Driving_Licence_Info	'0521h'	10	SC1	NEV
├─ EF Events_Data	'0502h'	12	SC1	SM-MAC-G2
├─ EF Faults_Data	'0503h'	13	SC1	SM-MAC-G2
├─ EF Driver_Activity_Data	'0504h'	14	SC1	SM-MAC-G2
├─ EF Vehicles_Used	'0505h'	15	SC1	SM-MAC-G2
├─ EF Places	'0506h'	16	SC1	SM-MAC-G2
├─ EF Current_Usage	'0507h'	17	SC1	SM-MAC-G2
├─ EF Control_Activity_Data	'0508h'	18	SC1	SM-MAC-G2
├─ EF Specific_Conditions	'0522h'	19	SC1	SM-MAC-G2
├─ EF VehicleUnits_Used	'0523h'	20	SC1	SM-MAC-G2
└─ EF GNSS_Places	'0524h'	21	SC1	SM-MAC-G2

Neste quadro utiliza-se a abreviatura seguinte para o controlo de acesso:

SC1 ALW OR SM-MAC-G2

TCS_153 Todas as estruturas de EF são transparentes.

TCS_154 A aplicação para cartão de condutor da geração 2 tem a seguinte estrutura de dados:

▼B

File / Data element	No of Records	Size (bytes) Min	Size (bytes) Max	Default Values
DF Tachograph_G2		*19510*	*39306*	
EF Application_Identification		*15*	*15*	
DriverCardApplicationIdentification		*15*	*15*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		2	2	{00}
noOfGNSSCDRecords		2	2	{00 00}
noOfSpecificConditionRecords		2	2	{00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CardSignCertificate		*204*	*341*	
CardSignCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*143*	*143*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
DriverCardHolderIdentification		*78*	*78*	
cardHolderName		*72*	*72*	
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderBirthDate		4	4	{00..00}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*4*	*4*	
LastCardDownload		4	4	
EF Driving_Licence_Info		*53*	*53*	
CardDrivingLicenceInformation		*53*	*53*	
drivingLicenceIssuingAuthority		36	36	{00, 20..20}
drivingLicenceIssuingNation		1	1	{00}
drivingLicenceNumber		16	16	{20..20}
EF Events_Data		*1584*	*3168*	
CardEventData		*1584*	*3168*	
cardEventRecords	11	*144*	*288*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*576*	*1152*	
CardFaultData		*576*	*1152*	
cardFaultRecords	2	*288*	*576*	
CardFaultRecord	n_2	*24*	*24*	

▼B

├─faultType		1	1	{00}
├─faultBeginTime		4	4	{00..00}
├─faultEndTime		4	4	{00..00}
└─faultVehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*5548*	*13780*	
└CardDriverActivity		*5548*	*13780*	
├─activityPointerOldestDayRecord		2	2	{00 00}
├─activityPointerNewestRecord		2	2	{00 00}
└─activityDailyRecords	n_6	5544	13776	{00..00}
EF Vehicles_Used		*4034*	*9602*	
└CardVehiclesUsed		*4034*	*9602*	
├─vehiclePointerNewestRecord		2	2	{00 00}
└─cardVehicleRecords		*4032*	*9600*	
└─CardVehicleRecord	n_3	*48*	*48*	
├─vehicleOdometerBegin		3	3	{00..00}
├─vehicleOdometerEnd		3	3	{00..00}
├─vehicleFirstUse		4	4	{00..00}
├─vehicleLastUse		4	4	{00..00}
├─vehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
├─vuDataBlockCounter		2	2	{00 00}
└─vehicleIdentificationNumber		17	17	{20..20}
EF Places		*1766*	*2354*	
└CardPlaceDailyWorkPeriod		*1766*	*2354*	
├─placePointerNewestRecord		2	2	{00 00}
└─placeRecords		*1764*	*2352*	
└─PlaceRecord	n_4	*21*	*21*	
├─entryTime		4	4	{00..00}
├─entryTypeDailyWorkPeriod		1	1	{00}
├─dailyWorkPeriodCountry		1	1	{00}
├─dailyWorkPeriodRegion		1	1	{00}
├─vehicleOdometerValue		3	3	{00..00}
└─entryGNSSPlaceRecord		11	11	
├─timeStamp		4	4	{00..00}
├─gnssAccuracy		1	1	{00}
└─geoCoordinates		6	6	{00..00}
EF Current_Usage		*19*	*19*	
└CardCurrentUse		*19*	*19*	
├─sessionOpenTime		4	4	{00..00}
└─sessionOpenVehicle				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
└CardControlActivityDataRecord		*46*	*46*	
├─controlType		1	1	{00}
├─controlTime		4	4	{00..00}
├─controlCardNumber				
├─cardType		1	1	{00}
├─cardIssuingMemberState		1	1	{00}
└─cardNumber		16	16	{20..20}
├─controlVehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
├─controlDownloadPeriodBegin		4	4	{00..00}
└─controlDownloadPeriodEnd		4	4	{00..00}

▼B

EF Specific_Conditions		*282*	*562*	
SpecificConditions		*282*	*562*	
conditionPointerNewestRecord		2	2	{00 00}
specificConditionRecords		*280*	*560*	
SpecificConditionRecord	n_9	*5*	*5*	
entryTime		4	4	{00..00}
specificConditionType		1	1	{00}
EF VehicleUnits_Used		*842*	*2002*	
CardVehicleUnitsUsed		*842*	*2002*	
vehicleUnitPointerNewestRecord		2	2	{00 00}
cardVehicleUnitRecords		*840*	*2000*	
CardVehicleUnitRecord	n_7	*10*	*10*	
timeStamp		4	4	{00..00}
manufacturerCode		1	1	{00}
deviceID		1	1	{00}
vuSoftwareVersion		4	4	{00..00}
EF GNSS_Places		*3782*	*5042*	
GNSSContinuousDriving		*3782*	*5042*	
gnssCDPointerNewestRecord		2	2	{00 00}
gnssContinuousDrivingRecords		3780	5040	{00}
GNSSContinuousDrivingRecord	n_8	*15*	*15*	
timeStamp		4	4	{00..00}
gnssPlaceRecord		11	11	
timeStamp		4	4	{00..00}
gnssAccuracy		1	1	{00}
geoCoordinates		6	6	{00..00}

TCS_155 Os valores seguintes, que servem para fornecer as dimensões no quadro anterior, são os valores mínimos e máximos do número de registos que a estrutura de dados do cartão de condutor deve utilizar numa aplicação da geração 2:

		Min	Max
n_1	NoOfEventsPerType	6	12
n_2	NoOfFaultsPerType	12	24
n_3	NoOfCardVehicleRecords	84	200
n_4	NoOfCardPlaceRecords	84	112
n_6	CardActivityLengthRange	5 544 bytes (28 dias * 93 mudanças de atividade)	13 776 Bytes (28 dias * 240 mudanças de atividade)
n_7	NoOfCardVehicleUnitRecords	84	200
n_8	NoOfGNSSCDRecords	252	336
n_9	NoOfSpecificConditionRecords	56	112

4.3. **Aplicações para cartão de oficina**

4.3.1 *Aplicação para cartão de oficina da geração 1*

TCS_156 Uma vez personalizada, a aplicação para cartão de oficina da geração 1 terá permanentemente as seguintes estrutura de ficheiro e regras de acesso do ficheiro:

▼B

		Access rules		
File	**File ID**	**Read**	**Select**	**Update**
└DF Tachograph	'0500h'		SC1	
├EF Application_Identification	'0501h'	SC2	SC1	NEV
├EF Card_Certificate	'C100h'	SC2	SC1	NEV
├EF CA_Certificate	'C108h'	SC2	SC1	NEV
├EF Identification	'0520h'	SC2	SC1	NEV
├EF Card_Download	'0509h'	SC2	SC1	**SC1**
├EF Calibration	'050Ah'	SC2	SC1	SC3
├EF Sensor_Installation_Data	'050Bh'	**SC4**	SC1	NEV
├EF Events_Data	'0502h'	SC2	SC1	SC3
├EF Faults_Data	'0503h'	SC2	SC1	SC3
├EF Driver_Activity_Data	'0504h'	SC2	SC1	SC3
├EF Vehicles_Used	'0505h'	SC2	SC1	SC3
├EF Places	'0506h'	SC2	SC1	SC3
├EF Current_Usage	'0507h'	SC2	SC1	SC3
├EF Control_Activity_Data	'0508h'	SC2	SC1	SC3
└EF Specific_Conditions	'0522h'	SC2	SC1	SC3

Neste quadro utilizam-se as abreviaturas seguintes para o controlo de acesso:

SC1 ALW OR SM-MAC-G2

SC2 ALW OR SM-MAC-G1 OR SM-MAC-G2

SC3 SM-MAC-G1 OR SM-MAC-G2

SC4 Para o comando READ BINARY com byte INS par:

(PLAIN-C E SM-R-ENC-G1) OU (SM-C-MAC-G1 E SM-R-ENC-MAC-G1) OU

(SM-C-MAC-G2 E SM-R-ENC-MAC-G2)

Para o comando READ BINARY com byte INS ímpar (quando aceite): NEV

TCS_157 Todas as estruturas de EF são transparentes.

TCS_158 A aplicação para cartão de oficina da geração 1 tem a seguinte estrutura de dados:

▼B

File / Data element	No of Records	Size (Bytes) Min	Size (Bytes) Max	Default Values
DF Tachograph		*11055*	*29028*	
EF Application_Identification		*11*	*11*	
WorkshopCardApplicationIdentification		*11*	*11*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		1	1	{00}
noOfCalibrationRecords		1	1	{00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*211*	*211*	
CardIdentification		65	65	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
WorkshopCardHolderIdentification		*146*	*146*	
workshopName		36	36	{00, 20..20}
workshopAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*2*	*2*	
NoOfCalibrationsSinceDownload		2	2	{00 00}
EF Calibration		*9243*	*26778*	
WorkshopCardCalibrationData		*9243*	*26778*	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		1	1	{00}
calibrationRecords		*9240*	*26775*	
WorkshopCardCalibrationRecord	n_5	*105*	*105*	
calibrationPurpose		1	1	{00}
vehicleIdentificationNumber		17	17	{20..20}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
wVehicleCharacteristicConstant		2	2	{00 00}
kConstantOfRecordingEquipment		2	2	{00 00}
lTyreCircumference		2	2	{00 00}
tyreSize		15	15	{20..20}
authorisedSpeed		1	1	{00}
oldOdometerValue		3	3	{00..00}
newOdometerValue		3	3	{00..00}
oldTimeValue		4	4	{00..00}
newTimeValue		4	4	{00..00}
nextCalibrationDate		4	4	{00..00}
vuPartNumber		16	16	{20..20}
vuSerialNumber		8	8	{00..00}
sensorSerialNumber		8	8	{00..00}

▼B

EF Sensor_Installation_Data		*16*	*16*	
SensorInstallationSecData		16	16	{00..00}
EF Events_Data		*432*	*432*	
CardEventData		*432*	*432*	
cardEventRecords	6	*72*	*72*	
CardEventRecord	n_1	*24*	*24*	
eventType		1	1	{00}
eventBeginTime		4	4	{00..00}
eventEndTime		4	4	{00..00}
eventVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*288*	*288*	
CardFaultData		*288*	*288*	
cardFaultRecords	2	*144*	*144*	
CardFaultRecord	n_2	*24*	*24*	
faultType		1	1	{00}
faultBeginTime		4	4	{00..00}
faultEndTime		4	4	{00..00}
faultVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*202*	*496*	
CardDriverActivity		*202*	*496*	
activityPointerOldestDayRecord		2	2	{00 00}
activityPointerNewestRecord		2	2	{00 00}
activityDailyRecords	n_6	198	492	{00..00}
EF Vehicles_Used		*126*	*250*	
CardVehiclesUsed		*126*	*250*	
vehiclePointerNewestRecord		2	2	{00 00}
cardVehicleRecords		*124*	*248*	
CardVehicleRecord	n_3	*31*	*31*	
vehicleOdometerBegin		3	3	{00..00}
vehicleOdometerEnd		3	3	{00..00}
vehicleFirstUse		4	4	{00..00}
vehicleLastUse		4	4	{00..00}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
vuDataBlockCounter		2	2	{00 00}
EF Places		*61*	*81*	
CardPlaceDailyWorkPeriod		*61*	*81*	
placePointerNewestRecord		1	1	{00}
placeRecords		*60*	*80*	
PlaceRecord	n_4	*10*	*10*	
entryTime		4	4	{00..00}
entryTypeDailyWorkPeriod		1	1	{00}
dailyWorkPeriodCountry		1	1	{00}
dailyWorkPeriodRegion		1	1	{00}
vehicleOdometerValue		3	3	{00..00}
EF Current_Usage		*19*	*19*	
CardCurrentUse		*19*	*19*	
sessionOpenTime		4	4	{00..00}
sessionOpenVehicle				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}

▼B

EF Control_Activity_Data		*46*	*46*	
CardControlActivityDataRecord		*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}
EF Specific_Conditions		*10*	*10*	
SpecificConditionRecord	2	*5*	*5*	
entryTime		4	4	{00..00}
SpecificConditionType		1	1	{00}

TCS_159 Os valores seguintes, que servem para fornecer as dimensões no quadro anterior, são os valores mínimos e máximos do número de registos que a estrutura de dados do cartão de oficina deve utilizar para a aplicação da geração 1:

		Min	Max
n_1	NoOfEventsPerType	3	3
n_2	NoOfFaultsPerType	6	6
n_3	NoOfCardVehicleRecords	4	8
n_4	NoOfCardPlaceRecords	6	8
n_5	NoOfCalibrationRecords	88	255
n_6	CardActivityLengthRange	198 bytes (1 dia * 93 mudanças de atividade)	492 bytes (1 dia * 240 mudanças de atividade)

4.3.2 *Aplicação para cartão de oficina da geração 2*

TCS_160 Uma vez personalizada, a aplicação para cartão de oficina da geração 2 terá permanentemente as seguintes estrutura de ficheiro e regras de acesso do ficheiro.

Nota: Ao SFID do identificador EF curto é atribuído um número decimal: por exemplo, o valor 30 corresponde a 11110 em binário.

			Access rules		
File	**File ID**	**SFID**	**Read**	**Select**	**Update**
DF Tachograph_G2			SC1	SC1	
EF Application_Identification	'0501h'	1	SC1	SC1	NEV
EF CardMA_Certificate	'C100h'	2	SC1	SC1	NEV
EF CardSignCertificate	'C101h'	3	SC1	SC1	NEV
EF CA_Certificate	'C108h'	4	SC1	SC1	NEV
EF Link_Certificate	'C109h'	5	SC1	SC1	NEV
EF Identification	'0520h'	6	SC1	SC1	NEV
EF Card_Download	'0509h'	7	SC1	SC1	SC1
EF Calibration	'050Ah'	10	SC1	SC1	SM-MAC-G2
EF Sensor_Installation_Data	'050Bh'	11	**SC5**	SM-MAC-G2	NEV
EF Events_Data	'0502h'	12	SC1	SC1	SM-MAC-G2
EF Faults_Data	'0503h'	13	SC1	SC1	SM-MAC-G2
EF Driver_Activity_Data	'0504h'	14	SC1	SC1	SM-MAC-G2
EF Vehicles_Used	'0505h'	15	SC1	SC1	SM-MAC-G2
EF Places	'0506h'	16	SC1	SC1	SM-MAC-G2
EF Current_Usage	'0507h'	17	SC1	SC1	SM-MAC-G2
EF Control_Activity_Data	'0508h'	18	SC1	SC1	SM-MAC-G2
EF Specific_Conditions	'0522h'	19	SC1	SC1	SM-MAC-G2
EF VehicleUnits_Used	'0523h'	20	SC1	SC1	SM-MAC-G2
EF GNSS_Places	'0524h'	21	SC1	SC1	SM-MAC-G2

▼B

Neste quadro utilizam-se as abreviaturas seguintes para o controlo de acesso:

SC1 ALW OR SM-MAC-G2

SC5 Para o comando READ BINARY com byte INS par: SM-C-MAC-G2 E SM-R-ENC-MAC-G2

Para o comando READ BINARY com byte INS ímpar (quando aceite): NEV

TCS_161 Todas as estruturas de EF são transparentes.

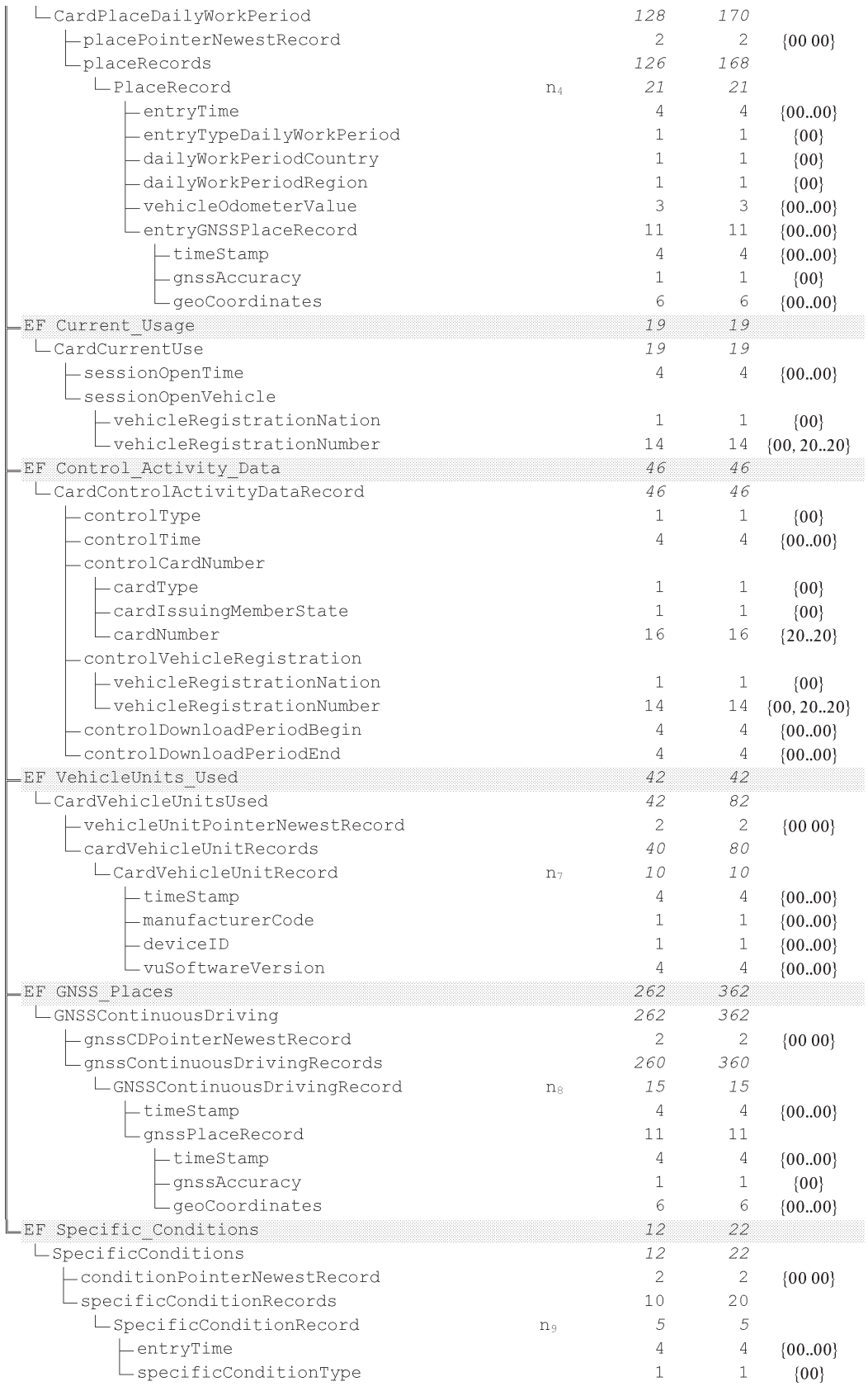
TCS_162 A aplicação para cartão de oficina da geração 2 tem a seguinte estrutura de dados:

File / Data element	No of Records	Size (Bytes) Min	Size (Bytes) Max	Default Values
DF Tachograph_G2		*17837*	*47163*	
EF Application_Identification		*17*	*17*	
WorkshopCardApplicationIdentification		*17*	*17*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfEventsPerType		1	1	{00}
noOfFaultsPerType		1	1	{00}
activityStructureLength		2	2	{00 00}
noOfCardVehicleRecords		2	2	{00 00}
noOfCardPlaceRecords		2	2	{00}
noOfCalibrationRecords		2	2	{00}
noOfGNSSCDRecords		2	2	{00..00}
noOfSpecificConditionRecords		2	2	{00..00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CardSignCertificate		*204*	*341*	
CardSignCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
WorkshopCardHolderIdentification		*146*	*146*	
workshopName		36	36	{00, 20..20}
workshopAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Card_Download		*2*	*2*	
NoOfCalibrationsSinceDownload		2	2	{00 00}
EF Calibration		*14788*	*42844*	
WorkshopCardCalibrationData		*14788*	*42844*	
calibrationTotalNumber		2	2	{00 00}
calibrationPointerNewestRecord		2	2	{00}
calibrationRecords		*14784*	*42840*	
WorkshopCardCalibrationRecord	n_5	*168*	*168*	
calibrationPurpose		1	1	{00}
vehicleIdentificationNumber		17	17	{20..20}
vehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
wVehicleCharacteristicConstant		2	2	{00 00}
kConstantOfRecordingEquipment		2	2	{00 00}
lTyreCircumference		2	2	{00 00}
tyreSize		15	15	{20..20}
authorisedSpeed		1	1	{00}
oldOdometerValue		3	3	{00..00}
newOdometerValue		3	3	{00..00}

▼B

├─oldTimeValue		4	4	{00..00}
├─newTimeValue		4	4	{00..00}
├─nextCalibrationDate		4	4	{00..00}
├─vuPartNumber		16	16	{20..20}
├─vuSerialNumber		8	8	{00..00}
├─sensorSerialNumber		8	8	{00..00}
├─sensorGNSSSerialNumber		8	8	{00..00}
├─rcmSerialNumber		8	8	{00..00}
├─vuAbility		1	1	{00}
└─sealDataCard		46	46	
├─noOfSealRecords		1	1	{00}
└─SealRecords		45	45	
└─SealRecord	5	9	9	
├─equipmentType		1	1	{00}
└─extendedSealIdentifier		8	8	{00..00}
EF Sensor_Installation_Data		*18*	*102*	
└─SensorInstallationSecData		18	102	{00..00}
EF Events_Data		*792*	*792*	
└─CardEventData		*792*	*792*	
└─cardEventRecords	11	*72*	*72*	
└─CardEventRecord	n_1	*24*	*24*	
├─eventType		1	1	{00}
├─eventBeginTime		4	4	{00..00}
├─eventEndTime		4	4	{00..00}
└─eventVehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Faults_Data		*288*	*288*	
└─CardFaultData		*288*	*288*	
└─cardFaultRecords	2	*144*	*144*	
└─CardFaultRecord	n_2	*24*	*24*	
├─faultType		1	1	{00}
├─faultBeginTime		4	4	{00..00}
├─faultEndTime		4	4	{00..00}
└─faultVehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
EF Driver_Activity_Data		*202*	*496*	
└─CardDriverActivity		*202*	*496*	
├─activityPointerOldestDayRecord		2	2	{00 00}
├─activityPointerNewestRecord		2	2	{00 00}
└─activityDailyRecords	n_6	198	492	{00..00}
EF Vehicles_Used		*194*	*386*	
└─CardVehiclesUsed		*194*	*386*	
├─vehiclePointerNewestRecord		2	2	{00 00}
└─cardVehicleRecords		*192*	*384*	
└─CardVehicleRecord	n_3	*48*	*48*	
├─vehicleOdometerBegin		3	3	{00..00}
├─vehicleOdometerEnd		3	3	{00..00}
├─vehicleFirstUse		4	4	{00..00}
├─vehicleLastUse		4	4	{00..00}
├─vehicleRegistration				
├─vehicleRegistrationNation		1	1	{00}
└─vehicleRegistrationNumber		14	14	{00, 20..20}
├─vuDataBlockCounter		2	2	{00 00}
└─vehicleIdentificationNumber		*17*	17	{20..20}
EF Places		*128*	*170*	

▼B



└CardPlaceDailyWorkPeriod		*128*	*170*	
├placePointerNewestRecord		2	2	{00 00}
└placeRecords		*126*	*168*	
└PlaceRecord	n_4	*21*	*21*	
├entryTime		4	4	{00..00}
├entryTypeDailyWorkPeriod		1	1	{00}
├dailyWorkPeriodCountry		1	1	{00}
├dailyWorkPeriodRegion		1	1	{00}
├vehicleOdometerValue		3	3	{00..00}
└entryGNSSPlaceRecord		11	11	{00..00}
├timeStamp		4	4	{00..00}
├gnssAccuracy		1	1	{00}
└geoCoordinates		6	6	{00..00}
EF Current_Usage		*19*	*19*	
└CardCurrentUse		*19*	*19*	
├sessionOpenTime		4	4	{00..00}
└sessionOpenVehicle				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
EF Control_Activity_Data		*46*	*46*	
└CardControlActivityDataRecord		*46*	*46*	
├controlType		1	1	{00}
├controlTime		4	4	{00..00}
├controlCardNumber				
├cardType		1	1	{00}
├cardIssuingMemberState		1	1	{00}
└cardNumber		16	16	{20..20}
├controlVehicleRegistration				
├vehicleRegistrationNation		1	1	{00}
└vehicleRegistrationNumber		14	14	{00, 20..20}
├controlDownloadPeriodBegin		4	4	{00..00}
└controlDownloadPeriodEnd		4	4	{00..00}
EF VehicleUnits_Used		*42*	*42*	
└CardVehicleUnitsUsed		*42*	*82*	
├vehicleUnitPointerNewestRecord		2	2	{00 00}
└cardVehicleUnitRecords		*40*	*80*	
└CardVehicleUnitRecord	n_7	*10*	*10*	
├timeStamp		4	4	{00..00}
├manufacturerCode		1	1	{00..00}
├deviceID		1	1	{00..00}
└vuSoftwareVersion		4	4	{00..00}
EF GNSS_Places		*262*	*362*	
└GNSSContinuousDriving		*262*	*362*	
├gnssCDPointerNewestRecord		2	2	{00 00}
└gnssContinuousDrivingRecords		*260*	*360*	
└GNSSContinuousDrivingRecord	n_8	*15*	*15*	
├timeStamp		4	4	{00..00}
└gnssPlaceRecord		11	11	
├timeStamp		4	4	{00..00}
├gnssAccuracy		1	1	{00}
└geoCoordinates		6	6	{00..00}
EF Specific_Conditions		*12*	*22*	
└SpecificConditions		*12*	*22*	
├conditionPointerNewestRecord		2	2	{00 00}
└specificConditionRecords		10	20	
└SpecificConditionRecord	n_9	*5*	*5*	
├entryTime		4	4	{00..00}
└specificConditionType		1	1	{00}

▼B

TCS_163 Os valores seguintes, que servem para fornecer as dimensões no quadro anterior, são os valores mínimos e máximos do número de registos que a estrutura de dados do cartão de oficina deve utilizar numa aplicação da geração 2:

		Min	Max
n_1	NoOfEventsPerType	3	3
n_2	NoOfFaultsPerType	6	6
n_3	NoOfCardVehicleRecords	4	8
n_4	NoOfCardPlaceRecords	6	8
n_5	NoOfCalibrationRecords	88	255
n_6	CardActivityLengthRange	198 bytes (1 dia * 93 mudanças de atividade)	492 bytes (1 dia * 240 mudanças de atividade)
n_7	NoOfCardVehicleUnitRecords	4	8
n_8	NoOfGNSSCDRecords	18	24
n_9	NoOfSpecificConditionRecords	2	4

4.4. Aplicações para cartão de controlo

4.4.1 *Aplicação para cartão de controlo da geração 1*

TCS_164 Uma vez personalizada, a aplicação para cartão de controlo da geração 1 terá permanentemente as seguintes estrutura de ficheiro e regras de acesso do ficheiro do ficheiro:

		Access rules		
File	**File ID**	**Read**	**Select**	**Update**
└─DF Tachograph	'0500h'			
├─EF Application_Identification	'0501h'	SC2	SC1	NEV
├─EF Card_Certificate	'C100h'	SC2	SC1	NEV
├─EF CA_Certificate	'C108h'	SC2	SC1	NEV
├─EF Identification	'0520h'	**SC6**	SC1	NEV
└─EF Controller_Activity_Data	'050Ch'	SC2	SC1	SC3

Neste quadro utilizam-se as abreviaturas seguintes para o controlo de acesso:

SC1 ALW OR SM-MAC-G2

SC2 ALW OR SM-MAC-G1 OR SM-MAC-G2

SC3 SM-MAC-G1 OR SM-MAC-G2

SC6 EXT-AUT-G1 OU SM-MAC-G1 OR SM-MAC-G2

TCS_165 Todas as estruturas de EF são transparentes.

TCS_166 A aplicação para cartão de controlo da geração 1 tem a seguinte estrutura de dados:

▼B

File / Data element	No of Records	Size (Bytes) Min	Max	
DF Tachograph		*11186*	*24526*	
EF Application_Identification		*5*	*5*	
ControlCardApplicationIdentification		*5*	*5*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfControlActivityRecords		2	2	{00 00}
EF Card_Certificate		*194*	*194*	
CardCertificate		194	194	{00..00}
EF CA_Certificate		*194*	*194*	
MemberStateCertificate		194	194	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
ControlCardHolderIdentification		*146*	*146*	
controlBodyName		36	36	{00, 20..20}
controlBodyAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Controller_Activity_Data		*10582*	*23922*	
ControlCardControlActivityData		*10582*	*23922*	
controlPointerNewestRecord		2	2	{00 00}
controlActivityRecords		*10580*	*23920*	
controlActivityRecord	n_7	*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlledCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlledVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}

TCS_167 Os valores seguintes, que servem para fornecer as dimensões no quadro anterior, são os valores mínimos e máximos do número de registos que a estrutura de dados do cartão de controlo deve utilizar para a aplicação da geração 1:

		Min	Max
n_7	NoOfControlActivityRecords	230	520

4.4.2 *Aplicação para cartão de controlo da geração 2*

TCS_168 Uma vez personalizada, a aplicação para cartão de controlo da geração 2 terá permanentemente as seguintes estrutura de ficheiro e regras de acesso do ficheiro.

Nota: Ao SFID do identificador EF curto é atribuído um número decimal: por exemplo, o valor 30 corresponde a 11110 em binário.

▼B

File	File ID	SFID	Access rules: Read / Select	Access rules: Update
DF Tachograph_G2			SC1	
EF Application_Identification	'0501h'	1	SC1	NEV
EF CardMA_Certificate	'C100h'	2	SC1	NEV
EF CA_Certificate	'C108h'	4	SC1	NEV
EF Link_Certificate	'C109h'	5	SC1	NEV
EF Identification	'0520h'	6	SC1	NEV
EF Controller_Activity_Data	'050Ch'	14	SC1	SM-MAC-G2

Neste quadro utiliza-se a abreviatura seguinte para o controlo de acesso:

SC1 ALW OR SM-MAC-G2

TCS_169 Todas as estruturas de EF são transparentes.

TCS_170 A aplicação para cartão de controlo da geração 2 tem a seguinte estrutura de dados:

File / Data element	No of Records	Size (Bytes) Min	Size (Bytes) Max	
DF Tachograph_G2		*11410*	*25161*	
EF Application_Identification		*5*	*5*	
ControlCardApplicationIdentification		*5*	*5*	
typeOfTachographCardId		1	1	{00}
cardStructureVersion		2	2	{00 00}
noOfControlActivityRecords		2	2	{00 00}
EF CardMA_Certificate		*204*	*341*	
CardMACertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF Identification		*211*	*211*	
CardIdentification		*65*	*65*	
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
cardIssuingAuthorityName		36	36	{00, 20..20}
cardIssueDate		4	4	{00..00}
cardValidityBegin		4	4	{00..00}
cardExpiryDate		4	4	{00..00}
ControlCardHolderIdentification		*146*	*146*	
controlBodyName		36	36	{00, 20..20}
controlBodyAddress		36	36	{00, 20..20}
cardHolderName				
holderSurname		36	36	{00, 20..20}
holderFirstNames		36	36	{00, 20..20}
cardHolderPreferredLanguage		2	2	{20 20}
EF Controller_Activity_Data		*10582*	*23922*	
ControlCardControlActivityData		*10582*	*23922*	
controlPointerNewestRecord		2	2	{00 00}
controlActivityRecords		*10580*	*23920*	
controlActivityRecord	n_7	*46*	*46*	
controlType		1	1	{00}
controlTime		4	4	{00..00}
controlledCardNumber				
cardType		1	1	{00}
cardIssuingMemberState		1	1	{00}
cardNumber		16	16	{20..20}
controlledVehicleRegistration				
vehicleRegistrationNation		1	1	{00}
vehicleRegistrationNumber		14	14	{00, 20..20}
controlDownloadPeriodBegin		4	4	{00..00}
controlDownloadPeriodEnd		4	4	{00..00}

TCS_171 Os valores seguintes, que servem para fornecer as dimensões no quadro anterior, são os valores mínimos e máximos do número de registos que a estrutura de dados do cartão de controlo deve utilizar numa aplicação da geração 2:

▼B

		Min	Max
n_7	NoOfControlActivityRecords	230	520

4.5. Aplicações para cartão de empresa

4.5.1 *Aplicação para cartão de empresa da geração 1*

TCS_172 Uma vez personalizada, a aplicação para cartão de empresa da geração 1 terá permanentemente as seguintes estrutura de ficheiro e regras de acesso do ficheiro:

		Access rules		
File	**File ID**	**Read**	**Select**	**Update**
└DF Tachograph	'0500h'		SC1	
├EF Application_Identification	'0501h'	SC2	SC1	NEV
├EF Card_Certificate	'C100h'	SC2	SC1	NEV
├EF CA_Certificate	'C108h'	SC2	SC1	NEV
├EF Identification	'0520h'	**SC6**	SC1	NEV
└EF Company_Activity_Data	'050Dh'	SC2	SC1	SC3

Neste quadro utilizam-se as abreviaturas seguintes para o controlo de acesso:

SC1 ALW OR SM-MAC-G2

SC2 ALW OR SM-MAC-G1 OR SM-MAC-G2

SC3 SM-MAC-G1 OR SM-MAC-G2

SC6 EXT-AUT-G1 OU SM-MAC-G1 OR SM-MAC-G2

TCS_173 Todas as estruturas de EF são transparentes.

TCS_174 A aplicação para cartão de empresa da geração 1 tem a seguinte estrutura de dados:

File / Data element	No of Records	Size (bytes) Min	Size (bytes) Max	Default Values
└DF Tachograph		*11114*	*24454*	
├EF Application_Identification		*5*	*5*	
│└CompanyCardApplicationIdentification		*5*	*5*	
│├typeOfTachographCardId		1	1	{00}
│├cardStructureVersion		2	2	{00 00}
│└noOfCompanyActivityRecords		2	2	{00 00}
├EF Card_Certificate		*194*	*194*	
│└CardCertificate		194	194	{00..00}
├EF CA_Certificate		*194*	*194*	
│└MemberStateCertificate		194	194	{00..00}
├EF Identification		*139*	*139*	
│├CardIdentification		*65*	*65*	
││├cardIssuingMemberState		1	1	{00}
││├cardNumber		16	16	{20..20}
││├cardIssuingAuthorityName		36	36	{00, 20..20}
││├cardIssueDate		4	4	{00..00}
││├cardValidityBegin		4	4	{00..00}
││└cardExpiryDate		4	4	{00..00}
│└CompanyCardHolderIdentification		*74*	*74*	
│├companyName		36	36	{00, 20..20}
│├companyAddress		36	36	{00, 20..20}
│└cardHolderPreferredLanguage		2	2	{20 20}
├EF Company_Activity_Data		*10582*	*23922*	
│└CompanyActivityData		*10582*	*23922*	
│├companyPointerNewestRecord		2	2	{00 00}
│└companyActivityRecords		*10580*	*23920*	
│└companyActivityRecord	n_8	*46*	*46*	
│├companyActivityType		1	1	{00}
│├companyActivityTime		4	4	{00..00}
│├cardNumberInformation				
││├cardType		1	1	{00}
││├cardIssuingMemberState		1	1	{00}
││└cardNumber		16	16	{20..20}
│├vehicleRegistrationInformation				
││├vehicleRegistrationNation		1	1	{00}
││└vehicleRegistrationNumber		14	14	{00, 20..20}
│├downloadPeriodBegin		4	4	{00..00}
│└downloadPeriodEnd		4	4	{00..00}

▼B

TCS_175 Os valores seguintes, que servem para fornecer as dimensões no quadro anterior, são os valores mínimos e máximos do número de registos que a estrutura de dados do cartão de empresa deve utilizar numa aplicação da geração 1:

		Min	Max
n_8	NoOfCompanyActivityRecords	230	520

4.5.2 *Aplicação para cartão de empresa da geração 2*

TCS_176 Uma vez personalizada, a aplicação para cartão de empresa da geração 2 terá permanentemente as seguintes estrutura de ficheiro e regras de acesso do ficheiro.

Nota: Ao SFID do identificador EF curto é atribuído um número decimal: por exemplo, o valor 30 corresponde a 11110 em binário.

			Access rules	
File	**File ID**	**SFID**	**Read / Select**	**Update**
└DF Tachograph_G2			SC1	
├EF Application_Identification	'0501h'	1	SC1	NEV
├EF CardMA_Certificate	'C100h'	2	SC1	NEV
├EF CA_Certificate	'C108h'	4	SC1	NEV
├EF Link_Certificate	'C109h'	5	SC1	NEV
├EF Identification	'0520h'	6	SC1	NEV
└EF Company_Activity_Data	'050Dh'	14	SC1	SM-MAC-G2

Neste quadro utiliza-se a abreviatura seguinte para o controlo de acesso:

SC1 ALW OR SM-MAC-G2

TCS_177 Todas as estruturas de EF são transparentes.

TCS_178 A aplicação para cartão de empresa da geração 2 tem a seguinte estrutura de dados:

File / Data element	No of Records	Size (bytes) Min	Size (bytes) Max	Default Values
└DF Tachograph_G2		*11338*	*25089*	
├EF Application_Identification		*5*	*5*	
│└CompanyCardApplicationIdentification		*5*	*5*	
│├typeOfTachographCardId		1	1	{00}
│├cardStructureVersion		2	2	{00 00}
│└noOfCompanyActivityRecords		2	2	{00 00}
├EF CardMA_Certificate		*204*	*341*	
│└CardMACertificate		204	341	{00..00}
├EF CA_Certificate		*204*	*341*	
│└MemberStateCertificate		204	341	{00..00}
├EF Link_Certificate		*204*	*341*	
│└LinkCertificate		204	341	{00..00}
├EF Identification		*139*	*139*	
│├CardIdentification		*65*	*65*	
││├cardIssuingMemberState		1	1	{00}
││├cardNumber		16	16	{20..20}
││├cardIssuingAuthorityName		36	36	{00, 20..20}
││├cardIssueDate		4	4	{00..00}
││├cardValidityBegin		4	4	{00..00}
││└cardExpiryDate		4	4	{00..00}
│└CompanyCardHolderIdentification		*74*	*74*	
│├companyName		36	36	{00, 20..20}
│├companyAddress		36	36	{00, 20..20}
│└cardHolderPreferredLanguage		2	2	{20 20}
├EF Company_Activity_Data		*10582*	*23922*	
│└CompanyActivityData		*10582*	*23922*	
│├companyPointerNewestRecord		2	2	{00 00}
│└companyActivityRecords		*10580*	*23920*	
│└companyActivityRecord	n_8	*46*	*46*	
│├companyActivityType		1	1	{00}
│├companyActivityTime		4	4	{00..00}
│├cardNumberInformation				
││├cardType		1	1	{00}
││├cardIssuingMemberState		1	1	{00}
││└cardNumber		16	16	{20..20}
│├vehicleRegistrationInformation				
││├vehicleRegistrationNation		1	1	{00}
││└vehicleRegistrationNumber		14	14	{00, 20..20}
│├downloadPeriodBegin		4	4	{00..00}
│└downloadPeriodEnd		4	4	{00..00}

▼B

TCS_179 Os valores seguintes, que servem para fornecer as dimensões no quadro anterior, são os valores mínimos e máximos do número de registos que a estrutura de dados do cartão de empresa deve utilizar numa aplicação da geração 2:

		Min	Max
n_8	NoOfCompanyActivityRecords	230	520

▼B

Apêndice 3

PICTOGRAMAS

PIC_001 O tacógrafo pode, opcionalmente, utilizar os seguintes pictogramas e combinações de pictograma (ou pictogramas e combinação de pictogramas suficientemente semelhantes para serem inequivocamente identificáveis com estes):

1. PICTOGRAMAS BÁSICOS

	Pessoas	**Ações**	**Modos de funcionamento**
	Empresa		Modo de empresa
	Controlador	Controlo	Modo de controlo
	Condutor	Condução	Modo de operação
	Oficina/estação de ensaio	Inspeção/calibração	Modo de calibração
	Fabricante		

	Atividades	**Duração**
	Disponível	Período de disponibilidade em curso
	Condução	Tempo de condução contínuo
	Descanso	Período de descanso em curso
	Outro trabalho	Período de trabalho em curso
	Pausa	Tempo acumulado de pausas
	Desconhecido	

	Equipamento	**Funções**
	Ranhura do condutor	
	Ranhura do ajudante	
	Cartão	
	Relógio	
	Visor	Visualização
	Memorização externa	Descarregamento
	Alimentação elétrica	
	Impressora	Impressão
	Sensor	
	Medida do pneumático	
	Veículo/ unidade-veículo	
	Módulo GNSS	
	Sistema de deteção à distância	
	Interface ITS	

▼B

Condições específicas

OUT	Fora de âmbito
	Travessia de batelão/comboio

Diversos

	Incidentes		Falhas
	Início do período de trabalho diário		Final do período de trabalho diário
	Localização		
M	Introdução manual das atividades do condutor		
	Segurança		
	Velocidade		
	Hora		
Σ	Total/síntese		

Qualificadores

24h	Diariamente
I	Semanalmente
II	Quinzenalmente
+	De ou para

2. COMBINAÇÕES DE PICTOGRAMAS

Diversos

+	Lugar do controlo		
+	Local de início do período de trabalho diário	+	Local de final do período de trabalho diário
+	Das horas	+	Às horas
+	Do veículo		
OUT +	Início de fora de âmbito	+ OUT	Final de fora de âmbito

Cartões

	Cartão de condutor
	Cartão de empresa
	Cartão de controlo
	Cartão de oficina
– – –	Ausência de cartão

Condução

	Condução em regime de tripulação
I	Tempo de condução por uma semana
II	Tempo de condução por duas semanas

▼B

Impressão

	Atividades do condutor, com base na impressão diária do cartão
	Atividades do condutor, com base na impressão diária da VU
	Incidentes e falhas, com base na impressão do cartão
	Incidentes e falhas, com base na impressão da VU
	Impressão de dados técnicos
	Impressão de excesso de velocidade

Incidentes

	Inserção de cartão não válido
	Conflito de cartões
	Sobreposição de tempos
	Condução sem cartão adequado
	Inserção de cartão durante a condução
	Última sessão de cartão encerrada incorretamente
	Excesso de velocidade
	Interrupção da alimentação elétrica
	Erro nos dados de movimento
	Conflito relativo ao movimento do veículo
	Violação da segurança
	Ajustamento do tempo (pela oficina)
	Controlo do excesso de velocidade

Falhas

	Falha do cartão (ranhura do condutor)
	Falha do cartão (ranhura do ajudante)
	Falha do visor
	Falha do descarregamento
	Falha da impressora
	Falha do sensor
	Falha interna da VU
	Falha do GNSS
	Falha da deteção à distância

Procedimento de introdução manual de dados

	Ainda o mesmo período de trabalho diário?
	Final do anterior período de trabalho?
	Confirmar ou introduzir local do final do período de trabalho
	Introduzir hora do início
	Introduzir local do início do período de trabalho.

Nota: O apêndice 4 apresenta outras combinações de pictogramas para formar carateres de impressão ou identificadores de registo.

▼B

Apêndice 4

IMPRESSÃO

ÍNDICE

1. GENERALIDADES

Cada impressão é concretizada encadeando diversos blocos de dados, eventualmente identificados por um identificador de bloco.

Um bloco de dados contém um ou mais registos, eventualmente identificados por um identificador de registo.

PRT_001 Se um identificador de bloco preceder imediatamente um identificador de registo, este último não é impresso.

PRT_002 Caso um atributo de dado seja desconhecido ou não deva ser impresso por razões associadas a direitos de acesso aos dados, são impressos espaços no seu lugar.

PRT_003 Se o conteúdo de uma linha inteira for desconhecido ou não precisar de ser impresso, a linha inteira é omitida.

PRT_004 Os campos relativos a dados numéricos são impressos com alinhamento à direita, com um espaço de separação entre milhares e milhões e sem zeros não significativos.

PRT_005 Os campos relativos a dados em sequência são impressos com alinhamento à esquerda e, conforme necessário, preenchidos com espaços segundo o comprimento dos atributos dos dados ou truncados segundo o comprimento dos atributos dos dados (nomes e endereços).

PRT_006 No caso de uma quebra de linha devido a texto longo, deve ser impresso um caráter especial (ponto a meia altura da linha, «•») como primeiro caráter na nova linha.

2. ESPECIFICAÇÕES RELATIVAS AOS BLOCOS DE DADOS

Nesta secção, aplicam-se as seguintes convenções à notação de formato:

— carateres a **negro (bold)** indicam texto normal a imprimir (a impressão vem em carateres normais),

▼B

— carateres normais indicam variáveis (pictogramas ou dados) a substituir pelos seus valores para impressão

— ao lado dos nomes das variáveis acrescentam-se travessões que indicam o comprimento de atributo de dados disponível para cada variável

— as datas são especificadas pelo formato «dd/mm/aaaa» (dia, mês, ano), podendo também utilizar-se um formato «dd.mm.aaaa»

— o termo «identificação do cartão» traduz-se pela seguinte composição: tipo do cartão, mediante uma combinação de pictogramas; código do Estado-Membro emissor do cartão; barra inclinada para a frente; número do cartão (com os índices de substituição e de renovação separados por um espaço:

P	■	x	x	x	/	x	x	x	x	x	x	x	x	x	x	x	x	x		x		x
Combinações de pictogramas do cartão		Código do Estado-Membro emissor				Primeiros 14 carateres do número do cartão (que inclui eventualmente um índice consecutivo)														Índice de substituição		Índice de renovação

▼B

PRT_007 Na impressão utilizam-se os seguintes blocos de dados e/ou registos de dados, com os seguintes significados e formatos:

Número do bloco ou do registo Significado	Formato dos dados
1 *Data e hora de impressão do documento*	▼ dd/mm/aaaa hh:mm **(UTC)**
2 *Tipo de impressão* Identificador de bloco Combinação de pictogramas de impressão (ver apêndice 3), fixação do dispositivo de limitação da velocidade (apenas impressão do excesso de velocidade)	----------▼---------- Picto xxx **km/h**
3 *Identificação do titular do cartão* Identificador de bloco. P = pictograma de pessoa Apelido do titular do cartão Nome próprio do titular (eventual) Identificação do cartão Prazo de validade do cartão (eventual) e número de geração do cartão (GEN 1 ou GEN 2) (*)	----------P---------- P Apelido_____ Nome_Próprio_____ Identificação_do_cartão _____ dd/mm/aaaa - GEN 2

Se se tratar de um cartão não pessoal, ao qual não se aplique apelido do titular, o nome impresso será o da empresa, da oficina ou do organismo de controlo.

(*) O número da geração do cartão só pode ser impresso pelo tacógrafo inteligente.

4 *Identificação do veículo* Identificador de bloco VIN Estado-Membro de matrícula e VRN	----------🚘---------- 🚘 VIN_____ Nac/VRN_____
5 *Identificação da VU (unidade-veículo)* Identificador de bloco Nome do fabricante da VU Número de peça da VU Número da geração da VU (*)	----------⊟---------- ⊟ Fabricante_da_VU_____ Número_de_peça_da_VU____ GEN 2

(*) O número da geração do cartão só pode ser impresso pelo tacógrafo inteligente.

6 *Última calibração do tacógrafo* Identificador de bloco Nome da oficina Identificação do cartão de oficina Data da calibração	----------🔧---------- 🔧 Nome_____ Identificação_do_cartão _____ 🔧 dd/mm/aaaa

▼B

7 ***Último controlo (por um agente controlador)***

Identificador de bloco

Identificação do cartão do controlador

Identificação_do_cartão _____

```
----------D----------
Data, hora e tipo do controlo
D dd/mm/aaaa hh:mm ppppp
```

Tipo de controlo: até cinco pictogramas. O tipo de controlo pode ser (eventualmente em combinação):

▪: descarregamento do cartão ↧: descarregamento da VU ⮧: impressão □: visualização ⮉: controlo de calibração de estrada

8 ***Atividades de condutor memorizadas num cartão por ordem de ocorrência***

Identificador de bloco

Data do pedido (dia que é alvo da impressão) + Contador de presença diária do cartão

```
----------⊡----------
    dd/mm/aaaa  xxx
```

8a *Condição fora de âmbito no início deste dia* (deixar em branco se não estiver aberta nenhuma condição fora de âmbito)

```
----------OUT----------
```

8.1 *Período durante o qual o cartão não esteve inserido*

8.1a Identificador de registo (início do período)

8.1b *Período desconhecido*. Hora de início, duração

8.1c *Atividade introduzida manualmente*.

Pictograma da atividade, hora de início, duração

```
  --------------------
?       hh:mm hhhmm
A       hh:mm hhhmm
```

8.2 *Inserção do cartão na ranhura S*

Identificador de registo; S = pictograma de ranhura

Estado-Membro de matrícula e VRN do veículo

Valor do conta-quilómetros do veículo no momento da inserção do cartão

```
  ---------S---------
A Nac/VRN__________
  x xxx xxx km
```

8.3 *Atividade (enquanto o cartão esteve inserido)*

Pictograma da atividade, hora de início, duração, situação da condução (pictograma de tripulação se for CREW, em branco se for SINGLE)

```
A       hh:mm hhhmm ⊡⊡
```

8.3a *Condição especial*. Hora de introdução, pictograma da condição especial (ou combinação de pictogramas)

```
        hh:mm ---pppp---
```

8.4 *Retirada do cartão*

Valor do conta-quilómetros do veículo e distância percorrida desde a última inserção com valor do conta-quilómetros conhecido

```
  x xxx xxx km; x xxx km
```

9 ***Atividades de condutor memorizadas numa VU por ranhura e em ordem cronológica***

Identificador de bloco

Data do pedido (dia que é objeto da impressão)

Valor do conta-quilómetros do veículo às 00h00 e às 24h00

```
----------⊡----------
       dd/mm/aaaa
x xxx xxx - x xxx xxx km
```

10 ***Atividades tratadas na ranhura S***

Identificador de bloco

```
----------S----------
```

10a *Condição fora de âmbito no início deste dia* (deixar em branco se não estiver aberta nenhuma condição fora de âmbito)

```
----------OUT----------
```

10.1 *Período em que não esteve nenhum cartão inserido na ranhura S*

Identificador de registo

Nenhum cartão inserido

Valor do conta-quilómetros do veículo no início do período

```
  --------------------
⊡▪---
  x xxx xxx km
```

10.2 *Inserção de cartão*

Identificador de registo da inserção do cartão

Nome do condutor

```
  --------------------
⊡ Apelido_____________
```

▼B

	Nome próprio do condutor	Nome_Próprio_____
	Identificação do cartão de condutor	Identificação_do_cartão _____
	Prazo de validade do cartão (eventual) e número de geração do cartão (GEN 1 ou GEN 2) (*)	dd/mm/aaaa - GEN 2
	Estado-Membro de matrícula e VRN do veículo anterior	Nac/VRN_____
	Data e hora de retirada do cartão do veículo anterior	dd/mm/aaaa hh:mm
	Linha em branco	
	Valor do conta-quilómetros do veículo no momento da inserção do cartão, indicador a indicar se houve introdução manual de atividades de condutor (M se sim, em branco se não)	x xxx xxx km M
	Se não houve inserção de cartão de condutor no dia em que é feita a impressão, utiliza-se no bloco 10.2 a leitura dos dados do conta-quilómetros para a última inserção de cartão disponível antes desse dia	
10.3	*Atividade*	
	Pictograma da atividade, hora de início, duração, situação da condução (pictograma de tripulação se for CREW, em branco se for SINGLE).	A hh:mm hhhmm ⊙⊙
10.3a	*Condição especial*. Hora de introdução, pictograma da condição especial (ou combinação de pictogramas)	hh:mm ---pppp---
10.4	*Retirada do cartão ou final do período «sem cartão»*	
	Valor do conta-quilómetros do veículo no momento da retirada do cartão ou no final do período «sem cartão» e distância percorrida desde a inserção ou desde o início do período «sem cartão»	x xxx xxx km; x xxx km

(*) O número da geração do cartão só pode ser impresso pelo tacógrafo inteligente.

11	***Síntese diária***	
	Identificador de bloco	----------Σ----------
11.1	***Síntese da VU para os períodos sem cartão na ranhura do condutor***	
	Identificador de bloco	1⊙▬---
11.2	***Síntese da VU para os períodos sem cartão na ranhura do ajudante***	
	Identificador de bloco	2⊙▬---
11.3	***Síntese da VU por cada condutor***	
	Identificador de registo	----------
	Apelido do condutor	⊙ Apelido_____
	Nome(s) próprio(s) do condutor	Nome_Próprio_____
	Identificação do cartão de condutor	Identificação_do_cartão_
11.4	*Introdução do lugar de início e/ou final de um período de trabalho diário*	
	pi = pictograma de local de início/final, hora, país, região	pihh:mm Cou Reg
	Valor do conta-quilómetros	x xxx xxx km
11.5	*Introdução do lugar de início e/ou final de um período de trabalho diário*	
	e após três horas de tempo de condução contínua	⁘ hh:mm
	Valor do conta-quilómetros	x xxx xxx km

11.6	*Totais de atividade (de um cartão)*	
	Duração total da condução, distância percorrida	⊙ hhhmm x xxx km
	Duração total do trabalho e da disponibilidade	✻ hhhmm ⧈ hhhmm
	Duração total dos períodos de repouso e desconhecidos	⊢ hhhmm ? hhhmm
	Duração total das atividades da tripulação	⊙⊙ hhhmm
11.7	*Totais de atividade (períodos sem ranhura de cartão de condutor principal)*	
	Duração total da condução, distância percorrida	⊙ hhhmm x xxx km
	Duração total do trabalho e da disponibilidade	✻ hhhmm ⧈ hhhmm
	Duração total dos períodos de repouso	⊢ hhhmm

▼B

11.8	*Totais de atividade (períodos sem ranhura de cartão de ajudante)*	
	Duração total do trabalho e da disponibilidade	hhhmm hhhmm
	Duração total dos períodos de repouso	hhhmm
11.9	*Totais de atividade (por condutor, incluídas ambas as ranhuras)*	
	Duração total da condução, distância percorrida	hhhmm x xxx **km**
	Duração total do trabalho e da disponibilidade	hhhmm hhhmm
	Duração total dos períodos de repouso	hhhmm
	Duração total das atividades da tripulação	hhhmm

Se se pretender uma impressão deste tipo para a data atual, a síntese diária é calculada com base nos dados disponíveis no momento da impressão.

12	***Incidentes e/ou falhas memorizados num cartão***	
12.1	Identificador de bloco para os últimos cinco «incidentes e falhas» do cartão	----------!×----------
12.2	Identificador de bloco para todos os «incidentes» registados no cartão	----------!----------
12.3	Identificador de bloco para todas as «falhas» registadas no cartão	----------×----------
12.4	*Registo de incidente e/ou falha*	
	Identificador de registo	----------
	Pictograma do incidente/falha, objetivo do registo, data e hora de início	Pic (p) dd/mm/aaaa hh:mm
	Código adicional do incidente/falha (eventual), duração	!xx hhhmm
	Estado-Membro de matrícula e VRN do veículo no qual se produziu o incidente ou a falha	Nac/VRN_____

13	***Incidentes e/ou falhas memorizados ou em curso numa VU***	
13.1	Identificador de bloco para os últimos cinco «incidentes e falhas» da VU	----------!×----------
13.2	Identificador de bloco para todos os «incidentes» registados ou em curso na VU	----------!----------
13.3	Identificador de bloco para todas as «falhas» registadas ou em curso na VU	----------×----------
13.4	*Registo de incidente e/ou falha*	
	Identificador de registo	----------
	Pictograma do incidente/falha, objetivo do registo, data e hora de início	Pic (p) dd/mm/aaaa hh:mm
	Código adicional do incidente/falha (eventual), quantidade de incidentes similares nesse dia, duração	!xx (xxx) hhhmm
	Identificação dos cartões inseridos no início ou final do incidente ou falha (até quatro linhas, sem repetir duas vezes os mesmos números de cartão)	Identificação_do_cartão _____ Identificação_do_cartão _____ Identificação_do_cartão _____ Identificação_do_cartão _____
	Caso em que não esteja nenhum cartão inserido	---
	Dados específicos do fabricante	< Literal><ErrorCode>

O objetivo do registo (p) é um código numérico que explica por que foi registado o incidente ou a falha, codificados segundo o elemento de dado `EventFaultRecordPurpose`.

O `Literal` é um literal específico do fabricante de tacógrafos com 12 carateres no máximo.

O `ErrorCode` é um código de erro específico do fabricante de tacógrafos com 12 carateres no máximo.

▼B

14	***Identificação da VU***	
	Identificador de bloco	----------B----------
	Nome do fabricante da VU	B Nome_____
	Endereço do fabricante da VU	Endereço_____
	Número de peça da VU	Número_de_peça _____
	Número de homologação da VU	Homol_____
	Número de série da VU	N.°_de_série_____
	Ano de fabrico da VU	AAAA
	Versão do software da VU e respetiva data de instalação	V xxxx dd/mm/aaaa
15	***Identificação do sensor***	
	Identificador de bloco	----------Л----------
15.1	*Registo do emparelhamento*	
	Número de série do sensor	Л N.°_de_série _____
	Número de homologação do sensor	Homol _____
	Data do emparelhamento do sensor	dd/mm/aaaa hh:mm
16	***Identificação GNSS***	
	Identificador de bloco	----------▚----------
16.1	*Registo do acoplamento*	
	Número de série do módulo GNSS externo	▚ N.°_de_série _____
	Número de homologação do módulo GNSS externo	Homol _____
	Data do acoplamento do módulo GNSS	dd/mm/aaaa hh:mm
17	***Dados relativos à calibração***	
	Identificador de bloco	----------T----------
17.1	*Registo da calibração*	
	Identificador de registo	---
	Oficina que efetuou a calibração	T Nome_da_oficina_____
	Endereço da oficina	Endereço_da_oficina_____
	Identificação do cartão de oficina	Identificação_do_cartão _____
	Prazo de validade do cartão de oficina	dd/mm/aaaa
	Linha em branco	
	Data da calibração + objetivo da calibração	T dd/mm/aaaa (p)
	VIN	A VIN_____
	Estado-Membro de matrícula e VRN	Nac/VRN _____
	Coeficiente característico do veículo	w xx xxx Imp/km
	Constante do aparelho de controlo	k xx xxx Imp/km
	Effective circumference of wheel tyres	l xx xxx mm
	Dimensão dos pneumáticos montados	● TyreSize_____
	Instalação do dispositivo de limitação da velocidade	> xxx km/h
	Valores antigos e novos do conta-quilómetros	x xxx xxx – x xxx xxx km

O objetivo da calibração (p) é um código numérico que explica por que foram registados estes parâmetros de calibração, codificados segundo o elemento de dado `CalibrationPurpose`.

▼B

18	***Ajustamento do tempo***	
	Identificador de bloco	----------◷----------
18.1	*Registo do ajustamento do tempo*	
	Identificador de registo	----------
	Data e hora antigas	!◷ dd/mm/aaaa hh:mm
	Data e hora novas	◷ Oficina que efetuou o ajustamento do tempo
	dd/mm/aaaa hh:mm	Nome_da_oficina_____
	Endereço da oficina	Identificação do cartão de oficina
	Prazo de validade do cartão de oficina	Endereço_da_oficina_____
	Identificação_do_cartão _____	dd/mm/aaaa

19	***Incidente e falha mais recentes registados na VU***	
	Identificador de bloco	----------!×🚙----------
	Data e hora do incidente mais recente	! dd/mm/aaaa hh:mm
	Data e hora da falha mais recente	× dd/mm/aaaa hh:mm

20	***Informação relativa ao controlo do excesso de velocidade***	
	Identificador de bloco	----------»----------
	Data e hora do último CONTROLO DO EXCESSO DE VELOCIDADE	»▫dd/mm/aaaa hh:mm
	Data e hora do primeiro excesso de velocidade e quantidade de tais incidentes desde então	»»dd/mm/aaaa hh:mm (nnn)

21	***Registo do excesso de velocidade***	
21.1	Identificador do bloco «primeiro excesso de velocidade desde a última calibração»	--------»»T---------
21.2	Identificador do bloco «os cinco mais graves nos últimos 365 dias»	-------»»(365)------
21.3	Identificador do bloco «o mais grave de cada um dos últimos 10 dias de ocorrência»	-------»»(10)-------
21.4	Identificador de registo	----------
	Data, hora e duração	»»dd/mm/aaaa hh:mm hhhmm
	Velocidades máxima e média, quantidade de incidentes similares no mesmo dia	xxx **km/h** xxx **km/h**(xxx)
	Apelido do condutor	◙ Apelido_____
	Nome próprio do condutor	Nome_Próprio_____
	Identificação do cartão do condutor	Identificação_do_cartão _____
21.5	Não havendo registo de excesso de velocidade no bloco	»---

22	***Informação manuscrita***	
	Identificador de bloco	----------
22.1	Local do controlo	▫• .....
22.2	Assinatura do controlador	▫ .....
22.3	Das horas	◷+ .....
22.4	às horas	+◷ .....
22.5	Assinatura do condutor	◙ .....

«Informação manuscrita»; inserir linhas em branco em quantidade suficiente para poder escrever a informação necessária ou proceder à assinatura.

▼B

23 ***Cartões mais recentes inseridos na VU***

Identificador de bloco

23.1 Cartão inserido

Identificador de registo

Tipo de cartão, geração, versão, fabricante (*)

Identificação do cartão

Número de série do cartão

Data e hora da última inserção do cartão

```
-------- ⊟◪◔ --------


----
⍑ <gen> <version> <MC>
Identificação do cartão
Número de série do cartão
dd/mm/aaaa hh:mm
```

(*) (tudo numa linha)

com

tipo de cartão: pictograma, um caráter + espaço

gen: GEN1 ou GEN2, 4 carateres + espaço

versão: até 10 carateres

MC: código do fabricante, 3 carateres

3. ESPECIFICAÇÕES APLICÁVEIS À IMPRESSÃO

Nesta secção aplicam-se as seguintes convenções de notação:

N	Número de bloco ou de registo de impressão N
N	Número de bloco ou de registo de impressão N, repetido as vezes necessárias
X/Y	Blocos ou registos de impressão X e/ou Y, conforme necessário e repetidos as vezes necessárias

3.1. **Atividades de condutor, na impressão diária dos cartões**

PRT_008 As atividades de condutor, na impressão diária do cartão, devem respeitar o seguinte formato:

1	Data e hora de impressão do documento
2	Tipo de impressão
3	Identificação do controlador (se inserido um cartão de controlo na VU)
3	Identificação do condutor (com base no cartão que é alvo da impressão + GEN)
4	Identificação do veículo (veículo do qual a impressão é tomada)
5	Identificação da VU (VU da qual a impressão é tomada + GEN)
6	Última calibração desta VU
7	Último controlo a que o condutor foi sujeito
8	Delimitador das atividades de condutor
8a	Condição fora de âmbito no início deste dia
8.1a / 8.1b / 8.1c / 8.2 / 8.3 / 8.3a / 8.4	Atividades do condutor por ordem de ocorrência
11	Delimitador da síntese diária

▼B

11.4	Locais introduzidos, por ordem cronológica
11.5	Dados GNSS
11.6	Totais de atividade
12.1	Incidentes ou falhas, com base no delimitador do cartão
12.4	Registos de incidente/falha (últimos cinco incidentes ou falhas memorizados no cartão)
13.1	Incidentes ou falhas, com base no delimitador da VU
13.4	Registos de incidente/falha (últimos 5 incidentes ou falhas memorizados ou em curso na VU)
22.1	Local do controlo
22.2	Assinatura do controlador
22.5	Assinatura do condutor

3.2. **Atividades de condutor, na impressão diária da VU**

PRT_009 As atividades de condutor, na impressão diária da VU, devem respeitar o seguinte formato:

1	Data e hora de impressão do documento
2	Tipo de impressão
3	Identificação do titular do cartão (para todos os cartões inseridos na VU + GEN)
4	Identificação do veículo (veículo do qual a impressão é tomada)
5	Identificação da VU (VU da qual a impressão é tomada + GEN)
6	Última calibração desta VU
7	Último controlo neste tacógrafo
9	Delimitador das atividades de condutor
10	Delimitador da ranhura do condutor (ranhura 1)
10a	Condição fora de âmbito no início deste dia
10.1 / 10.2 / 10.3 / 10.3a / 10.4	Atividades por ordem cronológica (ranhura do condutor)
10	Delimitador da ranhura do ajudante (ranhura 2)
10a	Condição fora de âmbito no início deste dia
10.1 / 10.2 / 10.3 / 10.3a / 10.4	Atividades por ordem cronológica (ranhura do ajudante)
11	Delimitador da síntese diária
11.1	Síntese dos períodos sem cartão na ranhura do condutor
11.4	Locais introduzidos, por ordem cronológica
11.5	Dados GNSS

▼B

11.6	Totais de atividade
11.2	Síntese dos períodos sem cartão na ranhura do ajudante
11.4	Locais introduzidos, por ordem cronológica
11.5	Dados GNSS
11.7	Totais de atividade
11.3	Síntese das atividades de um condutor, incluídas ambas as ranhuras
11.4	Locais introduzidos por este condutor, por ordem cronológica
11.5	Dados GNSS
11.8	Totais de atividade para este condutor
13.1	Delimitador de incidentes/falhas
12.4	Registos de incidente/falha (últimos cinco incidentes ou falhas memorizados ou em curso na VU)
13.1	Local do controlo
22.2	Assinatura do controlador
22.3	Das horas (espaço disponível para um condutor sem cartão indicar os períodos pertinentes para si próprio)
22.4	às horas
22.5	Assinatura do condutor

3.3. **Incidentes e falhas, da impressão dos cartões**

PRT_010 Os incidentes e falhas, na impressão diária do cartão, devem respeitar o seguinte formato:

1	Data e hora de impressão do documento
2	Tipo de impressão
3	Identificação do controlador (se inserido um cartão de controlo na VU + GEN)
3	Identificação do condutor (com base no cartão que é alvo da impressão)
4	Identificação do veículo (veículo do qual a impressão é tomada)
12.2	Delimitador de incidentes
12.4	Registos de incidentes (todos os incidentes memorizados no cartão)
12.3	Delimitador de falhas
12.4	Registos de falhas (todas as falhas memorizadas no cartão)
22.1	Local do controlo
22.2	Assinatura do controlador
22.5	Assinatura do condutor

▼B

3.4. **Incidentes e falhas, da impressão da VU**

PRT_011 Os incidentes e falhas, na impressão diária da VU, devem respeitar o seguinte formato:

1	Data e hora de impressão do documento
2	Tipo de impressão
3	Identificação do titular do cartão (para todos os cartões inseridos na VU + GEN)
4	Identificação do veículo (veículo do qual a impressão é tomada)
13.2	Delimitador de incidentes
13.4	Registos de incidentes (todos os incidentes memorizados ou em curso na VU)
13.3	Delimitador de falhas
13.4	Registos de falhas (todas as falhas memorizadas ou em curso na VU)
22.1	Local do controlo
22.2	Assinatura do controlador
22.5	Assinatura do condutor

3.5. **Impressão de dados técnicos**

PRT_012 A impressão de dados técnicos deve respeitar o seguinte formato:

1	Data e hora de impressão do documento
2	Tipo de impressão
3	Identificação do titular do cartão (para todos os cartões inseridos na VU + GEN)
4	Identificação do veículo (veículo do qual a impressão é tomada)
14	Identificação da VU
15	Identificação do sensor
15.1	Dados do emparelhamento do sensor (todos os dados disponíveis por ordem cronológica)
16	Identificação GNSS
16.1	Dados do acoplamento do módulo GNSS externo (disponíveis por ordem cronológica)
17	Delimitador dos dados de calibração
17.1	Registos de calibração (disponíveis por ordem cronológica)
18	Delimitador do ajustamento do tempo
18.1	Registos de ajustamento do tempo (todos os registos disponíveis de ajustamento do tempo e de registo de dados da calibração)
19	Incidente e falha mais recentes registados na VU

▼B

3.6. **Impressão do excesso de velocidade**

PRT_013 A impressão do excesso de velocidade deve respeitar o seguinte formato:

1	Data e hora de impressão do documento
2	Tipo de impressão
3	Identificação do titular do cartão (para todos os cartões inseridos na VU + GEN)
4	Identificação do veículo (veículo do qual a impressão é tomada)
20	Informação relativa ao controlo do excesso de velocidade
21.1	Identificador dos dados de excesso de velocidade
21.4 / 21.5	Primeiro excesso de velocidade desde a última calibração
21.2	Identificador dos dados de excesso de velocidade
21.4 / 21.5	Os cinco incidentes mais graves de excesso de velocidade dos últimos 365 dias
21.3	Identificador dos dados de excesso de velocidade
21.4 / 21.5	O mais grave excesso de velocidade de cada um dos últimos 10 dias
22.1	Local do controlo
22.2	Assinatura do controlador
22.5	Assinatura do condutor

3.7. **Histórico de cartões inseridos**

PRT_014 A impressão do histórico de cartões inseridos deve respeitar o seguinte formato:

1	Data e hora de impressão do documento
2	Tipo de impressão
3	Identificações do titular do cartão (para todos os cartões inseridos na VU)
23	Cartão mais recente inserido na VU
23.1	Cartões inseridos (até 88 registos)
12.3	Delimitador de falhas

▼B

Apêndice 5

VISUALIZAÇÃO

No presente apêndice, aplicam-se as seguintes convenções à notação de formato:

— carateres a **negro (bold)** indicam texto normal a visualizar (a visualização vem em carateres normais),

— carateres normais indicam variáveis (pictogramas ou dados) a substituir pelos seus valores na visualização,

  — dd mm aaaa: dia, mês, ano

  — hh: horas

  — mm: minutos

  — D: pictograma de duração

  — EF: combinação de pictogramas de incidente ou falha

  — O: pictograma de modo de funcionamento

DIS_001 O tacógrafo deve exibir os dados mediante os seguintes formatos:

Dados	Formato
Visualização por defeito	
Hora local	hh:mm
Modo de funcionamento	O
Informação relativa ao condutor	**1** Dhh**h**mm **II**hh**h**mm
Informação relativa ao ajudante	**2** Dhh**h**mm
Condição «fora de âmbito» aberta	OUT
Visualização de alerta	
Ultrapassagem do tempo de condução contínua	**1** ⊙ hh**h**mm **II**hh**h**mm
Incidente ou falha	EF
Outras visualizações	
Data UTC tempo	UTC ⊙ dd/mm/aaaa ou UTC ⊙ dd.mm.aaaa hh:mm
Tempo de condução contínua e pausas acumuladas do condutor	**1** ⊙ hh**h**mm **II**hh**h**mm
Tempo de condução contínua e pausas acumuladas do ajudante	**2** ⊙ hh**h**mm **II**hh**h**mm
Tempo acumulado de condução contínua do condutor nas semanas anterior e em curso	**1** ⊙ **II** hhh**h**mm
Tempo acumulado de condução contínua do ajudante nas semanas anterior e em curso	**2** ⊙ **II** hhh**h**mm

▼B

Apêndice 6

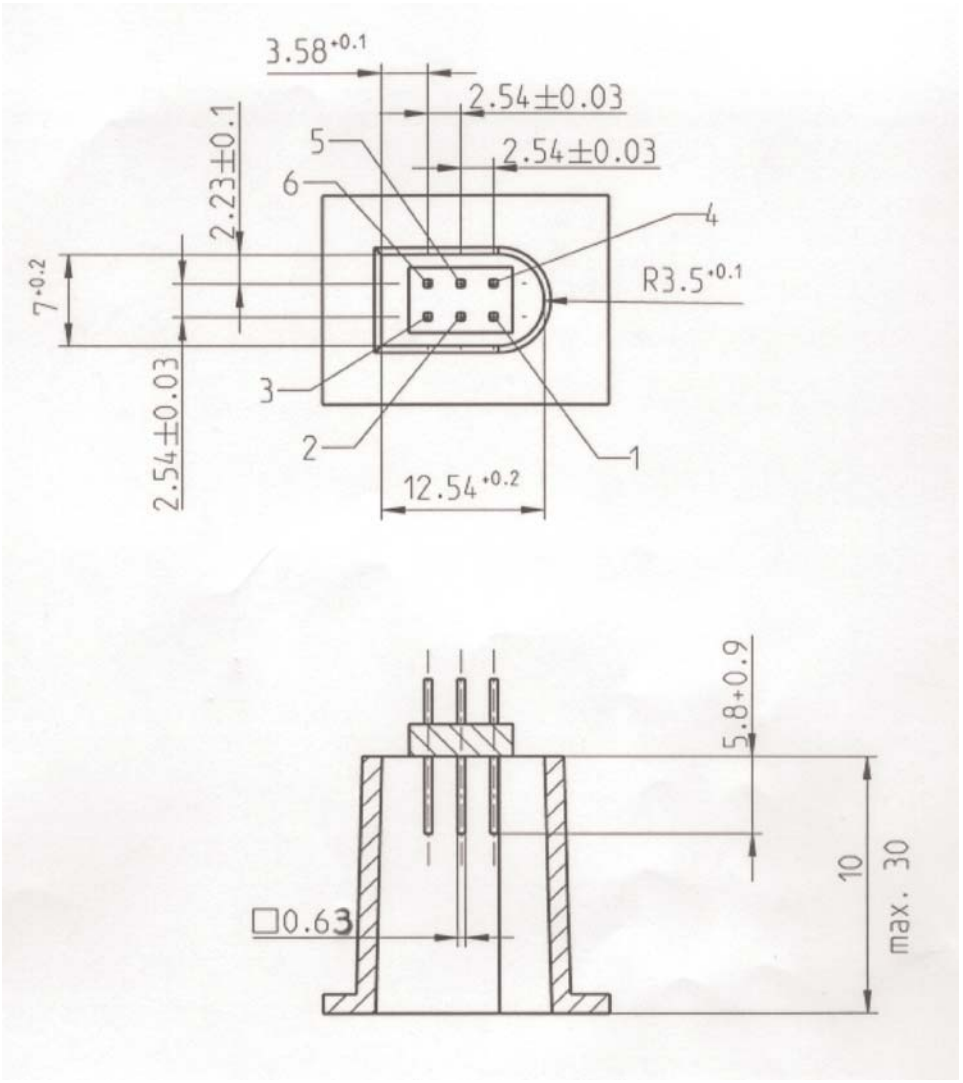
CONECTOR DA FRENTE PARA CALIBRAÇÃO E DESCARREGAMENTO

ÍNDICE

1. EQUIPAMENTO INFORMÁTICO

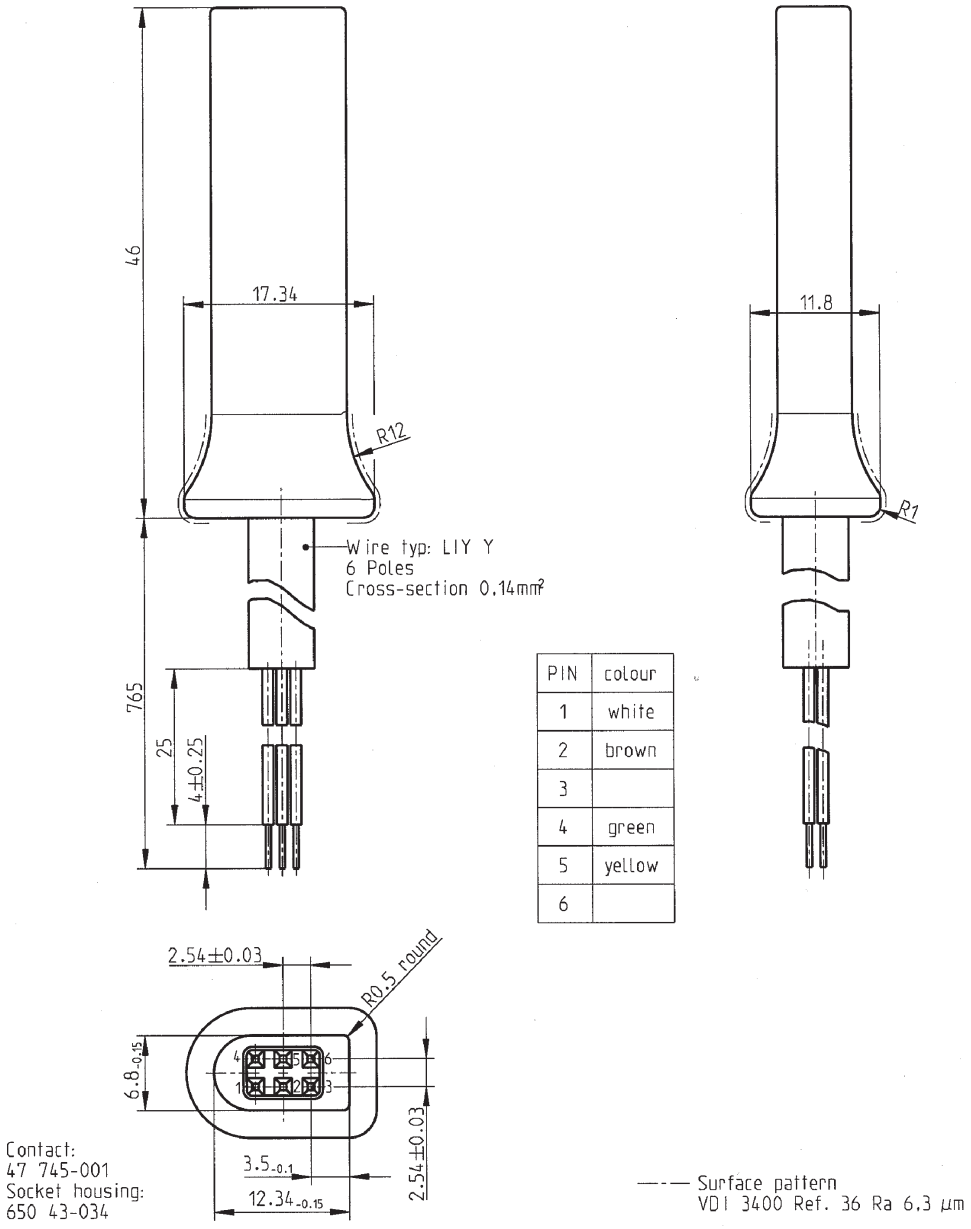
1.1. **Conector**

INT_001 O conector de descarregamento/calibração deve ser de 6 pinos, acessível no painel frontal sem necessidade de desligar qualquer peça do tacógrafo, e deve corresponder ao seguinte esquema (dimensões em milímetros):



▼B

O diagrama seguinte indica uma ficha de ligação de 6 pinos típica:



1.2. **Distribuição dos contactos**

INT_002 Os contactos distribuem-se em conformidade com a seguinte tabela:

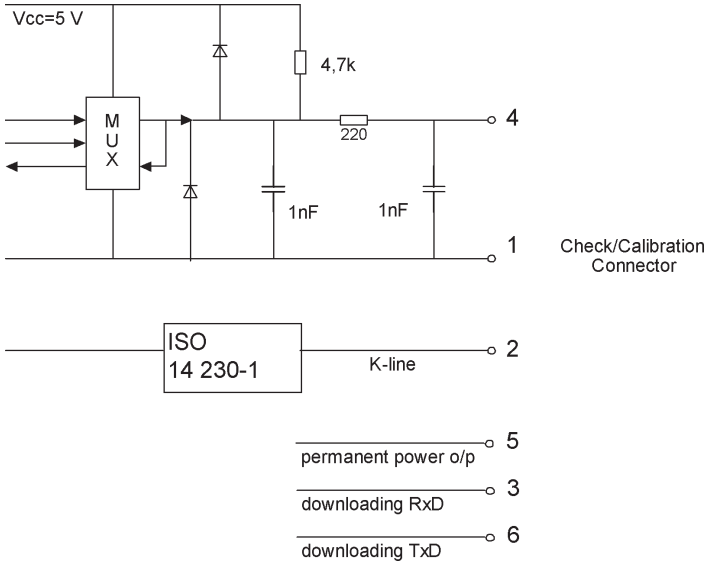
Pino	Descrição	Observação
1	Polo negativo da bateria	Ligado ao polo negativo da bateria do veículo
2	Comunicação de dados	Linha-K (ISO 14230-1)
3	Descarregamento RxD	Entrada de dados no tacógrafo
4	Sinal de entrada/saída	Calibração

▼B

Pino	Descrição	Observação
5	Valor permanente de potência de saída	A tensão nominal é igual à do veículo subtraída de 3 V, tendo em conta a queda de tensão através do circuito de proteção Saída de 40 mA
6	Descarregamento TxD	Saída de dados do tacógrafo

1.3. **Diagrama de blocos**

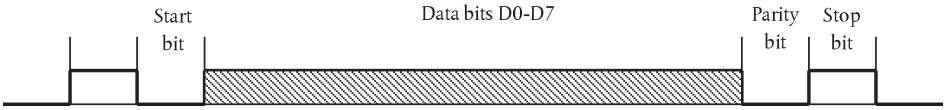
INT_003 O diagrama de blocos deve obedecer ao seguinte esquema:



2. INTERFACE DE DESCARREGAMENTO

INT_004 A interface de descarregamento deve cumprir as especificações RS232.

INT_005 A interface de descarregamento deve utilizar 1 bit de início, 8 bits de dados LSB first, 1 bit de paridade e 1 bit de paragem.



Organização dos bytes de dados

Bit de início: um bit com nível lógico 0

Bits de dados: transmitidos com LSB first

Bit de paridade: paridade par

Bit de paragem: um bit com nível lógico 1

Se forem transmitidos dados numéricos compostos por mais de um byte, o byte mais significativo é transmitido em primeiro lugar e o menos significativo em último lugar.

INT_006 A frequência dos báudios de transmissão deve ser ajustável de 9 600 bps a 115 200 bps. A transmissão deve ser concretizada à velocidade mais elevada possível, fixando-se a frequência em 9 600 bps uma vez iniciada a comunicação.

▼B

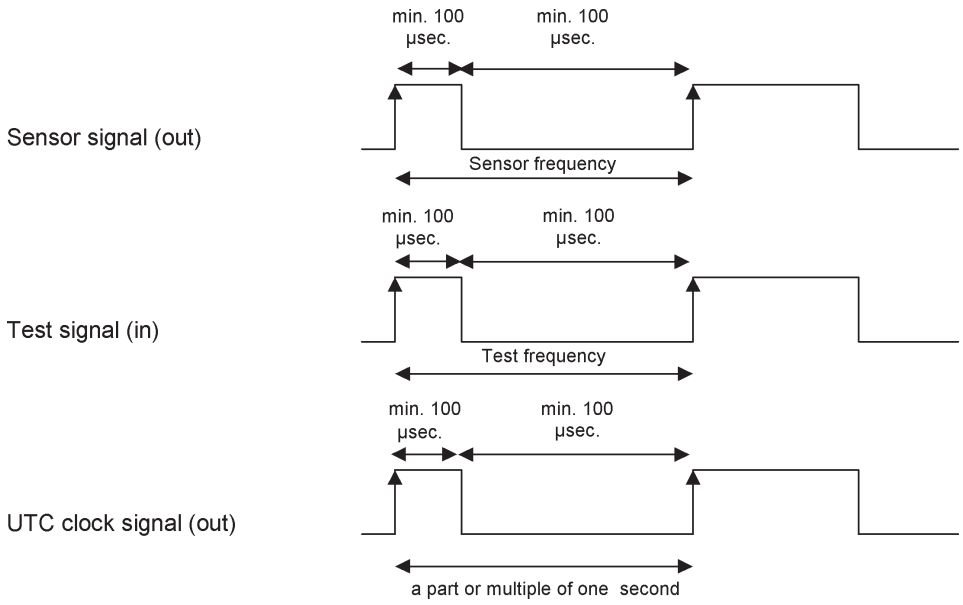
3. INTERFACE DE CALIBRAÇÃO

INT_007 A comunicação de dados deve obedecer à norma ISO 14230-1 Road Vehicles — Diagnostic systems — Keyword protocol 2000 — Part 1: Physical layer, First edition: 1999.

INT_008 O sinal de entrada/saída deve cumprir a seguinte especificação elétrica:

Parâmetro	Mínimo	Típico	Máximo	Observação
U_{low} (in)			1,0 V	I = 750 μA
U_{high} (in)	4 V			I = 200 μA
Frequência			4 kHz	
U_{low} (out)			1,0 V	I = 1 mA
U_{high} (out)	4 V			I = 1 mA

INT_009 O sinal de entrada/saída deve cumprir os seguintes diagramas cronológicos:



▼B

Apêndice 7

PROTOCOLOS APLICÁVEIS AO DESCARREGAMENTO DE DADOS

ÍNDICE

▼B

2.2.5 Tratamento de erros

2.2.5.1 Fase de início da comunicação

2.2.5.2 Fase de Comunicação

2.2.6 Conteúdo da mensagem de resposta

2.2.6.1 Positive Response Transfer Data Overview

2.2.6.2 Positive Response Transfer Data Activities

2.2.6.3 Positive Response Transfer Data Events and Faults

2.2.6.4 Positive Response Transfer Data Detailed Speed

2.2.6.5 Positive Response Transfer Data Technical Data

2.3. Memorização de ficheiros ESM

3. PROTOCOLO APLICÁVEL AO DESCARREGAMENTO DE DADOS DE CARTÕES TACOGRÁFICOS

3.1. Âmbito de aplicação

3.2. Definições

3.3. Descarregamento do cartão

3.3.1 Sequência de inicialização

3.3.2 Sequência para ficheiros de dados não assinados

3.3.3 Sequência para ficheiros de dados assinados

3.3.4 Sequência para reinicializar o contador de calibração.

3.4. Formato de memorização dos dados

3.4.1 Introdução

3.4.2 Formato do ficheiro

4. DESCARREGAMENTO DE UM CARTÃO TACOGRÁFICO VIA UMA UNIDADE-VEÍCULO.

1. INTRODUÇÃO

O presente apêndice especifica os procedimentos a adotar na execução dos diversos tipos de descarregamento de dados para meios externos de memorização ou armazenamento (ESM), juntamente com os protocolos que se devem aplicar para assegurar a transferência correta dos dados e a compatibilidade total do formato dos dados descarregados, a fim de que um controlador, antes de os analisar, possa inspecioná-los e controlar a sua autenticidade e a sua integridade.

1.1. **Âmbito de aplicação**

Pode haver descarregamento de dados para um ESM:

— a partir de uma unidade-veículo, por meio de um equipamento dedicado inteligente (IDE) ligado à unidade-veículo (VU)

— a partir de um cartão tacográfico, por meio de um IDE equipado com dispositivo de interface para o cartão (IFD)

▼B

— a partir de um cartão tacográfico, via uma unidade-veículo, por meio de um IDE ligado a essa VU.

Para possibilitar a verificação da autenticidade e da integridade dos dados descarregados memorizados num ESM, o descarregamento é feito com uma assinatura apensa em conformidade com o apêndice 11 (Mecanismos comuns de segurança). A identificação do equipamento-fonte (VU ou cartão) e os respetivos certificados de segurança (Estado-Membro e equipamento) são também descarregados. O verificador dos dados deve possuir, independentemente, uma chave pública europeia aprovada.

DDP_001 Os dados descarregados durante uma sessão devem ser memorizados no ESM dentro de um ficheiro único.

1.2. **Acrónimos e notações**

No presente apêndice, utilizam-se os seguintes acrónimos:

AID Identificador de aplicação

ATR Resposta à reinicialização

CS Byte de soma de teste

DF Ficheiro dedicado

DS_ Sessão de diagnóstico

EF Ficheiro elementar

ESM Meio externo de memorização ou armazenamento

FID Identificador de ficheiro (ID de ficheiro)

FMT Byte de formato (primeiro byte de um cabeçalho de mensagem)

ICC Cartão com circuito integrado

IDE Equipamento dedicado inteligente: o equipamento utilizado para executar o descarregamento dos dados para o ESM (por exemplo, computador pessoal)

IFD Dispositivo de interface

KWP Protocolo de palavra-chave 2000

LEN Byte de comprimento (último byte de um cabeçalho de mensagem)

PPS Seleção dos parâmetros do protocolo

PSO Executar operação de segurança

SID Identificador de serviço

SRC Byte-fonte

TGT Byte-alvo

TLV Valor do comprimento de um marcador

TREP Parâmetro de resposta de transferência

TRTP Parâmetro de pedido de transferência

VU Unidade-veículo

▼B

2. DESCARREGAMENTO DE DADOS DE UMA VU

2.1. **Procedimento relativo ao descarregamento**

Para descarregar dados de uma VU, o utilizador executa as seguintes operações:

— inserir o cartão tacográfico numa ranhura da VU (*)

— ligar o IDE ao conector de descarregamento da VU

— estabelecer a ligação entre o IDE e a VU

— selecionar no IDE os dados a descarregar e enviar o pedido à VU

— encerrar a sessão de descarregamento.

2.2. **Protocolo de descarregamento dos dados**

O protocolo é estruturado numa base «mestre-escravo» (ou principal/secundário), em que o IDE desempenha o papel de mestre e a VU o de escravo.

A estrutura, os tipos e o fluxo da mensagem baseiam-se principalmente no Protocolo de palavra-chave 2000 (KWP) (norma ISO 14230-2 Road vehicles — Diagnostic systems — Keyword protocol 2000 — Part 2: Data link layer).

O nível de aplicação (*application layer*) baseia-se principalmente no atual projeto da norma ISO 14229-1 (Road vehicles — Diagnostic systems — Part 1: Diagnostic services, versão 6, de 22 de fevereiro de 2001).

2.2.1 *Estrutura da mensagem*

DDP_002 Todas as mensagens trocadas entre o IDE e a VU são formatadas com uma estrutura dividida em três partes:

— cabeçalho, composto por um byte de formato (FMT), um byte-alvo (TGT), um byte-fonte (SRC) e, possivelmente, um byte de comprimento (LEN)

— campo de dados, composto por um byte de identificador de serviço (SID) e um número variável de bytes de dados, que podem incluir um byte opcional de sessão de diagnóstico (DS_) ou um byte opcional de parâmetro de transferência (TRTP ou TREP)

— soma de teste, composta por um byte de soma de teste (CS).

Cabeçalho				Campo de dados					Soma de teste
FMT	TGT	SRC	LEN	SID	DA-DOS	…	…	…	CS
4 bytes				Máx. 255 bytes					1 byte

Os bytes TGT e SRC representam o endereço físico do destinatário e do emitente da mensagem. Os valores são F0 Hex para o IDE e EE Hex para a VU.

O byte LEN é o comprimento da parte campo de dados.

O byte soma de teste é o módulo 256 da série soma de 8 bits de todos os bytes da mensagem, excluindo o próprio CS.

Os bytes FMT, SID, DS_, TRTP e TREP serão definidos adiante.

(*) O cartão inserido desencadeia os devidos direitos de acesso à função de descarregamento e aos dados. Contudo, deve ser possível descarregar dados de um cartão de condutor inserido numa das ranhuras da VU quando não está inserido outro tipo de cartão na outra ranhura.

▼B

DDP_003 Nos casos em que os dados a transportar pela mensagem sejam superiores ao espaço disponível na parte campo de dados, a mensagem é dividida em várias submensagens, cada uma das quais contém um cabeçalho, os mesmos SID e TREP e um contador de submensagem de 2 bytes indicando o número da submensagem no contexto da mensagem total. Para verificar erros e abortar, o IDE reconhece cada uma das submensagens. O IDE pode aceitar a submensagem, pedir a sua retransmissão, pedir o recomeço à VU ou abortar a transmissão.

DDP_004 Se a última submensagem contiver exatamente 255 bytes no campo de dados, deve ser apensa uma submensagem final com um campo de dados vazio (excetuando SID, TREP e o contador dessa submensagem), para indicar que terminou a mensagem.

Exemplo:

Cabeçalho	SID	TREP	Mensagem	CS
4 bytes	Comprimento superior a 255 bytes			

é transmitido sob a seguinte forma:

Cabeçalho	SID	TREP	00	01	Submensagem 1	CS
4 bytes	255 bytes					

Cabeçalho	SID	TREP	00	02	Submensagem 2	CS
4 bytes	255 bytes					

…

Cabeçalho	SID	TREP	xx	yy	Submensagem n	CS
4 bytes	Menos de 255 bytes					

ou sob a seguinte forma:

Cabeçalho	SID	TREP	00	01	Submensagem 1	CS
4 bytes	255 bytes					

Cabeçalho	SID	TREP	00	02	Submensagem 2	CS
4 bytes	255 bytes					

…

Cabeçalho	SID	TREP	xx	yy	Submensagem n	CS
4 bytes	255 bytes					

Cabeçalho	SID	TREP	xx	yy + 1	CS
4 bytes	4 bytes				

▼B

2.2.2 *Tipos de mensagens*

O protocolo de comunicação para descarregamento de dados entre a VU e o IDE exige o intercâmbio de 8 tipos diferentes de mensagens.

O quadro seguinte sintetiza essas mensagens.

Message Structure	Max 4 Bytes Header				Max 255 Bytes Data			1 Byte Check-Sum
IDE -> <- VU	FMT	TGT	SRC	LEN	SID	DS_/TRTP	DATA	CS
Start Communication Request	81	EE	F0		81			E0
Positive Response Start Communication	80	F0	EE	03	C1		EA, 8F	9B
Start Diagnostic Session Request	80	EE	F0	02	10	81		F1
Positive Response Start Diagnostic	80	F0	EE	02	50	81		31
Link Control Service								
Verify Baud Rate (stage 1)								
9 600 Bd	80	EE	F0	04	87		01,01,01	EC
19 200 Bd	80	EE	F0	04	87		01,01,02	ED
38 400 Bd	80	EE	F0	04	87		01,01,03	EE
57 600 Bd	80	EE	F0	04	87		01,01,04	EF
115 200 Bd	80	EE	F0	04	87		01,01,05	F0
Positive Response Verify Baud Rate	80	F0	EE	02	C7		01	28
Transition Baud Rate (stage 2)	80	EE	F0	03	87		02,03	ED
Request Upload	80	EE	F0	0A	35		00,00,00,00,00, FF,FF,FF,FF	99
Positive Response Request Upload	80	F0	EE	03	75		00,FF	D5
Transfer Data Request								
Overview	80	EE	F0	02	36	01		97
Activities	80	EE	F0	06	36	02	Date	CS
Events & Faults	80	EE	F0	02	36	03		99
Detailed Speed	80	EE	F0	02	36	04		9A
Technical Data	80	EE	F0	02	36	05		9B
Card download	80	EE	F0	02	36	06	Slot	CS
Positive Response Transfer Data	80	F0	EE	Len	76	TREP	Data	CS
Request Transfer Exit	80	EE	F0	01	37			96
Positive Response Request Transfer Exit	80	F0	EE	01	77			D6

▼B

Message Structure	Max 4 Bytes Header				Max 255 Bytes Data			1 Byte Check-Sum
IDE -> <- VU	FMT	TGT	SRC	LEN	SID	DS_/TRTP	DATA	CS
Stop Communication Request	80	EE	F0	01	82			E1
Positive Response Stop Communication	80	F0	EE	01	C2			21
Acknowledge sub message	80	EE	F0	Len	83		Data	CS
Negative responses								
General reject	80	F0	EE	03	7F	Sid Req	10	CS
Service not supported	80	F0	EE	03	7F	Sid Req	11	CS
Sub function not supported	80	F0	EE	03	7F	Sid Req	12	CS
Incorrect Message Length	80	F0	EE	03	7F	Sid Req	13	CS
Conditions not correct or Request sequence error	80	F0	EE	03	7F	Sid Req	22	CS
Request out of range	80	F0	EE	03	7F	Sid Req	31	CS
Upload not accepted	80	F0	EE	03	7F	Sid Req	50	CS
Response pending	80	F0	EE	03	7F	Sid Req	78	CS
Data not available	80	F0	EE	03	7F	Sid Req	FA	CS

Notas:

— Sid Req = o SID do pedido correspondente.

— TREP = o TRTP do pedido correspondente.

— As células a negro indicam que nada é transmitido.

— O termo «carregamento» (visto do IDE) é utilizado para compatibilidade com a norma ISO 14229. Significa o mesmo que «descarregamento» (visto da VU).

— Contadores de submensagens potenciais de 2 bytes não figuram neste quadro.

— Ranhura é o número da ranhura, quer seja «1» (cartão na ranhura do condutor) ou «2» (cartão na ranhura do ajudante)

— Caso a ranhura não seja especificada, a VU seleciona a ranhura 1, se for inserido um cartão nesta ranhura e seleciona a ranhura 2 apenas quando esta é especificamente selecionada pelo utilizador.

2.2.2.1 Start Communication Request (SID 81)

DDP_005 Esta mensagem é emitida pelo IDE para estabelecer o elo de comunicação com a VU. As comunicações iniciais são sempre executadas a 9 600 bauds (até o número de bauds ser alterado por meio dos serviços competentes de controlo de elo).

▼B

2.2.2.2 Positive Response Start Communication (SID C1)

DDP_006 Esta mensagem é emitida pela VU em resposta positiva a um pedido de começo da comunicação. Inclui os 2 bytes--chave 'EA' e '8F', o que indica que a unidade é compatível com o protocolo com cabeçalho, incluindo informação sobre o alvo, a fonte e o comprimento.

2.2.2.3 Start Diagnostic Session Request (SID 10)

DDP_007 A mensagem Start Diagnostic Session Request é emitida pelo IDE para pedir uma nova sessão de diagnóstico com a VU. A subfunção «default session» ou «sessão por defeito» (81 Hex) indica que vai ser aberta uma sessão normal de diagnóstico.

2.2.2.4 Positive Response Start Diagnostic (SID 50)

DDP_008 A mensagem Positive Response Start Diagnostic é enviada pela VU em resposta positiva ao Diagnostic Session Request.

2.2.2.5 Link Control Service (SID 87)

DDP_052 O Link Control Service é utilizado pelo IDE para iniciar uma modificação no número de bauds, o que ocorre em duas fases. Na primeira fase, o IDE propõe a modificação do número de bauds, indicando o novo ritmo. Ao receber uma mensagem positiva da VU, o IDE envia-lhe a confirmação da modificação no número de bauds (segunda fase) e adota o novo ritmo. Depois de receber a confirmação, a VU passa, por sua vez, para o novo número de bauds.

2.2.2.6 Link Control Positive Response (SID C7)

DDP_053 A VU emite a mensagem Link Control Positive Response em resposta positiva ao pedido de Link Control Service (primeira fase). Note-se que não é dada resposta ao pedido de confirmação (segunda fase).

2.2.2.7 Request Upload (SID 35)

DDP_009 O IDE emite a mensagem Request Upload para especificar à VU que é pedida uma operação de descarregamento. Em cumprimento da norma ISO 14229, são incluídos elementos sobre o endereço, o tamanho e o formato dos dados pedidos. Como o IDE os desconhece antes de um descarregamento, o endereço da memória é colocado a 0, o formato é desencriptado e descomprimido e o tamanho da memória é fixado no máximo.

2.2.2.8 Positive Response Request Upload (SID 75)

DDP_010 Esta mensagem é enviada pela VU para indicar ao IDE que está pronta para descarregar dados. Em cumprimento da norma ISO 14229, nesta mensagem de resposta positiva são incluídos dados que indicam ao IDE que as futuras mensagens de Positive Response Transfer Data (resposta positiva ao pedido de transferência de dados) incluirão no máximo 00FF hex bytes.

▼B

2.2.2.9 Transfer Data Request (SID 36)

DDP_011 Esta mensagem (pedido de transferência de dados) é enviada pelo IDE para especificar à VU o tipo dos dados que devem ser descarregados. O tipo de transferência é indicado por um Transfer Request Parameter (TRTP ou parâmetro de pedido de transferência) de um byte.

Há seis tipos de transferência de dados:

— Panorâmica (TRTP 01)

— Atividades de data especificada (TRTP 02)

— Incidentes e falhas (TRTP 03)

— Velocidade detalhada (TRTP 04)

— Dados técnicos (TRTP 05)

— Descarregamento do cartão (TRTP 06).

DDP_054 Durante uma sessão de descarregamento, o IDE tem obrigatoriamente de pedir a transferência de dados panorâmica (TRTP 01), pois só assim os certificados da VU são registados no ficheiro descarregado (e só assim pode ser verificada a assinatura digital).

No segundo caso (TRTP 02), a mensagem Transfer Data Request inclui a indicação do dia a descarregar (formato `TimeReal`).

2.2.2.10 Positive Response Transfer Data (SID 76)

DDP_012 Esta mensagem é enviada pela VU em resposta positiva a Transfer Data Request (pedido de transferência de dados). Contém os dados pedidos, com um TREP (Transfer Response Parameter ou parâmetro de resposta de transferência) correspondente ao TRTP do pedido.

DDP055 No primeiro caso (TREP 01), a VU envia dados para ajudar o utilizador do IDE a escolher os que pretende descarregar mais tarde. A informação contida nesta mensagem é a seguinte:

— certificados de segurança

— identificação do veículo

— data e hora atuais da VU

— data descarregável mínima e máxima (dados da VU)

— indicação de presença de cartões na VU

— descarregamento prévio para uma empresa

— bloqueios de empresa

— controlos prévios.

▼B

2.2.2.11 Request Transfer Exit (SID 37)

DDP_013 A mensagem Request Transfer Exit (saída do pedido de transferência) é enviada pelo IDE para informar a VU de que a sessão de descarregamento está terminada.

2.2.2.12 Positive Response Request Transfer Exit (SID 77)

DDP_014 Esta mensagem é enviada pela VU para acusar a mensagem Request Transfer Exit.

2.2.2.13 Stop Communication Request (SID 82)

DDP_015 Esta mensagem é enviada pelo IDE para desligar o elo de comunicação com a VU.

2.2.2.14 Positive Response Stop Communication (SID C2)

DDP_016 Esta mensagem é enviada pela VU para acusar a mensagem Stop Communication Request.

2.2.2.15 Acknowledge Sub Message (SID 83)

DDP_017 Esta mensagem é enviada pelo IDE para confirmar a receção de cada parte de uma mensagem que seja transmitida sob a forma de diversas submensagens. O campo de dados contém o SID recebido da VU e um código de 2 bytes, a saber:

— MsgC + 1 acusa a receção correta da submensagem n.º MsgC.

Pedido do IDE à VU para que envie a submensagem seguinte

— MsgC indica um problema na receção da submensagem n.º MsgC.

Pedido do IDE à VU para que envie novamente a submensagem.

— FFFF pede que a mensagem seja interrompida.

O IDE pode recorrer a este código para parar, por alguma razão, a transmissão da mensagem da VU.

A última submensagem de uma mensagem (byte LEN < 255) pode ser acusada por intermédio de qualquer um destes códigos, ou não ser acusada.

A resposta da VU que consiste em diversas submensagens é a seguinte:

— Positive Response Transfer Data (SID 76)

▼B

2.2.2.16 Negative Response (SID 7F)

DDP_018 Quando a VU não consegue satisfazer os pedidos contidos nas mensagens supramencionadas, envia esta mensagem. O campo de dados desta mensagem contém o SID da resposta (7F), o SID do pedido e um código que especifica a razão da resposta negativa. São os seguintes os códigos disponíveis:

— 10 rejeição geral

A ação não pode ser executada por uma razão não contemplada adiante.

— 11 serviço não compatível

O SID do pedido não é entendido.

— 12 subfunção não compatível

O DS_ ou o TRTP do pedido não são entendidos ou não há mais submensagens a transmitir.

— 13 comprimento de mensagem incorreto

O comprimento da mensagem recebida está errado.

— 22 condições incorretas ou erro de sequência do pedido

O serviço requerido não está ativo ou a sequência das mensagens de pedido não é correta.

— 31 pedido fora de alcance

O registo do parâmetro de pedido (campo de dados) não é válido.

— 50 carregamento não aceite

O pedido não pode ser executado (VU num modo de funcionamento inadequado ou falha interna da VU).

— 78 resposta pendente

A ação pedida não pode ser completada a tempo e a VU não está preparada para aceitar outro pedido.

— FA dados não disponíveis

O objeto de um pedido de transferência de dados não está disponível na VU (por exemplo, não há cartão inserido, etc.).

2.2.3 *Fluxo de mensagens*

O fluxo típico de mensagens durante um procedimento normal de descarregamento de dados é o seguinte:

IDE		VU
Start Communication Request	⇨	
	⇦	Positive Response
Start Diagnostic Service Request	⇨	
	⇦	Positive Response
Request Upload	⇨	
	⇦	Positive Response

▼B

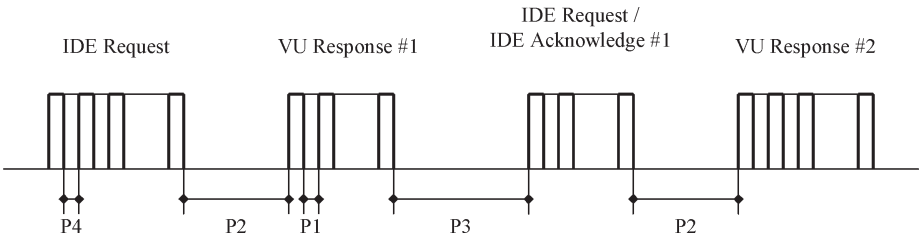
IDE		VU
Transfer Data Request Overview	⇨	
	⇦	Positive Response
Transfer Data Request #2	⇨	
	⇦	Positive Response #1
Acknowledge Sub Message #1	⇨	
	⇦	Positive Response #2
Acknowledge Sub Message #2	⇨	
	⇦	Positive Response #m
Acknowledge Sub Message #m	⇨	
	⇦	Positive Response (Data Field<255 Bytes)
Acknowledge Sub Message (optional)	⇨	
…		
Transfer Data Request #n	⇨	
	⇦	Positive Response
Request Transfer Exit	⇨	
	⇦	Positive Response
Stop Communication Request	⇨	
	⇦	Positive Response

2.2.4 *Temporização*

DDP_019 Durante o funcionamento normal, destacam-se os parâmetros de temporização indicados no esquema seguinte:

Esquema 1

Fluxo de mensagens, temporização



Em que:

P1 = intervalo interbytes para a resposta da VU.

P2 = intervalo entre o final do pedido do IDE e o começo da resposta da VU, ou entre o final da acusação por parte do IDE e o começo da resposta seguinte da VU.

P3 = intervalo entre o final da resposta da VU e o começo do novo pedido do IDE ou entre o final da resposta da VU e o começo da acusação por parte do IDE ou ainda entre o final do pedido do IDE e o começo de novo pedido do IDE se a VU não responder.

P4 = intervalo interbytes para o pedido do IDE.

P5 = valor alargado de P3 para descarregamento de cartões.

▼B

Os valores autorizados para os parâmetros de temporização são indicados no quadro seguinte (conjunto de parâmetros de temporização alargado do KWP, utilizado em caso de endereçamento físico para maior rapidez de comunicação):

Parâmetro de temporização	Valor do limite inferior (mm)	Valor do limite máximo (mm)
P1	0	20
P2	20	1 000 (*)
P3	10	5 000
P4	5	20
P5	10	20 minutos

(*) Se a VU responder com uma Negative Response contendo um código que signifique «pedido corretamente recebido, resposta pendente», este valor é alargado para o mesmo limite superior de P3.

2.2.5 *Tratamento de erros*

Se ocorrer um erro durante o intercâmbio de mensagens, o fluxo é modificado, consoante o equipamento que tiver detetado o erro e a mensagem que lhe tiver dado origem.

Nos esquemas 2 e 3 são indicados os procedimentos de tratamento de erros, respetivamente para a VU e para o IDE.

2.2.5.1 Fase de início da comunicação

DDP_020 Se o IDE detetar um erro durante a fase de início da comunicação, quer pela temporização quer pela sucessão de bits, aguarda durante um período P3mín antes de emitir novamente o pedido.

DDP_021 Se a VU detetar um erro na sequência proveniente do IDE, não envia qualquer resposta e aguarda nova mensagem Start Communication Request durante um período P3máx.

2.2.5.2 Fase de Comunicação

Podem definir-se duas áreas distintas de tratamento de erros:

1. **A VU deteta um erro de transmissão do IDE**

DDP_022 Por cada mensagem recebida, a VU deteta erros de temporização, erros de formato dos bytes (por exemplo, violações nos bits de início e de fim) e erros de enquadramento (número errado de bytes recebidos, byte errado de soma de teste).

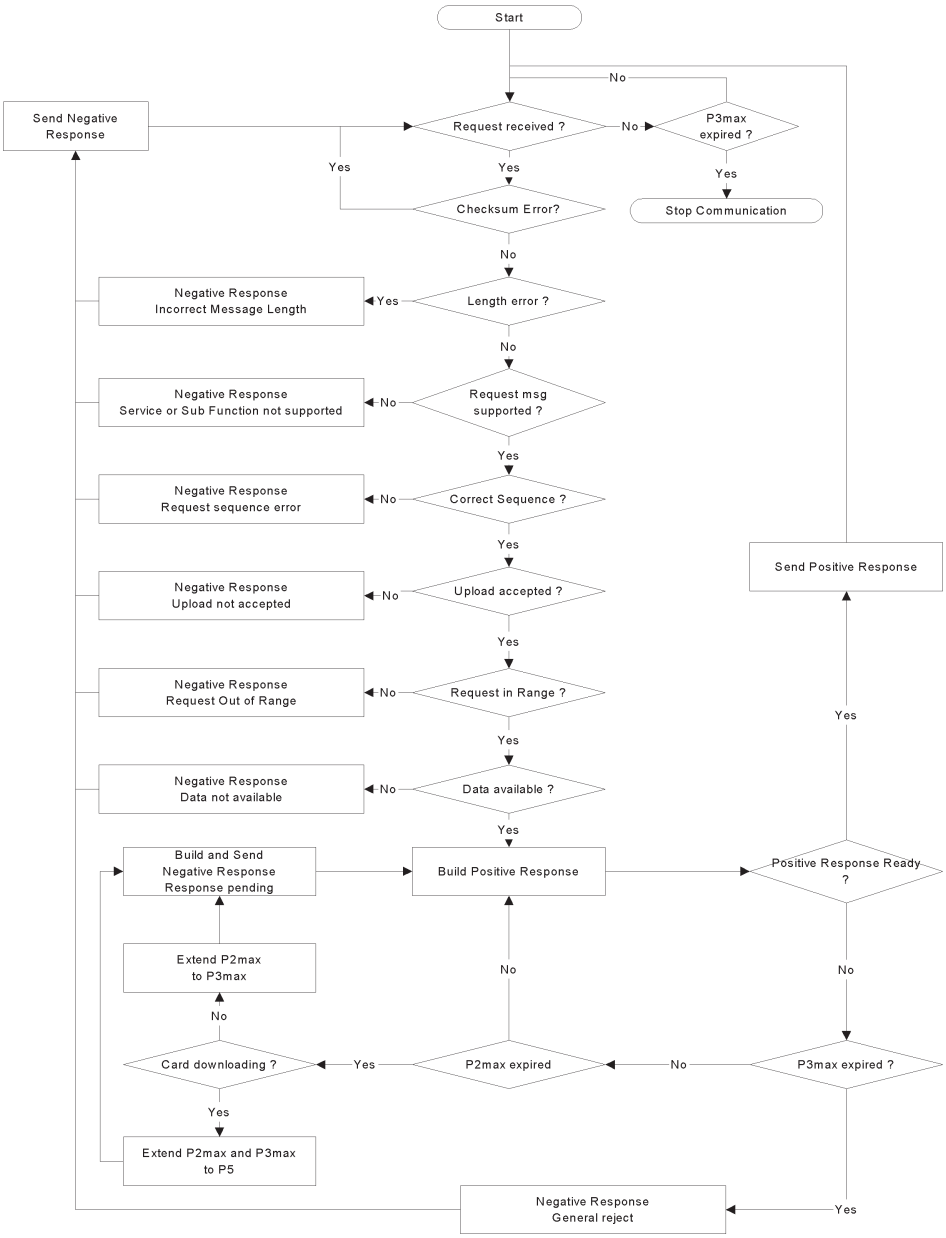
DDP_023 Se a VU detetar um dos erros supra, não envia qualquer resposta e ignora a mensagem recebida.

DDP_024 A VU pode detetar outros erros no formato ou no conteúdo da mensagem recebida (por exemplo, mensagem não aceite), mesmo que a mensagem satisfaça os requisitos de comprimento e de soma de teste. Em tal caso, a VU responde ao IDE com uma mensagem Negative Response, especificando a natureza do erro.

▼B

Esquema 2

Tratamento de erros por parte da VU



2. **O IDE deteta um erro de transmissão da VU**

DDP_025 Por cada mensagem recebida, o IDE deteta erros de temporização, erros de formato dos bytes (por exemplo, violações nos bits de início e de fim) e erros de enquadramento (número errado de bytes recebidos, byte errado de soma de teste).

DDP_026 O IDE deteta erros de sequência, como, por exemplo, incrementos incorretos no contador de submensagens, em mensagens recebidas sucessivamente.

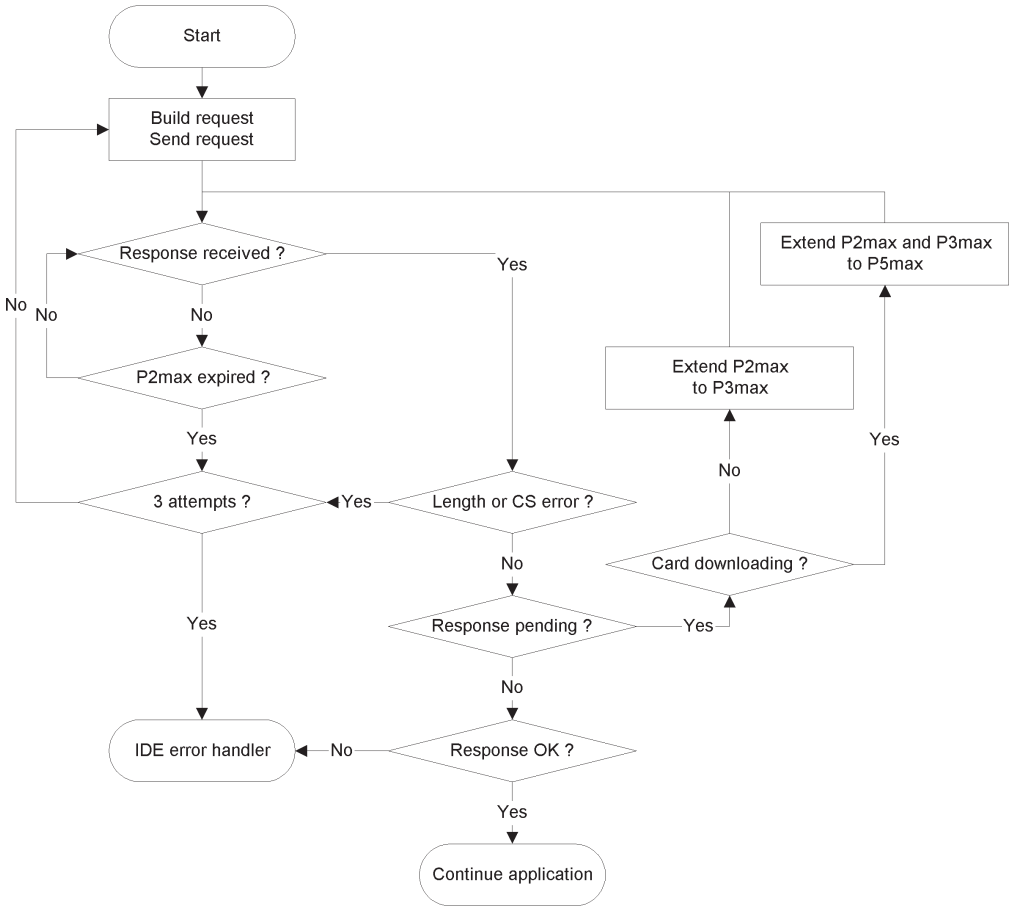
DDP_027 Se o IDE detetar um erro ou não houver resposta da VU dentro de um período P2máx, a mensagem de pedido é novamente enviada, num máximo de três transmissões ao todo. Para efeitos desta deteção de erro, a acusação de uma submensagem será considerada como um pedido à VU.

▼B

DDP_028 O IDE aguarda pelo menos durante um período P3mín antes de iniciar cada transmissão. O período de espera é medido a partir da última ocorrência calculada de um bit de fim depois de detetado o erro.

Esquema 3

Tratamento de erros por parte do IDE



2.2.6 *Conteúdo da mensagem de resposta*

Esta secção especifica o conteúdo dos campos de dados das várias mensagens de resposta positiva.

Os elementos de dados são definidos no apêndice 1 (Dicionário de dados).

Observação: Em relação aos descarregamentos da geração 2, cada elemento de dados de topo é representado por uma matriz de registos, mesmo que contenha apenas um registo. A matriz de registos começa com um cabeçalho. Este cabeçalho contém o tipo de registo, o tamanho do registo e o número de registos. Nos quadros a seguir, as matrizes de registo são denominadas «... RecordArray» (com cabeçalho).

2.2.6.1 Positive Response Transfer Data Overview

DDP_029 O campo de dados da mensagem «Positive Response Transfer Data Overview» fornece os seguintes dados, segundo a ordem indicada, sob o SID 76 Hex e o TREP 01 Hex e com uma divisão e uma contagem adequadas das submensagens:

▼B

Estrutura de dados da geração 1

Elemento de dados	Observação
MemberStateCertificate VUCertificate	Certificados de segurança da VU
VehicleIdentificationNumber VehicleRegistrationIdentification	Identificação do veículo
CurrentDateTime	Data e hora atuais da VU
VuDownloadablePeriod	Período descarregável
CardSlotsStatus	Tipo de cartões inseridos na VU
VuDownloadActivityData	Descarregamento prévio da VU
VuCompanyLocksData	Todos os bloqueios de empresa memorizados. Se o perfil estiver vazio, é enviado apenas noOfLocks = 0.
VuControlActivityData	Todos os registos de controlo memorizados na VU. Se o perfil estiver vazio, é enviado apenas noOfControls = 0
Signature	Assinatura RSA de todos os dados (exceto certificados) a partir de VehicleIdentificationNumber para baixo até ao último byte do último VuControlActivityData.

Estrutura de dados da geração 2:

Elemento de dados	Observação
MemberStateCertificateRecordArray	Certificado do Estado-Membro
VUCertificateRecordArray	Certificado VU
VehicleIdentificationNumberRecordArray	Identificação do veículo
VehicleRegistrationNumberRecordArray	Número de matrícula do veículo
CurrentDateTimeRecordArray	Data e hora atuais da VU
VuDownloadablePeriodRecordArray	Período descarregável
CardSlotsStatusRecordArray	Tipo de cartões inseridos na VU
VuDownloadActivityDataRecordArray	Descarregamento prévio da VU
VuCompanyLocksRecordArray	Todos os bloqueios de empresa memorizados. Se o perfil estiver vazio, é enviado um cabeçalho da matriz com noOfRecords = 0
VuControlActivityRecordArray	Todos os registos de controlo memorizados na VU. Se o perfil estiver vazio, é enviado um cabeçalho da matriz com noOfRecords = 0
SignatureRecordArray	Assinatura ECC de todos os dados precedentes, com exceção dos certificados.

2.2.6.2 Positive Response Transfer Data Activities

DDP_030 O campo de dados da mensagem «Positive Response Transfer Data Activities» fornece os seguintes dados, segundo a ordem indicada, sob o SID 76 Hex e o TREP 02 Hex e com uma divisão e uma contagem adequadas das submensagens:

▼B

Estrutura de dados da geração 1

Elemento de dados	Observação
TimeReal	Data do dia descarregado
OdometerValueMidnight	Conta-quilómetros no final do dia descarregado
VuCardIWData	Dados dos ciclos de inserção e retirada de cartões. — Se este perfil não tiver dados disponíveis, é enviado apenas noOfVuCardIWRecords = 0. — Quando um VuCardIWRecord se encontra a 00:00 (inserção do cartão no dia anterior) ou a 24:00 (retirada do cartão no dia seguinte) deve aparecer integralmente nos dois dias em causa.
VuActivityDailyData	Situação das ranhuras às 00:00 e mudanças de atividade registadas em relação ao dia descarregado.
VuPlaceDailyWorkPeriodData	Dados relacionados com locais registados em relação ao dia descarregado. Se o perfil estiver vazio, é enviado apenas noOfPlaceRecords = 0.
VuSpecificConditionData	Dados relativos às condições específicas registados em relação ao dia descarregado. Se o perfil estiver vazio, é enviado apenas noOfSpecificConditionRecords = 0
Signature	Assinatura RSA de todos os dados a partir de TimeReal para baixo até ao último byte do último registo das condições específicas.

Estrutura de dados da geração 2:

Elemento de dados	Observação
DateOfDayDownloadedRecordArray	Data do dia descarregado
OdometerValueMidnightRecordArray	Conta-quilómetros no final do dia descarregado
VuCardIWRecordArray	Dados dos ciclos de inserção e retirada de cartões. — Se este perfil não tiver dados disponíveis, é enviado um cabeçalho da matriz com noOfRecords = 0. — Se um VuCardIWRecord se encontrar a 00:00 (inserção do cartão no dia anterior) ou a 24:00 (retirada do cartão no dia seguinte) deve aparecer integralmente nos dois dias em causa.
VuActivityDailyRecordArray	Situação das ranhuras às 00:00 e mudanças de atividade registadas em relação ao dia descarregado.
VuPlaceDailyWorkPeriodRecordArray	Dados relacionados com locais registados em relação ao dia descarregado. Se o perfil estiver vazio, é enviado um cabeçalho da matriz com noOfRecords = 0.
VuGNSSCDRecordArray	Posições GNSS do veículo se o tempo de condução contínua do condutor atingir um múltiplo de três horas. Se o perfil estiver vazio, é enviado um cabeçalho da matriz com noOfRecords = 0.
VuSpecificConditionRecordArray	Dados relativos às condições específicas, registados em relação ao dia descarregado. Se o perfil estiver vazio, é enviado um cabeçalho da matriz com noOfRecords = 0
SignatureRecordArray	Assinatura ECC de todos os dados precedentes.

▼B

2.2.6.3 Positive Response Transfer Data Events and Faults

DDP_031 O campo de dados da mensagem «Positive Response Transfer Data Events and Faults» fornece os seguintes dados, segundo a ordem indicada, sob o SID 76 Hex e o TREP 03 Hex e com uma divisão e uma contagem adequadas das submensagens:

Estrutura de dados da geração 1

Elemento de dados	Observação
VuFaultData	Todas as falhas memorizadas ou em curso na VU. Se o perfil estiver vazio, é enviado apenas noOfVuFaults = 0.
VuEventData	Todos os incidentes (exceto o excesso de velocidade) memorizados ou em curso na VU. Se o perfil estiver vazio, é enviado apenas noOfVuEvents = 0.
VuOverSpeedingControlData	Dados relativos ao último controlo do excesso de velocidade (valor por defeito se não existirem dados).
VuOverSpeedingEventData	Todos os incidentes de excesso de velocidade memorizados na VU. Se o perfil estiver vazio, é enviado apenas noOfVuOverSpeedingEvents = 0.
VuTimeAdjustmentData	Todos os incidentes de ajuste de tempo memorizados na VU (fora do enquadramento de uma calibração completa). Se o perfil estiver vazio, é enviado apenas noOfVuTimeAdjRecords = 0.
Signature	Assinatura RSA de todos os dados a partir de noOfVuFaults para baixo até ao último byte do último registo de ajuste de tempo

Estrutura de dados da geração 2:

Elemento de dados	Observação
VuFaultRecordArray	Todas as falhas memorizadas ou em curso na VU. Se o perfil estiver vazio, é enviado um cabeçalho da matriz com noOfRecords = 0.
VuEventRecordArray	Todos os incidentes (exceto o excesso de velocidade) memorizados ou em curso na VU. Se o perfil estiver vazio, é enviado um cabeçalho da matriz com noOfRecords = 0.
VuOverSpeedingControlDataRecordArray	Dados relativos ao último controlo do excesso de velocidade (valor por defeito se não existirem dados).
VuOverSpeedingEventRecordArray	Todos os incidentes de excesso de velocidade memorizados na VU. Se o perfil estiver vazio, é enviado um cabeçalho da matriz com noOfRecords = 0.
VuTimeAdjustmentRecordArray	Todos os incidentes de ajuste de tempo memorizados na VU (fora do enquadramento de uma calibração completa). Se o perfil estiver vazio, é enviado um cabeçalho da matriz com noOfRecords = 0.
VuTimeAdjustmentGNSSRecordArray	
SignatureRecordArray	Assinatura ECC de todos os dados precedentes.

▼B

2.2.6.4 Positive Response Transfer Data Detailed Speed

DDP_032 O campo de dados da mensagem «Positive Response Transfer Data Detailed Speed» fornece os seguintes dados, segundo a ordem indicada, sob o SID 76 Hex e o TREP 04 Hex e com uma divisão e uma contagem adequadas das submensagens:

Estrutura de dados da geração 1

Elemento de dados	Observação
VuDetailedSpeedData	Toda a velocidade detalhada memorizada na VU (um bloco de velocidade por minuto durante o qual o veículo esteve em movimento) 60 valores de velocidade por minuto (um por segundo).
Signature	Assinatura RSA de todos os dados a partir de noOfSpeedBlocks para baixo até ao último byte do último bloco de velocidade.

Estrutura de dados da geração 2:

Elemento de dados	Observação
VuDetailedSpeedBlockRecordArray	Toda a velocidade detalhada memorizada na VU (um bloco de velocidade por minuto durante o qual o veículo esteve em movimento) 60 valores de velocidade por minuto (um por segundo).
SignatureRecordArray	Assinatura ECC de todos os dados precedentes.

2.2.6.5 Positive Response Transfer Data Technical Data

DDP_033 O campo de dados da mensagem «Positive Response Transfer Data Technical Data» fornece os seguintes dados, segundo a ordem indicada, sob o SID 76 Hex e o TREP 05 Hex e com divisão e contagem adequadas das submensagens:

Estrutura de dados da geração 1

Elemento de dados	Observação
VuIdentification	
SensorPaired	
VuCalibrationData	Todos os registos de calibração memorizados na VU.
Signature	Assinatura RSA de todos os dados a partir de vuManufacturerName para baixo até ao último byte do último VuCalibrationRecord.

▼B

Estrutura de dados da geração 2:

Elemento de dados	Observação
VuIdentificationRecordArray	
VuSensorPairedRecordArray	Todos os emparelhamentos de EM memorizados na VU
VuSensorExternalGNSSCoupledRecordArray	Todos os acoplamentos do módulo GNSS externo memorizados na VU
VuCalibrationRecordArray	Todos os registos de calibração memorizados na VU.
VuCardRecordArray	Todos os dados de inserção do cartão memorizados na VU.
VuITSConsentRecordArray	
VuPowerSupplyInterruptionRecordArray	
SignatureRecordArray	Assinatura ECC de todos os dados precedentes.

2.3. **Memorização de ficheiros ESM**

DDP_034 Se uma sessão de descarregamento tiver incluído uma transferência de dados da VU, o IDE memoriza no espaço de um ficheiro físico único todos os dados recebidos da VU durante a sessão, dentro de mensagens Positive Response Transfer Data. Os dados memorizados não incluem cabeçalhos de mensagens, contadores de submensagens, submensagens vazias ou somas de teste, mas incluem o SID e o TREP (apenas da primeira submensagem, se houver várias).

3. PROTOCOLO APLICÁVEL AO DESCARREGAMENTO DE DADOS DE CARTÕES TACOGRÁFICOS

3.1. **Âmbito de aplicação**

A presente secção incide no descarregamento direto dos dados de um cartão tacográfico para um IDE. Como este último não faz parte do ambiente securizado, não se efetua qualquer autenticação entre o cartão e o IDE.

3.2. **Definições**

Sessão de descarregamento: Cada operação de descarregar dados do ICC. A sessão abrange o processo completo desde a reinicialização do ICC por um IFD até à desativação do ICC (retirada do cartão ou reinicialização seguinte).

Ficheiro de dados assinado: Um ficheiro do ICC. O ficheiro é transferido em texto simples para o IFD. No ICC, o ficheiro é dividido e assinado, com transferência da assinatura para o IFD.

3.3. **Descarregamento do cartão**

DDP_035 O descarregamento de um cartão tacográfico inclui as seguintes fases:

— Descarregamento da informação comum do cartão para os EF ICCe IC. Esta informação, opcional, não é securizada com assinatura digital.

▼B

— Descarregamento dos EF Card_Certificate (ou CardSignCertificate) e CA_Certificate. Esta informação não é securizada com assinatura digital.

É obrigatório descarregar estes ficheiros por cada sessão de descarregamento.

— Descarregamento dos outros EF de dados de aplicação (dentro do Tachograph DF e Tachograph_G2 DFse for o caso), com exceção do EF Card_Download. Esta informação é securizada com assinatura digital.

— É obrigatório descarregar pelo menos os EF Application_Identification e ID por cada sessão de descarregamento.

— No descarregamento de um cartão de condutor é também obrigatório descarregar os seguintes EF:

- Events_Data,
- Faults_Data,
- Driver_Activity_Data,
- Vehicles_Used,
- Places,
- GNSS_Places (se relevante),
- Control_Activity_Data,
- Specific_Conditions.

— No descarregamento de um cartão de condutor, atualizar a data de LastCardDownload no Card_Download

— No descarregamento de um cartão de oficina, reinicializar o contador de calibração no EF Card_Download

— No descarregamento de um cartão de oficina, o EF Sensor_Installation_Data não deve ser descarregado.

3.3.1 *Sequência de inicialização*

DDP_036 O IDE inicia a sequência do seguinte modo:

Cartão	Direção	IDE/IFD	Significado/Observações
	⇦	Reinicialização do *hardware*	
ATR	⇨		

É opcional utilizar PPS para passar a um número mais elevado de bauds, desde que o ICC o aceite.

3.3.2 *Sequência para ficheiros de dados não assinados*

DDP_037 A sequência de descarregamento dos EF, ICC, IC, Card_Certificate (ou CardSignCertificate) e CA_Certificate é a seguinte:

Cartão	Direção	IDE/IFD	Significado/Observações
	⇦	**Select File**	Seleção por identificadores de ficheiro
OK	⇨		

▼B

Cartão	Direção	IDE/IFD	Significado/Observações
	⇦	**READ BINARY**	Se o ficheiro contiver mais dados do que o tamanho do tampão do leitor ou do cartão, tem de se repetir o comando até todo o ficheiro ficar lido.
Dados do ficheiro OK	⇨	Memorizar dados no ESM	Segundo **3.4** Data storage format

Nota 1: Antes de selecionar o EF Card_Certificate (ou CardSignCertificate), deve selecionar-se a aplicação tacográfica (seleção por AID).

Note 2: A seleção e leitura de um ficheiro também pode ser realizada numa única fase mediante a utilização de um comando READ BINARY com um identificador EF curto.

3.3.3 *Sequência para ficheiros de dados assinados*

DDP_038 Utiliza-se a seguinte sequência para cada um dos seguintes ficheiros, que têm de ser descarregados com as respetivas assinaturas:

Cartão	Dir	IDE/IFD	Significado/Observações
	⇦	**Select File**	
OK	⇨		
	⇦	**Perform Hash of File**	Calcula o valor hash sobre o conteúdo dos dados do ficheiro selecionado, utilizando o algoritmo prescrito nos termos do apêndice 11. Este comando não é um ISO-Command.
Calcular Hash of File e memorizar valor Hash temporariamente			
OK	⇨		
	⇦	**Read Binary**	Se o ficheiro contiver mais dados do que o tampão do leitor ou o cartão aceitar, o comando tem de ser repetido até todo o ficheiro ter sido lido.
Dados do ficheiro OK	⇨	Memorizar no ESM dados recebidos	Segundo **3.4** Data storage format

▼B

Cartão	Dir	IDE/IFD	Significado/Observações
	⇦	**PSO: Compute Digital Signature**	
Executar operação de segurança «Compute Digital Signature» utilizando o valor Hash temporariamente memorizado			
Assinatura OK	⇨	Juntar os dados aos anteriormente memorizados no ESM	Segundo **3.4** Data storage format

Nota: A seleção e a leitura de um ficheiro também podem ser realizadas numa única fase, utilizando um comando READ BINARY com um identificador EF curto. Neste caso, o EF pode ser selecionado e lido antes de se aplicar o comando PERFORM HASH OF FILE.

3.3.4 *Sequência para reinicializar o contador de calibração.*

DDP_039 É a seguinte a sequência utilizada para reinicializar o contador `NoOfCalibrationsSinceDownload` no EF`Card_Download` num cartão de oficina:

Cartão	Dir	IDE/IFD	Significado/Observações
	⇦	**Select File** EF Card_Download	Seleção por identificadores de ficheiro
OK	⇨		
	⇦	**Update Binary** NoOfCalibrationsSinceDownload = '00 00'	
Reinicializa o número de descarregamento do cartão			
OK	⇨		

Nota: A seleção e a atualização de um ficheiro também podem ser realizada numa única fase, utilizando um comando UPDATE BINARY com um identificador EF curto.

3.4. **Formato de memorização dos dados**

3.4.1 *Introdução*

DDP_040 Os dados descarregados têm de ser memorizados, em conformidade com as seguintes condições:

— Os dados devem ser memorizados transparentes. Ou seja, na sua transferência a partir do cartão, é mantida a ordem dos bytes, tal como a ordem dos bits dentro de cada byte.

— Todos os ficheiros do cartão descarregados no âmbito de uma sessão de descarregamento são memorizados num ficheiro no ESM.

▼B

3.4.2 *Formato do ficheiro*

DDP_041 O formato dos ficheiros é uma concatenação de diversos objetos de TLV.

DDP_042 O marcador para um EF é o FID mais o apêndice «00».

DDP_043 O marcador de uma assinatura de EF é o FID do ficheiro mais o apêndice «01».

DDP_044 O comprimento é um valor de dois bytes. O valor define o número de bytes no campo de valor. O valor «FF FF» no campo do comprimento é reservado para utilização posterior.

DDP_045 Se um ficheiro não for descarregado, nada que com ele se relacione é memorizado (marcador ou comprimento zero).

DDP_046 Uma assinatura é memorizada como o objeto TLV imediatamente a seguir ao objeto TLV que contém os dados do ficheiro.

Definição	Significado	Comprimento
FID (2 Bytes) || «00»	Marcador para EF (FID)	3 bytes
FID (2 Bytes) || «01»	Marcador para assinatura de EF (FID)	3 bytes
xx xx	Comprimento do campo de valor	2 bytes

Exemplo dos dados num ficheiro de descarregamento para um ESM:

Marcador	Comprimento	Valor
00 02 00	00 11	Dados do EF ICC
C1 00 00	00 C2	Dados do EF Card_Certificate
		…
05 05 00	0A 2E	Dados do EFVehicles_Used
05 05 01	00 80	Assinatura do EFVehicles_Used

4. DESCARREGAMENTO DE UM CARTÃO TACOGRÁFICO VIA UMA UNIDADE-VEÍCULO.

DDP_047 A VU deve permitir descarregar para um IDE conectado o conteúdo de um cartão de condutor inserido.

DDP_048 Para iniciar este modo, o IDE envia à VU uma mensagem «Transfer Data Request Card Download» (ver 2.2.2.9).

DDP_049 A VU descarrega então todo o cartão, ficheiro a ficheiro, em conformidade com o protocolo de descarregamento do cartão, definido na secção 3, e encaminha todos os dados recebidos do cartão para o IDE dentro do formato adequado TLV do ficheiro (ver 3.4.2) e encapsulados dentro de uma mensagem «Positive Response Transfer Data».

▼B

DDP_050 O IDE recupera os dados da mensagem «Positive Response Transfer Data» (excluindo todos os cabeçalhos, SID, TREP, contadores de submensagens e somas de teste) e memoriza-os num ficheiro físico único, em conformidade com a secção 2.3.

DDP_051 Conforme o caso, a VU atualiza então o ficheiro `Control_Activity_Data` ou o ficheiro `Card_Download` do cartão de condutor.

▼B

Apêndice 8

PROTOCOLO APLICÁVEL À CALIBRAÇÃO

ÍNDICE

▼B

7. CONTROLO DOS IMPULSOS DE TESTE — UNIDADE FUNCIONAL DE CONTROLO DE ENTRADA/SAÍDA

7.1. Serviço InputOutputControlByIdentifier

7.1.1 Descrição da mensagem

7.1.2 Formato da mensagem

7.1.3 Definição de parâmetros

8. FORMATOS DOS DATARECORDS

8.1. Gamas de parâmetros transmitidos

8.2. Formatos dos dataRecords

1. INTRODUÇÃO

O presente apêndice incide no modo como os dados são intercambiados entre uma unidade-veículo (VU) e um dispositivo de teste através da linha K, que faz parte da interface de calibração referida no apêndice 6. Descreve também o controlo da linha de sinal entrada/saída no conector de calibração.

O estabelecimento das comunicações linha K é referido na secção 4 — «Serviços de comunicação».

O presente apêndice recorre à ideia de «sessões» de diagnóstico para determinar o âmbito do controlo da linha K sob variadas condições. A sessão «por defeito» é a «StandardDiagnosticSession» (sessão normal de diagnóstico), em que qualquer dado pode ser lido de uma unidade-veículo mas nenhum dado pode ser escrito para uma unidade-veículo.

A seleção da sessão de diagnóstico é referida na secção 5 — «Serviços de gestão».

O presente apêndice tem de ser considerado pertinente para ambas as gerações de VU e cartões de oficina, em conformidade com os requisitos de interoperabilidade previstos no regulamento.

CPR_001 A «ECUProgrammingSession» (sessão de programação da ECU) permite a entrada de dados na unidade-veículo. No caso da entrada de dados de calibração, a unidade-veículo deve, ademais, encontrar-se no modo de funcionamento CALIBRAÇÃO.

A transferência de dados através da linha K é descrita na secção 6 — «Serviços de transmissão de dados». Os formatos dos dados transferidos são descritos na secção 8 — «Formatos dos dataRecords».

CPR_002 A «ECUAdjustmentSession» permite selecionar o modo I/O da linha de calibração de sinal I/O através da interface linha K. O controlo da linha de calibração de sinal I/O é descrito na secção 7 — «Controlo dos impulsos de teste — unidade funcional de controlo de entrada/saída».

CPR_003 Ao longo do presente documento, o endereço do dispositivo de teste é referido como ‘tt’. Embora possa haver endereços preferenciais para dispositivos de teste, a VU responde corretamente a qualquer endereço. O endereço físico da VU é 0xEE.

▼B

2. TERMOS, DEFINIÇÕES E REFERÊNCIAS

Os protocolos, mensagens e códigos de erro baseiam-se principalmente num projeto da norma ISO 14229-1 (Road vehicles — Diagnostic systems — Part 1: Diagnostic services, version 6 of 22 February 2001).

Utiliza-se codificação de bytes e valores hexadecimais para os identificadores de serviço, os pedidos e respostas de serviço e os parâmetros-padrão.

O termo «dispositivo de teste» refere-se ao equipamento utilizado para introduzir dados de programação/calibração na VU.

Os termos «cliente» e «servidor» referem-se, respetivamente, ao dispositivo de teste e à VU.

O termo ECU significa «unidade de controlo eletrónico» (Electronic Control Unit) e refere-se à VU.

Referências:

ISO 14230-2: Road Vehicles — Diagnostic Systems — Keyword Protocol 2000 — Part 2: Data Link Layer.

First edition: 1999.

Vehicles — Diagnostic.

3. PANORÂMICA DOS SERVIÇOS

3.1. **Serviços disponíveis**

O quadro que se segue fornece uma panorâmica dos serviços disponíveis no tacógrafo e que são definidos no presente documento.

CPR_004 O quadro indica os serviços disponíveis numa sessão de diagnóstico ativada.

— A **1.ª coluna** enuncia os serviços disponíveis.

— A **2.ª coluna** indica o número da secção do presente apêndice onde o serviço é tratado com mais detalhe.

— A **3.ª coluna** indica os valores dos identificadores de serviço para mensagens de pedido.

— A **4.ª coluna** especifica os serviços da **«StandardDiagnosticSession» (SD)** que devem ser executados em cada VU.

— A **5.ª coluna** especifica os serviços da **«ECUAdjustmentSession» (ECUAS)** que devem ser executados para permitir o controlo da linha de sinal I/O no conector de calibração do painel frontal da VU.

— A **6.ª coluna** especifica os serviços da **«ECUProgrammingSession» (ECUPS)** que devem ser executados para permitir a programação de parâmetros na VU.

▼B

Quadro 1

Síntese de valores dos identificadores de serviços

			Sessões de diagnóstico		
Nome do serviço de diagnóstico	Secção n.º	SId Valor de pedido	SD	ECUAS	ECUPS
StartCommunication	4.1	81	■	■	■
StopCommunication	4.2	82	■		
TesterPresent	4.3	3E	■	■	■
StartDiagnosticSession	5.1	10	■	■	■
SecurityAccess	5.2	27	■	■	■
ReadDataByIdentifier	6.1	22	■	■	■
WriteDataByIdentifier	6.2	2E			■
InputOutputControlByIdentifier	7.1	2F		■	

■ Este símbolo indica que o serviço é obrigatório na sessão de diagnóstico.
A ausência de símbolo indica que o serviço não é permitido na sessão de diagnóstico.

3.2. **Códigos de resposta**

São definidos códigos de resposta para cada serviço.

4. SERVIÇOS DE COMUNICAÇÃO

São necessários alguns serviços para estabelecer e manter uma comunicação. Não aparecem no nível de aplicação. Os serviços disponíveis figuram no seguinte quadro:

Quadro 2

Serviços de comunicações

Nome do serviço	Descrição
StartCommunication	O cliente pede para começar uma sessão de comunicação com um ou mais servidores.
StopCommunication	O cliente pede para parar a sessão de comunicação em curso.
TesterPresent	O cliente indica ao servidor que ainda está presente.

CPR_005 O serviço StartCommunication é utilizado para desencadear uma comunicação. Para a execução de qualquer serviço, a comunicação tem de ser iniciada e os seus parâmetros têm de ser adequados ao modo pretendido.

4.1. **Serviço StartCommunication**

CPR_006 Ao receber uma primitiva de indicação StartCommunication, a VU verifica se o elo de comunicação solicitado pode ser desencadeado sob as condições vigentes. As condições aplicáveis à iniciação de um elo de comunicação constam da norma ISO 14230-2.

▼B

CPR_007 A VU executa então as ações necessárias para desencadear o elo de comunicação e envia uma primitiva de resposta StartCommunication, com os parâmetros Positive Response (resposta positiva) selecionados.

CPR_008 Se uma VU que já tiver sido inicializada (e tiver introduzido uma sessão de diagnóstico) receber um novo StartCommunication Request (devido, p. ex., a recuperação de erro no dispositivo de teste), este novo pedido de início de comunicação é aceite e a VU reinicializa-se.

CPR_009 Se, por alguma razão, o elo de comunicação não puder ser iniciado, a VU continua a funcionar tal como imediatamente antes da tentativa de iniciação da ligação.

CPR_010 A mensagem StartCommunication Request deve ser fisicamente endereçada.

CPR_011 A VU é inicializada para serviços mediante um método de «inicialização rápida»:

— Há um tempo morto antes de qualquer atividade.

— O dispositivo de teste envia então um modelo de inicialização.

— Toda a informação necessária ao estabelecimento da comunicação está contida na resposta da VU.

CPR_012 Após a conclusão da inicialização:

— Todos os parâmetros de comunicação são colocados em valores definidos no quadro 4, em conformidade com os bytes-chave.

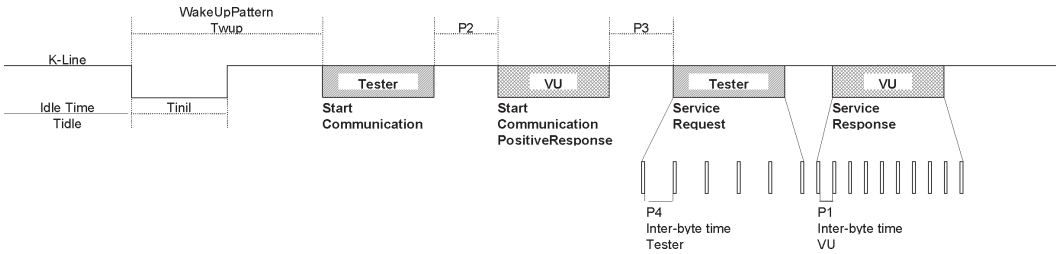
— A VU fica a aguardar o primeiro pedido do dispositivo de teste.

— A VU está no modo de diagnóstico por defeito, ou seja, StandardDiagnosticSession.

— A linha de calibração de sinal I/O está no estado por defeito, ou seja, fora de serviço, desativada.

CPR_014 A velocidade de transmissão dos dados na linha K será de 10 400 bauds.

CPR_016 A inicialização rápida é desencadeada com o dispositivo de teste a transmitir um «modelo de despertar» (Wup) sobre a linha K. O modelo começa a seguir ao tempo morto na linha K, com um tempo baixo de Tinil. O dispositivo de teste transmite o primeiro bit do serviço StartCommunication depois de um tempo de Twup a seguir ao primeiro flanco descendente.



▼B

CPR_017 Os valores cronológicos para a inicialização rápida e as comunicações, em geral, são indicados no quadro seguinte. Há diferentes possibilidades para o tempo morto:

— Primeira transmissão a seguir a comutação, Tidle = 300 ms.

— Após a conclusão de um serviço StopCommunication, Tidle = P3 min.

— Depois de parar a comunicação no tempo-limite P3 max, Tidle = 0.

Quadro 3

Valores cronológicos para inicialização rápida

Parâmetro		Valor mínimo	Valor máximo
Tinil	25 ± 1 ms	24 ms	26 ms
Twup	50 ± 1 ms	49 ms	51 ms

Quadro 4

Valores cronológicos de comunicação

Parâmetro cronológico	Descrição do parâmetro	Valores-limite inferiores [ms]	Valores-limite superiores [ms]
		Mín.	Máx.
P1	Tempo interbytes para resposta da VU	0	20
P2	Tempo entre pedido do dispositivo de teste e resposta da VU ou duas respostas da VU	25	250
P3	Tempo entre final das respostas da VU e começo do novo pedido do dispositivo de teste	55	5 000
P4	Tempo interbytes para pedido do dispositivo de teste	5	20

CPR_018 O formato da mensagem de inicialização rápida é indicado no quadro seguinte (NOTA: «hex» significa «hexadecimal»):

Quadro 5

Mensagem de pedido StartCommunication

N.º do byte	Nome do parâmetro	Valor hex	Mnemónica
#1	Byte de formato — endereçamento físico	81	FMT
#2	Byte de endereço-alvo	EE	TGT
#3	Byte de endereço-fonte	tt	SRC

▼B

N.º do byte	Nome do parâmetro	Valor hex	Mnemónica
#4	**Id do serviço de pedido StartCommunication**	**81**	**SCR**
#5	Soma de teste	00-FF	CS

Quadro 6

Mensagem StartCommunication Positive Response

N.º do byte	Nome do parâmetro	Valor hex	Mnemónica
#1	Byte de formato — endereçamento físico	80	FMT
#2	Byte de endereço-alvo	tt	TGT
#3	Byte de endereço-fonte	EE	SRC
#4	Byte adicional de comprimento	03	LEN
#5	**StartCommunication Positive Response Service Id**	**C1**	**SCRPR**
#6	Byte-chave 1	EA	KB1
#7	Byte-chave 2	8F	KB2
#8	Soma de teste	00-FF	CS

CPR_019 Não existe resposta negativa à mensagem de pedido StartCommunication. Se não houver mensagem de resposta positiva a transmitir, a VU não se inicializa, mantém-se no seu funcionamento normal e nada é transmitido.

4.2. **Serviço StopCommunication**

4.2.1 *Descrição da mensagem*

O propósito deste serviço de nível de comunicação é interromper uma sessão de comunicação.

CPR_020 Ao receber uma primitiva de indicação StopCommunication, a VU verifica se as condições vigentes permitem parar a comunicação em curso. Em caso afirmativo, a VU executa as ações necessárias para pôr termo à comunicação.

CPR_021 Se for possível pôr termo à comunicação, a VU emite uma primitiva de resposta StopCommunication, com os parâmetros Positive Response selecionados, antes de a comunicação ser interrompida.

CPR_022 Se, por alguma razão, não for possível pôr termo à comunicação, a VU emite uma primitiva de resposta StopCommunication, com os parâmetros Negative Response (resposta negativa) selecionados.

CPR_023 Se a VU detetar o tempo-limite P3max, é posto termo à comunicação, sem emissão de qualquer primitiva de resposta.

▼B

4.2.2 *Formato da mensagem*

CPR_024 Os formatos das mensagens para as primitivas StopCommunication figuram nos quadros seguintes:

Quadro 7

Mensagem de pedido StopCommunication

N.º do byte	Nome do parâmetro	Valor hex	Mnemónica
#1	Byte de formato — endereçamento físico	80	FMT
#2	Byte de endereço-alvo	EE	TGT
#3	Byte de endereço-fonte	tt	SRC
#4	Byte adicional de comprimento	01	LEN
#5	**Id do serviço de pedido StopCommunication**	**82**	**SPR**
#6	Soma de teste	00-FF	CS

Quadro 8

Mensagem StopCommunication Positive Response

N.º do byte	Nome do parâmetro	Valor hex	Mnemónica
#1	Byte de formato — endereçamento físico	80	FMT
#2	Byte de endereço-alvo	tt	TGT
#3	Byte de endereço-fonte	EE	SRC
#4	Byte adicional de comprimento	01	LEN
#5	**StopCommunication Positive Response Service Id**	**C2**	**SPRPR**
#6	Soma de teste	00-FF	CS

Quadro 9

Mensagem StopCommunication Negative Response

N.º do byte	Nome do parâmetro	Valor hex	Mnemónica
#1	Byte de formato — endereçamento físico	80	FMT
#2	Byte de endereço-alvo	tt	TGT
#3	Byte de endereço-fonte	EE	SRC
#4	Byte adicional de comprimento	03	LEN

▼B

N.º do byte	Nome do parâmetro	Valor hex	Mnemónica
#5	**negative Response Service Id**	**7F**	**NR**
#6	Identificação do serviço de pedido StopCommunication	82	SPR
#7	responseCode = generalReject	10	RC_GR
#8	Soma de teste	00-FF	CS

4.2.3 *Definição de parâmetros*

Este serviço não requer definição de parâmetros.

4.3. **Serviço TesterPresent**

4.3.1 *Descrição da mensagem*

O serviço TesterPresent é utilizado pelo dispositivo de teste para indicar ao servidor que está ainda presente, a fim de evitar que o servidor regresse automaticamente ao funcionamento normal e possa interromper a comunicação. Este serviço, enviado periodicamente, mantém ativa a sessão de diagnóstico/comunicação recolocando no seu estado de defeito o cronómetro P3 cada vez que é recebido um pedido relativo ao serviço.

4.3.2 *Formato da mensagem*

CPR_079 Os formatos das mensagens para as primitivas TesterPresent figuram nos quadros seguintes:

Quadro 10

Mensagem de pedido TesterPresent

N.º do byte	Nome do parâmetro	Valor hex	Mnemónica
#1	Byte de formato — endereçamento físico	80	FMT
#2	Byte de endereço-alvo	EE	TGT
#3	Byte de endereço-fonte	tt	SRC
#4	Byte adicional de comprimento	02	LEN
#5	**Id do serviço de pedido TesterPresent**	**3E**	**TP**
#6	Sub Função = responseRequired = [sim	01	RESPREQ_Y
	não]	02	RESPREQ_NO
#7	Soma de teste	00-FF	CS

CPR_080 Se o parâmetro responseRequired tomar o valor «sim», o servidor responde com a mensagem de resposta positiva que a seguir se apresenta. Se o parâmetro responseRequired tomar o valor «não», o servidor não envia qualquer resposta.

▼B

Quadro 11

Mensagem TesterPresent Positive Response

N.º do byte	Nome do parâmetro	Valor hex	Mnemónica
#1	Byte de formato — endereçamento físico	80	FMT
#2	Byte de endereço-alvo	tt	TGT
#3	Byte de endereço-fonte	EE	SRC
#4	Byte adicional de comprimento	01	LEN
#5	**TesterPresent Positive Response Service Id**	**7E**	**TPPR**
#6	Soma de teste	00-FF	CS

CPR_081 O serviço deve aceitar os seguintes códigos de resposta negativa:

Quadro 12

Mensagem TesterPresent Negative Response

N.º do byte	Nome do parâmetro		Valor hex	Mnemónica
#1	Byte de formato — endereçamento físico		80	FMT
#2	Byte de endereço-alvo		tt	TGT
#3	Byte de endereço-fonte		EE	SRC
#4	Byte adicional de comprimento		03	LEN
#5	**negative Response Service Id**		**7F**	**NR**
#6	Identificação do serviço de pedido TesterPresent		3E	TP
#7	responseCode =	[SubFunctionNotSupported-InvalidFormat	12	RC_SFNS_IF
		incorrectMessageLength]	13	RC_IML
#8	Soma de teste		00-FF	CS

▼B

5. SERVIÇOS DE GESTÃO

Os serviços disponíveis figuram no seguinte quadro:

Quadro 13

Serviços de gestão

Nome do serviço	Descrição
StartDiagnosticSession	O cliente pede para começar uma sessão de diagnóstico com uma VU.
SecurityAccess	O cliente pede acesso a funções restritas a utilizadores autorizados.

5.1. **Serviço StartDiagnosticSession**

5.1.1 *Descrição da mensagem*

CPR_025 O serviço StartDiagnosticSession é utilizado para ativar diversas sessões de diagnóstico no servidor. Uma sessão de diagnóstico ativa um conjunto específico de serviços, em conformidade com o quadro 17. Uma sessão pode ativar serviços não contemplados no presente documento e que são específicos do fabricante de veículos. As regras de execução devem cumprir os seguintes requisitos:

— Haverá sempre exatamente uma sessão de diagnóstico ativa na VU.

— Uma vez ligada, a VU iniciará sempre a StandardDiagnosticSession. Se não se iniciar outra sessão de diagnóstico, a StandardDiagnosticSession prosseguirá enquanto a VU estiver ligada.

— Se uma sessão de diagnóstico em curso tiver sido pedida pelo dispositivo de teste, a VU enviará uma mensagem de resposta positiva.

— Sempre que o dispositivo de teste pedir uma nova sessão de diagnóstico, a VU enviará uma mensagem de resposta positiva StartDiagnosticSession antes de a nova sessão ser ativada nela. Se não puder iniciar a nova sessão de diagnóstico pedida, a VU enviará uma resposta negativa StartDiagnosticSession e a sessão em curso prosseguirá.

CPR_026 Uma sessão de diagnóstico só se inicia se tiver sido estabelecida comunicação entre o cliente e a VU.

CPR_027 Os parâmetros cronológicos definidos no quadro 4 devem ficar ativos após um começo StartDiagnosticSession bem sucedido, com o parâmetro diagnosticSession levado ao valor «StandardDiagnosticSession» na mensagem de pedido, se outra sessão de diagnóstico tiver estado previamente ativa.

5.1.2 *Formato da mensagem*

CPR_028 Os formatos das mensagens para as primitivas StartDiagnosticSession figuram nos quadros seguintes:

▼B

Quadro 14

Mensagem de pedido StartDiagnosticSession

N.º do byte	Nome do parâmetro	Valor hex	Mnemónica
#1	Byte de formato — endereçamento físico	80	FMT
#2	Byte de endereço-alvo	EE	TGT
#3	Byte de endereço-fonte	tt	SRC
#4	Byte adicional de comprimento	02	LEN
#5	**Id do serviço de pedido StartDiagnosticSession**	**10**	**STDS**
#6	diagnosticSession = [um valor de quadro 17]	XX	DS_…
#7	Soma de teste	00-FF	CS

Quadro 15

Mensagem StartDiagnosticSession Positive Response

N.º do byte	Nome do parâmetro	Valor hex	Mnemónica
#1	Byte de formato — endereçamento físico	80	FMT
#2	Byte de endereço-alvo	tt	TGT
#3	Byte de endereço-fonte	EE	SRC
#4	Byte adicional de comprimento	02	LEN
#5	**StartDiagnosticSession Positive Response Service Id**	**50**	**STDSPR**
#6	diagnosticSession = [mesmo valor que o byte #6 quadro 14]	XX	DS_…
#7	Soma de teste	00-FF	CS

Quadro 16

Mensagem StartDiagnosticSession Negative Response

N.º do byte	Nome do parâmetro	Valor hex	Mnemónica
#1	Byte de formato — endereçamento físico	80	FMT
#2	Byte de endereço-alvo	tt	TGT
#3	Byte de endereço-fonte	EE	SRC

▼B

N.º do byte	Nome do parâmetro		Valor hex	Mnemónica
#4	Byte adicional de comprimento		03	LEN
#5	**Negative Response Service Id**		**7F**	**NR**
#6	Id do serviço de pedido StartDiagnosticSession		10	STDS
#7	Response-Code =	[subFunctionNotSupported ([a])	12	RC_SFNS
		incorrectMessageLength ([b])	13	RC_IML
		conditionsNotCorrect ([c])	22	RC_CNC
#8	Soma de teste		00-FF	CS

([a]) — O valor inserido no byte #6 da mensagem de pedido não é aceite (não consta do quadro 17).
([b]) —Erro no comprimento da mensagem.
([c]) — Não cumpridos os critérios no pedido StartDiagnosticSession.

5.1.3 *Definição de parâmetros*

CPR_029 O parâmetro ***diagnosticSession (DS_)*** é utilizado pelo serviço StartDiagnosticSession para selecionar o comportamento específico do(s) servidor(es). No presente documento especificam-se as seguintes sessões de diagnóstico:

Quadro 17

Definição de valores diagnosticSession

Hex	Descrição	Mnemónica
81	**StandardDiagnosticSession** Esta sessão de diagnóstico possibilita todos os serviços especificados no **quadro 1, coluna 4, «SD»**. Estes serviços permitem a leitura de dados de um servidor (VU). Esta sessão de diagnóstico fica ativa uma vez concluída com êxito a inicialização entre o cliente (dispositivo de teste) e o servidor (VU). Esta sessão de diagnóstico pode ser sobreposta por outras sessões de diagnóstico especificadas na presente secção.	**SD**
85	**ECUProgrammingSession** Esta sessão de diagnóstico possibilita todos os serviços especificados no **quadro 1, coluna 6, «ECUPS»**. Estes serviços são compatíveis com a programação da memória de um servidor (VU). Esta sessão de diagnóstico pode ser sobreposta por outras sessões de diagnóstico especificadas na presente secção.	**ECUPS**

▼B

Hex	Descrição	Mnemónica
87	**ECUAdjustmentSession** Esta sessão de diagnóstico possibilita todos os serviços especificados no **quadro 1, coluna 5, «ECUAS».** Estes serviços são compatíveis com o controlo da entrada/saída de um servidor (VU). Esta sessão de diagnóstico pode ser sobreposta por outras sessões de diagnóstico especificadas **na presente** secção.	**ECUAS**

5.2. **Serviço SecurityAccess**

Se a VU não estiver em modo CALIBRAÇÃO, não é possível escrever dados de calibração. Para se garantir o acesso ao modo CALIBRAÇÃO, é necessário introduzir na VU o PIN devido, além de um cartão válido de oficina.

Se a VU estiver em modo CALIBRAÇÃO ou CONTROLO, o acesso à linha de calibração de entrada/saída é também possível.

O serviço SecurityAccess fornece um meio para introduzir o PIN e indicar ao dispositivo de teste se a VU está ou não em modo CALIBRAÇÃO.

São aceitáveis métodos alternativos para introduzir o PIN.

5.2.1 *Descrição da mensagem*

O serviço SecurityAccess consiste numa mensagem SecurityAccess «requestSeed», seguida de uma mensagem SecurityAccess «sendKey». O serviço SecurityAccess deve ser executado depois do serviço StartDiagnosticSession.

CPR_033 O dispositivo de teste utiliza a mensagem SecurityAccess «requestSeed» para verificar se a unidade-veículo está pronta a aceitar um PIN.

CPR_034 Se já estiver em modo CALIBRAÇÃO, a VU responde ao pedido enviando um «seed» de 0x0000 por meio do serviço SecurityAccess Positive Response.

CPR_035 Se estiver pronta a aceitar um PIN para verificação por um cartão de oficina, a VU responde ao pedido enviando um «seed» maior do que 0x0000 por meio do serviço SecurityAccess Positive Response.

CPR_036 Se não estiver pronta para aceitar um PIN do dispositivo de teste (quer porque o cartão de oficina inserido não é válido, quer porque não foi inserido nenhum cartão de oficina, quer ainda porque espera o PIN por outro método), a VU responde ao pedido por uma Negative Response, com um código de resposta expresso por conditionsNotCorrectOrRequestSequenceError.

CPR_037 O dispositivo de teste recorre então à mensagem SecurityAccess «sendKey» para encaminhar o PIN para a unidade-veículo. A fim de permitir que se efetue o processo de autenticação do cartão, a VU utiliza o código de resposta negativa requestCorrectlyReceived-ResponsePending para ampliar o tempo destinado à resposta. No entanto, o tempo

▼B

máximo de resposta não deve exceder 5 minutos. Logo que o serviço pedido esteja concluído, a VU envia uma mensagem de resposta positiva ou uma mensagem de resposta negativa com um código de resposta diferente deste. O código de resposta negativa requestCorrectlyReceived-ResponsePending pode ser repetido pela VU até o serviço pedido estar concluído e a mensagem de resposta final ser enviada.

CPR_038 A VU responde a este pedido utilizando o serviço SecurityAccess Positive Response somente quando em modo CALIBRAÇÃO.

CPR_039 Nos casos que se seguem, a VU responde a este pedido por uma Negative Response, com os seguintes códigos de resposta:

— subFunctionNot supported: formato não válido para o parâmetro da subfunção (accessType)

— conditionsNotCorrectOrRequestSequenceError: unidade-veículo não preparada para aceitar entrada de PIN

— invalidKey: PIN não válido e número de tentativas de verificação do PIN não excedido

— exceededNumberOfAttempts: PIN não válido e número de tentativas de verificação do PIN excedido

— generalReject: PIN correto mas falhou autenticação mútua com o cartão de oficina.

5.2.2 *Formato da mensagem — SecurityAccess — requestSeed*

CPR_040 Os formatos das mensagens para as primitivas SecurityAccess «requestSeed» figuram nos quadros seguintes:

Quadro 18

Mensagem SecurityAccessRequest-requestSeed)

N.º do byte	Nome do parâmetro	Valor hex	Mnemónica
#1	Byte de formato — endereçamento físico	80	FMT
#2	Byte de endereço-alvo	EE	TGT
#3	Byte de endereço-fonte	tt	SRC
#4	Byte adicional de comprimento	02	LEN
#5	**Id do serviço de pedido SecurityAccess**	**27**	**SA**
#6	accessType — requestSeed	7D	AT_RSD
#7	Soma de teste	00-FF	CS

▼B

Quadro 19

SecurityAccess — requestSeed Positive Response

N.º do byte	Nome do parâmetro	Valor hex	Mnemónica
#1	Byte de formato — endereçamento físico	80	FMT
#2	Byte de endereço-alvo	tt	TGT
#3	Byte de endereço-fonte	EE	SRC
#4	Byte adicional de comprimento	04	LEN
#5	**SecurityAccess Positive Response Service Id**	**67**	**SAPR**
#6	accessType — requestSeed	7D	AT_RSD
#7	Seed elevada	00-FF	SEEDH
#8	Seed baixa	00-FF	SEEDL
#9	Soma de teste	00-FF	CS

Quadro 20

Mensagem SecurityAccess Negative Response

N.º do byte	Nome do parâmetro	Valor hex	Mnemónica
#1	Byte de formato — endereçamento físico	80	FMT
#2	Byte de endereço-alvo	tt	TGT
#3	Byte de endereço-fonte	EE	SRC
#4	Byte adicional de comprimento	03	LEN
#5	**negativeResponse Service Id**	**7F**	**NR**
#6	Id do serviço de pedido SecurityAccess	27	SA
#7	responseCode = [conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
	incorrectMessageLength]	13	RC_IML
#8	Soma de teste	00-FF	CS

▼B

5.2.3 *Formato da mensagem — SecurityAccess — sendKey*

CPR_041 Os formatos das mensagens para as primitivas SecurityAccess «sendKey» figuram nos quadros seguintes:

Quadro 21

Mensagem SecurityAccess Request-sendKey)

N.º do byte	Nome do parâmetro	Valor hex	Mnemónica
#1	Byte de formato — endereçamento físico	80	FMT
#2	Byte de endereço-alvo	EE	TGT
#3	Byte de endereço-fonte	tt	SRC
#4	Byte adicional de comprimento	m+2	LEN
#5	**Id do serviço de pedido SecurityAccess**	**27**	**SA**
#6	accessType — sendKey	7E	AT_SK
#7 to #m+6	Key #1 (elevado) … Chave #m (baixa: m deve ser no mínimo 4 e no máximo 8)	XX … XX	KEY
#m+7	Soma de teste	00-FF	CS

Quadro 22

Mensagem SecurityAccess-sendKey Positive Response

N.º do byte	Nome do parâmetro	Valor hex	Mnemónica
#1	Byte de formato — endereçamento físico	80	FMT
#2	Byte de endereço-alvo	tt	TGT
#3	Byte de endereço-fonte	EE	SRC
#4	Byte adicional de comprimento	02	LEN
#5	**SecurityAccess Positive Response Service Id**	**67**	**SAPR**
#6	accessType — sendKey	7E	AT_SK
#7	Soma de teste	00-FF	CS

▼B

Quadro 23

Mensagem SecurityAccess Negative Response

N.º do byte	Nome do parâmetro		Valor hex	Mnemónica
#1	Byte de formato — endereçamento físico		80	FMT
#2	Byte de endereço-alvo		tt	TGT
#3	Byte de endereço-fonte		EE	SRC
#4	Byte adicional de comprimento		03	LEN
#5	**NegativeResponse Service Id**		**7F**	**NR**
#6	Id do serviço de pedido SecurityAccess		27	SA
#7	ResponseCode =	[generalReject	10	RC_GR
		subFunctionNotSupported	12	RC_SFNS
		incorrectMessageLength	13	RC_IML
		conditionsNotCorrectOrRequestSequenceError	22	RC_CNC
		invalidKey	35	RC_IK
		exceededNumberOfAttempts	36	RC_ENA
		requestCorrectlyReceived-ResponsePending]	78	RC_RCR_RP
#8	Soma de teste		00-FF	CS

6. SERVIÇOS DE TRANSMISSÃO DE DADOS

Os serviços disponíveis figuram no seguinte quadro:

Quadro 24

Serviços de transmissão de dados

Nome do serviço	Descrição
ReadDataByIdentifier	O cliente pede a transmissão do valor atual de um registo com acesso por recordDataIdentifier.
WriteDataByIdentifier	O cliente pede para escrever um registo com acesso por recordDataIdentifier.

▼B

6.1. **Serviço ReadDataByIdentifier**

6.1.1 *Descrição da mensagem*

CPR_050 O serviço ReadDataByIdentifier é utilizado pelo cliente para pedir valores de registo de dados a um servidor. Os dados são identificados por um recordDataIdentifier. Compete ao fabricante da VU assegurar o respeito das condições do servidor quando da execução deste serviço.

6.1.2 *Formato da mensagem*

CPR_051 Os formatos das mensagens para as primitivas ReadDaTaByIdentifier figuram nos quadros seguintes:

Quadro 25

Mensagem de pedido ReadDataByIdentifier

N.º do byte	Nome do parâmetro	Valor hex	Mnemónica
#1	Byte de formato — endereçamento físico	80	FMT
#2	Byte de endereço-alvo	EE	TGT
#3	Byte de endereço-fonte	tt	SRC
#4	Byte adicional de comprimento	03	LEN
#5	**Id do serviço de pedido ReadDataByIdentifier**	**22**	**RDBI**
#6 a #7	recordDataIdentifier = [um valor do quadro 28]	xxxx	RDI_…
#8	Soma de teste	00-FF	CS

Quadro 26

Mensagem ReadDataByIdentifier Positive Response

N.º do byte	Nome do parâmetro	Valor hex	Mnemónica
#1	Byte de formato — endereçamento físico	80	FMT
#2	Byte de endereço-alvo	tt	TGT
#3	Byte de endereço-fonte	EE	SRC
#4	Byte adicional de comprimento	m+3	LEN
#5	**ReadDataByIdentifier Positive Response Service Id**	**62**	**RDBIPR**
#6 e #7	recordDataIdentifier = [o mesmo valor que bytes #6 e #7, quadro 25]	xxxx	RDI_…

▼B

N.º do byte	Nome do parâmetro		Valor hex	Mnemónica
#8 a #m+7	dataRecord[] =	[data#1	XX	DREC_DATA1
		:	:	:
		data#m]	XX	DREC_DATAm
#m+8	Soma de teste		00-FF	CS

Quadro 27

Mensagem ReadDataByIdentifier Negative Response

N.º do byte	Nome do parâmetro		Valor hex	Mnemónica
#1	Byte de formato — endereçamento físico		80	FMT
#2	Byte de endereço-alvo		tt	TGT
#3	Byte de endereço-fonte		EE	SRC
#4	Byte adicional de comprimento		03	LEN
#5	**NegativeResponse Service Id**		**7F**	**NR**
#6	Id do serviço de pedido ReadDataByIdentifier		22	RDBI
#7	ResponseCode=	[requestOutOfRange	31	RC_ROOR
		incorrectMessageLength	13	RC_IML
		conditionsNotCorrect]	22	RC_CNC
#8	Soma de teste		00-FF	CS

6.1.3 *Definição de parâmetros*

CPR_052 O parâmetro ***recordDataIdentifier (RDI_)***, na mensagem de pedido readDataByIdentifier, identifica um registo de dados.

CPR_053 Os valores recordDataIdentifier definidos pelo presente documento figuram no quadro infra.

O quadro recordDataIdentifier consiste em quatro colunas e múltiplas linhas:

— A **1.ª coluna (Hex)** inclui o «valor hex» atribuído ao recordDataIdentifier especificado na 3.ª coluna.

— **A 2.ª coluna (Elemento de dados)** especifica o elemento do apêndice 1 no qual se baseia o recordDataIdentifier (é por vezes necessária transcodificação).

▼B

— A **3.ª coluna (Descrição)** especifica o nome do recordDataIdentifier correspondente.

— A **4.ª coluna (Mnemónica)** especifica a mnemónica deste recordDataIdentifier.

Quadro 28

Valores de definição do recordDataIdentifier

Hex	Elemento de dados	Nome do recordDataIdentifier (ver formato na secção 8.2)	Mnemónica
F90B	CurrentDateTime	TimeDate	RDI_TD
F912	HighResOdometer	HighResolutionTotalVehicleDistance	RDI_HRTVD
F918	K-ConstantOfRecordingEquipment	Kfactor	RDI_KF
F91C	L-TyreCircumference	LfactorTyreCircumference	RDI_LF
F91D	W-VehicleCharacteristicConstant	WvehicleCharacteristicFactor	RDI_WVCF
F921	TyreSize	TyreSize	RDI_TS
F922	nextCalibrationDate	NextCalibrationDate	RDI_NCD
F92C	SpeedAuthorised	SpeedAuthorised	RDI_SA
F97D	vehicleRegistrationNation	RegisteringMemberState	RDI_RMS
F97E	VehicleRegistrationNumber	VehicleRegistrationNumber	RDI_ VRN
F190	VehicleIdentificationNumber	VIN	RDI_ VIN

CPR_054 O parâmetro ***dataRecord (DREC_)*** é utilizado pela mensagem de resposta positiva readDataByIdentifier para fornecer ao cliente (dispositivo de teste) o valor de registo de dado identificado pelo recordDataIdentifier. Os formatos dos dados são especificados na secção 8. Outros dataRecords opcionais do utilizador, incluindo dados de entrada, internos e de saída específicos da VU, podem ser adicionalmente aplicados, mas não são definidos no presente documento.

6.2. **Serviço WriteDataByIdentifier**

6.2.1 *Descrição da mensagem*

CPR_056 O serviço WriteDataByIdentifier é utilizado pelo cliente para escrever valores de registo de dados num servidor. Os dados são identificados por um recordDataIdentifier. Compete ao fabricante da VU assegurar o respeito das condições do servidor quando da execução deste serviço. Para atualizar os parâmetros constantes do quadro 28, a VU deve estar em modo CALIBRAÇÃO.

6.2.2 *Formato da mensagem*

CPR_057 Os formatos das mensagens para as primitivas WriteDataByIdentifier figuram nos quadros seguintes:

▼B

Quadro 29

Mensagem de pedido WriteDataByIdentifier Request

N.º do byte	Nome do parâmetro	Valor hex	Mnemónica
#1	Byte de formato — endereçamento físico	80	FMT
#2	Byte de endereço-alvo	EE	TGT
#3	Byte de endereço-fonte	tt	SRC
#4	Byte adicional de comprimento	m+3	LEN
#5	**Id do serviço de pedido WriteDataByIdentifier**	**2E**	**WDBI**
#6 a #7	recordDataIdentifier = [um valor do quadro 28]	xxxx	RDI_…
#8 a m+7	dataRecord[] = [data#1 : data#m]	XX : XX	DREC_DATA1 : DREC_DATAm
#m+8	Soma de teste	00-FF	CS

Quadro 30

Mensagem WriteDataByIdentifier Positive Response

N.º do byte	Nome do parâmetro	Valor hex	Mnemónica
#1	Byte de formato — endereçamento físico	80	FMT
#2	Byte de endereço-alvo	tt	TGT
#3	Byte de endereço-fonte	EE	SRC
#4	Byte adicional de comprimento	03	LEN
#5	**WriteDataByIdentifier Positive Response Service Id**	**6E**	**WDBIPR**
#6 a #7	recordDataIdentifier = [o mesmo valor que bytes #6 e #7, quadro 29]	xxxx	RDI_…
#8	Soma de teste	00-FF	CS

▼B

Quadro 31

Mensagem WriteDataByIdentifier Negative Response

N.º do byte	Nome do parâmetro		Valor hex	Mnemónica
#1	Byte de formato — endereçamento físico		80	FMT
#2	Byte de endereço-alvo		tt	TGT
#3	Byte de endereço-fonte		EE	SRC
#4	Byte adicional de comprimento		03	LEN
#5	**NegativeResponse Service Id**		**7F**	**NR**
#6	Id do serviço de pedido WriteDataByIdentifier		2E	WDBI
#7	ResponseCode=	[requestOutOfRange	31	RC_ROOR
		incorrectMessageLength	13	RC_IML
		conditionsNotCorrect]	22	RC_CNC
#8	Soma de teste		00-FF	CS

6.2.3 *Definição de parâmetros*

O parâmetro ***recordDataIdentifier (RDI_)*** é definido no quadro 28.

O parâmetro ***dataRecord (DREC_)*** é utilizado pela mensagem WriteDataByIdentifier para fornecer ao servidor (VU) os valores de registo de dados identificados pelo recordDataIdentifier. Os formatos dos dados são especificados na secção 8.

7. CONTROLO DOS IMPULSOS DE TESTE — UNIDADE FUNCIONAL DE CONTROLO DE ENTRADA/SAÍDA

Os serviços disponíveis figuram no seguinte quadro:

Quadro 32

Unidade funcional de controlo de entrada/saída

Nome do serviço	Descrição
InputOutputControlByIdentifier	O cliente pede o controlo de uma entrada/saída específica do servidor.

7.1. **Serviço InputOutputControlByIdentifier**

7.1.1 *Descrição da mensagem*

Através do conector frontal, há uma ligação que permite controlar ou acompanhar os impulsos de teste por meio de um dispositivo de teste adequado.

▼B

CPR_058 Esta linha de calibração de sinal I/O pode ser configurada pelo comando da linha K por intermédio do serviço InputOutputControlByIdentifier, a fim de selecionar a função de entrada ou de saída pretendida para a linha. Estados que a linha pode apresentar:

— desativado,

— speedSignalInput, em que a linha de calibração de sinal I/O é utilizada para dar entrada a um sinal de velocidade (sinal de teste) em substituição do sinal de velocidade do sensor de movimentos (função não disponível em modo CONTROLO),

— realTimeSpeedSignalOutputSensor, em que a linha de calibração de sinal I/O é utilizada para dar saída ao sinal de velocidade do sensor de movimentos,

— RTCOutput, em que a linha de calibração de sinal I/O é utilizada para dar saída ao sinal do relógio UTC (função não disponível em modo CONTROLO).

CPR_059 Para configurar o estado da linha, a unidade-veículo deve ter dado entrada a uma sessão de ajustamento e estar em modo CALIBRAÇÃO ou CONTROLO. Se a VU estiver em modo CALIBRAÇÃO, podem ser selecionados os quatro estados da linha (desativado, speedSignalInput, realTimeSpeedSignalOutputSensor e RTCOutput). Se a VU estiver em modo CONTROLO, só podem ser selecionados dois estados da linha (desativado e realTimeSpeedOutputSensor). Saindo da sessão de ajustamento ou do modo CALIBRAÇÃO ou CONTROLO, a VU deve assegurar que a linha de sinal I/O regressa ao estado «desativado» (por defeito).

CPR_060 Se forem recebidos impulsos de velocidade na linha de entrada do sinal de velocidade em tempo real da VU enquanto a linha de calibração de sinal I/O estiver apontada para entrada, então a linha de sinal I/O deve ser apontada para saída ou recolocada em estado desativado.

CPR_061 A sequência será:

— estabelecer comunicações pelo serviço StartCommunication

— introduzir uma sessão de ajustamento pelo serviço StartDiagnosticSession e ficar em modo de funcionamento CALIBRAÇÃO ou CONTROLO (a ordem destas duas operações é arbitrária)

— mudar o estado da saída pelo serviço InputOutputControlByIdentifier.

7.1.2 *Formato da mensagem*

CPR_062 Os formatos das mensagens para as primitivas InputOutputControlByIdentifier figuram nos quadros seguintes:

▼B

Quadro 33

Mensagem de pedido InputOutputControlByIdentifier

N.º do byte	Nome do parâmetro	Valor hex	Mnemónica
#1	Byte de formato — endereçamento físico	80	FMT
#2	Byte de endereço-alvo	EE	TGT
#3	Byte de endereço-fonte	tt	SRC
#4	Byte adicional de comprimento	XX	LEN
#5	**InputOutputControlByIdentifier Request Sid**	**2F**	**IOCBI**
#6 e #7	InputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 ou #8 a #9	ControlOptionRecord = [		COR_…
	inputOutputControlParameter — um valor do quadro 36	XX	IOCP_…
	controlState — um valor do quadro 37 (ver nota infra)]	XX	CS_…
#9 ou #10	Soma de teste	00-FF	CS

Nota: O parâmetro controlState está presente somente em alguns casos (ver 7.1.3).

Quadro 34

Mensagem InputOutputControlByIdentifier Positive Response

N.º do byte	Nome do parâmetro	Valor hex	Mnemónica
#1	Byte de formato — endereçamento físico	80	FMT
#2	Byte de endereço-alvo	tt	TGT
#3	Byte de endereço-fonte	EE	SRC
#4	Byte adicional de comprimento	XX	LEN
#5	**inputOutputControlByIdentifier Positive Response SId**	**6F**	**IOCBIPR**
#6 e #7	inputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 ou #8 a #9	controlStatusRecord = [		CSR_
	inputOutputControlParameter (mesmo valor que byte #8, quadro 33)	XX	IOCP_…
	controlState (mesmo valor que byte #9, quadro 33)] (se for o caso)	XX	CS_…
#9 ou #10	Soma de teste	00-FF	CS

▼B

Quadro 35

Mensagem InputOutputControlByIdentifier Negative Response

N.º do byte	Nome do parâmetro	Valor hex	Mnemónica
#1	Byte de formato — endereçamento físico	80	FMT
#2	Byte de endereço-alvo	tt	TGT
#3	Byte de endereço-fonte	EE	SRC
#4	Byte adicional de comprimento	03	LEN
#5	**negativeResponse Service Id**	**7F**	**NR**
#6	inputOutputControlByIdentifier Request SId	2F	IOCBI
#7	responseCode=[		
	incorrectMessageLength	13	RC_IML
	conditionsNotCorrect	22	RC_CNC
	requestOutOfRange	31	RC_ROOR
	deviceControlLimitsExceeded]	7A	RC_DCLE
#8	Soma de teste	00-FF	CS

7.1.3 *Definição de parâmetros*

CPR_064 O parâmetro ***inputOutputControlParameter (IOCP_)*** é definido no quadro seguinte:

Quadro 36

Definição de valores inputOutputControlParameter

Hex	Descrição	Mnemónica
00	**ReturnControlToECU** Este valor indica ao servidor (VU) que o dispositivo de teste deixou de ter controlo sobre a linha de calibração de sinal I/O.	RCTECU
01	**ResetToDefault** Este valor indica ao servidor (VU) que lhe é pedido recolocar no seu estado por defeito a linha de calibração de sinal I/O.	RTD

▼B

Hex	Descrição	Mnemónica
03	**ShortTermAdjustment** Este valor indica ao servidor (VU) que lhe é pedido ajustar ao valor incluído no parâmetro controlState a linha de calibração de sinal I/O.	STA

CPR_065 O parâmetro ***controlState***, definido no quadro seguinte, está presente somente quando o inputOutputControlParameter é colocado em ShortTermAdjustment:

Quadro 37

Definição de valores de controlState

Modo	Valor hex	Descrição
Desativar	00	Linha I/O desativada (estado por defeito)
Ativar	01	Ativar a linha I/O como speedSignalInput
Ativar	02	Ativar a linha I/O como realTimeSpeedSignalOutputSensor
Ativar	03	Ativar a linha I/O como RTCOutput

8. FORMATOS DOS DATARECORDS

A presente secção incide em:

— regras gerais a aplicar às gamas dos parâmetros transmitidos pela unidade-veículo ao dispositivo de teste

— formatos a utilizar na transferência de dados através dos serviços de transmissão de dados, descritos na secção 6.

CPR_067 Todos os parâmetros identificados devem ser aceites pela VU.

CPR_068 Os dados transmitidos pela VU ao dispositivo de teste em resposta a uma mensagem de pedido devem ser do tipo medido (ou seja, valor atual do parâmetro pedido, tal como o mede ou observa a VU).

8.1. **Gamas de parâmetros transmitidos**

CPR_069 O quadro 38 define as gamas utilizadas para determinar a validade de um parâmetro transmitido.

CPR_070 Os valores da gama «error indicator» (indicador de erro) servem para a unidade-veículo indicar imediatamente que não estão de momento disponíveis dados paramétricos válidos, devido a erro de algum tipo no tacógrafo.

CPR_071 Os valores da gama «not available» (indisponível) servem para a unidade-veículo transmitir uma mensagem contendo um parâmetro não disponível ou não aceite no módulo em questão. Os valores da gama «not requested» (não pedido) servem para um dispositivo transmitir uma mensagem de comando e identificar esses parâmetros quando não for esperada resposta do dispositivo recetor.

▼B

CPR_072 Se a falha de um componente impedir a transmissão de dados válidos relativos a um parâmetro, deve utilizar-se o indicador de erro descrito no quadro 38 em vez dos dados relativos a esse parâmetro. No entanto, se o dado medido ou calculado tiver produzido um valor válido mas excedendo a gama definida para o parâmetro, não se deve utilizar o indicador de erro. Os dados serão transmitidos utilizando o valor adequado, mínimo ou máximo, do parâmetro.

Quadro 38

Gamas de dataRecords

Nome da gama	1 byte (valor hex)	2 bytes (valor hex)	4 bytes (valor hex)	ASCII
Sinal válido	00 a FA	0000 a FAFF	00000000 a FAFFFFFF	1 a 254
Indicador específico do parâmetro	FB	FB00 a FBFF	FB000000 a FBFFFFFF	nenhum
Gama reservada para futuros bits de indicador	FC a FD	FC00 a FDFF	FC000000 a FDFFFFFF	nenhum
Indicador de erro	FE	FE00 a FEFF	FE000000 a FEFFFFFF	0
Indisponível ou não pedido	FF	FF00 a FFFF	FF000000 a FFFFFFFF	FF

CPR_073 No caso dos parâmetros codificados em ASCII, o caráter «*» é reservado como delimitador.

8.2. **Formatos dos dataRecords**

Do quadro 39 ao quadro 42, referem-se os formatos a utilizar pelos serviços ReadDataByIdentifier e WriteDataByIdentifier.

CPR_074 O quadro 39 indica o comprimento, a resolução e a gama de funcionamento de cada parâmetro identificado pelo seu recordDataIdentifier:

Quadro 39

Formatos dos dataRecords

Nome do parâmetro	Comprimento dos dados (bytes)	Resolução	Gama de funcionamento
TimeDate	8	Ver informações no quadro 40	
HighResolutionTotalVehicleDistance	4	ganho de 5 m/bit, deslocamento de 0 m	0 a +21 055 406 km
Kfactor	2	ganho de 0,001 imp./m/bit, deslocamento de 0	0 a 64,255 imp./m
LfactorTyreCircumference	2	ganho de $0{,}125 \times 10^{-3}$ m/bit, deslocamento de 0	0 a 8,031
WvehicleCharacteristicFactor	2	ganho de 0,001 imp./m/bit, deslocamento de 0	0 a 64,255 imp./m
TyreSize	15	ASCII	ASCII
NextCalibrationDate	3	Ver informações no quadro 41	
SpeedAuthorised	2	ganho de 1/256 km/h/bit, deslocamento de 0	0 a 250 996 km/h

▼B

Nome do parâmetro	Comprimento dos dados (bytes)	Resolução	Gama de funcionamento
RegisteringMemberState	3	ASCII	ASCII
VehicleRegistrationNumber	14	Ver informações no quadro 42	
VIN	17	ASCII	ASCII

CPR_075 O quadro 40 indica os formatos dos diversos bytes do parâmetro TimeDate:

Quadro 40

Formatos detalhados do parâmetro TimeDate (valor # F90B do recordDataIdentifier)

Byte	Definição de parâmetros	Resolução	Gama de funcionamento
1	Segundos	ganho de 0,25 s/bit, deslocamento de 0 s	0 a 59,75s
2	Minutos	ganho de 1 min/bit, deslocamento de 0 min	0 a 59 min
3	Horas	ganho de 1 h/bit, deslocamento de 0 h	0 a 23 h
4	Mês	ganho de 1 mês/bit, deslocamento de 0 meses	1 a 12 meses
5	Dia	ganho de 0,25 dia/bit, deslocamento de 0 dias (ver nota infra, quadro 41)	0,25 a 31,75 dias
6	Ano	ganho de 1 ano/bit, deslocamento de + 1985 anos (ver nota infra, quadro 41)	1985 a 2235 anos
7	Deslocamento local em minutos	ganho de 1 min/bit, deslocamento de – 125 min	– 59 a + 59 min
8	Deslocamento local em horas	ganho de 1 h/bit, deslocamento de – 125 h	– 23 a + 23 h

CPR_076 O quadro 41 indica os formatos dos diversos bytes do parâmetro NextCalibrationDate:

Quadro 41

Formatos detalhados do parâmetro NextCalibrationDate (valor # F922 do recordDataIdentifier)

Byte	Definição de parâmetros	Resolução	Gama de funcionamento
1	Mês	ganho de 1 mês/bit, deslocamento de 0 meses	1 a 12 meses
2	Dia	ganho de 0,25 dia/bit, deslocamento de 0 dias (ver nota infra)	0,25 a 31,75 dias
3	Ano	ganho de 1 ano/bit, deslocamento de + 1985 anos (ver nota infra)	1985 a 2235 anos

▼B

Nota relativa à utilização do parâmetro «Dia»:

1) O valor 0 para a data é nulo. Os valores 1, 2, 3 e 4 são utilizados para identificar o primeiro dia do mês; os valores 5, 6, 7 e 8 identificam o segundo dia do mês; etc.

2) Este parâmetro não influi no parâmetro «Horas» nem o altera.

Nota relativa à utilização do parâmetro «Ano»:

O valor 0 para o ano identifica o ano de 1985; o valor 1 identifica o ano de 1986; etc.

CPR_078 O quadro 42 indica os formatos dos diversos bytes do parâmetro VehicleRegistrationNumber:

Quadro 42

Formatos detalhados do parâmetro VehicleRegistrationNumber (valor # F97E do recordDataIdentifier)

Byte	Definição de parâmetros	Resolução	Gama de funcionamento
1	Code Page (cf. definição no apêndice 1)	ASCII	01 a 0A
2 — 14	VehicleRegistrationNumber (cf. definição no apêndice 1)	ASCII	ASCII

▼B

Apêndice 9.

HOMOLOGAÇÃO DE TIPO RELAÇÃO DOS ENSAIOS MÍNIMOS EXIGIDOS

ÍNDICE

1. INTRODUÇÃO

1.1. **Homologação de tipo**

A homologação CE de tipo para um aparelho de controlo (ou componente) ou para um cartão tacográfico tem por base:

— uma **certificação de segurança**, baseada em especificações de critérios comuns, em relação a uma meta de segurança totalmente compatível com o apêndice 10 do presente anexo (a concluir/ modificar)

— uma **certificação de funcionalidade**, efetuada por uma autoridade do Estado-Membro, a certificar que o elemento ensaiado cumpre o prescrito no presente anexo em termos de funções executadas, de rigor de medição e de características ambientais

— uma **certificação de interoperabilidade**, efetuada pelo organismo competente, a certificar que o aparelho de controlo (ou cartão tacográfico) é totalmente interoperável com os modelos necessários de cartão tacográfico (ou de aparelho de controlo) (ver capítulo 8 do presente anexo).

O presente apêndice especifica os ensaios mínimos a efetuar pela autoridade nacional no âmbito dos ensaios de funcionalidade, bem como os ensaios mínimos a efetuar pelo organismo competente no âmbito dos ensaios de interoperabilidade. Não se dão mais pormenores sobre os procedimentos de execução nem sobre o tipo de ensaios.

O presente apêndice não aborda os aspetos relativos à certificação de segurança. Se, durante o processo de certificação e de avaliação da segurança, se executarem alguns dos ensaios requeridos para efeitos da homologação de tipo, não é necessário repeti-los. Em tal eventualidade, somente os resultados destes ensaios de segurança poderão ser inspecionados. Para informação: os requisitos que, no âmbito da certificação de segurança, devam ser ensaiados (ou se relacionem estreitamente com ensaios que devam ser executados) aparecem marcados com «*» no presente apêndice.

Os requisitos numerados referem-se ao corpo do anexo, ao passo que os restantes requisitos se referem a outros apêndices (por exemplo, PIC_001 refere-se ao requisito PIC_001 do apêndice 3 — «Pictogramas»).

O presente apêndice considera a homologação de tipo do sensor de movimentos separadamente da unidade-veículo e do módulo GNSS externo, como componentes do aparelho de controlo. Cada componente terá o seu próprio certificado de homologação de tipo, no qual se mencionarão os

▼B

outros componentes compatíveis. O ensaio de funcionalidade do sensor de movimentos (ou módulo GNSS externo) é realizado em conjunto com o da unidade-veículo e vice-versa.

Não é necessária interoperabilidade entre todos os modelos de sensor de movimentos (ou de módulo GNSS externo) e todos os modelos de unidade--veículo. Nesse caso, a homologação de tipo de um sensor de movimentos (ou de um módulo GNSS externo) só pode ser concedida em combinação com a homologação de tipo da VU pertinente e vice-versa.

1.2. **Referências**

No presente apêndice, utilizam-se as seguintes referências:

IEC 60068-2-1: Environmental testing — Part 2-1: Tests — Test A: Cold

IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat (sinusoidal).

IEC 60068-2-6: Environmental testing — Part 2: Tests — Test Fc: Vibration

IEC 60068-2-14: Environmental testing; Part 2-14: Tests; Test N: Change of temperature

IEC 60068-2-27: Environmental testing. Part 2: Tests. Test Ea and guidance: Shock

IEC 60068-2-30: Environmental testing — Part 2-30: Tests — Test Db: Damp heat, cyclic (12 h + 12 h cycle)

IEC 60068-2-64: Environmental testing — Part 2-64: Tests — Test Fh: Vibration, broadband random and guidance

IEC 60068-2-78 Environmental testing — Part 2-78: Tests — Test Cab: Damp heat, steady state

ISO 16750-3 — Mechanical loads (2012-12)

ISO 16750-4 — Climatic loads (2010-04).

ISO 20653: Road vehicles — Degree of protection (IP code) — Protection of electrical equipment against foreign objects, water and access

ISO 10605:2008 + Technical Corrigendum:2010 + AMD1:2014 Road vehicles — Test methods for electrical disturbances from electrostatic discharge

ISO 7637-1:2002 + AMD1: 2008 Road vehicles — Electrical disturbances from conduction and coupling — Part 1: Definitions and general considerations

ISO 7637-2 Road vehicles — Electrical disturbances from conduction and coupling — Part 2: Electrical transient conduction along supply lines only

ISO 7637-3 Road vehicles — Electrical disturbances from conduction and coupling — Part 3: Electrical transient transmission by capacitive and inductive coupling via lines other than supply lines

ISO/IEC 7816-1 Identification cards — Integrated circuit(s) cards with contacts — Part 1: Physical characteristics

▼B

ISO/IEC 7816-2 Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 2: Dimensions and location of the contacts

ISO/IEC 7816-3 Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 3: Electronic signals and transmission protocol

ISO/IEC 10373-1:2006 + AMD1:2012 Identification cards — Test methods — Part 1: General characteristics

ISO/IEC 10373-3:2010 + Technical Corrigendum:2013 Identification cards — Test methods — Part 3: Integrated circuit cards with contacts and related interface devices

ISO 16844-3:2004, Cor 1:2006 Road vehicles — Tachograph systems — Part 3: Motion sensor interface (with vehicle units)

ISO 16844-4 Road vehicles — Tachograph systems — Part 4: CAN interface

ISO 16844-6 Road vehicles — Tachograph systems — Part 6: Diagnostics

ISO 16844-7 Road vehicles — Tachograph systems — Part 7: Parameters

ISO 534 Paper and board — Determination of thickness, density and specific volume

UN ECE R10 Uniform provisions concerning the approval of vehicles with regard to electromagnetic compatibility (United Nation Economic Commission for Europe)

2. ENSAIOS DE FUNCIONALIDADE DA UNIDADE-VEÍCULO

N.º	Ensaio	Descrição	Requisitos correlatos
1	**Exame administrativo**		
1.1	Documentação	Adequação da documentação	
1.2	Resultados dos ensaios do fabricante	Resultados do ensaio efetuado pelo fabricante durante a integração. Demonstrações em papel.	88, 89, 91
2	**Inspeção visual**		
2.1	Conformidade com a documentação		
2.2	Identificação/marcações		224 a 226
2.3	Materiais		219 a 223
2.4	Selagem		398, 401 a 405
2.5	Interfaces externas		
3	**Ensaios de funcionalidade**		
3.1	Funções disponíveis		03, 04, 05, 07, 382
3.2	Modos de funcionamento		09 a 11*, 132, 133
3.3	Direitos de acesso a funções e a dados		12* 13*, 382, 383, 386 a 389
3.4	Controlo da inserção e da retirada de cartões		15, 16, 17, 18, 19*, 20*, 132
3.5	Medição da velocidade e da distância		21 a 31

▼B

N.º	Ensaio	Descrição	Requisitos correlatos
3.6	Medição do tempo (ensaio efetuado a 20 °C)		38 a 43
3.7	Controlo das atividades do condutor		44 a 53, 132
3.8	Controlo da situação de condução		54, 55, 132
3.9	Entradas efetuadas manualmente		56 a 62
3.10	Gestão dos bloqueamentos da empresa		63 a 68
3.11	Vigilância das atividades de controlo		69, 70
3.12	Deteção de incidentes e/ou falhas		71 a 88 132
3.13	Dados de identificação do aparelho		93*, 94*, 97, 100
3.14	Dados relativos à inserção e à retirada de cartões de condutor		102* a 104*
3.15	Dados relativos à atividade de condutor		105* a 107*
3.16	Dados dos locais e posições		108* a 112*
3.17	Dados do conta-quilómetros		113* a 115*
3.18	Dados detalhados da velocidade		116*
3.19	Dados relativos a incidentes		117*
3.20	Dados relativos a falhas		118*
3.21	Dados relativos à calibração		119* a 121*
3.22	Dados relativos ao ajustamento da hora		124*, 125*
3.23	Dados relativos à atividade de controlo		126*, 127*
3.24	Dados relativos aos bloqueamentos da empresa		128*
3.25	Dados relativos à atividade de descarregamento		129*
3.26	Dados relativos às condições especiais		130*, 131*
3.27	Registo e memorização de dados nos cartões tacográficos		134, 135, 136*, 137*, 139*, 140, 141 142, 143, 144*, 145*, 146*, 147, 148
3.28	Visualização		90, 132, 149 a 166, PIC_001, DIS_001
3.29	Impressão		90, 132, 167 a 179, PIC_001, PRT_001 a PRT_014
3.30	Alerta		132, 180 a 189, PIC_001
3.31	Descarregamento de dados para meios externos		90, 132, 190 a 194
3.32	Comunicação à distância para controlos de estrada seletivos		195 a 197
3.33	Transmissão ou saída de dados para dispositivos externos adicionais		198, 199

▼B

N.º	Ensaio	Descrição	Requisitos correlatos
3.34	Calibração		202 a 206*, 383, 384, 386 a 391
3.35	Controlo de calibração de estrada		207 a 209
3.36	Ajustamento do tempo		210 a 212*
3.37	Não-interferência de funções adicionais		06, 425
3.38	Interface do sensor de movimentos		02, 122
3.39	Módulo GNSS externo		03, 123
3.40	Verificar se a VU deteta, regista e memoriza o(s) incidente(s) e/ou falha(s) definidos pelo fabricante da VU quando um sensor de movimentos emparelhado reage a campos magnéticos que perturbam a deteção do movimento do veículo.		217
3.41	Parâmetros de domínio normalizados e de sequência de cifras		CSM_48, CSM_50
4	**Ensaios ambientais**		
4.1	Temperatura	Verificar funcionalidade por meio de: Ensaio de acordo com a norma ISO 16750-4, capítulo 5.1.1.2: Low temperature operation test (72 h a – 20 °C) Este ensaio refere-se à norma IEC 60068-2-1: Environmental testing — Part 2-1: Tests — Test A: Cold Ensaio de acordo com a norma ISO 16750-4: capítulo 5.1.2.2: High temperature operation test (72 h a 70 °C) Este ensaio refere-se à norma IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat Ensaio de acordo com a norma ISO 16750-4: capítulo 5.3.2: Rapid change of temperature with specified transition duration (– 20 °C/ 70 °C, 20 ciclos; duração do ensaio 2 horas a cada temperatura) Pode ser efetuado um conjunto reduzido de ensaios (entre os definidos na secção 3 deste quadro) à temperatura mais baixa, à temperatura mais alta e durante os ciclos de temperatura	213
4.2	Humidade	Verificar se a unidade-veículo suporta variações cíclicas de humidade (ensaio térmico) por meio da norma IEC 60068-2-30, ensaio Db, seis ciclos de 24 horas, variando cada temperatura de + 25 °C a + 55 °C e com humidade relativa de 97 % a + 25 °C e de 93 % a + 55 °C	214

▼B

N.º	Ensaio	Descrição	Requisitos correlatos
4.3	Mecânica	1. Vibrações sinusoidais. Verificar se a unidade-veículo suporta vibrações sinusoidais com as seguintes características: deslocamento constante entre 5 e 11 Hz: pico de 10 mm aceleração constante entre 11 e 300 Hz: 5 g Este requisito é verificado por meio da norma IEC 60068-2-6, ensaio Fc, com a duração mínima de 3 × 12 horas (12 horas por eixo) A norma ISO 16750-3 não exige ensaio de vibração sinusoidal em dispositivos localizados na cabina do veículo separada. 2. Vibrações aleatórias: Ensaio de acordo com a norma ISO 16750-3: capítulo 4.1.2.8: Test VIII: Commercial vehicle, decoupled vehicle cab Ensaio de vibração aleatória, 10...2 000 Hz, RMS vertical 21,3 m/s^2, RMS longitudinal 11,8 m/s^2, RMS lateral 13,1 m/s^2, 3 eixos, 32 h por eixo, incluindo o ciclo de temperatura – 20 °C ... 70 °C. Este ensaio refere-se à norma IEC 60068-2--64: Environmental testing — Part 2-64: Tests — Test Fh: Vibration, broadband random and guidance 3. Choques: choque mecânico com 3 g de meio seio, de acordo com a norma ISO 16750. Os dois ensaios supra são executados sobre duas amostras distintas do tipo de equipamento em ensaio.	219
4.4	Proteção contra água e corpos estranhos	Ensaio de acordo com a norma ISO 20653: Road vehicles — Degree of protection (IP code) — Protection of electrical equipment against foreign objects, water and access (Sem alterações nos parâmetros); valor mínimo IP 40	220, 221
4.5	Proteção contra sobretensão	Verificar se a unidade-veículo suporta as seguintes tensões de alimentação: Versões de 24 V: 34 V a +40 °C, 1 hora Versões de 12 V: 17 V a +40 °C, 1 hora (ISO 16750-2)	216

▼B

N.º	Ensaio	Descrição	Requisitos correlatos
4.6	Proteção contra polaridade inversa	Verificar se a unidade-veículo suporta uma inversão na alimentação elétrica (ISO 16750-2)	216
4.7	Proteção contra curto-circuito	Verificar se os sinais de entrada-saída estão protegidos contra curtos-circuitos na alimentação elétrica e na terra (ISO 16750-2)	216
5	**Ensaios de CEM**		
5.1	Emissões radiadas e suscetibilidade	Conformidade com o Regulamento ECE R10	218
5.2	Descarga eletrostática	Conformidade com a norma ISO 10605:2008 + Retificação técnica: 2010 + AMD1:2014: +/– 4 kV para contacto e +/– 8 kV para descarga de ar	218
5.3	Suscetibilidade do transitório conduzido em relação à alimentação elétrica	Para versões de 24 V: conformidade com a norma ISO 7637 – 2 + Regulamento ECE n.º 10 rev. 3: impulso 1a: Vs = – 450 V Ri = 50 ohms impulso 2a: Vs = + 37 V Ri = 2 ohms impulso 2b: Vs = + 20 V Ri = 0,05 ohms impulso 3a: Vs = – 150 V Ri = 50 ohms impulso 3b: Vs = + 150 V Ri = 50 ohms impulso 4: Vs = – 16 V Va = – 12 V t6 = 100 ms impulso 5: Vs = + 120 V Ri = 2,2 ohms td = 250 ms Para versões de 12 V: conformidade com a norma ISO 7637 – 1 + Regulamento ECE n.º 10 rev. 3: impulso 1: Vs = – 75 V Ri = 10 ohms impulso 2a: Vs = + 37 V Ri = 2 ohms impulso 2b: Vs = + 10 V Ri = 0,05 ohms impulso 3a: Vs = – 112 V Ri = 50 ohms impulso 3b: Vs = + 75 V Ri = 50 ohms impulso 4: Vs = –6 V Va = –5 V t6 = 15 ms impulso 5: Vs = + 65 V Ri = 3 ohms td = 100 ms O ensaio do impulso 5 só é efetuado em unidades-veículo destinadas a veículos sem proteção externa comum contra descarga. Relativamente a propostas de descarga, consultar a norma ISO 16750-2, 4.ª edição, capítulo 4.6.4.	218

▼B

3. ENSAIOS DE FUNCIONALIDADE DO SENSOR DE MOVIMENTOS

Não	Ensaio	Descrição	Requisitos correlatos
1.	**Exame administrativo**		
1.1	Documentação	Adequação da documentação	
2.	**Inspeção visual**		
2.1.	Conformidade com a documentação		
2.2.	Identificação/marcações		225, 226
2.3	Materiais		219 a 223
2.4.	Selagem		398, 401 a 405
3.	**Ensaios de funcionalidade**		
3.1	Dados de identificação do sensor de movimentos		95 a 97*
3.2	Emparelhamento do sensor de movimentos com a unidade-veículo		122*, 204
3.3	Deteção de movimentos Precisão da medição de movimentos		30 a 35
3.4	Interface da unidade-veículo		02
3.5	Verificar se o sensor de movimentos é imune ao campo magnético. Em alternativa, verificar se o sensor de movimentos reage a campos magnéticos que perturbam a deteção de movimentos do veículo de forma a que uma VU emparelhada possa detetar, registar e memorizar falhas do sensor		217
4.	**Ensaios ambientais**		
4.1	Temperatura de funcionamento	Verificar funcionalidade (cf. definição no ensaio 3.3) na amplitude térmica [–40°C; +135°C], por meio de: IEC 60068-2-1 ensaio Ad, com a duração de 96 horas à temperatura mais baixa To_{min}, IEC 60068-2-2 ensaio Bd, com a duração de 96 horas à temperatura mais alta To_{max} Ensaio de acordo com a norma ISO 16750-4: capítulo 5.1.1.2: Low temperature operation test (24 h a –40°C) Este ensaio refere-se à norma IEC 60068-2-1: Environmental testing — Part 2-1: Tests — Test A: Cold IEC 68-2-2 ensaio Ad, com a duração de 96 horas à temperatura mais baixa de –40°C. Ensaio de acordo com a norma ISO 16750-4: capítulo 5.1.2.2: High temperature operation test (96 h a 135°C) Este ensaio refere-se à norma IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat	213

▼B

Não	Ensaio	Descrição	Requisitos correlatos
4.2	Ciclos térmicos	Ensaio de acordo com a norma ISO 16750-4: capítulo 5.3.2: Rapid change of temperature with specified transition duration (–40°C/135°C, 20 ciclos; duração do ensaio 30 minutos a cada temperatura) IEC 60068-2-14: Environmental testing; Part 2--14: Tests; Test N: Change of temperature	213
4.3	Ciclos de humidade	Verificar funcionalidade (cf. definição no ensaio 3.3) por meio da norma IEC 60068-2-30, ensaio Db, seis ciclos de 24 horas, variando cada temperatura de +25°C a +55°C e com humidade relativa de 97 % a +25°C e de 93 % a +55°C	214
4.4	Vibração	ISO 16750-3: capítulo 4.1.2.6: Test VI: Commercial vehicle, engine, gearbox Ensaio de vibração do modo misto que inclui: a) Ensaio de vibração sinusoidal, 20...520 Hz, 11.4 ... 120 m/s^2, <= 0,5 oct/min b) Ensaio de vibração aleatória, 10 … 2 000 Hz, RMS 177 m/s^2 94 horas por eixo, incluindo o ciclo térmico –20°C ... 70°C Este ensaio refere-se à norma IEC 60068-2-80: Environmental testing — Part 2-80: Tests — Test Fi: Vibration — Mixed mode	219
4.5	Choque mecânico	ISO 16750-3: capítulo 4.2.3: Test VI: Test for devices in or on the gearbox choque semi-sinusoidal, aceleração a acordar no intervalo 3 000...15 000 m/s^2, duração do impulso a acordar, no entanto, <1 ms, número de choques: a acordar Este ensaio refere-se à norma IEC 60068-2-27: Environmental testing. Part 2: Tests. Test Ea and guidance: Shock	219
4.6	Proteção contra água e corpos estranhos	Ensaio de acordo com a norma ISO 20653: Road vehicles — Degree of protection (IP code) — Protection of electrical equipment against foreign objects, water and access (Valor-alvo IP 64)	220, 221
4.7	Proteção contra polaridade inversa	Verificar se o sensor de movimentos suporta uma inversão na alimentação elétrica	216
4.8	Proteção contra curto-circuito	Verificar se os sinais de entrada-saída estão protegidos contra curtos-circuitos na alimentação elétrica e na terra	216

▼B

Não	Ensaio	Descrição	Requisitos correlatos
5.	**Ensaios de compatibilidade eletromagnética**		
5.1	Emissões radiadas e suscetibilidade	Verificar conformidade com o Regulamento ECE R10	218
5.2	Descarga eletrostática	Conformidade com a norma ISO 10605:2008 + Retificação técnica: 2010 + AMD1:2014: +/– 4 kV para contacto e +/– 8 kV para descarga de ar	218
5.3	Suscetibilidade do transitório conduzido em relação às linhas de dados)	Para versões de 24 V: conformidade com a norma ISO 7637-2 + Regulamento ECE n.º 10 Rev. 3: impulso 1a: Vs = –450 V Ri = 50 ohms impulso 2a: Vs = +37 V Ri = 2 ohms impulso 2b: Vs = +20V Ri = 0,05 ohms impulso 3a: Vs = –150 V Ri = 50 ohms impulso 3b: Vs = +150 V Ri = 50 ohms impulso 4: Vs = –16 V Va = –12 V t6 = 100ms impulso 5: Vs = +120 V Ri = 2,2 ohms td = 250ms Para versões de 12 V: conformidade com a norma ISO 7637-1 + Regulamento ECE n.º 10 Rev. 3: impulso 1: Vs = –75 V Ri = 10 ohms impulso 2a: Vs = +37 V Ri = 2 ohms impulso 2b: Vs = +10 V Ri = 0,05 ohms impulso 3a: Vs = –112 V Ri = 50 ohms impulso 3b: Vs = +75 V Ri = 50 ohms impulso 4: Vs = –6 V Va = –5 V t6 = 15ms impulso 5: Vs = +65 V Ri = 3ohms td = 100ms O ensaio do impulso 5 só é efetuado em unidades-veículo destinadas a veículos sem proteção externa comum contra descarga. Relativamente a propostas de descarga, consultar a norma ISO 16750-2, 4.ª edição, capítulo 4.6.4	218

4. ENSAIOS DE FUNCIONALIDADE DOS CARTÕES TACOGRÁFICOS

Os ensaios, de acordo com a presente secção 4,

n.º 5 — ‘Ensaios de protocolo’,

n.º 6 — ‘Estrutura do cartão’ e

n.º 7 — ‘Ensaios de funcionalidade’

podem ser executados pelo avaliador ou certificador durante o processo de certificação de segurança por critérios comuns (CC), destinado ao módulo de pastilha.

Os ensaios números 2.3 e 4.2 são os mesmos. Trata-se dos ensaios mecânicos combinados do corpo do cartão e do módulo de pastilha. Se um destes componentes (corpo do cartão, módulo de pastilha) for alterado, estes ensaios são necessários.

▼B

N.º	Ensaio	Descrição	Requisitos correlatos
1.	**Exame administrativo**		
1.1	Documentação	Adequação da documentação	
2	**Corpo do cartão**		
2.1	Projeto impresso	Verificar se todos os elementos de proteção e dados visíveis estão conformes e corretamente impressos no cartão. [Designador] Anexo 1C, capítulo 4.1 «Dados visíveis», 227) O anverso do cartão terá o seguinte conteúdo os termos «Cartão de condutor», «Cartão de controlo», «Cartão de oficina» ou «Cartão de empresa», consoante o tipo de cartão, impressos em maiúsculas na(s) língua(s) oficial(is) do Estado-Membro emissor. [Nome do Estado-Membro] Anexo 1C, capítulo 4.1 «Dados visíveis», 228) O anverso do cartão terá o seguinte conteúdo: Nome do Estado-Membro que emite o cartão (facultativo). [Sinal] Anexo 1C, capítulo 4.1 «Dados visíveis», 229) O anverso do cartão terá o seguinte conteúdo: Símbolo distintivo do Estado-Membro que emite o cartão, impresso em negativo num retângulo azul e rodeado de 12 estrelas amarelas. [Enumeração] Anexo 1C, capítulo 4.1 «Dados visíveis», 232) O verso do cartão terá o seguinte conteúdo: explicação dos elementos numerados que constam do anverso. [Cor] Anexo 1C, capítulo 4.1 «Dados visíveis», 234) Os cartões tacográficos devem ser impressos com as seguintes colorações de fundo: — cartão de condutor: branco — cartão de oficina: vermelho, — cartão de controlo: azul, — cartão de empresa: amarelo.	227 a 229, 232, 234 a 236

▼B

N.º	Ensaio	Descrição	Requisitos correlatos
		[Segurança] Anexo 1C, capítulo 4.1 «Dados visíveis», 235) Os cartões tacográficos devem ter as seguintes características de proteção contra falsificações: — fundo de segurança em guilhoché fino e impressão irisada — pelo menos uma linha de microimpressão bicromática.	
		[Marcações] Anexo 1C, capítulo 4.1 «Dados visíveis», 236) Os Estados-Membros podem acrescentar cores ou marcações, como símbolos nacionais e elementos de segurança.	
		[Marca de homologação] Os cartões tacográficos devem conter uma marca de homologação, com a seguinte composição: — um retângulo, no interior do qual é colocada a letra «e», seguida de uma letra ou de um número distintivo do país que tiver concedido a homologação — o número de homologação, correspondente ao número do certificado de homologação de um cartão tacográfico, colocado na proximidade do retângulo.	
2.2	Ensaios mecânicos	[Tamanho do cartão] Os cartões tacográficos devem cumprir a norma ISO/IEC 7810, Identification cards — Physical characteristics, [5] Dimension of card, [5.1] Card size, [5.1.1] Card dimensions and tolerances, card type ID-1 Unused card	240, 243 ISO/IEC 7810
		[Rebordos do cartão] Os cartões tacográficos devem cumprir a norma ISO/IEC 7810, Identification cards — Physical characteristics, [5] Dimension of card, [5.1] Card size, [5.1.2] Card edges	

▼B

N.º	Ensaio	Descrição	Requisitos correlatos
		[Estrutura do cartão] Os cartões tacográficos devem cumprir a norma ISO/IEC 7810, Identification cards — Physical characteristics, [6] Card construction	
		[Materiais do cartão] Os cartões tacográficos devem cumprir a norma ISO/IEC 7810, Identification cards — Physical characteristics, [7] Card materials	
		[Rigidez à dobragem] Os cartões tacográficos devem cumprir a norma ISO/IEC 7810, Identification cards — Physical characteristics, [8] Card characteristics, [8.1] Bending stiffness	
		[Toxicidade] Os cartões tacográficos devem cumprir a norma ISO/IEC 7810, Identification cards — Physical characteristics, [8] Card characteristics, [8.3] Toxicity	
		[Resistência a agentes químicos] Os cartões tacográficos devem cumprir a norma ISO/IEC 7810, Identification cards — Physical characteristics, [8] Card characteristics, [8.4] Resistance to chemicals	
		[Estabilidade do cartão] Os cartões tacográficos devem cumprir a norma ISO/IEC 7810, Identification cards — Physical characteristics, [8] Card characteristics, [8.5] Card dimensional stability and warpage with temperature and humidity	

▼B

N.º	Ensaio	Descrição	Requisitos correlatos
		[Luz] Os cartões tacográficos devem cumprir a norma ISO/IEC 7810, Identification cards — Physical characteristics, [8] Card characteristics, [8.6] Light	
		[Durabilidade] Anexo 1C, capítulo 4.4 «Especificações ambientais e elétricas», 241) Os cartões tacográficos devem poder funcionar corretamente durante um período de cinco anos, desde que utilizados em conformidade com as especificações ambientais e elétricas.	
		[Resistência ao rasgamento] Os cartões tacográficos devem cumprir a norma ISO/IEC 7810, Identification cards — Physical characteristics, [8] Card characteristics, [8.8] Peel strength	
		[Adesão ou bloqueamento] Os cartões tacográficos devem cumprir a norma ISO/IEC 7810, Identification cards — Physical characteristics, [8] Card characteristics, [8.9] Adhesion or blocking	
		[Deformação] Os cartões tacográficos devem cumprir a norma ISO/IEC 7810, Identification cards — Physical characteristics, [8] Card characteristics, [8.11] Overall card warpage	
		[Resistência ao calor] Os cartões tacográficos devem cumprir a norma ISO/IEC 7810, Identification cards — Physical characteristics, [8] Card characteristics, [8.12] Resistance to heat	

▼B

N.º	Ensaio	Descrição	Requisitos correlatos
		[Distorções de superfície] Os cartões tacográficos devem cumprir a norma ISO/IEC 7810, Identification cards — Physical characteristics, [8] Card characteristics, [8.13] Surface distortions	
		[Contaminação] Os cartões tacográficos devem cumprir a norma ISO/IEC 7810, Identification cards — Physical characteristics, [8] Card characteristics, [8.14] Contamination and interaction of card components	
2.3	Ensaios mecânicos com módulo de pastilha integrado	[Curvatura] Os cartões tacográficos devem cumprir a norma ISO/IEC 7810:2003/Amd. 1:2009, Identification cards — Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.2] Dynamic bending stress Número total de ciclos de curvatura: 4 000.	ISO/IEC 7810
		[Torção] Os cartões tacográficos devem cumprir a norma ISO/IEC 7810:2003/Amd. 1:2009, Identification cards — Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.3] Dynamic torsional stress Número total de ciclos de torção: 4 000.	
3	**Módulo**		
3.1	Módulo	O módulo é a encapsulação de pastilhas e a placa de contacto.	ISO/IEC 7816
		[Perfil da superfície] Os cartões tacográficos devem cumprir a norma ISO/IEC 7816-1:2011, Identification cards — Integrated circuit cards — Part 1: Cards with contacts — Physical characteristics [4.2] Surface profile of contacts	

▼B

N.º	Ensaio	Descrição	Requisitos correlatos
		[Resistência mecânica] Os cartões tacográficos devem cumprir a norma ISO/IEC 7816-1:2011, Identification cards — Integrated circuit cards — Part 1: Cards with contacts — Physical characteristics [4.3] Mechanical strength (of a card and contacts)	
		[Resistência elétrica] Os cartões tacográficos devem cumprir a norma ISO/IEC 7816-1:2011, Identification cards — Integrated circuit cards — Part 1: Cards with contacts — Physical characteristics [4.4] Electrical resistance (of contacts)	
		[Dimensões] Os cartões tacográficos devem cumprir a norma ISO/IEC 7816-2:2007, Identification cards — Integrated circuit cards — Part 2: Cards with contacts — Dimension and location of the contacts [3] Dimension of the contacts	
		[Localização] Os cartões tacográficos devem cumprir a norma ISO/IEC 7816-2:2007, Identification cards — Integrated circuit cards — Part 2: Cards with contacts — Dimension and location of the contacts [4] Number and location of the contacts No caso dos módulos com seis contactos, os contactos «C4» e «C8» não são parte integrante do presente requisito de ensaio.	
4	**Pastilha**		
4.1	Pastilha	[Temperatura de funcionamento] A pastilha do cartão tacográfico deve funcionar numa amplitude térmica entre – 25 °C e + 85 °C.	241 a 244 Regulamento ECE R10 ISO/IEC 7810 ISO/IEC 10373

▼B

N.º	Ensaio	Descrição	Requisitos correlatos
		[Temperatura e humidade] Anexo 1C, capítulo 4.4 «Especificações ambientais e elétricas», 241) Os cartões tacográficos devem poder funcionar corretamente nas condições climáticas normais do território da União Europeia e pelo menos na amplitude térmica de – 25 °C a + 70 °C, com picos ocasionais até + 85 °C, entendendo-se por «ocasionais» ocorrências de duração não superior a 4 horas e em número não superior a 100 ao longo do período de vida útil do cartão. Expõem-se os cartões tacográficos à sequência de temperaturas e humidades durante o tempo determinado e em etapas consecutivas. Após cada etapa, testam-se quanto à funcionalidade elétrica. 1. Temperatura de – 20 °C, durante 2 horas. 2. Temperatura de +/– 0 °C, durante 2 horas. 3. Temperatura de + 20 °C, 50 % de HR (humidade relativa), durante 2 horas. 4. Temperatura de + 50 °C, 50 % de HR, durante 2 horas. 5. Temperatura de + 70 °C, 50 % de HR, durante 2 horas. A temperatura é aumentada de modo intermitente para + 85 °C, 50 % de HR, durante 60 minutos. 6. Temperatura de + 70 °C, 85 % de HR, durante 2 horas. A temperatura é aumentada de modo intermitente para + 85 °C, 85 % de HR, durante 30 minutos.	
		[Humidade] Anexo 1C, capítulo 4.4 «Especificações ambientais e elétricas», 242) Os cartões tacográficos devem poder funcionar corretamente no intervalo de humidade entre 10 % e 90 %.	
		[Compatibilidade eletromagnética — EMC] Anexo 1C, capítulo 4.4 «Especificações ambientais e elétricas», 244) Durante o seu funcionamento, os cartões tacográficos devem cumprir o disposto no Regulamento ECE R10, relativo à compatibilidade eletromagnética.	

▼B

N.º	Ensaio	Descrição	Requisitos correlatos
		[Eletricidade estática] Anexo 1C, capítulo 4.4 «Especificações ambientais e elétricas», 244) Durante o seu funcionamento, os cartões tacográficos devem estar protegidos contra as descargas eletrostáticas. Os cartões tacográficos devem cumprir a norma ISO/IEC 7810:2003/Amd. 1:2009, Identification cards — Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.4] Static electricity [9.4.1] Contact IC cards Tensão de ensaio: 4 000 V.	
		[Raios X] Os cartões tacográficos devem cumprir a norma ISO/IEC 7810:2003/Amd. 1:2009, Identification cards — Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.1] X-rays	
		[Luz ultravioleta] ISO/IEC 10373-1:2006, Identification cards — Test methods — Part 1: General characteristics [5.11] Ultraviolet light	
		[3-wheel] Os cartões tacográficos devem cumprir a norma ISO/IEC 10373-1:2006/Amd. 1:2012, Identification cards — Test methods — Part 1: General characteristics, Amendment 1 [5.22] ICC — Mechanical strength: 3 wheel test for ICCs with contacts	
		[Acondicionamento] Os cartões tacográficos devem cumprir a norma MasterCard CQM V2.03:2013 [11.1.3] R-L3-14-8: Wrapping Test Robustness [13.2.1.32] TM-422: Mechanical Reliability: Wrapping Test	

▼B

N.º	Ensaio	Descrição	Requisitos correlatos
4.2	Ensaios mecânicos do módulo de pastilha integrado no corpo do cartão (o mesmo que 2.3)	[Dobragem] Os cartões tacográficos devem cumprir a norma ISO/IEC 7810:2003/Amd. 1:2009, Identification cards — Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.2] Dynamic bending stress Número total de ciclos de dobragem: 4 000. [Torção] Os cartões tacográficos devem cumprir a norma ISO/IEC 7810:2003/Amd. 1:2009, Identification cards — Physical characteristics, Amendment 1: Criteria for cards containing integrated circuits [9.3] Dynamic torsional stress Número total de ciclos de torção: 4 000.	ISO/IEC 7810
5	**Ensaios de protocolo**		
5.1	ATR	Verificar a conformidade da ATR	ISO/IEC 7816-3 TCS_14, TCS_17, TCS_18
5.2	T=0	Verificar a conformidade do protocolo T=0	ISO/IEC 7816-3 TCS_11, TCS_12, TCS_13, TCS_15
5.3	PTS	Verificar a conformidade do comando PTS, passando de T=0 a T=1.	ISO/IEC 7816-3 TCS_12, TCS_19, TCS_20, TCS_21
5.4	T=1	Verificar a conformidade do protocolo T=1	ISO/IEC 7816-3 TCS_11, TCS_13, TCS_16
6	**Estrutura do cartão**		
6.1		Verificar a conformidade da estrutura de ficheiro do cartão, controlando a presença dos ficheiros obrigatórios no cartão e as suas condições de acesso	TCS_22 a TCS_28 TCS_140 a TCS_179
7	**Ensaios de funcionalidade**		
7.1	Processamento normal	Verificar pelo menos uma vez cada uma das utilizações autorizadas de cada comando (por exemplo, ensaiar o comando UPDATE BINARY com CLA = '00' e CLA = '0C' e com diferentes parâmetros P1, P2 e Lc) Verificar se as operações foram realmente executadas no cartão (ex: ler o ficheiro no qual o comando foi executado)	TCS_29 a TCS_139

▼B

N.º	Ensaio	Descrição	Requisitos correlatos
7.2	Mensagens de erro	Verificar pelo menos uma vez cada uma das mensagens de erro (cf. apêndice 2) para cada comando Verificar pelo menos uma vez cada um dos erros genéricos (exceto os erros de integridade '6400' controlados durante a certificação de segurança)	
7.3	Parâmetros de domínio normalizados e de sequência de cifras		CSM_48, CSM_50
8	**Personalização**		
8.1	Personalização ótica	Anexo 1C, capítulo 4.1 «Dados visíveis», 230) O anverso do cartão terá o seguinte conteúdo: elementos específicos do cartão emitido.	230, 231, 235
		Anexo 1C, capítulo 4.1 «Dados visíveis», 231) O anverso do cartão terá o seguinte conteúdo: datas, com o formato «dd/mm/aaaa» ou «dd.mm.aaaa» (dia, mês, ano).	
		Anexo 1C, capítulo 4.1 «Dados visíveis», 235) Os cartões tacográficos devem ter as seguintes características de proteção contra falsificações: — na zona da fotografia, sobreposição do fundo de segurança e da fotografia.	

5. ENSAIOS DO MÓDULO GNSS EXTERNO

N.º	Ensaio	Descrição	Requisitos correlatos
1.	**Exame administrativo**		
1.1	Documentação	Adequação da documentação	
2.	**Inspeção visual do módulo GNSS externo**		
2.1.	Conformidade com a documentação		
2.2.	Identificação/marcações		224 a 226
2.3	Materiais		219 a 223
3.	**Ensaios de funcionalidade**		
3.1	Dados de identificação do sensor de movimentos		98, 99
3.2	Módulo GNSS externo — acoplamento da unidade-veículo		123, 205

▼B

N.º	Ensaio	Descrição	Requisitos correlatos
3.3	Posição GNSS		36, 37
3.4	Interface da unidade-veículo quando o recetor GNSS é externo à unidade-veículo		03
3.5	Parâmetros de domínio normalizados e de sequência de cifras		CSM_48, CSM_50
4.	**Ensaios ambientais**		
4.1	Temperatura	Verificar funcionalidade por meio de: Ensaio de acordo com a norma ISO 16750-4, capítulo 5.1.1.2: Low temperature operation test (72 h a – 20 °C) Este ensaio refere-se à norma IEC 60068-2-1: Environmental testing — Part 2-1: Tests — Test A: Cold Ensaio de acordo com a norma ISO 16750-4: capítulo 5.1.2.2: High temperature operation test (72 h, 70 °C) Este ensaio refere-se à norma IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat Ensaio de acordo com a norma ISO 16750-4: capítulo 5.3.2: Rapid change of temperature with specified transition duration (–20°C/70°C, 20 ciclos; duração do ensaio 1 hora a cada temperatura) Pode ser efetuado um conjunto reduzido de ensaios (entre os definidos na secção 3 deste quadro) à temperatura mais baixa, à temperatura mais alta e durante os ciclos de temperatura	213
4.2	Humidade	Verificar se a unidade-veículo suporta variações cíclicas de humidade (ensaio térmico) por meio da norma IEC 60068-2--30, ensaio Db, seis ciclos de 24 horas, variando cada temperatura de + 25 °C a + 55 °C e com humidade relativa de 97 % a + 25 °C e de 93 % a +55 °C	214
4.3	Mecânica	1. Vibrações sinusoidais: Verificar se a unidade-veículo suporta vibrações sinusoidais com as seguintes características: deslocamento constante entre 5 e 11 Hz: pico de 10 mm aceleração constante entre 11 e 300 Hz: 5 g Este requisito é verificado por meio da norma IEC 60068-2-6, ensaio Fc, com a duração mínima de 3 × 12 horas (12 horas por eixo) A norma ISO 16750-3 não exige ensaio de vibração sinusoidal em dispositivos localizados na cabina do veículo separada.	219

▼B

N.º	Ensaio	Descrição	Requisitos correlatos
		2. Vibrações aleatórias: Ensaio de acordo com a norma ISO 16750-3: capítulo 4.1.2.8: Test VIII: Commercial vehicle, decoupled vehicle cab Ensaio de vibração aleatória, 10…2 000 Hz, RMS vertical 21,3 m/s^2, RMS longitudinal 11,8 m/s^2, RMS lateral 13,1 m/s^2, 3 eixos, 32 h por eixo, incluindo o ciclo de temperatura –20 °C ... 70 °C. Este ensaio refere-se à norma IEC 60068-2-64: Environmental testing — Part 2-64: Tests — Test Fh: Vibration, broadband random and guidance 3. Choques Choque mecânico com 3 g de meio seio, de acordo com a norma ISO 16750. Os dois ensaios *supra* são executados sobre diferentes amostras do tipo de equipamento em ensaio.	
4.4	Proteção contra água e corpos estranhos	Ensaio de acordo com a norma ISO 20653: Road vehicles — Degree of protection (IP code) — Protection of electrical equipment against foreign objects, water and access (Sem alterações nos parâmetros)	220, 221
4.5	Proteção contra sobretensão	Verificar se a unidade-veículo suporta as seguintes tensões de alimentação: Versões de 24 V: 34 V a +40 °C, 1 hora Versões de 12 V: 17 V a +40 °C, 1 hora (ISO 16750-2, capítulo 4.3)	216
4.6	Proteção contra polaridade inversa	Verificar se a unidade-veículo suporta uma inversão na alimentação elétrica (ISO 16750-2, capítulo 4.7)	216
4.7	Proteção contra curto-circuito	Verificar se os sinais de entrada-saída estão protegidos contra curtos-circuitos na alimentação elétrica e na terra (ISO 16750-2, capítulo 4.10)	216
5	**Ensaios de CEM**		
5.1	Emissões radiadas e suscetibilidade	Conformidade com o Regulamento ECE R10	218

▼B

N.º	Ensaio	Descrição	Requisitos correlatos
5.2	Descarga eletrostática	Conformidade com a norma ISO 10605:2008 + Retificação técnica: 2010 + AMD1:2014: +/– 4 kV para contacto e +/– 8 kV para descarga de ar	218
5.3	Suscetibilidade do transitório conduzido em relação à alimentação elétrica	Para versões de 24 V: conformidade com a norma ISO 7637-2 + Regulamento ECE n.º 10 Rev. 3: impulso 1a: Vs = – 450 V Ri = 50 ohms impulso 2a: Vs = + 37 V Ri = 2 ohms impulso 2b: Vs = + 20 V Ri = 0,05 ohms impulso 3a: Vs = – 150 V Ri = 50 ohms impulso 3b: Vs = + 150 V Ri = 50 ohms impulso 4: Vs = – 16 V Va = – 12 V t6 = 100 ms impulso 5: Vs = + 120 V Ri = 2,2 ohms td = 250 ms Para versões de 12 V: conformidade com a norma ISO 7637-1 + Regulamento ECE n.º 10 Rev. 3: impulso 1: Vs = – 75 V Ri = 10 ohms impulso 2a: Vs = + 37 V Ri = 2 ohms impulso 2b: Vs = + 10 V Ri = 0,05 ohms impulso 3a: Vs = – 112 V Ri = 50 ohms impulso 3b: Vs = + 75 V Ri = 50 ohms impulso 4: Vs = – 6 V Va = – 5 V t6 = 15 ms impulso 5: Vs = + 65 V Ri = 3 ohms td = 100 ms O ensaio do impulso 5 só é efetuado em unidades-veículo destinadas a veículos sem proteção externa comum contra descarga. Relativamente a propostas de descarga, consultar a norma ISO 16750-2, 4.ª edição, capítulo 4.6.4.	218

6. ENSAIOS DO SISTEMA DE COMUNICAÇÃO À DISTÂNCIA

N.º	Ensaio	Descrição	Requisitos correlatos
1.	**Exame administrativo**		
1.1	Documentação	Adequação da documentação	
2.	**Inspeção visual**		
2.1.	Conformidade com a documentação		
2.2.	Identificação/marcações		225, 226
2.3	Materiais		219 a 223
4.	**Ensaios ambientais**		
4.1	Temperatura	Verificar funcionalidade por meio de: Ensaio segundo a norma ISO 16750-4, capítulo 5.1.1.2: Low temperature operation test (72 h a – 20 °C) Este ensaio refere-se à norma IEC 60068-2-1: Environmental testing — Part 2-1: Tests — Test A: Cold	213

▼B

N.º	Ensaio	Descrição	Requisitos correlatos
		Ensaio de acordo com a norma ISO 16750-4: capítulo 5.1.2.2: High temperature operation test (72 h a 70 °C) Este ensaio refere-se à norma IEC 60068-2-2: Basic environmental testing procedures; part 2: tests; tests B: dry heat Ensaio de acordo com a norma ISO 16750-4: capítulo 5.3.2: Rapid change of temperature with specified transition duration (– 20 °C/ 70 °C, 20 ciclos; duração do ensaio: 1 hora a cada temperatura) Pode ser efetuado um conjunto reduzido de ensaios (entre os definidos na secção 3 deste quadro) à temperatura mais baixa, à temperatura mais alta e durante os ciclos de temperatura	
4.4	Proteção contra água e corpos estranhos	Ensaio de acordo com a norma ISO 20653: Road vehicles — Degree of protection (IP code) — Protection of electrical equipment against foreign objects, water and access (valor visado IP40)	220, 221
5	**Ensaios de CEM**		
5.1	Emissões radiadas e suscetibilidade	Conformidade com o Regulamento ECE R10	218
5.2	Descarga eletrostática	Conformidade com a norma ISO 10605:2008 + Retificação técnica: 2010 + AMD1:2014: +/– 4 kV para contacto e +/– 8 kV para descarga de ar	218
5.3	Suscetibilidade do transitório conduzido em relação à alimentação elétrica	Para versões de 24 V: conformidade com a norma ISO 7637-2 + Regulamento ECE n.º 10 Rev. 3: impulso 1a: Vs = – 450 V Ri = 50 ohms impulso 2a: Vs = + 37 V Ri = 2 ohms impulso 2b: Vs = + 20 V Ri = 0,05 ohms impulso 3a: Vs = – 150 V Ri = 50 ohms impulso 3b: Vs = + 150 V Ri = 50 ohms impulso 4: Vs = – 16 V Va = – 12 V t6 = 100 ms impulso 5: Vs = + 120 V Ri = 2,2 ohms td = 250 ms Para versões de 12 V: conformidade com a norma ISO 7637-1 + Regulamento ECE n.º 10 Rev. 3: impulso 1: Vs = – 75 V Ri = 10 ohms impulso 2a: Vs = + 37 V Ri = 2 ohms impulso 2b: Vs = + 10 V Ri = 0,05 ohms impulso 3a: Vs = – 112 V Ri = 50 ohms impulso 3b: Vs = + 75 V Ri = 50 ohms impulso 4: Vs = – 6 V Va = – 5 V t6 = 15 ms impulso 5: Vs = + 65 V Ri = 3 ohms td = 100 ms O ensaio do impulso 5 só é efetuado em unidades-veículo destinadas a veículos sem proteção externa comum contra descarga. Relativamente a propostas de descarga, consultar a norma ISO 16750-2, 4.ª edição, capítulo 4.6.4.	218

▼B

7. ENSAIOS DE FUNCIONALIDADE EM PAPEL

N.º	Ensaio	Descrição	Requisitos correlatos
1.	**Exame administrativo**		
1.1	Documentação	Adequação da documentação	
2	**Ensaios gerais**		
2.1	Número de carateres por linha	Inspeção visual das impressões	172
2.2	Tamanho mínimo do caráter	Inspeção visual da impressão e inspeção do caráter	173
2.3	Conjuntos de carateres aceites	A impressora deve aceitar os carateres indicados no apêndice 1, capítulo 4 «Conjuntos de carateres»	174
2.4	Definição das impressões	Verificação da homologação de tipo do tacógrafo e inspeção visual das impressões	174
2.5	Legibilidade e identificação das impressões	Inspeção das impressões Demonstrada por relatórios e protocolos de ensaio, pelo fabricante Todos os números de homologação de tacógrafos com os quais pode ser utilizado o papel da impressora são impressos no papel	175, 177, 178
2.6	Adição de notas manuscritas	Inspeção visual: Está disponível o campo para assinatura do condutor Estão disponíveis campos para outras notas manuscritas	180
2.7	Pormenores adicionais no rosto do papel	O rosto e o verso do papel podem apresentar pormenores e informações adicionais Estes pormenores e informações adicionais não podem interferir na legibilidade das impressões Inspeção visual	177, 178
3	**Ensaios de memorização**		
3.1	Calor seco	Pré-condicionamento: 16 horas a +23 °C ± 2 °C/55 % ± 3 % de humidade relativa Ambiente de ensaio: 72 horas a +70 °C ± 2 °C Recuperação: 16 horas a + 23 °C ± 2 °C/55 % ± 3 % de humidade relativa	176, 178 IEC 60068-2-2-Bb
2.2	Calor húmido	Pré-condicionamento: 16 horas a + 23 °C ± 2 °C/55 % ± 3 % de humidade relativa Ambiente de ensaio: 144 horas a + 55 °C ± 2 °C e 93 % ± 3 % de humidade relativa Recuperação: 16 horas a + 23 °C ± 2 °C/55 % ± 3 % de humidade relativa	176, 178 IEC 60068-2-78-Cab

▼B

N.º	Ensaio	Descrição	Requisitos correlatos
4	**Ensaios de papel contínuo**		
4.1	Contexto de resistência à humidade (papel não impresso)	Pré-condicionamento: 16 horas a + 23 °C ± 2 °C/55 % ± 3 % de humidade relativa Ambiente de ensaio: 144 horas a + 55 °C ± 2 °C e 93 % ± 3 % de humidade relativa Recuperação: 16 horas a + 23 °C ± 2 °C/55 % ± 3 % de humidade relativa	176, 178 IEC 60068-2-78-Cab
4.2	Capacidade de impressão	Pré-condicionamento: 24 horas a +40 °C ± 2 °C/93 % ±3 % de humidade relativa Ambiente de ensaio: impressão produzida a + 23 °C ± 2 °C Recuperação: 16 horas a + 23 °C ± 2 °C/55 % ± 3 % de humidade relativa	176, 178
4.3	Resistência ao pó	Pré-condicionamento: 16 horas a + 23 °C ± 2 °C/55 % ± 3 % de humidade relativa Ambiente de ensaio: 2 horas a + 70 °C ± 2 °C, calor seco Recuperação: 16 horas a + 23 °C ± 2 °C/55 % ± 3 % de humidade relativa	176, 178 IEC 60068-2-2-Bb
4.4	Resistência a baixas temperaturas	Pré-condicionamento: 16 horas a + 23 °C ± 2 °C/55 % ± 3 % de humidade relativa Ambiente de ensaio: 24 horas – 20 °C ± 3 °C, frio seco Recuperação: 16 horas a + 23 °C ± 2 °C/55 % ± 3 % de humidade relativa	176, 178 ISO 60068-2-1-Ab
4.5	Resistência à luz	Pré-condicionamento: 16 horas a + 23 °C ± 2 °C/55 % ± 3 % de humidade relativa Ambiente de ensaio: 100 horas sob 5 000 Lux de iluminação a + 23 °C ± 2 °C/55 % ± 3 % de humidade relativa Recuperação: 16 horas a + 23 °C ± 2 °C/55 % ± 3 % de humidade relativa	176, 178

Critérios de legibilidade para os ensaios 3.x e 4.x:

A legibilidade da impressão está garantida se as densidades óticas cumprirem os seguintes limites:

Carateres impressos: mín. 1,0

Fundo (papel não impresso): máx. 0,2

As densidades óticas das impressões obtidas devem ser medidas de acordo com a norma DIN EN ISO 534.

As impressões não podem apresentar alterações das dimensões e devem ser bem legíveis.

8. ENSAIOS DE INTEROPERABILIDADE

N.º	Ensaio	Descrição
9.1 Ensaios de interoperabilidade entre unidades-veículo e cartões tacográficos		
1	Autenticação mútua	Verificar se funciona normalmente a autenticação mútua entre a unidade-veículo e o cartão tacográfico

▼B

N.º	Ensaio	Descrição
2	Ensaios de leitura/escrita	Encenar uma atividade típica na unidade-veículo. O cenário deve ser adaptado ao tipo de cartão em ensaio e envolver escritas em tantos EF quantos os possíveis no cartão Por meio de um descarregamento da unidade-veículo, verificar se todos os registos correspondentes foram executados corretamente Por meio de um descarregamento do cartão, verificar se todos os registos correspondentes foram executados corretamente Por meio de impressões diárias, verificar se todos os registos correspondentes podem ser lidos corretamente
	9.2 Ensaios de interoperabilidade entre unidades-veículo e sensores de movimento	
1	Emparelhamento	Verificar se funciona normalmente o emparelhamento entre as unidades-veículo e os sensores de movimento
2	Ensaios de atividade	Encenar uma atividade típica no sensor de movimento. O cenário deve implicar uma atividade normal e criar tantos incidentes ou falhas quantos os possíveis. Por meio de um descarregamento da unidade-veículo, verificar se todos os registos correspondentes foram executados corretamente Por meio de um descarregamento do cartão, verificar se todos os registos correspondentes foram executados corretamente Por meio de uma impressão diária do cartão, verificar se todos os registos correspondentes podem ser lidos corretamente
	9.3 Ensaios de interoperabilidade entre as unidades-veículo e os módulos GNSS externos (quando aplicável)	
1	Autenticação mútua	Verificar se funciona normalmente a autenticação mútua (acoplamento) entre a unidade-veículo e o módulo GNSS externo.
2	Ensaios de atividade	Executar um cenário de atividade típica com o GNSS externo. O cenário deve envolver uma atividade normal e criar tantos incidentes ou falhas quanto possível. Por meio de um descarregamento da unidade-veículo, verificar se todos os registos correspondentes foram executados corretamente. Por meio de um descarregamento do cartão, verificar se todos os registos correspondentes foram executados corretamente. Por meio de uma impressão diária, verificar se todos os registos correspondentes podem ser corretamente lidos.

▼B

Apêndice 10

REQUISITOS DE SEGURANÇA

O presente apêndice especifica os requisitos de segurança de TI para os componentes do sistema tacográfico inteligente (tacógrafo da segunda geração).

SEC_001 Os componentes do sistema tacográfico inteligente a seguir indicados devem ter certificação de segurança, de acordo com o sistema de critérios comuns:

— unidade-veículo

— cartão tacográfico

— sensor de movimentos

— módulo GNSS externo

SEC_002 Os requisitos mínimos de segurança de TI a cumprir por cada componente que exija certificação de segurança devem ser definidos no perfil de proteção do componente, de acordo com o sistema de critérios comuns.

SEC_003 A Comissão Europeia garantirá que quatro perfis de proteção conformes com o presente anexo são patrocinados, desenvolvidos, homologados pelos organismos governamentais de certificação de segurança de TI no âmbito do Grupo de Trabalho Conjunto de Interpretação (JIWG) que apoia o reconhecimento mútuo de certificados sob a égide do SOGIS-MRA europeu (Acordo sobre o Reconhecimento Mútuo dos Certificados de Avaliação de Segurança da Tecnologia da Informação) e registados:

— perfil de proteção para unidade-veículo

— perfil de proteção para cartão tacográfico

— perfil de proteção para sensor de movimentos

— perfil de proteção para módulo GNSS externo

O perfil de proteção para a unidade-veículo deve abordar as situações em que a VU é concebida para ser utilizada ou não com um módulo GNSS externo. Os requisitos de segurança do módulo GNSS externo são fornecidos no perfil de proteção dedicado.

SEC_004 Os fabricantes de componentes devem aperfeiçoar e completar o perfil de proteção adequado dos componentes na medida do necessário, sem alterarem ou eliminarem eventuais ameaças, objetivos, meios de procedimento ou especificações de funções de concretização da segurança, a fim de elaborar objetivos de segurança relativamente aos quais podem pedir a certificação de segurança do componente.

SEC_005 Durante o processo de avaliação, deve indicar-se a conformidade estrita dos objetivos de segurança específicos com o correspondente perfil de proteção.

SEC_006 O nível de garantia para cada perfil de proteção é EAL4 aumentado pelos componentes de garantia ATE_DPT.2 e AVA_VAN.5.

▼B

Apêndice 11

MECANISMOS COMUNS DE SEGURANÇA

ÍNDICE

▼B

▼B

▼B

PREÂMBULO

O presente apêndice especifica os mecanismos de segurança que garantem:

— autenticação mútua entre os diversos componentes do sistema tacográfico

— confidencialidade, integridade, autenticidade e/ou não-repúdio de dados transferidos entre os diversos componentes do sistema tacográfico ou descarregados para meios externos de memorização.

O presente apêndice é constituído por duas partes: a parte A define os mecanismos de segurança para o sistema tacográfico da primeira geração (tacógrafo digital); a parte B define os mecanismos de segurança para o sistema tacográfico da segunda geração (tacógrafo inteligente).

Aplicam-se os mecanismos previstos na parte A do presente apêndice se, pelo menos, um dos componentes do sistema tacográfico envolvido numa autenticação mútua e/ou num processo de transferência de dados for da primeira geração.

Aplicam-se os mecanismos previstos na parte B se, pelo menos, um dos componentes do sistema tacográfico envolvido na autenticação mútua e/ou no processo de transferência de dados for da segunda geração.

O apêndice 15 fornece mais informações sobre a utilização de componentes da primeira geração em combinação com componentes da segunda geração.

PARTE A

SISTEMA TACOGRÁFICO DA PRIMEIRA GERAÇÃO

1. INTRODUÇÃO

1.1. **Referências**

No presente apêndice, utilizam-se as seguintes referências:

SHA-1	National Institute of Standards and Technology (Instituto Nacional de Normas e Tecnologia, NIST). *FIPS Publication 180-1: Secure Hash Standard*. Abril de 1995.
PKCS1	RSA Laboratories. PKCS # 1: *RSA Encryption Standard*. Versão 2.0. Outubro de 1998.
TDES	National Institute of Standards and Technology (NIST). *FIPS Publication 46-3: Data Encryption Standard*. Projeto 1999.
TDES-OP	ANSI X9.52, Triple Data Encryption Algorithm Modes of Operation (Modos de Funcionamento do Algoritmo Triplo de Criptagem dos Dados). 1998.
ISO/IEC 7816-4	Information Technology — Identification cards — Integrated circuit(s) cards with contacts — Part 4: Interindustry commands for interexchange. First edition: 1995 + Amendment 1: 1997.
ISO/IEC 7816-6	Information Technology — Identification cards — Integrated circuit(s) cards with contacts — Part 6: Interindustry data elements. First edition: 1996 + Cor 1: 1998.
ISO/IEC 7816-8	Information Technology — Identification cards — Integrated circuit(s) cards with contacts — Part 8: Security related interindustry commands. First edition 1999.
ISO/IEC 9796-2	Information Technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Mechanisms using a hash function. First edition: 1997.

▼B

ISO/IEC 9798-3	Information Technology — Security techniques — Entity authentication mechanisms — Part 3: Entity authentication using a public key algorithm. Second edition 1998.
ISO 16844-3	Road vehicles — Tachograph systems — Part 3: Motion sensor interface.

1.2. **Notações e abreviaturas**

No presente apêndice, utilizam-se as seguintes notações e abreviaturas:

(K_a, K_b, K_c)	feixe de chaves utilizado pelo algoritmo triplo de criptagem dos dados
CA	autoridade de certificação
CAR	referência da autoridade de certificação
CC	soma criptográfica de teste
CG	criptograma
CH	cabeçalho de comando
CHA	autorização do titular do certificado
CHR	referência do titular do certificado
D()	decifragem com DES (Data Encryption Standard)
DE	elemento de dados
DO	objeto de dados
d	chave privada/expoente privado RSA
e	chave pública/expoente público RSA
E()	criptagem com DES
EQT	equipamento
Hash()	valor Hash, saído de *Hash*
Hash	função hash
KID	identificador de chave
Km	chave TDES (chave de segurança definida na norma ISO 16844-3)
Km_{VU}	chave TDES inserida em unidades-veículo
Km_{WC}	chave TDES inserida em cartões de oficina
m	representante de mensagem (número inteiro entre 0 e *n*-1)
n	chaves RSA, módulo
PB	bytes de preenchimento
PI	byte indicador de preenchimento (utilizado em criptograma para DO de confidencialidade)
PV	valor simples (direto)
s	representante de assinatura (número inteiro entre 0 e *n*-1)
SSC	contador de sequências de envio
SM	segurança do envio de mensagens (envio seguro de mensagens)
TCBC	modo de funcionamento do TDEA (ver TDEA) por cifragem progressiva

▼B

TDEA	algoritmo triplo de criptagem dos dados
TLV	valor do comprimento de um marcador
VU	unidade-veículo
X.C	certificado do utilizador X, emitido por uma autoridade de certificação
X.CA	autoridade de certificação do utilizador X
X.CA.PK $_{o}$ X.C	operação de revelação de um certificado para extrair uma chave pública; trata-se de um operador infixo, cujo operando esquerdo é a chave pública de uma autoridade de certificação e cujo operando direito é o certificado emitido por essa autoridade de certificação; como resultado, obtém-se a chave pública do utilizador X, cujo certificado é o operando direito
X.PK	chave pública RSA de um utilizador X
X.PK[I]	cifragem RSA de informações I, utilizando a chave pública do utilizador X
X.SK	chave privada RSA de um utilizador X
X.SK[I]	cifragem RSA de informações I, utilizando a chave privada do utilizador X
'xx'	valor hexadecimal
||	operador de concatenação.

2. SISTEMAS E ALGORITMOS CRIPTOGRÁFICOS

2.1. **Sistemas criptográficos**

CSM_001 As unidades-veículo (VU) e os cartões tacográficos utilizam um sistema criptográfico clássico de chave pública RSA para obtenção dos seguintes mecanismos de segurança:

— autenticação mútua entre VU e cartões

— encaminhamento de chaves triplas de sessão DES entre VU e cartões tacográficos

— assinatura digital de dados descarregados das VU ou dos cartões tacográficos para meios de memorização externos.

CSM_002 As unidades-veículo e os cartões tacográficos utilizam um sistema criptográfico simétrico DES triplo para obtenção de um mecanismo de integridade dos dados durante o intercâmbio deles entre VU e cartões tacográficos e, se necessário, para obtenção de confidencialidade nesse intercâmbio.

2.2. **Algoritmos criptográficos**

2.2.1 *Algoritmo RSA*

CSM_003 O algoritmo RSA é plenamente definido pelas seguintes relações:

▼B

$$X.SK[m] = s = m^d \bmod n$$

$$X.PK[s] = m = s^e \bmod n$$

A referência PKCS1 contém uma descrição mais completa da função RSA. No cálculo desta função, o expoente público «e» é um inteiro entre 3 e n-1 que satisfaz a condição gcd(e, lcm(p-1, q-1))=1.

2.2.2 *Algoritmo hash*

CSM_004 Os mecanismos de assinatura digital utilizam o algoritmo Hash SHA-1 definido na referência [SHA-1].

2.2.3 *Algoritmo de criptagem dos dados*

CSM_005 No modo de funcionamento por cifragem progressiva utilizam-se os algoritmos de base DES.

3. CHAVES E CERTIFICADOS

3.1. **Criação e distribuição de chaves**

3.1.1 *Criação e distribuição de chaves RSA*

CSM_006 As chaves RSA são criadas segundo três níveis hierárquicos de funcionamento:

— nível europeu

— nível nacional (nível do Estado-Membro)

— nível do equipamento ou aparelho.

CSM_007 A nível europeu, é criado um único par de chaves (EUR.SK e EUR.PK). Utiliza-se a chave privada europeia para certificar as chaves públicas dos Estados-Membros. Devem ser mantidos registos de todas as chaves certificadas. Estas funções são asseguradas por uma autoridade europeia de certificação, sob a autoridade e responsabilidade da Comissão Europeia.

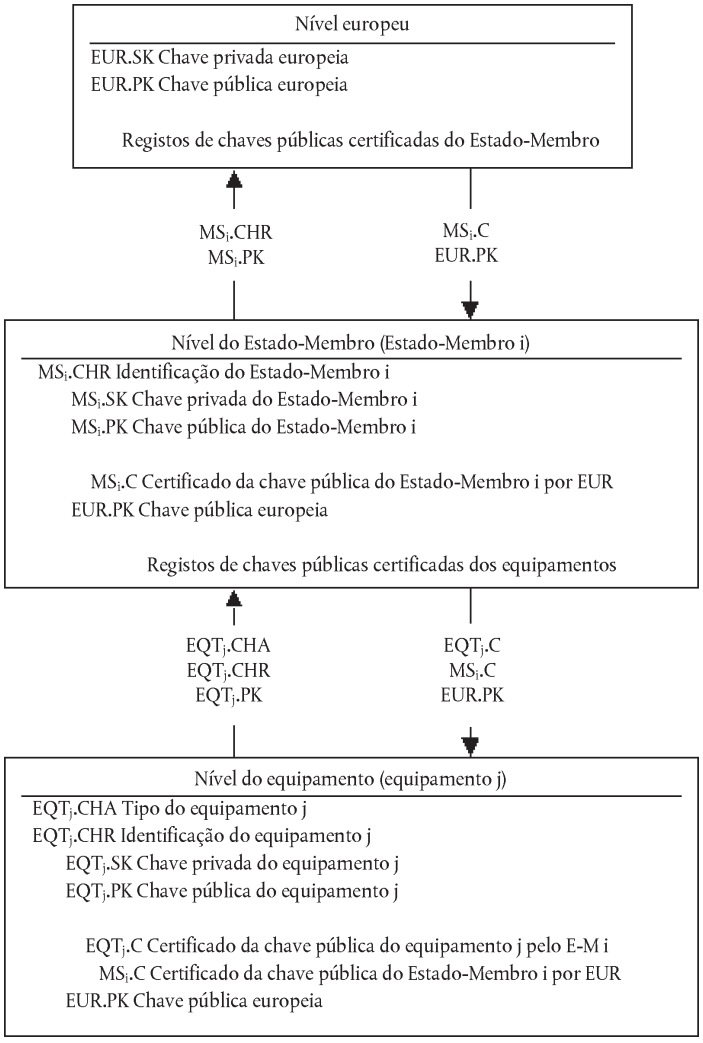
CSM_008 A nível nacional, é criado um par de chaves (MS.SK e MS.PK) para cada Estado-Membro. A autoridade europeia de certificação certifica as chaves públicas dos Estados-Membros. Utiliza-se a chave privada de um Estado-Membro para certificar as chaves públicas introduzidas no equipamento (VU ou cartão tacográfico). Devem ser mantidos, juntamente com a identificação do equipamento, registos de todas as chaves públicas certificadas que a ele se destinem. Estas funções são asseguradas por uma autoridade nacional de certificação. Os Estados-Membros podem modificar regularmente os seus pares de chaves.

CSM_009 A nível do equipamento, é criado um único par de chaves (EQT.SK e EQT.PK), que se introduz em cada aparelho. A autoridade nacional de certificação certifica as chaves públicas do equipamento. Estas funções podem ser asseguradas por fabricantes ou personalizadores do equipamento ou por autoridades do Estado-Membro. Este par de chaves é utilizado para autenticação, assinatura digital e serviços de cifragem.

CSM_010 Durante a criação, o eventual encaminhamento e a memorização, deve manter-se a confidencialidade das chaves privadas.

▼B

O quadro seguinte sintetiza o fluxo dos dados neste processo:



3.1.2 *Chaves de ensaio RSA*

CSM_011 Para efeitos de ensaio do equipamento (ensaios de interoperabilidade incluídos), a autoridade europeia de certificação cria um outro par único de chaves europeias de ensaio e pelo menos dois pares de chaves nacionais de ensaio, cujas chaves públicas são certificadas com a chave privada europeia de ensaio. Os fabricantes devem introduzir, no equipamento que é objeto dos ensaios de homologação de tipo, as chaves de ensaio certificadas por uma destas chaves nacionais de ensaio.

3.1.3 *Chaves de sensor de movimentos*

A confidencialidade das três chaves TDES a seguir descritas deve ser adequadamente mantida durante a criação, o eventual encaminhamento e a memorização.

Para que os componentes tacográficos cumpram a norma ISO 16844, as autoridades competentes para a certificação a nível europeu e a nível de cada Estado-Membro devem, complementarmente, assegurar o seguinte:

CSM_036 A autoridade europeia de certificação cria KmVU e KmWC, duas chaves DES triplas independentes e únicas, e cria Km como: $\boxed{Km = Km_{VU} \text{ XOR } Km_{WC}}$. Mediante um procedimento adequadamente securizado, envia seguidamente estas chaves às autoridades de certificação de cada Estado-Membro, a seu pedido.

▼B

CSM_037 A autoridade de certificação de cada Estado-Membro:

— utiliza Km para encriptar dados dos sensores de movimentos pedidos pelos seus fabricantes (esses dados são definidos na norma ISO 16844-3)

— mediante um procedimento adequadamente securizado, envia Km_{VU} aos fabricantes de unidades-veículo, para inserção nestas últimas

— assegura a inserção de Km_{WC} em todos os cartões de oficina (`SensorInstallationSecData` no ficheiro elementar `Sensor_Installation_Data`), durante a personalização do cartão.

3.1.4 *Criação e distribuição de chaves de sessão T-DES*

CSM_012 No âmbito do processo de autenticação mútua, as VU e os cartões tacográficos criam e intercambiam os dados necessários para elaborar uma chave de sessão DES tripla comum. A confidencialidade deste intercâmbio de dados é protegida por meio de um mecanismo de criptagem RSA.

CSM_013 Utiliza-se esta chave em todas as operações criptográficas subsequentes, por meio do envio seguro de mensagens. A sua validade termina no final da sessão (retirada ou reinicialização do cartão) e/ou após 240 utilizações (uma utilização da chave = um comando que utiliza o envio seguro de mensagens, transmitido ao cartão e seguido da correspondente resposta).

3.2. **Chaves**

CSM_014 As chaves RSA (independentemente do nível) têm os seguintes comprimentos: módulo *n* 1 024 bits, expoente público *e* 64 bits no máximo, expoente privado *d* 1 024 bits.

CSM_015 As chaves DES triplas têm a forma (K_a, K_b, K_a), onde K_a e K_b são chaves independentes com o comprimento de 64 bits. Não se repõem bits de deteção de erros de paridade.

3.3. **Certificados**

CSM_016 Os certificados de chaves públicas RSA são «non self-descriptive» («não autodescritivos») e «card verifiable» («verificáveis por cartão») (Ref.: ISO/IEC 7816-8)

3.3.1 *Conteúdo dos certificados*

CSM_017 Os certificados de chaves públicas RSA contêm os seguintes dados, pela ordem indicada:

Dados	Formato	Bytes	Observações
CPI	INTEIRO	1	Identificador de perfil do certificado (‘01’ para esta versão)
CAR	CADEIA DE OCTETOS	8	Referência da autoridade de certificação
CHA	CADEIA DE OCTETOS	7	Autorização do titular do certificado

▼B

Dados	Formato	Bytes	Observações
EOV	TimeReal	4	Prazo de validade do certificado. Opcional. Preenchido com 'FF' se não for utilizado
CHR	CADEIA DE OCTETOS	8	Referência do titular do certificado
n	CADEIA DE OCTETOS	128	Chave pública (módulo)
e	CADEIA DE OCTETOS	8	Chave pública (expoente público)
		164	

Notas:

1. O «identificador de perfil do certificado» (CPI) indica a estrutura exata de um certificado de autenticação. Pode ser utilizado como identificador interno de equipamento da lista de cabeçalho que descreve a concatenação dos elementos informativos contidos no certificado.

   É a seguinte a lista de cabeçalho associada ao conteúdo deste certificado:

'4D'	'16'	'5F 29'	'01'	'42'	'08'	'5F 4B'	'07'	'5F 24'	'04'	'5F 20'	'08'	'7F 49'	'05'	'81'	'81 80'	'82'	'08'
Marcador alargado da lista de cabeçalho	Comprimento da lista de cabeçalho	Marcador CPI	Comprimento CPI	Marcador CAR	Comprimento CAR	Marcador CHA	Comprimento CHA	Marcador EOV	Comprimento EOV	Marcador CHR	Comprimento CHR	Marcador de chave pública (Construído)	Comprimento de DO subsequentes	Marcador do módulo	Comprimento do módulo	Marcador do expoente público	Comprimento do expoente público

2. A «referência da autoridade de certificação» (CAR) destina-se a identificar a autoridade de certificação (CA) emissora do certificado, de modo que o elemento de dados possa ser utilizado ao mesmo tempo como identificador de chave de autoridade para referenciar a chave pública da autoridade de certificação (relativamente à codificação, ver adiante «identificador de chave»).

3. A «autorização do titular do certificado» (CHA) destina-se a identificar os direitos do titular do certificado. Consiste no ID de aplicação do tacógrafo e no tipo de equipamento a que se refere o certificado (consoante o elemento de dados `EquipmentType`, «00» para um Estado-Membro).

▼B

4. A «referência do titular do certificado» (CHR) destina-se a identificar como único o titular do certificado, de modo que o elemento de dados possa ser utilizado ao mesmo tempo como identificador de chave de objeto para referenciar a chave pública do titular do certificado.

5. Os identificadores de chave identificam como únicos os titulares de certificados e as autoridades de certificação. É a seguinte a sua codificação:

5.1. Equipamento (VU ou cartão):

Dados	Número de série do equipamento	Data	Tipo	Fabricante
Comprimento	4 bytes	2 bytes	1 byte	1 byte
Valor	Número inteiro	Codificação BCD mm aa	Específico do fabricante	Código do fabricante

Tratando-se de uma VU, o fabricante, ao requerer um certificado, pode conhecer ou não a identificação do aparelho no qual as chaves serão inseridas.

Se a conhecer, o fabricante transmite a identificação do aparelho, juntamente com a chave pública, à autoridade de certificação competente do Estado-Membro. Deste modo, o certificado conterá a identificação do aparelho, e o fabricante deve garantir que as chaves e o certificado são inseridos no aparelho a que se destinam. O identificador de chave tem a forma atrás indicada.

Se não conhecer a identificação do aparelho, o fabricante deve identificar como único cada pedido de certificado, enviando essa identificação, juntamente com a chave pública, à autoridade de certificação competente do Estado-Membro. Deste modo, o certificado conterá a identificação do pedido. Após a instalação da chave no equipamento, o fabricante deve informar o Estado-Membro competente sobre os elementos de atribuição de chave ao equipamento (ou seja, identificação do pedido de certificado e identificação do aparelho). O identificador de chave tem a seguinte forma:

Dados	Número de série do pedido de certificado	Data	Tipo	Fabricante
Comprimento	4 bytes	2 bytes	1 byte	1 byte
Valor	Número inteiro	Codificação BCD mm aa	‘FF’	Código do fabricante

▼B

5.2 Autoridade de certificação:

Dados	Identificação da autoridade	Número de série da chave	Informações adicionais	Identificador
Comprimento	4 bytes	1 byte	2 bytes	1 byte
Valor	Código numérico nacional, 1 byte Código alfanumérico nacional, 3 bytes	Número inteiro	Codificação adicional (específico da CA) 'FF FF' se não houver utilização	'01'

O número de série serve para distinguir as diversas chaves de um Estado-Membro, na eventualidade de mudança de chave.

6. Os verificadores de certificados sabem, implicitamente, que a chave pública certificada é uma chave RSA destinada à autenticação e à verificação e cifragem da assinatura digital, para efeitos de confidencialidade (o certificado não contém qualquer identificador de objeto que o especifique).

3.3.2 *Certificados emitidos*

CSM_018 O certificado emitido é uma assinatura digital com recuperação parcial do conteúdo do certificado, nos termos da norma ISO/IEC 9796-2 (com exceção do seu anexo A4), tendo apensa a «referência da autoridade de certificação».

$$X.C = X.CA.SK[\text{'6A'} \parallel C_r \parallel \mathit{Hash}(Cc) \parallel \text{'BC'}] \parallel C_n \parallel X.CAR$$

Com conteúdo de certificado = Cc = C_r || C_n

106 bytes 58 bytes

Notas:

1. Este certificado tem 194 bytes de comprimento.
2. A CAR oculta pela assinatura é também apensa a esta, de modo a que a chave pública da autoridade de certificação possa ser selecionada para a verificação do certificado.
3. O verificador conhece, implicitamente, o algoritmo utilizado pela autoridade de certificação para assinar o certificado.
4. É a seguinte a lista de cabeçalho associada a este certificado emitido:

'7F 21'	'09'	'5F 37'	'81 80'	'5F 38'	'3A'	'42'	'08'
Marcador do certificado CV (construído)	Comprimento de DO subsequentes	Marcador da assinatura	Comprimento da assinatura	Marcador do remanescente	Comprimento do remanescente	Marcador da CAR	Comprimento da CAR

▼B

3.3.3 *Verificação e revelação de certificados*

A verificação e a revelação de um certificado consistem em verificar se a assinatura obedece à norma ISO/IEC 9796-2, extraindo o conteúdo do certificado e a chave pública contida: X.PK = X.CA.PK $_{o}$ X.C, e verificando a validade do certificado.

CSM_019 Esta operação inclui os seguintes passos:

Verificação da assinatura e extração do conteúdo:

— de X.C, extrair Sign, C_n 'e CAR': X.C = Sign (128 bytes) || C_n' (58 bytes) || CAR' (8 bytes)

— a partir de CAR', selecionar a pertinente chave pública da autoridade de certificação (se tal não tiver sido feito antes por outros meios)

— abrir Sign com a chave pública do CA: Sr'= X.CA.PK [Sign],

— verificar se Sr' começa por '6A' e termina por 'BC'

— calcular C_r' e H' a partir de: Sr' = '6A' || C_r' (106 bytes) || H' (20 bytes) || 'BC'

— recuperar o conteúdo do certificado C' = C_r' C_n',

— verificar *Hash*(C') = H'

Se todas as verificações conferirem, o certificado é genuíno e o seu conteúdo é C'.

Verificar validade. A partir de C':

— se for o caso, verificar a data de expiração da validade.

De C', extrair e memorizar a chave pública, o identificador da chave, a autorização do titular do certificado e a data de expiração da validade do certificado:

— X.PK = n || e

— X.KID = CHR

— X.CHA = CHA

— X.EOV = EOV

4. MECANISMO DE AUTENTICAÇÃO MÚTUA

A autenticação mútua entre cartões e unidades-veículo baseia-se no seguinte princípio:

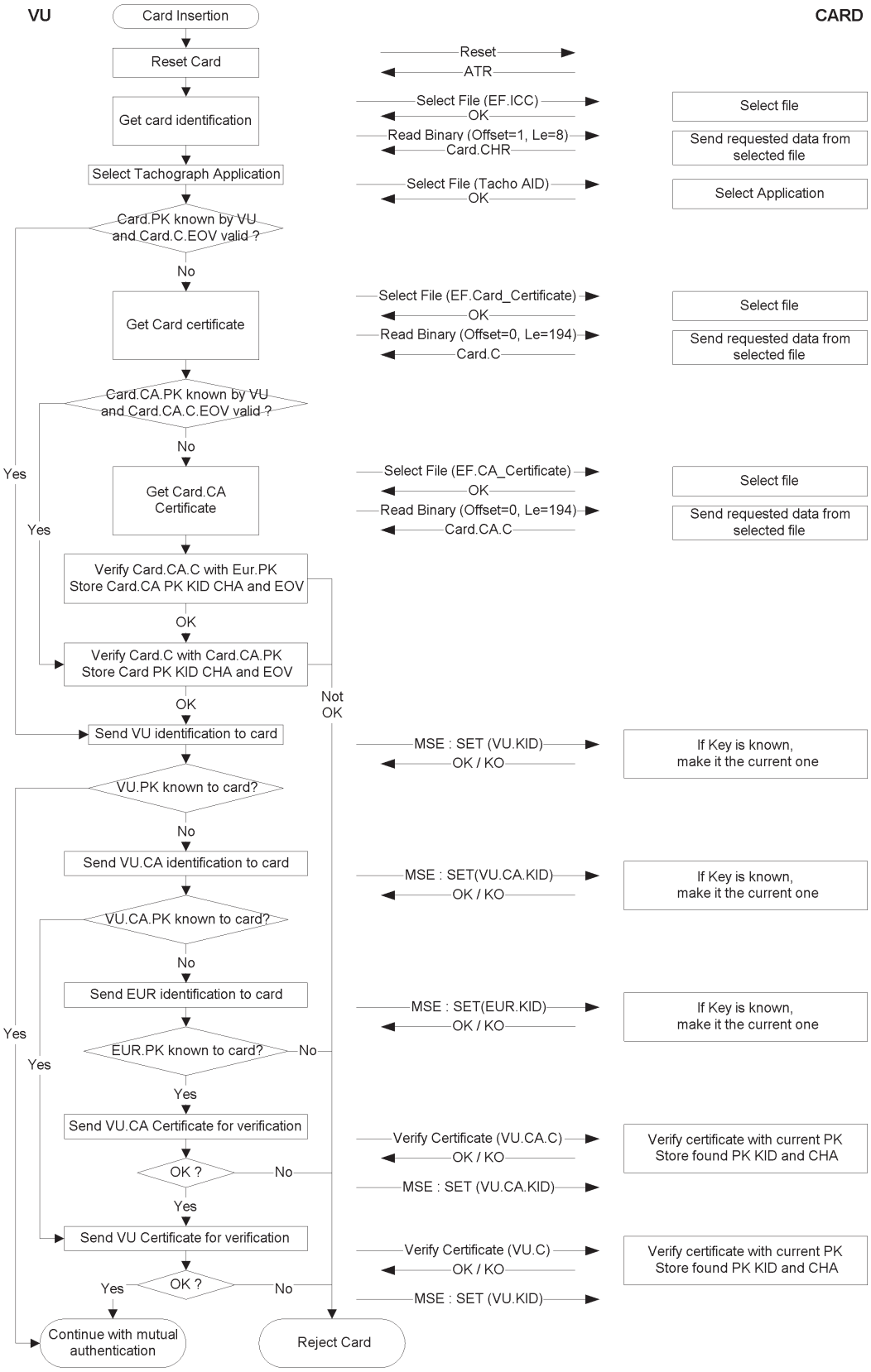
Cada parte demonstra à outra parte que possui um par válido de chaves, no qual a chave pública foi certificada pela autoridade de certificação competente do Estado-Membro, por sua vez certificado pela autoridade de certificação europeia.

A demonstração é feita assinando com a chave privada um número aleatório enviado pela outra parte, a qual recupera esse número quando verifica esta assinatura.

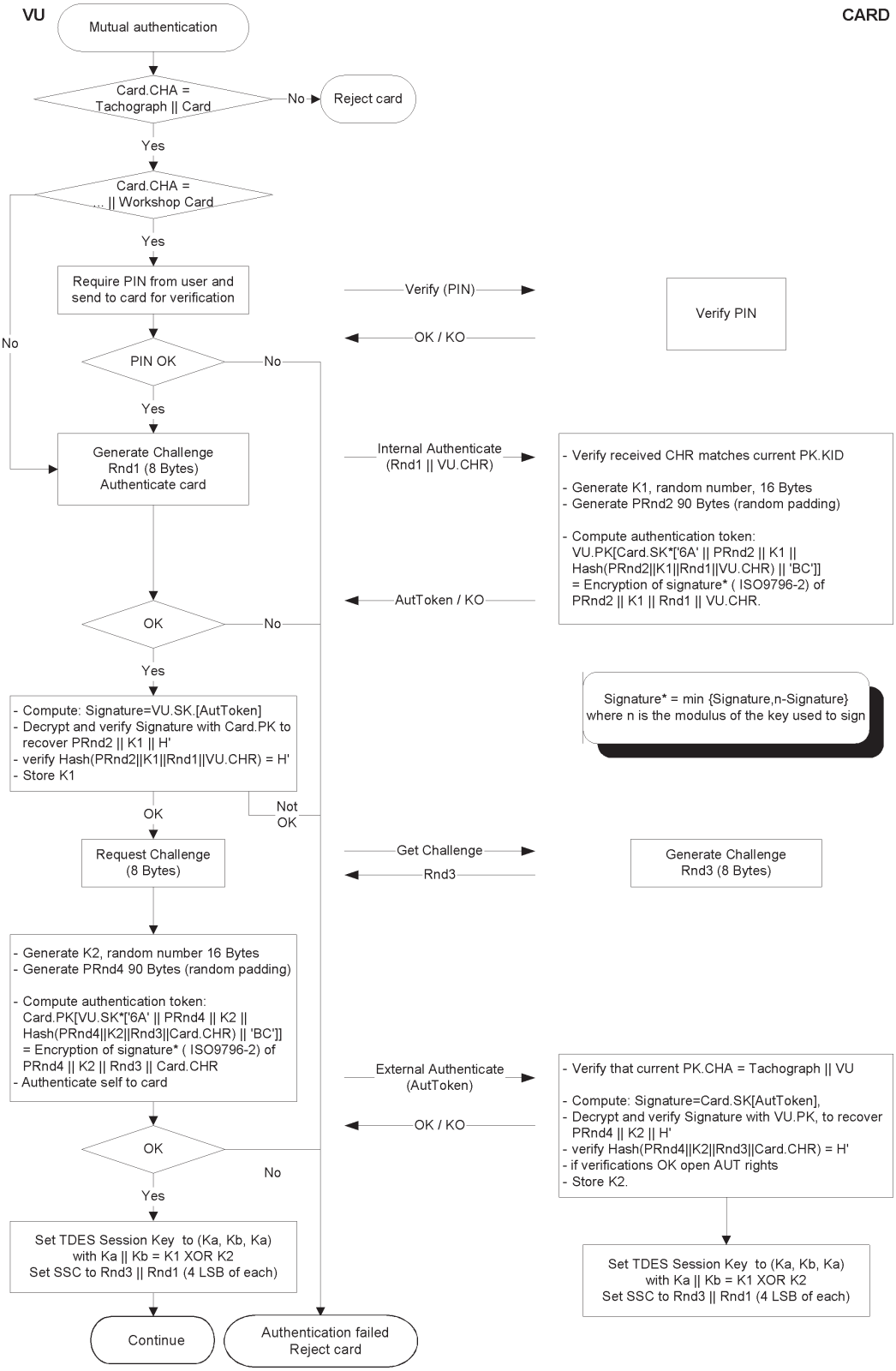
O mecanismo é desencadeado pela VU logo que haja inserção de um cartão. Inicia-se com o intercâmbio de certificados e a revelação das chaves públicas e termina com o estabelecimento de uma chave de sessão.

▼B

CSM_020 Utiliza-se o seguinte protocolo (as setas indicam comandos e dados intercambiados — ver apêndice 2):



▼B


VU
CARD
Mutual authentication
Card.CHA = Tachograph || Card
No
Reject card
Yes
Card.CHA = ... || Workshop Card
Yes
Require PIN from user and send to card for verification
Verify (PIN)
Verify PIN
OK / KO
No
PIN OK
No
Yes
Generate Challenge Rnd1 (8 Bytes) Authenticate card
Internal Authenticate (Rnd1 || VU.CHR)
- Verify received CHR matches current PK.KID
- Generate K1, random number, 16 Bytes
- Generate PRnd2 90 Bytes (random padding)
- Compute authentication token: VU.PK[Card.SK*['6A' || PRnd2 || K1 || Hash(PRnd2||K1||Rnd1||VU.CHR) || 'BC']] = Encryption of signature* (ISO9796-2) of PRnd2 || K1 || Rnd1 || VU.CHR.
AutToken / KO
OK
No
Yes
Signature* = min {Signature,n-Signature} where n is the modulus of the key used to sign
- Compute: Signature=VU.SK.[AutToken]
- Decrypt and verify Signature with Card.PK to recover PRnd2 || K1 || H'
- verify Hash(PRnd2||K1||Rnd1||VU.CHR) = H'
- Store K1
Not OK
OK
Request Challenge (8 Bytes)
Get Challenge
Rnd3
Generate Challenge Rnd3 (8 Bytes)
- Generate K2, random number 16 Bytes
- Generate PRnd4 90 Bytes (random padding)
- Compute authentication token: Card.PK[VU.SK*['6A' || PRnd4 || K2 || Hash(PRnd4||K2||Rnd3||Card.CHR) || 'BC']] = Encryption of signature* (ISO9796-2) of PRnd4 || K2 || Rnd3 || Card.CHR
- Authenticate self to card
External Authenticate (AutToken)
- Verify that current PK.CHA = Tachograph || VU
- Compute: Signature=Card.SK[AutToken],
- Decrypt and verify Signature with VU.PK, to recover PRnd4 || K2 || H'
- verify Hash(PRnd4||K2||Rnd3||Card.CHR) = H'
- if verifications OK open AUT rights
- Store K2.
OK / KO
OK
No
Yes
Set TDES Session Key to (Ka, Kb, Ka) with Ka || Kb = K1 XOR K2
Set SSC to Rnd3 || Rnd1 (4 LSB of each)
Set TDES Session Key to (Ka, Kb, Ka) with Ka || Kb = K1 XOR K2
Set SSC to Rnd3 || Rnd1 (4 LSB of each)
Continue
Authentication failed Reject card

▼B

5. MECANISMOS DE CONFIDENCIALIDADE, INTEGRIDADE E AUTENTICAÇÃO NA TRANSFERÊNCIA DE DADOS ENTRE VU E CARTÕES

5.1. **Envio seguro de mensagens**

CSM_021 A integridade das transferências de dados entre as VU e os cartões é protegida mediante o mecanismo de segurança do envio de mensagens, em conformidade com as normas ISO/ /IEC 7816-4 e ISO/IEC 7816-8.

CSM_022 Se for necessário proteger os dados durante a transferência, apensa-se um objeto de dados «soma criptográfica de controlo», incorporado no comando ou na resposta, aos objetos de dados enviados. A soma criptográfica de controlo é verificada pelo recetor.

CSM_023 A soma criptográfica de controlo dos dados enviados integra o cabeçalho do comando no qual é incorporada e todos os objetos de dados enviados (=>CLA = '0C' e todos os objetos de dados devem ser encapsulados com marcadores nos quais b1 = 1).

CSM_024 Os bytes de informação sobre a situação da resposta são protegidos por uma soma criptográfica de controlo se a resposta não contiver campo de dados.

CSM_025 As somas criptográficas de controlo têm 4 bytes de comprimento.

Se se recorrer ao envio seguro de mensagens, a estrutura dos comandos e das respostas 'r, portanto, a seguinte:

Os DO (objetos de dados) utilizados são um subconjunto dos DO de envio seguro de mensagens referidos na norma ISO/ /IEC 7816-4:

Marcador	Mnemónica	Significado
'81'	T_{PV}	Valor simples não codificado em BER-TLV (a proteger por CC)
'97'	$\mathbf{T_{LE}}$	Valor de Le no comando não seguro (a proteger por CC)
'99'	T_{SW}	Informação sobre situação (a proteger por CC)
'8E'	T_{CC}	Soma criptográfica de teste
'87'	$T_{PI\ CG}$	Criptograma do byte indicador de preenchimento || (valor simples não codificado em BER-TLV)

▼B

Dado um par de resposta a um comando não seguro:

Cabeçalho do comando				Corpo do comando		
CLA	INS	P1	P2	[Campo L_c]	[Campo de dados]	[Campo L_e]
quatro bytes				bytes L, indicados de B_1 a B_L		

Corpo da resposta	Indicador de fim da resposta	
[Campo de dados]	SW1	SW2
bytes dos dados L_r	dois bytes	

É o seguinte o correspondente par de resposta de comando seguro:

Comando seguro:

Cabeçalho do comando (CH)				Corpo do comando										
CLA	INS	P1	P2	[Novo campo L_c]	[Novo campo de dados]									[Novo campo L_e]
‘OC’				Comprimento do novo campo de dados	T_{PV}	L_{PV}	PV	T_{LE}	L_{LE}	L_e	T_{CC}	L_{CC}	CC	‘00’
					‘81’	L_c	Campo de dados	‘97’	‘01’	L_e	‘8E’	‘04’	CC	

Dados a integrar na soma de teste = CH || PB || T_{PV} || L_{PV} || PV || T_{LE} || L_{LE} || L_e || PB

PB = Bytes de preenchimento (80 .. 00), segundo as normas ISO/IEC 7816-4 e ISO 9797 e método 2.

Os objetos de dados PV e LE estão presentes somente se houver dados correspondentes no comando não seguro.

Resposta segura:

1. Caso em que o campo de dados da resposta não está vazio e não precisa de ser protegido para efeitos de confidencialidade:

Corpo da resposta						Indicador de fim da resposta
[Novo campo de dados]						Novo SW1 SW2
T_{PV}	L_{PV}	PV	T_{CC}	L_{CC}	CC	
‘81’	L_r	Campo de dados	‘8E’	‘04’	CC	

Dados a integrar na soma de teste = T_{PV} || L_{PV} || PV || PB

2. Caso em que o campo de dados da resposta não está vazio e precisa de ser protegido para efeitos de confidencialidade:

▼B

Corpo da resposta						Indicador de fim da resposta
[Novo campo de dados]						Novo SW1 SW2
$T_{PI\ CG}$	$L_{PI\ CG}$	PI CG	T_{CC}	L_{CC}	CC	
'87'		PI ‖ CG	'8E'	'04'	CC	

Dados a executar por CG: dados não codificados em BER-TLV e bytes de preenchimento.

Dados a integrar na soma de teste = $T_{PI\ CG}$ ‖ $L_{PI\ CG}$ ‖ PI CG ‖ PB

3. Caso em que o campo de dados da resposta está vazio:

Corpo da resposta						Indicador de fim da resposta
[Novo campo de dados]						Novo SW1 SW2
T_{SW}	L_{SW}	SW	T_{CC}	L_{CC}	CC	
'99'	'02'	Novo SW1 SW2	'8E'	'04'	CC	

Dados a integrar na soma de teste = T_{SW} ‖ L_{SW} ‖ SW ‖ PB

5.2. **Tratamento de erros no envio seguro de mensagens**

CSM_026 Quando, ao interpretar um comando, o cartão tacográfico reconhece um erro de SM, os bytes de situação («status bytes») devem ser devolvidos sem SM. Nos termos da norma ISO/IEC 7816-4, definem-se os seguintes bytes de situação para indicar erros de SM:

'66 88': Falha na verificação da soma criptográfica de teste

'69 87': Ausência de objetos de dados SM esperados

'69 88': Incorreção dos objetos de dados SM.

CSM_027 Se o cartão tacográfico devolver bytes de situação sem DO de SM ou com um DO de SM errado, a sessão deve ser interrompida pela VU.

5.3. **Algoritmo para calcular somas criptográficas de teste**

CSM_028 As somas criptográficas de teste são constituídas com recurso a um controlo de acesso ao meio (MAC) pormenorizado, nos termos da norma ANSI X9.19 com DES:

— fase de arranque: o bloco inicial de verificação y0 é E(Ka, SSC)

— fase sequencial: os blocos de verificação y1, .., Yn são calculados mediante a utilização de Ka

— fase final: a soma criptográfica de teste é calculada com base no último bloco de verificação yn, do seguinte modo: E(Ka, D(Kb, yn)),

onde E() representa a criptagem com DES, e D() a decifragem com DES.

Os quatro bytes mais significativos da soma criptográfica de teste são transferidos.

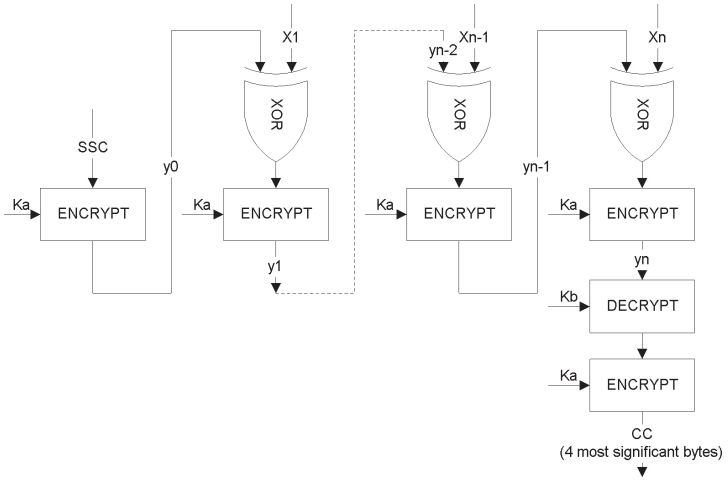
▼B

CSM_029 O contador de sequências de envio (SSC) é iniciado durante o processo de concordância de chaves:

SSC inicial: Rnd3 (4 bytes menos significativos) || Rnd1 (4 bytes menos significativos).

CSM_030 O contador de sequências de envio é acrescido de uma unidade antes de cada MAC ser calculado (ou seja, o SSC para o primeiro comando é SSC inicial + 1, o SSC para a primeira resposta é SSC inicial + 2).

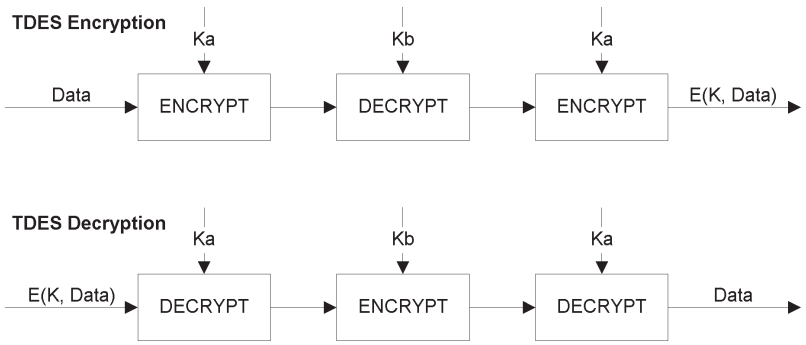
O esquema seguinte representa o cálculo do MAC pormenorizado:



5.4. **Algoritmo para o cálculo de criptogramas para DO de confidencialidade**

CSM_031 Os criptogramas são calculados utilizando o TDEA no modo de funcionamento TCBC, em conformidade com as referências TDES e TDES-OP e com o vetor nulo como bloco de valor inicial.

O esquema seguinte representa a aplicação de chaves em TDES:



▼B

6. MECANISMOS DE ASSINATURA DIGITAL DO DESCARREGAMENTO DE DADOS

CSM_032 O equipamento dedicado inteligente (IDE) memoriza num ficheiro físico os dados recebidos de um aparelho (VU ou cartão) durante uma sessão de descarregamento. Este ficheiro deve conter os certificados MS_i.C e EQT.C. Contém as assinaturas digitais de blocos de dados, em conformidade com o apêndice 7 (protocolos aplicáveis ao descarregamento de dados).

CSM_033 As assinaturas digitais dos dados descarregados utilizam um esquema de assinatura digital com apêndice, de modo a que os dados descarregados possam, se necessário, ser lidos sem decifragem.

6.1. **Criação da assinatura**

CSM_034 A criação da assinatura dos dados pelo equipamento obedece ao esquema de assinatura digital com apêndice, definido na referência PKCS1, com a função hash SHA-1:

Assinatura = EQT.SK[‘00’ || ‘01’ || *PS* || ‘00’ || DER(SHA-1 (dados))]

PS = Cadeia de octetos de preenchimento com valor ‘FF’ tal que o comprimento é 128.

DER(SHA-1(*M*)) é a codificação do algoritmo ID para a função hash e o valor hash num valor ASN.1 do tipo DigestInfo (regras distintas de codificação):

‘30’||‘21’||‘30’||‘09’||‘06’||‘05’||‘2B’||‘0E’||‘03’||‘02’||‘1A’|| ‘05’||‘00’||‘04’||‘14’||valor Hash.

6.2. **Verificação da assinatura**

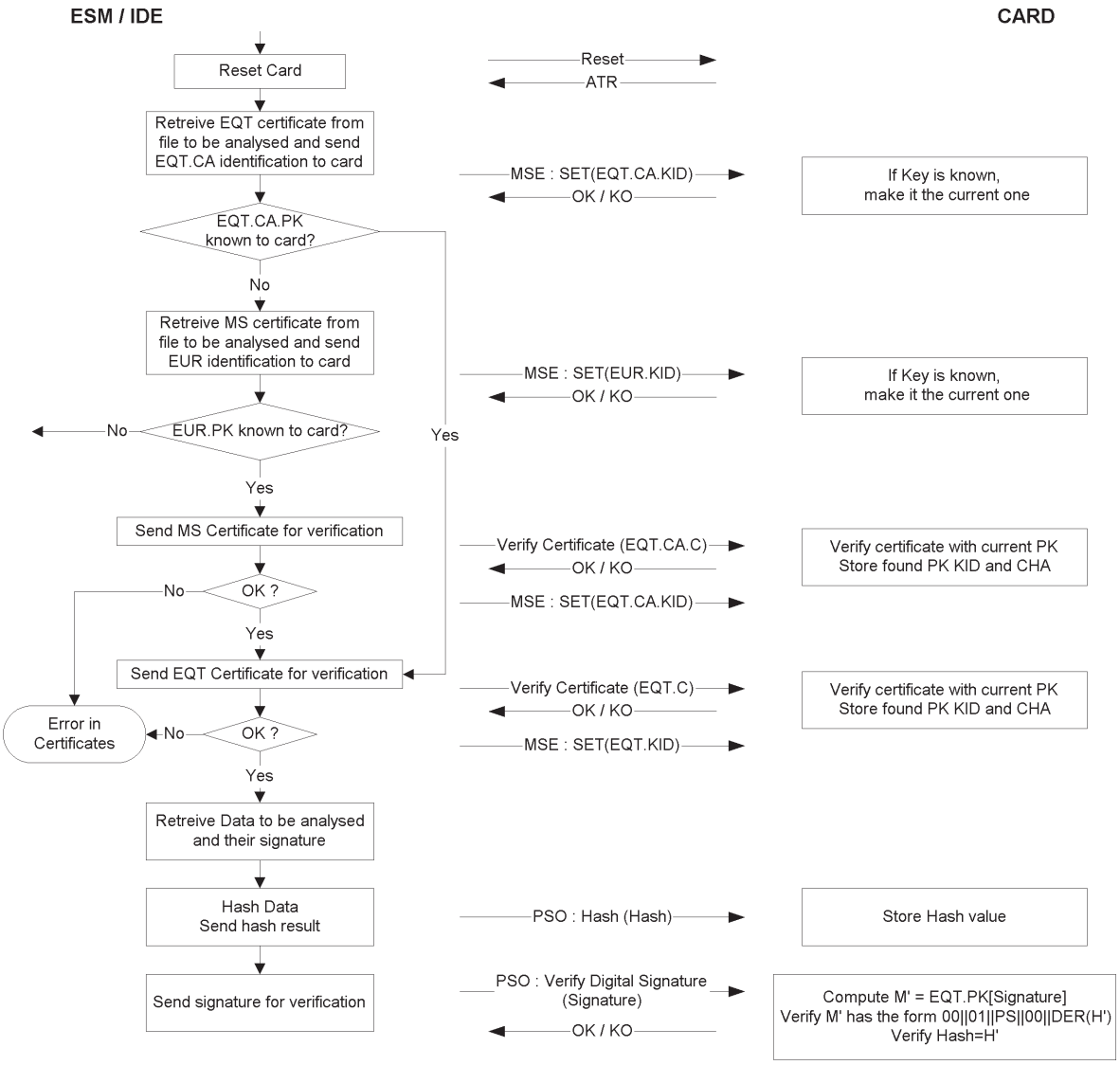
CSM_035 A verificação da assinatura relativa a dados descarregados obedece ao esquema de assinatura com apêndice definido na referência PKCS1, com a função hash SHA-1.

A chave pública europeia EUR.PK tem de ser conhecida (e aprovada) independentemente pelo verificador.

O diagrama seguinte ilustra o protocolo que um IDE com cartão de controlo pode seguir para verificar a integridade dos dados descarregados e memorizados nos ESM (meios externos de memorização). O cartão de controlo é utilizado para a decifragem das assinaturas digitais. Em tal caso, esta função pode não ser executada no IDE.

O equipamento que descarregou e assinou os dados a analisar é designado EQT.

▼B



PARTE B

SISTEMA TACOGRÁFICO DA SEGUNDA GERAÇÃO

7. INTRODUÇÃO

7.1. **Referências**

Nesta parte do presente apêndice, utilizam-se as seguintes referências:

AES	National Institute of Standards and Technology (NIST), FIPS PUB 197: Advanced Encryption Standard (AES), November 26, 2001
DSS	National Institute of Standards and Technology (NIST), FIPS PUB 186-4: Digital Signature Standard (DSS), July 2013
ISO 7816-4	ISO/IEC 7816-4, Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange. Third edition 2013-04-15
ISO 7816-8	ISO/IEC 7816-8, Identification cards — Integrated circuit cards — Part 8: Commands for security operations. Second edition 2004-06-01

▼B

ISO 8825-1	ISO/IEC 8825-1, Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER). Fourth edition, 2008-12-15
ISO 9797-1	ISO/IEC 9797-1, Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher. Second edition, 2011-03-01
ISO 10116	ISO/IEC 10116, Information technology — Security techniques — Modes of operation of an *n*-bit block cipher. Third edition, 2006-02-01
ISO 16844-3	ISO/IEC 16844-3, Road vehicles — Tachograph systems — Part 3: Motion sensor interface. First edition 2004, including Technical Corrigendum 1 2006
RFC 5480	Elliptic Curve Cryptography Subject Public Key Information, March 2009
RFC 5639	Elliptic Curve Cryptography (ECC) — Brainpool Standard Curves and Curve Generation, 2010
RFC 5869	HMAC-based Extract-and-Expand Key Derivation Function (HKDF), May 2010
SHS	National Institute of Standards and Technology (NIST), FIPS PUB 180-4: Secure Hash Standard, March 2012
SP 800-38B	National Institute of Standards and Technology (NIST), Special Publication 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, 2005
TR-03111	BSI Technical Guideline TR-03111, Elliptic Curve Cryptography, version 2.00, 2012-06-28

7.2. **Notações e abreviaturas**

No presente apêndice, utilizam-se as seguintes notações e abreviaturas:

AES	norma avançada de cifragem
CA	autoridade de certificação
CAR	referência da autoridade de certificação
CBC	modo de funcionamento por cifragem progressiva
CH	cabeçalho de comando
CHA	autorização do titular de um certificado
CHR	referência do titular de um certificado
CV	vetor constante
DER	regras distintas de codificação
DO	objeto de dados
DSRC	comunicações dedicadas de curto alcance
ECC	criptografia de curva elíptica
ECDSA	algoritmo de assinatura digital de curva elíptica
ECDH	curva elíptica Diffie-Hellman (algoritmo de concordância de chaves)
EGF	módulo GNSS externo
EQT	equipamento

▼B

IDE	equipamento dedicado inteligente
K_M	chave de segurança do sensor de movimentos, que permite o emparelhamento de uma unidade-veículo com um sensor de movimentos
K_{M-VU}	chave inserida em unidades-veículo, que permite à VU derivar a chave de segurança do sensor de movimentos caso esteja inserido na VU um cartão de oficina
K_{M-WC}	chave inserida em cartões de oficina, que permite à VU derivar a chave de segurança do sensor de movimentos caso esteja inserido na VU um cartão de oficina
MAC	código de autenticação de mensagem
MoS	sensor de movimentos
MSB	bit mais significativo
PKI	infraestrutura de chave pública
RCF	sistema de comunicação à distância
SSC	contador de sequências de envio
SM	segurança do envio de mensagens (envio seguro de mensagens)
TDES	norma tripla de criptagem dos dados
TLV	valor do comprimento de um marcador
VU	unidade-veículo
X.C	certificado da chave pública do utilizador X
X.CA	autoridade de certificação que emitiu o certificado do utilizador X
X.CAR	referência da autoridade de certificação mencionada no certificado do utilizador X
X.CHR	referência do titular do certificado mencionada no certificado do utilizador X
X.PK	chave pública do utilizador X
X.SK	chave privada do utilizador X
$X.PK_{eph}$	chave pública efémera do utilizador X
$X.SK_{eph}$	chave privada efémera do utilizador X
'xx'	valor hexadecimal
||	operador de concatenação

7.3. **Definições**

As definições dos termos utilizados no presente apêndice figuram no anexo 1C, secção I.

8. SISTEMAS E ALGORITMOS CRIPTOGRÁFICOS

8.1. **Sistemas criptográficos**

CSM_38 As unidades-veículo (VU) e os cartões tacográficos utilizam um sistema criptográfico de chave pública com recurso à curva elíptica para obtenção dos seguintes serviços de segurança:

— autenticação mútua entre uma unidade-veículo e um cartão

▼B

— concordância de chaves de sessão AES entre uma unidade-veículo e um cartão

— garantir a autenticidade, a integridade e o não-repúdio de dados descarregados de unidades-veículo ou cartões tacográficos para meios externos.

CSM_39 As unidades-veículo e os módulos GNSS externos utilizam um sistema criptográfico de chave pública com recurso à curva elíptica para obtenção dos seguintes serviços de segurança:

— acoplamento de uma unidade-veículo e de um módulo GNSS externo

— autenticação mútua entre uma unidade-veículo e um módulo GNSS externo

— concordância de uma chave de sessão AES entre uma unidade-veículo e um módulo GNSS externo.

CSM_40 As unidades-veículo e os cartões tacográficos utilizam um sistema criptográfico simétrico com recurso a AES para obtenção dos seguintes serviços de segurança:

— garantir a autenticidade e a integridade dos dados intercambiados entre uma unidade-veículo e um cartão tacográfico

— se for caso disso, garantir a confidencialidade dos dados intercambiados entre uma unidade-veículo e um cartão tacográfico.

CSM_41 As unidades-veículo e os módulos GNSS externos utilizam um sistema criptográfico simétrico com recurso a AES para obtenção dos seguintes serviços de segurança:

— garantir a autenticidade e a integridade dos dados intercambiados entre uma unidade-veículo e um módulo GNSS externo.

CSM_42 As unidades-veículo e os sensores de movimento utilizam um sistema criptográfico simétrico com recurso a AES para obtenção dos seguintes serviços de segurança:

— emparelhamento de uma unidade-veículo com um sensor de movimentos

— autenticação mútua entre uma unidade-veículo e um sensor de movimentos

— garantir a confidencialidade dos dados intercambiados entre uma unidade-veículo e um sensor de movimentos.

CSM_43 As unidades-veículo e os cartões de controlo utilizam um sistema criptográfico simétrico com recurso a AES para obtenção dos seguintes serviços de segurança na interface de comunicação à distância:

— garantir a confidencialidade, a autenticidade e a integridade dos dados transmitidos de uma unidade-veículo para um cartão de controlo.

Notas:

— Em bom rigor, os dados são transmitidos a partir de uma unidade-veículo para um interrogador à distância, sob a supervisão de um agente de controlo, utilizando um sistema de comunicação à distância que pode ser interno ou externo à VU (ver apêndice 14). No entanto, o interrogador à distância envia os dados recebidos

▼B

para um cartão de controlo, para decifragem e validação da autenticidade. Do ponto de vista da segurança, o sistema de comunicação à distância e o interrogador à distância são completamente transparentes.

— Relativamente à interface DSRC, um cartão de oficina oferece os mesmos serviços de segurança que um cartão de controlo, o que permite a uma oficina validar o funcionamento adequado da interface de comunicação à distância da VU, incluindo a segurança. Consultar a secção 9.2.2 para mais informações.

8.2. **Algoritmos criptográficos**

8.2.1 *Algoritmos simétricos*

CSM_44 Unidades-veículo, cartões tacográficos, sensores de movimentos e módulos GNSS externos aceitam o algoritmo AES definido em [AES], com comprimentos de chave de 128, 192 e 256 bits.

8.2.2 *Parâmetros de domínio normalizados e de algoritmos assimétricos*

CSM_45 Unidades-veículo, cartões tacográficos e módulos GNSS externos aceitam criptografia de curva elíptica com um tamanho de chave de 256, 384 e 512/521 bits.

CSM_46 Unidades-veículo, cartões tacográficos e módulos GNSS externos aceitam o algoritmo de assinatura ECDSA, em conformidade com DSS.

CSM_47 Unidades-veículo, cartões tacográficos e módulos GNSS externos aceitam o algoritmo de concordância de chave ECKA-EG, em conformidade com TR 03111.

CSM_48 Unidades-veículo, cartões tacográficos e módulos GNSS externos aceitam todos os parâmetros de domínio normalizados especificados no quadro 1, de criptografia de curva elíptica.

Quadro 1

Parâmetros de domínio normalizados

Nome	Tamanho (bits)	Referência	Identificador de objeto
NIST P-256	256	[DSS], [RFC 5480]	`secp256r1`
BrainpoolP256r1	256	[RFC 5639]	`brainpoolP256r1`
NIST P-384	384	[DSS], [RFC 5480]	`secp384r1`
BrainpoolP384r1	384	[RFC 5639]	`brainpoolP384r1`
BrainpoolP512r1	512	[RFC 5639]	`brainpoolP512r1`
NIST P-521	521	[DSS], [RFC 5480]	`secp521r1`

▼B

Nota: os identificadores de objeto mencionados na última coluna do quadro 1 são especificados em RFC 5639 para as curvas Brainpool e em RFC 5480 para as curvas NIST.

Exemplo 1: o identificador de objeto da curva BrainpoolP256r1 é: `{iso(1) identified-organization(3) teletrust(36) algorithm(3) signaturealgorithm(3) ecSign(2) ecStdCurvesAndGeneration (8) ellipticCurve(1) versionOne(1) 7}`.

ou, em notação de ponto: `1.3.36.3.3.2.8.1.1.7`.

Exemplo 2: o identificador de objeto da curva NIST P-384 é

`{iso(1) identified-organization(3) certicom(132) curve(0) 34}`.

ou, em notação de ponto: `1.3.132.0.34`.

8.2.3 *Algoritmos de hash*

CSM_49 Unidades-veículo e cartões tacográficos aceitam os algoritmos SHA-256, SHA-384 e SHA-512, especificados em [SHS].

8.2.4 *Sequências de cifras*

CSM_50 No caso de se utilizarem conjuntamente algoritmos simétricos, algoritmos assimétricos e/ou algoritmos hash para formar um protocolo de segurança, os respetivos comprimentos de chave e tamanhos de hash serão, aproximadamente, da mesma resistência. O quadro 2 apresenta as sequências de cifras:

Quadro 2

Sequências de cifras permitidas

Id da sequência de cifras	Tamanho da chave ECC (bits)	Comprimento da chave AES (bits)	Algoritmo de hash	Comprimento do MAC (bytes)
CS#1	256	128	SHA-256	8
CS#2	384	192	SHA-384	12
CS#3	512/521	256	SHA-512	16

Nota: Para todos os efeitos no âmbito do presente apêndice, os tamanhos das chaves ECC de 512 bits e de 521 bits são considerados iguais no que se refere à resistência.

9. CHAVES E CERTIFICADOS

9.1. **Pares de chaves assimétricas e certificados de chave pública**

9.1.1 *Generalidades*

Nota: utilizam-se as chaves descritas na presente secção para autenticação mútua e envio seguro de mensagens entre unidades-veículo e cartões tacográficos, bem como entre unidades-veículo e módulos GNSS externos. Estes processos estão pormenorizados nos capítulos 10 e 11 do presente apêndice.

CSM_51 No sistema tacográfico inteligente europeu, os pares de chaves ECC e os certificados correspondentes são criados e geridos através de três níveis hierárquicos funcionais:

— nível europeu

— nível nacional (nível do Estado-Membro)

— nível do equipamento ou aparelho.

▼B

CSM_52 Em todo o sistema tacográfico inteligente europeu, as chaves públicas e privadas e os certificados são criados, geridos e comunicados por métodos seguros e normalizados.

9.1.2 *Nível europeu*

CSM_53 A nível europeu, é criado um par de chaves ECC original, designado EUR, que compreende uma chave privada (EUR.SK) e uma chave pública (EUR.PK). Este par de chaves constituirá o par de chaves de raiz de toda a infraestrutura de chave pública (PKI) tacográfica inteligente europeia. Estas funções são asseguradas por uma autoridade europeia de certificação de raiz (ERCA), sob a autoridade e a responsabilidade da Comissão Europeia.

CSM_54 A ERCA utiliza a chave privada europeia para assinar um certificado de raiz (autoassinado) da chave pública europeia e comunica este certificado de raiz europeia a todos os Estados-Membros.

CSM_55 Quando solicitado, a ERCA utiliza a chave privada europeia para assinar os certificados das chaves públicas dos Estados-Membros. A ERCA conserva registos de todos os certificados assinados de chave pública dos Estados-Membros.

CSM_56 Como mostra o esquema 1 na secção 9.1.7, a ERCA cria um novo par de chaves de raiz europeia de 17 em 17 anos. Nessa altura, cria um novo certificado de raiz autoassinado, destinado à nova chave pública europeia. O período de validade de um certificado de raiz europeia é de 34 anos e 3 meses.

Nota: A introdução de um novo par de chaves de raiz significa também que a ERCA cria uma nova chave de segurança para os sensores de movimentos e uma nova chave de segurança DSRC (ver secções 9.2.1.2 e 9.2.2.2).

CSM_57 Antes de criar um novo par de chaves de raiz europeia, a ERCA procede a uma análise da resistência criptográfica necessária para o novo par de chaves, dado que deve continuar seguro durante os próximos 34 anos. Se se revelar necessário, a ERCA muda para uma sequência de cifras mais forte do que a atual, em conformidade com o CSM_50.

CSM_58 Sempre que cria um novo par de chaves de raiz europeia, a ERCA cria um certificado de ligação para a nova chave pública europeia e assina-o com a chave privada europeia anterior. O período de validade do certificado de ligação será de 17 anos (esquema 1, na secção 9.1.7).

Nota: Dado que um certificado de ligação contém a chave pública ERCA da geração *X* e é assinado com a chave privada ERCA da geração *X-1*, esse certificado de ligação disponibiliza equipamentos atribuídos ao abrigo da geração *X-1*, um método de aprovação de equipamentos atribuídos ao abrigo da geração *X*.

CSM_59 Assim que um novo certificado de chave de raiz se torna válido, a ERCA não utiliza a chave privada de um par de chaves de raiz, seja para que fins for.

▼B

CSM_60 A ERCA dispõe, a qualquer momento, dos seguintes certificados e chaves criptográficas:

— o par de chaves EUR atual e o correspondente certificado

— todos os certificados EUR anteriores a utilizar na verificação dos certificados MSCA que ainda estão válidos

— certificados de ligação para todas as gerações de certificados EUR, com exceção do primeiro.

9.1.3 *Nível do Estado-Membro*

CSM_61 Ao nível dos Estados-Membros, todos os que são obrigados a assinar certificados para cartões tacográficos criam um ou mais pares únicos de chaves ECC, denominados MSCA_Card. Todos os Estados-Membros obrigados a assinar certificados para unidades-veículo ou módulos GNSS externos criam um ou mais pares únicos de chaves ECC, denominados MSCA_VU-EGF.

CSM_62 A função da criação de pares de chaves nacionais é assegurada por uma autoridade de certificação do Estado-Membro (MSCA). Sempre que uma MSCA cria um par de chaves do Estado-Membro, envia a chave pública para a ERCA, a fim de obter um certificado correspondente do Estado-Membro, assinado pela ERCA.

CSM_63 A MSCA deve escolher a resistência de um par de chaves do Estado-Membro igual à do par de chaves de raiz europeia utilizado para assinar o correspondente certificado do Estado-Membro.

CSM_64 Se existir, o par de chaves MSCA_VU-EGF é composto pela chave privada MSCA_VU-EGF.SK e pela chave pública MSCA_VU-EGF.PK. A MSCA utiliza a chave privada MSCA_VU-EGF.SK exclusivamente para assinar os certificados de chave pública de unidades-veículo e módulos GNSS externos.

CSM_65 Um par de chaves MSCA_Card é constituído pela chave privada MSCA_Card.SK e pela chave pública MSCA_Card.PK. A MSCA utiliza a chave privada MSCA_Card.SK exclusivamente para assinar os certificados de chave pública dos cartões tacográficos.

CSM_66 A MSCA conserva registos de todos os certificados assinados das VU, dos módulos GNSS externos e dos cartões, juntamente com a identificação do aparelho ao qual se destina cada certificado.

CSM_67 O período de validade de um certificado MSCA_VU-EGF é de 17 anos e 3 meses. O período de validade de um certificado MSCA_Card é de 7 anos e 1 mês.

CSM_68 Como mostra o esquema 1 na secção 9.1.7, a chave privada de um par de chaves MSCA_VU-EGF e a chave privada de um par de chaves MSCA_Card têm um período de utilização de dois anos.

▼B

CSM_69 Uma MSCA não volta a utilizar, seja para que fins for, a chave privada do par de chaves MSCA_VU-EGF ou a chave privada de um par de chaves MSCA_Card quando terminam os respetivos períodos de utilização.

CSM_70 A MSCA dispõe, a qualquer momento, dos seguintes certificados e chaves criptográficas:

— o par de chaves MSCA_Card atual e o certificado correspondente

— todos os certificados MSCA_Card anteriores a utilizar na verificação dos certificados dos cartões tacográficos que ainda estão válidos

— o certificado EUR atual necessário para a verificação do certificado MSCA atual

— todos os certificados EUR anteriores a utilizar na verificação de todos os certificados MSCA que ainda estão válidos.

CSM_71 Se uma MSCA for obrigada a assinar certificados para unidades-veículo ou módulos GNSS externos, disporá igualmente dos seguintes certificados e chaves:

— o par de chaves MSCA_VU-EGF atual e o correspondente certificado

— todas as chaves públicas MSCA_VU-EGF anteriores a utilizar na verificação dos certificados das VU ou dos módulos GNSS externos que ainda estão válidos.

9.1.4 *Nível do equipamento ou aparelho: unidades-veículo*

CSM_72 Para cada unidade-veículo, são criados dois pares de chaves ECC originais, denominados VU_MA e VU_Sign. Esta função é assegurada pelos fabricantes de VU. Sempre que for criado um par de chaves de VU, a parte que cria a chave envia a chave pública à MSCA do país de residência, a fim de obter o correspondente certificado de VU, assinado pela MSCA. Somente a unidade-veículo utiliza a chave privada.

CSM_73 Os certificados VU_MA e VU_Sign de uma determinada unidade-veículo têm a mesma data de vigência do certificado.

CSM_74 O fabricante da VU escolhe a resistência de um par de chaves de VU igual à do par de chaves MSCA utilizado para assinar o certificado correspondente da VU.

CSM_75 As unidades-veículo utilizam o seu par de chaves VU_MA, que consiste na chave privada VU_MA.SK e na chave pública VU_MA.PK, exclusivamente para efetuar a autenticação da VU em relação aos cartões tacográficos e módulos GNSS externos, em conformidade com as secções 10.3 e 11.4 do presente apêndice.

CSM_76 Uma unidade-veículo deve ser capaz de criar pares de chaves ECC efémeras e utiliza um par de chaves efémero exclusivamente para efetuar a concordância da chave de sessão com o cartão tacográfico ou módulo GNSS externo, em conformidade com as secções 10.4 e 11.4 do presente apêndice.

▼B

CSM_77 A unidade-veículo utiliza a chave privada VU_Sign.SK do seu par de chaves VU_Sign exclusivamente para assinar ficheiros de dados descarregados, em conformidade com o capítulo 14 do presente apêndice. A chave pública VU_Sign.PK correspondente é utilizada exclusivamente para verificar assinaturas criadas pela unidade-veículo.

CSM_78 Como mostra o esquema 1 na secção 9.1.7, o período de validade de um certificado VU_MA é de 15 anos e 3 meses. O período de validade de um certificado VU_Sign é igualmente de 15 anos e 3 meses.

Notas:

— O período de validade alargado de um certificado VU_Sign permite a uma unidade-veículo criar assinaturas válidas em dados descarregados durante os primeiros três meses após ter expirado, conforme previsto no Regulamento (UE) n.º 581/2010.

— O período de validade alargado de um certificado VU_MA é necessário para permitir que a VU autentique um cartão de controlo ou um cartão de empresa, durante os primeiros três meses após ter expirado, para possibilitar um descarregamento de dados.

CSM_79 Após o termo de validade do correspondente certificado, a unidade-veículo não utiliza a chave privada de um par de chaves de VU, seja para que fins for.

CSM_80 Depois de a unidade-veículo ser posta em funcionamento, os pares de chaves de VU (com exceção dos pares de chaves efémeras) e os correspondentes certificados de uma determinada unidade-veículo não são substituídos ou renovados no terreno.

Notas:

— Os pares de chaves efémeras não estão incluídos neste requisito, dado que, de cada vez que se realizar a autenticação da pastilha e a concordância da chave de sessão, a VU cria um novo par de chaves efémeras (ver secção 10.4). De salientar que os pares de chaves efémeras não têm certificados correspondentes.

— Este requisito não impede a substituição de pares de chaves de VU estáticas durante uma renovação ou reparação em ambiente seguro controlado pelo fabricante da VU.

CSM_81 Quando postas em funcionamento, as unidades-veículo contêm os seguintes certificados e chaves criptográficas:

— a chave privada VU_MA e o correspondente certificado

— a chave privada VU_Sign e o correspondente certificado

— o certificado MSCA_VU-EGF que contém a chave pública MSCA_VU-EGF.PK a utilizar para a verificação do certificado VU_MA e do certificado VU_Sign

▼B

— o certificado EUR que contém a chave pública EUR.PK a utilizar para a verificação do certificado MSCA_VU-EGF

— o certificado EUR cujo período de validade precede diretamente o período de validade do certificado EUR a utilizar para a verificação do certificado MSCA_VU-EGF, se existir

— o certificado de ligação que liga estes dois certificados EUR, se existir.

CSM_82 Além dos certificados e chaves criptográficas enumerados em CSM_81, as unidades-veículo contêm igualmente os certificados e chaves previstos na parte A do presente apêndice, que permitem a uma unidade-veículo interagir com cartões tacográficos da primeira geração.

9.1.5 *Nível do equipamento ou aparelho: cartões tacográficos*

CSM_83 Para cada cartão tacográfico é criado um par de chaves ECC original, denominado Card_MA. Para cada cartão de condutor e de oficina é criado adicionalmente um segundo par de chaves ECC original, denominado Card_Sign. Esta função pode ser assegurada pelos fabricantes ou personalizadores dos cartões. Quando é criado um par de chaves de cartão, a parte que cria a chave envia a chave pública à MSCA do país de residência, a fim de obter o correspondente certificado de cartão, assinado pela MSCA. A chave privada é utilizada somente pelo cartão tacográfico.

CSM_84 Os certificados Card_MA e Card_Sign de um determinado cartão de condutor ou cartão de oficina têm a mesma data de vigência do certificado.

CSM_85 O fabricante ou personalizador do cartão deve escolher a resistência de um par de chaves do cartão igual à do par de chaves MSCA utilizado para assinar o correspondente certificado do cartão.

CSM_86 O cartão tacográfico deve utilizar o seu par de chaves Card_MA, que consiste na chave privada Card_MA.SK e na chave pública Card_MA.PK, exclusivamente para efetuar a autenticação mútua e a concordância de chave de sessão em relação às unidades-veículo, em conformidade com as secções 10.3 e 10.4 do presente apêndice.

CSM_87 O cartão de condutor ou de oficina utiliza a chave privada Card_Sign.SK do seu par de chaves Card_Sign exclusivamente para assinar ficheiros de dados descarregados, em conformidade com o capítulo 14 do presente apêndice. A chave pública Card_Sign.PK correspondente é utilizada exclusivamente para verificar assinaturas criadas pelo cartão.

CSM_88 O período de validade de um certificado Card_MA é o seguinte:

— Para cartões de condutor: 5 anos

— Para cartões de empresa: 2 anos

— Para cartões de controlo: 2 anos

— Para cartões de oficina: 1 ano

▼B

CSM_89 O período de validade de um certificado Card_Sign é o seguinte:

— Para cartões de condutor: 5 anos e 1 mês

— Para cartões de oficina: 1 ano e 1 mês

Nota: o período de validade alargado de um certificado Card_Sign permite a um cartão de condutor criar assinaturas válidas em dados descarregados durante o primeiro mês após ter expirado. Com efeito, o Regulamento (UE) n.º 581/2010 exige a viabilidade de um descarregamento de dados do cartão do condutor até 28 dias após terem sido registados os últimos dados.

CSM_90 Os correspondentes pares de chaves e certificados de um determinado cartão tacográfico não são substituídos ou renovados depois de ter sido emitido o cartão.

CSM_91 Quando emitidos, os cartões tacográficos contêm os seguintes certificados e chaves criptográficas:

— a chave privada Card_MA e o correspondente certificado

— para cartões de condutor e cartões de oficina adicionais: a chave privada Card_Sign e o correspondente certificado

— o certificado MSCA_Card que contém a chave pública MSCA_Card.PK a utilizar para a verificação do certificado Card_MA e do certificado Card_Sign

— o certificado EUR que contém a chave pública EUR.PK a utilizar para a verificação do certificado MSCA_Card

— o certificado EUR cujo período de validade precede diretamente o período de validade do certificado EUR a utilizar para a verificação do certificado MSCA_Card, se existir.

— o certificado de ligação que liga estes dois certificados EUR, se existir.

CSM_92 Além dos certificados e chaves criptográficas enumerados em CSM_91, os cartões tacográficos contêm igualmente os certificados e chaves previstos na parte A do presente apêndice, que permitem a estes cartões tacográficos interagirem com VU da primeira geração.

9.1.6 *Nível do equipamento ou aparelho: módulos GNSS externos*

CSM_93 Para cada módulo GNSS externo é criado um par de chaves ECC original, denominado EGF_MA. Esta função é assegurada pelos fabricantes de módulos GNSS externos. Quando é criado um par de chaves EGF_MA, a chave pública é enviada à MSCA do país de residência, a fim de obter o correspondente certificado EGF_MA, assinado pela MSCA. A chave privada é utilizada somente pelo módulo GNSS externo.

CSM_94 O fabricante do EGF escolhe a resistência de um par de chaves EGF_MA igual à do par de chaves MSCA utilizado para assinar o correspondente certificado EGF_MA.

▼B

CSM_95 O módulo GNSS externo utiliza o seu par de chaves EGF_MA, que consiste na chave privada EGF_MA.SK e na chave pública EGF_MA.PK, exclusivamente para efetuar a autenticação mútua e a concordância de chave de sessão em relação às unidades-veículo, em conformidade com as secções 11.4 e 11.4 do presente apêndice.

CSM_96 O período de validade de um certificado EGF_MA é de 15 anos.

CSM_97 Após o termo de validade do correspondente certificado, o módulo GNSS externo não utiliza a chave privada do seu par de chaves EGF_MA para acoplamento a uma unidade-veículo.

Nota: tal como explicado na secção 11.3.3, um EGF pode eventualmente utilizar a sua chave privada para autenticação mútua em relação à VU a que já está acoplado, mesmo após o termo de validade do correspondente certificado.

CSM_98 O par de chaves EGF_MA e o correspondente certificado de um determinado módulo GNSS externo não são substituídos ou renovados no terreno depois de o EGF ter sido posto em funcionamento.

Nota: Este requisito não impede a substituição de pares de chaves EGF durante uma renovação ou reparação em ambiente seguro controlado pelo fabricante do EGF.

CSM_99 Quando posto em funcionamento, o módulo GNSS externo contém os seguintes certificados e chaves criptográficas:

— a chave privada EGF_MA e o correspondente certificado

— o certificado MSCA_VU-EGF que contém a chave pública MSCA_VU-EGF.PK a utilizar para a verificação do certificado EGF_MA

— o certificado EUR que contém a chave pública EUR.PK a utilizar para a verificação do certificado MSCA_VU-EGF

— o certificado EUR cujo período de validade precede diretamente o período de validade do certificado EUR a utilizar para a verificação do certificado MSCA_VU-EGF, se existir

— o certificado de ligação que liga estes dois certificados EUR, se existir

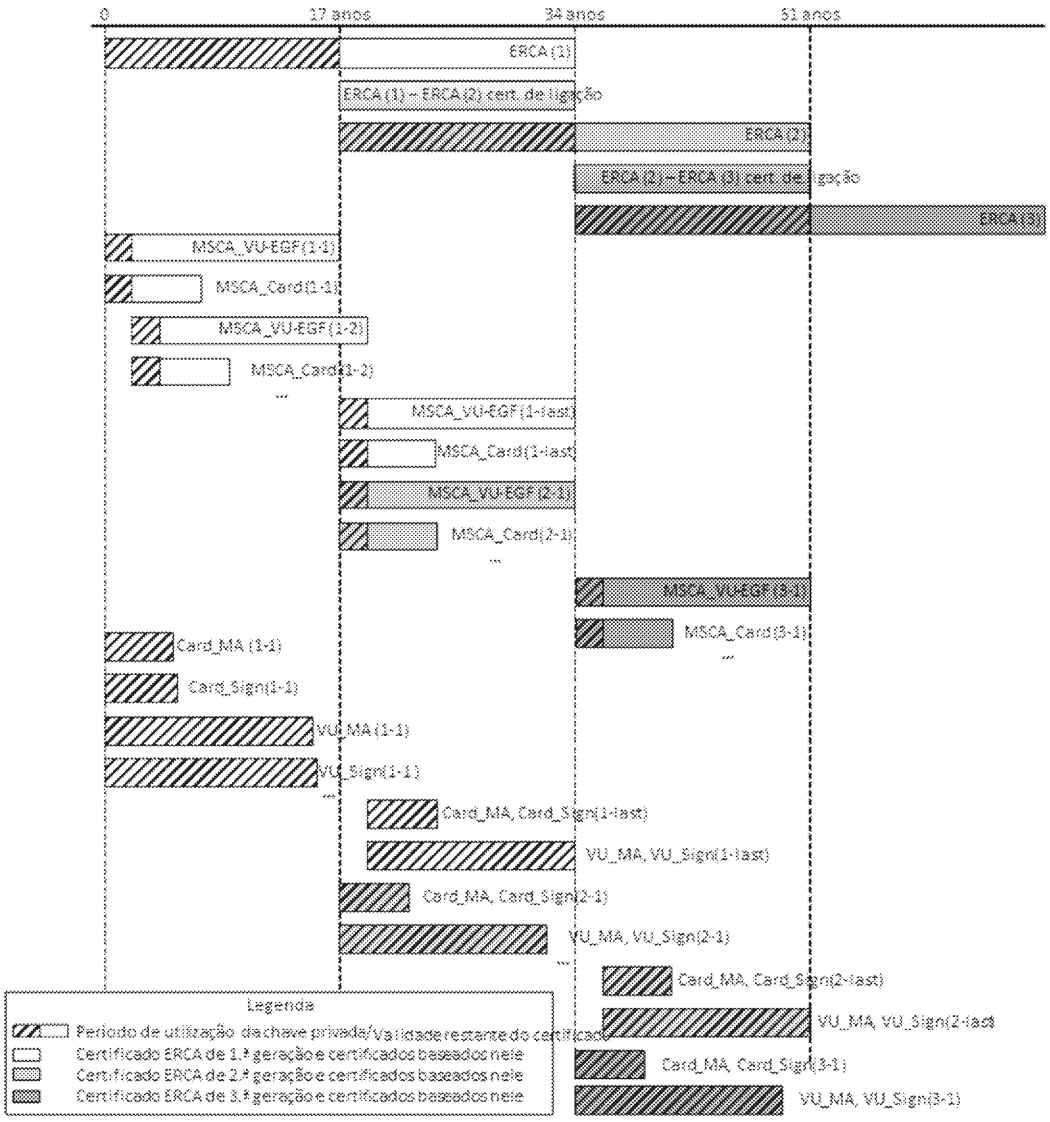
9.1.7 *Panorâmica: Substituição de certificados*

O esquema 1 mostra como os certificados de raiz ERCA, os certificados de ligação ERCA, os certificados MSCA e os certificados de equipamento ou aparelho (VU e cartão) de gerações diferentes são emitidos e utilizados ao longo do tempo:

▼B

Esquema 1

Emissão e utilização de certificados de raiz ERCA, certificados de ligação ERCA, certificados MSCA e certificados de equipamento ou aparelho de gerações diferentes



Notas ao esquema 1:

1. As diversas gerações do certificado de raiz são indicadas por um número entre parênteses. Por ex.: ERCA (1) é a primeira geração do certificado de raiz ERCA; ERCA (2) é a segunda geração, etc.

2. Outros certificados são indicados por dois números entre parênteses, o primeiro a indicar a geração do certificado de raiz ao abrigo do qual foram emitidos e o segundo a geração do próprio certificado. Por ex.: MSCA_Card (1-1) é o primeiro certificado MSCA_Card emitido ao abrigo de ERCA (1); MSCA_Card (2-1) é o primeiro certificado MSCA_Card emitido ao abrigo de ERCA (2); MSCA_Card (2-último) é o último certificado MSCA_Card emitido ao abrigo de ERCA (2); Card_MA(2-1) é o primeiro certificado de cartão para autenticação mútua emitido ao abrigo de ERCA (2), etc.

▼B

3. Os certificados MSCA_Card (2-1) e MSCA_Card (1-último) são emitidos quase, mas não exatamente, na mesma data. MSCA_Card (2-1) é o primeiro certificado MSCA_Card emitido ao abrigo de ERCA (2) e será emitido ligeiramente mais tarde do que MSCA_Card (1-último), o último certificado MSCA_Card ao abrigo de ERCA (1).

4. Tal como mostra o esquema, os primeiros certificados de VU e de cartão emitidos ao abrigo de ERCA (2) surgirão quase dois anos antes do aparecimento dos últimos certificados de VU e de cartão emitidos ao abrigo de ERCA (1), o que se deve ao facto de os certificados de VU e de cartão serem emitidos ao abrigo de um certificado MSCA, não diretamente ao abrigo de um certificado ERCA. O certificado MSCA (2-1) é emitido diretamente após ERCA (2) ficar válido, mas o certificado MSCA (1-último) apenas é emitido ligeiramente antes dessa data, no último momento de validade do certificado ERCA (1). Por conseguinte, estes dois certificados MSCA têm quase o mesmo período de validade, apesar de pertencerem a gerações diferentes.

5. O período de validade apresentado para os cartões é o dos cartões de condutor (5 anos).

6. Para poupar espaço, a diferença no período de validade entre os certificados Card_MA e Card_Sign e entre os certificados VU_MA e VU_Sign é apresentada somente para a primeira geração.

9.2. **Chaves simétricas**

9.2.1 *Chaves para proteção das comunicações do sensor de movimentos com a VU*

9.2.1.1 *Generalidades*

Nota: presume-se que os leitores da presente secção estão familiarizados com o conteúdo da norma ISO 16844-3, que descreve a interface entre uma unidade-veículo e um sensor de movimentos. O processo de emparelhamento entre uma VU e um sensor de movimentos é descrito em pormenor no capítulo 12 do presente apêndice.

CSM_100 São necessárias várias chaves simétricas para emparelhar unidades-veículo e sensores de movimentos, para autenticação mútua entre as unidades-veículo e os sensores de movimentos e para encriptar as comunicações entre as unidades-veículo e os sensores de movimentos, como mostra o quadro 3. Todas estas chaves são chaves AES, com um comprimento de chave igual ao comprimento da chave de segurança do sensor de movimentos, que está ligado ao comprimento (previsto) do par de chaves de raiz europeia, como descrito em CSM_50.

Quadro 3

Chaves para proteção das comunicações do sensor de movimentos com a VU

Chave	Símbolo	Gerado por	Método de geração	Memorizado por
Chave de segurança do sensor de movimentos — parte da VU	$K_{M\text{-}VU}$	ERCA	Aleatório	ERCA e MSCA que participam na emissão de certificados de VU, fabricantes de VU, unidades-veículo
Chave de segurança do sensor de movimentos — parte da oficina	$K_{M\text{-}WC}$	ERCA	Aleatório	ERCA, MSCA, fabricantes de cartões, cartões de oficina

▼B

Chave	Símbolo	Gerado por	Método de geração	Memorizado por
Chave de segurança do sensor de movimentos	K_M	Não gerados independentemente	Calculado como $K_M = K_{M\text{-}VU}$ XOR $K_{M\text{-}WC}$	ERCA e MSCA que participam na emissão de chaves de sensores de movimentos (facultativo) (*)
Chave de identificação	K_{ID}	Não gerados independentemente	Calculado do seguinte modo: $K_{ID} = K_M$ XOR CV, em que CV é especificado em CSM_106	ERCA e MSCA que participam na emissão de chaves de sensores de movimentos (facultativo) (*)
Chave de emparelha-mento	K_P	Fabricante do sensor de movimentos	Aleatório	Um sensor de movimentos
Chave de sessão	K_S	VU (durante o emparelhamento da VU com o sensor de movimentos)	Aleatório	Uma VU e um sensor de movimentos

(*) Memorização de K_M e K_{ID} é opcional, uma vez que estas chaves podem ser derivadas de $K_{M\text{-}VU}$, $K_{M\text{-}WC}$ e CV.

CSM_101 A autoridade europeia de certificação de raiz cria $K_{M\text{-}VU}$ e $K_{M\text{-}WC}$, duas chaves AES aleatórias e originais a partir das quais a chave de segurança do sensor de movimentos K_M pode ser calculada como $K_{M\text{-}VU}$ XOR $K_{M\text{-}WC}$. A ERCA transmite as chaves K_M, $K_{M\text{-}VU}$ e $K_{M\text{-}WC}$ às autoridades de certificação do Estado-Membro, a seu pedido.

CSM_102 A ERCA atribui a cada chave de segurança do sensor de movimentos K_M um número de versão único, igualmente aplicável às chaves constituintes $K_{M\text{-}VU}$ e $K_{M\text{-}WC}$ e à chave de identificação relativa K_{ID}. A ERCA informa as MSCA sobre o número de versão ao enviar-lhes as chaves $K_{M\text{-}VU}$ e $K_{M\text{-}WC}$.

Nota: O número de versão é utilizado para distinguir diferentes gerações dessas chaves, conforme explicado em pormenor na secção 9.2.1.2.

CSM_103 Uma autoridade europeia de certificação do Estado-Membro transmite aos fabricantes de unidades-veículo, a seu pedido, a chave $K_{M\text{-}VU}$, juntamente com o seu número de versão. Os fabricantes de VU inserem a chave $K_{M\text{-}VU}$ e o seu número de versão em todas as VU produzidas.

CSM_104 A autoridade de certificação do Estado-Membro assegura que a chave $K_{M\text{-}WC}$, juntamente com o respetivo número de versão, são inseridos em todos os cartões de oficina emitidos sob a sua responsabilidade.

Notas:

— Ver a descrição do tipo de dados `SensorInstallationSecData` no apêndice 2.

— Conforme explicado na secção 9.2.1.2, na realidade, podem ter de ser inseridas várias gerações de chaves $K_{M\text{-}WC}$ num único cartão de oficina.

▼B

CSM_105 Além da chave AES especificada no CSM_104, uma MSCA assegura que a chave TDES Km_{WC}, especificada no requisito CSM_037 (constante da parte A do presente apêndice), é inserida em todos os cartões de oficina emitidos sob a sua responsabilidade.

Notas:

— Tal permite a utilização de um cartão de oficina da segunda geração para acoplamento com uma VU da primeira geração.

— Um cartão de oficina da segunda geração terá duas aplicações diferentes, uma em conformidade com a parte B e a outra que obedece à parte A do presente apêndice. Esta última tem a chave TDES Km_{WC}.

CSM_106 Uma MSCA envolvida na emissão de sensores de movimentos deriva a chave de identificação da chave de segurança do sensor de movimentos através de XORing com um vetor CV constante. O valor de CV é o seguinte:

— Para chaves de segurança do sensor de movimentos de 128 bits: CV = ‘B6 44 2C 45 0E F8 D3 62 0B 7A 8A 97 91 E4 5E 83’

— Para chaves de segurança do sensor de movimentos de 192 bits: CV = ‘72 AD EA FA 00 BB F4 EE F4 99 15 70 5B 7E EE BB 1C 54 ED 46 8B 0E F8 25’

— Para chaves de segurança do sensor de movimentos de 256 bits: CV = ‘1D 74 DB F0 34 C7 37 2F 65 55 DE D5 DC D1 9A C3 23 D6 A6 25 64 CD BE 2D 42 0D 85 D2 32 63 AD 60’

Nota: os vetores constantes foram criados da seguinte forma:

Pi_10 = primeiros 10 bytes da parte decimal da constante matemática π = ‘24 3F 6A 88 85 A3 08 D3 13 19’

CV_128-bits = primeiros 16 bytes de SHA-256(Pi_10)

CV_192-bits = primeiros 24 bytes de SHA-384(Pi_10)

CV_256-bits = primeiros 32 bytes de SHA-512(Pi_10)

CSM_107 Os fabricantes de sensores de movimentos criam uma chave de emparelhamento K_P aleatória e original para cada sensor de movimentos e enviam todas as chaves de emparelhamento a uma autoridade de certificação do Estado-Membro. A MSCA encripta cada chave de emparelhamento individualmente com a chave de segurança do sensor de movimentos K_M e devolve a chave encriptada ao fabricante do sensor de movimentos. Relativamente a cada chave encriptada, a MSCA comunica ao fabricante do sensor de movimentos o número de versão da chave $K_M$associada.

Nota: tal como explicado na secção 9.2.1.2, na realidade, o fabricante de sensores de movimentos pode ter de criar múltiplas chaves de emparelhamento originais para um único sensor de movimentos.

▼B

CSM_108 Os fabricantes de sensores de movimentos criam um número de série único para cada sensor de movimentos e enviam todos os números de série a uma autoridade de certificação do Estado-Membro. A MSCA encripta cada número de série individualmente com a chave de identificação K_{ID} e devolve o número de série encriptado ao fabricante do sensor de movimentos. Relativamente a cada número de série encriptado, a MSCA comunica ao fabricante do sensor de movimentos o número de versão da chave K_{ID} associada.

CSM_109 Relativamente aos requisitos CSM_107 e CSM_108, a MSCA utiliza o algoritmo AES no modo de funcionamento por cifragem progressiva, conforme definido na norma ISO 10116, com um parâmetro intercalar $m = 1$ e um vetor de inicialização SV = '00' {16}, ou seja, dezasseis bytes com valor binário 0. Quando necessário, a MSCA utiliza o método de preenchimento 2 definido na norma ISO 9797-1.

CSM_110 O fabricante de sensores de movimentos memoriza a chave de emparelhamento encriptada e o número de série encriptado no sensor de movimentos a que se destina, juntamente com os valores de texto simples e o número de versão das chaves K_M e K_{ID} utilizadas para encriptação.

Nota: tal como explicado na secção 9.2.1.2, na realidade, o fabricante de sensores de movimentos pode ter de inserir múltiplas chaves de emparelhamento encriptadas e múltiplos números de série encriptados num único sensor de movimentos.

CSM_111 Além do material criptográfico com recurso a AES especificado no CSM_110, um fabricante de sensores de movimentos também pode memorizar em cada sensor de movimentos o material criptográfico com recurso a TDES especificado no requisito CSM_037 (parte A do presente apêndice).

Nota: este procedimento permite que um sensor de movimentos da segunda geração seja acoplado a uma VU da primeira geração.

CSM_112 O comprimento da chave de sessão K_S criada por uma VU durante o emparelhamento com um sensor de movimentos está ligado ao comprimento da respetiva chave $K_{M\text{-}VU}$, conforme descrito em CSM_50.

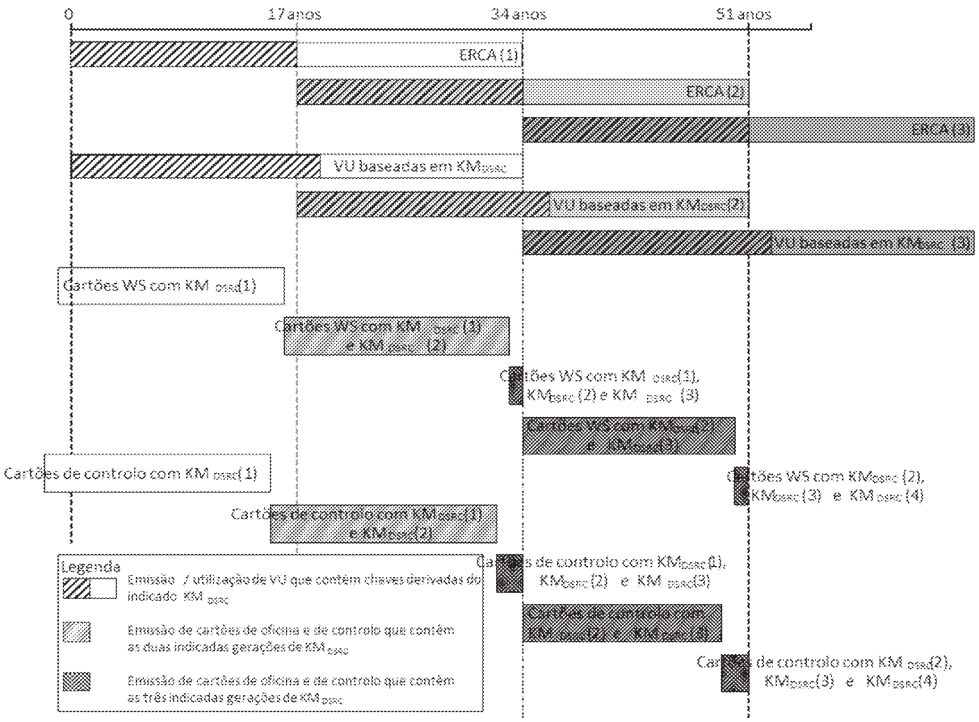
9.2.1.2 *Substituição da chave de segurança do sensor de movimentos em aparelhos da segunda geração*

CSM_113 Cada chave de segurança do sensor de movimentos e todas as chaves relacionadas (ver quadro 3) estão associadas a uma determinada geração do par de chaves de raiz ERCA. Essas chaves são, por conseguinte, substituídas de 17 em 17 anos. O período de validade de cada geração da chave de segurança do sensor de movimentos tem início um ano antes do início de validade do par de chaves de raiz ERCA associado e termina quando expirar a validade do par de chaves de raiz ERCA associado. Tal é descrito no esquema 2.

▼B

Esquema 2

Emissão e utilização de diferentes gerações da chave de segurança de sensores de movimentos em unidades-veículo, sensores de movimentos e cartões de oficina



CSM_114 Pelo menos um ano antes de criar um novo par de chaves de raiz europeia, conforme indicado no requisito CSM_56, a ERCA cria uma nova chave de segurança do sensor de movimentos K_M através de novas chaves K_{M-VU} e K_{M-WC}. O comprimento da chave de segurança do sensor de movimentos está ligado à resistência prevista do novo par de chaves de raiz europeia, de acordo com CSM_50. A ERCA comunica as novas chaves K_M, K_{M-VU} e K_{M-WC} às MSCA, a seu pedido, juntamente com o respetivo número de versão.

CSM_115 Uma MSCA deve assegurar que todas as gerações válidas de K_{M-WC} são memorizadas nos cartões de oficina emitidos sob a sua autoridade, juntamente com os respetivos números de versão, como mostra o esquema 2.

Nota: Tal implica que, no último ano do período de validade de um certificado ERCA, os cartões de oficina sejam emitidos com três gerações diferentes de chaves K_{M-WC}, como mostra o esquema 2.

CSM_116 No que se refere ao processo descrito em CSM_107 e CSM_108: Uma MSCA encripta cada chave de emparelhamento K_P que recebe de um fabricante de sensores de movimentos, separadamente com cada geração válida da chave de segurança do sensor de movimentos K_M. Encripta ainda cada número de série que recebe de um fabricante de sensores de movimentos, separadamente com cada geração válida da chave de identificação K_{ID}. Um fabricante de sensores de movimentos memoriza todas as encriptações da chave de emparelhamento e todas as encriptações do número de série no sensor de movimentos a que se destina, juntamente com os valores de texto simples e o número de versão das chaves K_M e K_{ID} utilizadas para encriptação.

▼B

Nota: Tal implica que, no último ano do período de validade de um certificado ERCA, os sensores de movimentos sejam emitidos com dados encriptados baseados em três gerações diferentes de chaves $K_{M,}$ como mostra o esquema 2.

CSM_117 No que se refere ao processo descrito em CSM_107: Dado que o comprimento da chave de emparelhamento K_P está ligado ao comprimento da chave K_M (ver CSM_100), o fabricante do sensor de movimentos pode ter de criar até três chaves de emparelhamento diferentes (de comprimentos diferentes) para um sensor de movimentos, se as gerações subsequentes de K_M tiverem comprimentos diferentes. Nesse caso, o fabricante envia todas as chaves de emparelhamento à MSCA. A MSCA garante que todas as chaves de emparelhamento estão encriptadas com a geração correta da chave de segurança do sensor de movimentos, ou seja, aquela que tem o mesmo comprimento.

Nota: Se o fabricante do sensor de movimentos escolher a criação de uma chave de emparelhamento com recurso a TDES para um sensor de movimentos da segunda geração (ver CSM_111), deve indicar à MSCA que a chave de segurança do sensor de movimentos com recurso a TDES tem de ser utilizada para encriptar essa chave de emparelhamento. Tal ocorre devido ao facto de o comprimento de uma chave TDES ser igual ao de uma chave AES; logo, a MSCA não pode considerar isoladamente o comprimento da chave.

CSM_118 Os fabricantes de unidades-veículo inserem apenas uma geração de $K_{M\text{-}VU}$ em cada unidade-veículo, juntamente com o respetivo número de versão. Esta geração de $K_{M\text{-}VU}$ está ligada ao certificado ERCA sobre o qual se baseiam os certificados das VU.

Notas:

— Uma unidade-veículo baseada no certificado ERCA da geração *X* contém unicamente a chave $K_{M\text{-}VU}$ da geração *X*, mesmo que seja emitida após o início do período de validade do certificado ERCA da geração *X+1* (ver esquema 2).

— Uma VU da geração *X* não pode ser emparelhada com um sensor de movimentos da geração *X-1*.

— Dado que o período de validade dos cartões de oficina é de um ano, resulta dos requisitos CSM_113 a CSM_118 que todos os cartões de oficina terão a nova chave $K_{M\text{-}WC}$ no momento da emissão da primeira VU que contém a nova chave $K_{M\text{-}VU}$. Por conseguinte, a VU conseguirá calcular sempre a nova chave K_M. Além disso, por essa altura, também os novos sensores de movimentos possuirão, na sua maioria, dados encriptados baseados na nova chave K_M.

9.2.2 *Chaves para comunicações DSRC seguras*

9.2.2.1 *Generalidades*

CSM_119 A autenticidade e a confidencialidade dos dados comunicados a uma autoridade de controlo a partir de uma unidade-veículo, através de um canal de comunicações à distância DSRC, são asseguradas por meio de um conjunto de chaves AES específicas da VU, derivadas de uma chave de segurança DSRC única, a KM_{DSRC}.

▼B

CSM_120 A chave de segurança DSRC KM_{DSRC} é uma chave AES criada, memorizada e distribuída de forma segura pela ERCA. O seu comprimento pode ser de 128, 192 ou 256 bits e está associado ao comprimento do par de chaves de raiz europeia, conforme se refere no requisito CSM_50.

CSM_121 A ERCA comunica, de forma segura, a chave de segurança DSRC às autoridades de certificação do Estado-Membro, a seu pedido, para que possam derivar chaves DSRC específicas da VU e para garantir que a chave de segurança DSRC é inserida em todos os cartões de controlo e de oficina emitidos sob a sua responsabilidade.

CSM_122 A ERCA atribui a cada chave de segurança DSRC um número de versão único e informa as MSCA sobre o número de versão ao enviar-lhes a chave de segurança DSRC.

Nota: O número de versão é utilizado para distinguir diferentes gerações da chave de segurança DSRC, conforme se explica em pormenor na secção 9.2.2.2.

CSM_123 Relativamente a todas as unidades-veículo: O fabricante de unidades-veículo cria um número de série de VU único e envia-o à autoridade de certificação do respetivo Estado-Membro, num pedido de obtenção de um conjunto de duas chaves DSRC específicas da VU. O número de série da VU tem o tipo de dados `VuSerialNumber`, devendo ser utilizadas para codificação as regras distintas de codificação (DER), em conformidade com a norma ISO 8825-1.

CSM_124 Ao receber um pedido de chaves DSRC específicas da VU, a MSCA deriva para a unidade-veículo duas chaves AES, denominadas K_VU_{DSRC}_ENC e K_VU_{DSRC}_MAC. Estas chaves específicas da VU têm o mesmo comprimento da chave de segurança DSRC. A MSCA utiliza a função de derivação de chave definida em [RFC 5869]. A função hash necessária para instanciar a função HMAC-Hash é ligada ao comprimento da chave de segurança DSRC, conforme refere o requisito CSM_50. A função de derivação de chave em [RFC 5869] é utilizada do seguinte modo:

Passo 1 (Extrair):

— *PRK* = HMAC-Hash (*salt, IKM*) onde *salt* é uma cadeia vazia e *IKM* é KM_{DSRC}.

Passo 2 (Expandir):

— *OKM* = *T(1)*, onde

T(1) = HMAC-Hash (*PRK*, *T(0)* || *info* || '01') com

▼B

— *T(0)* = uma cadeia vazia (‘’)

— *info* = número de série da VU, conforme especificado no CSM_123

— $K\_VU_{DSRC}\_ENC$ = primeiros octetos *L* de *OKM* e

$K\_VU_{DSRC}\_MAC$ = últimos octetos *L* de *OKM*

onde *L* é o comprimento necessário de $K\_VU_{DSRC}\_ENC$ e $K\_VU_{DSRC}\_MAC$ em octetos.

CSM_125 A MSCA distribui ao fabricante da VU, de forma segura, as chaves $K\_VU_{DSRC}\_ENC$ e $K\_VU_{DSRC}\_MAC$, para inserção na unidade-veículo a que se destinam.

CSM_126 Uma vez emitida, uma unidade-veículo terá memorizado as chaves $K\_VU_{DSRC}\_ENC$ e $K\_VU_{DSRC}\_MAC$ na respetiva memória segura, a fim de poder garantir a integridade, a autenticidade e a confidencialidade dos dados enviados através do canal de comunicação à distância. Uma unidade-veículo memoriza ainda o número de versão da chave de segurança DSRC utilizada para derivar essas chaves específicas da VU.

CSM_127 Uma vez emitidos, os cartões de controlo e de oficina terão memorizado KM_{DSRC} na respetiva memória segura, a fim de poderem verificar a integridade e a autenticidade dos dados enviados por uma VU através do canal de comunicação à distância e decifrar os dados. Os cartões de controlo e de oficina memorizam também o número de versão da chave de segurança DSRC.

Nota: Conforme se explica na secção 9.2.2.2, podem, na realidade, ter de ser inseridas várias gerações de chaves KM_{DSRC} num único cartão de controlo ou de oficina.

CSM_128 A MSCA mantém registos de todas as chaves DSRC específicas da VU que criou, os respetivos números de versão e a identificação da VU à qual se destina cada conjunto de chaves.

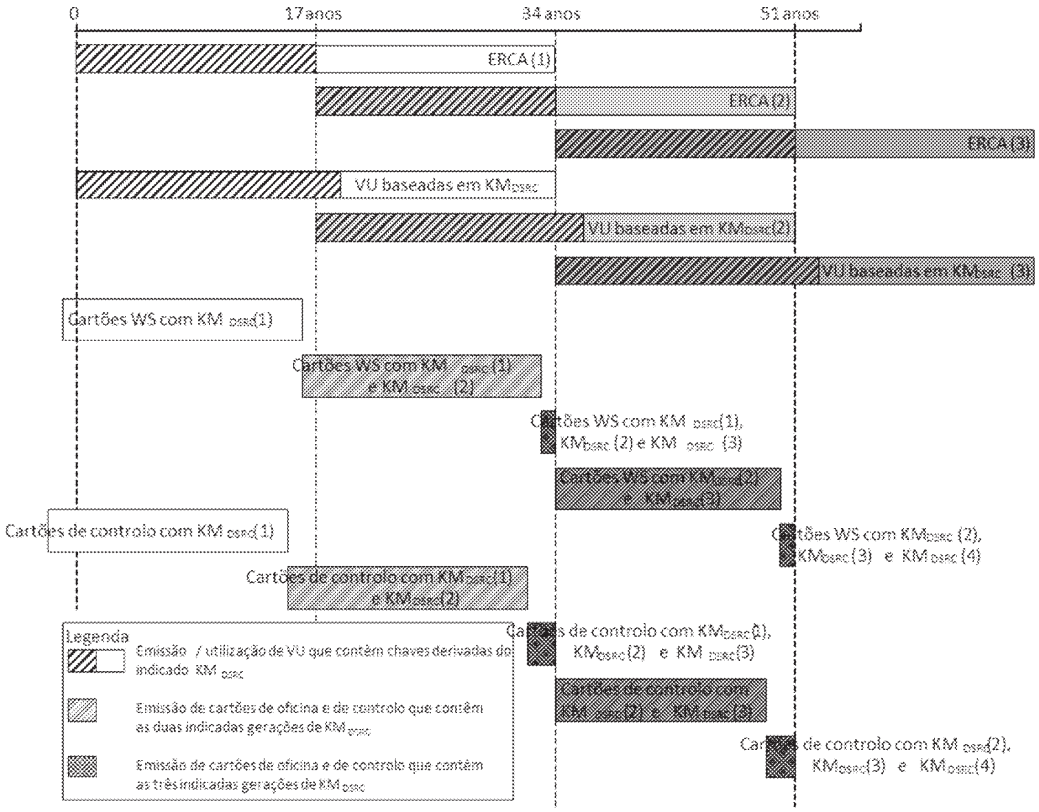
9.2.2.2 *Substituição da chave de segurança DSRC*

CSM_129 Cada chave de segurança DSRC está associada a uma determinada geração do par de chaves de raiz ERCA. Por conseguinte, a ERCA substitui a chave de segurança DSRC de 17 em 17 anos. O período de validade de cada geração da chave de segurança DSRC tem início dois anos antes do início de validade do par de chaves de raiz ERCA associado e termina quando expira a validade do par de chaves de raiz ERCA associado (ver esquema 3).

▼B

Esquema 3

Emissão e utilização de diferentes gerações da chave de segurança DSRC em unidades-veículo, cartões de oficina e cartões de controlo



CSM_130 Pelo menos dois anos antes da criação de um novo par de chaves de raiz europeia (descrição em CSM_56), a ERCA cria uma nova chave de segurança DSRC. O comprimento da chave DSRC é ligado à resistência prevista do novo par de chaves de raiz europeia, de acordo com CSM_50. A ERCA comunica a nova chave de segurança DSRC às MSCA, a seu pedido, juntamente com o respetivo número de versão.

CSM_131 Uma MSCA deve assegurar que todas as gerações válidas de KM_{DSRC} são memorizadas nos cartões de controlo emitidos sob a sua autoridade, juntamente com os respetivos números de versão, como mostra o esquema 3.

Nota: Tal implica que, nos últimos dois anos do período de validade de um certificado ERCA, os cartões de controlo serão emitidos com três gerações diferentes de chaves KM_{DSRC}, como mostra o esquema 3.

CSM_132 Uma MSCA assegura que todas as gerações de KM_{DSRC} que tenham estado válidas durante, pelo menos, um ano e continuam válidas, são memorizadas em todos os cartões de oficina emitidos sob a sua autoridade, juntamente com os respetivos números de versão, como mostra o esquema 3.

▼B

Nota: Tal implica que, no último ano do período de validade de um certificado ERCA, os cartões de oficina serão emitidos com três gerações diferentes de chaves KM_{DSRC}, como mostra o esquema 3.

CSM_133 Os fabricantes de unidades-veículo inserem apenas um conjunto de chaves DSRC específicas da VU em cada unidade-veículo, juntamente com o respetivo número de versão. Este conjunto de chaves é derivado da geração KM_{DSRC}, ligado ao certificado ERCA no qual se baseiam os certificados das VU.

Notas:

— Tal implica que uma unidade-veículo baseada no certificado ERCA da geração *X* contenha unicamente as chaves K_VU_{DSRC}_ENC e K_VU_{DSRC}_MAC da geração *X*, mesmo que a VU seja emitida após o início do período de validade do certificado ERCA da geração *X+1* (ver esquema 3).

— Dado que o período de validade dos cartões de oficina é de um ano e o dos cartões de controlo é de dois anos, resulta dos requisitos CSM_131 — CSM_133 que todos os cartões de oficina e de controlo terão a nova chave de segurança DSRC no momento da emissão da primeira VU que contém chaves específicas da VU baseadas nessa chave de segurança.

9.3. **Certificados**

9.3.1 *Generalidades*

CSM_134 No sistema tacográfico inteligente europeu, todos os certificados serão certificados autodescritivos e verificáveis do cartão (CV), em conformidade com as normas ISO 7816-4 e ISO 7816-8.

CSM_135 De acordo com a norma ISO 8825-1, utilizar-se-ão as regras distintas de codificação para codificar as estruturas de dados ASN.1 e os objetos de dados (específicos da aplicação) dentro dos certificados.

Nota: Esta codificação resulta numa estrutura Marcador-Comprimento-Valor (TLV), da seguinte forma:

Marcador: O marcador está codificado em um ou dois octetos e indica o conteúdo.

Comprimento: O comprimento é codificado como número inteiro não assinado, em um, dois ou três octetos, que resultam num comprimento máximo de 65 535 octetos. Deve utiliza-se o número mínimo de octetos.

Valor: O valor é codificado em zero ou mais octetos

9.3.2 *Conteúdo do certificado*

CSM_136 Todos os certificados têm a estrutura de perfil do certificado apresentada no quadro 4.

Quadro 4

Perfil do certificado, versão 1

Campo	ID do campo	Marcador	Compri-mento (bytes)	Tipo de dados ASN.1 (ver apêndice 1)
Certificado ECC	C	'7F 21'	var	
Corpo do certificado ECC	B	'7F 4E'	var	

▼B

Campo	ID do campo	Marcador	Compri-mento (bytes)	Tipo de dados ASN.1 (ver apêndice 1)
Identificador de perfil do certificado	CPI	‘5F 29’	‘01’	INTEGER(0..255)
Referência da autoridade de certificação	CAR	‘42’	‘08’	KeyIdentifier
Autorização do titular do certificado	CHA	‘5F 4C’	‘07’	CertificateHolder Authorisation
Chave pública	PK	‘7F 49’	var	
Parâmetros de domínio	DP	‘06’	var	IDENTIFICADOR DE OBJETO
Ponto público	PP	‘86’	var	CADEIA DE OCTETOS
Referência do titular do certificado	CHR	‘5F 20’	‘08’	KeyIdentifier
Data de vigência do certificado	CEfD	‘5F 25’	‘04’	TimeReal
Data de validade do certificado	CExD	‘5F 24’	‘04’	TimeReal
Assinatura do certificado ECC	S	‘5F 37’	var	CADEIA DE OCTETOS

Nota: O ID do campo será utilizado em secções posteriores do presente apêndice para indicar campos individuais de um certificado; por exemplo, X.CAR é a referência da autoridade de certificação referida no certificado do utilizador X.

9.3.2.1 Identificador de perfil do certificado

CSM_137 Os certificados utilizam um identificador de perfil do certificado para indicar o perfil do certificado utilizado. A versão 1, em conformidade com o quadro 4, é identificada por um valor de «00».

9.3.2.2 Referência da autoridade de certificação

CSM_138 Utiliza-se a referência da autoridade de certificação para identificar a chave pública a utilizar para verificar a assinatura do certificado. A referência da autoridade de certificação será, por conseguinte, igual à referência do titular do certificado, constante do certificado da correspondente autoridade de certificação.

CSM_139 Um certificado de raiz ERCA deve ser autoassinado, ou seja: no certificado, a referência da autoridade de certificação e a referência do titular do certificado são iguais.

▼B

CSM_140 Relativamente a um certificado de ligação ERCA, a referência do titular do certificado é igual à CHR do novo certificado de raiz ERCA. A referência da autoridade de certificação para um certificado de ligação é igual à CHR do anterior certificado de raiz ERCA.

9.3.2.3 Autorização do titular do certificado

CSM_141 Utiliza-se a autorização do titular do certificado para identificar o tipo de certificado. Consiste nos seis bytes mais significativos do ID da aplicação tacográfica, concatenados com o tipo de aparelho ao qual se destina o certificado.

9.3.2.4 Chave pública

A chave pública agrupa dois elementos de dados: os parâmetros de domínio normalizados, a utilizar com a chave pública no certificado, e o valor do ponto público.

CSM_142 Os parâmetros de domínio do elemento de dados contêm um dos identificadores de objeto especificados no quadro 1 para fazer referência a um conjunto de parâmetros de domínio normalizados.

CSM_143 O ponto público do elemento de dados contém o ponto público. Os pontos públicos da curva elíptica devem ser convertidos em cadeias de octetos, em conformidade com a Orientação Técnica TR-03111. Deve utilizar-se o formato de codificação não compactado. Ao recuperar um ponto de curva elíptica do seu formato codificado, devem efetuar-se sempre as validações descritas na Orientação Técnica TR-03111.

9.3.2.5 Referência do titular do certificado

CSM_144 A referência do titular do certificado é um identificador da chave pública fornecida no certificado. Utiliza-se para fazer referência a esta chave pública em outros certificados.

CSM_145 Relativamente a certificados de cartões e certificados de módulos GNSS externos, a referência do titular do certificado tem o tipo de dados `ExtendedSerialNumber`, especificado no apêndice 1.

CSM_146 No que se refere às unidades-veículo: sempre que pedir um certificado, o fabricante pode não conhecer o número de série específico do fabricante da VU para o qual se destina o certificado e a chave privada associada. Se o conhecer, a referência do titular do certificado tem o tipo de dados `ExtendedSerialNumber`, especificado no apêndice 1. Se não o conhecer, a referência do titular do certificado tem o tipo de dados `CertificateRequestID`, especificado no apêndice 1.

CSM_147 Em relação aos certificados ERCA e MSCA, a referência do titular do certificado tem o tipo de dados `CertificationAuthorityKID`, especificado no apêndice 1.

▼B

9.3.2.6 Data de vigência do certificado

CSM_148 A data de vigência do certificado indica a data e a hora de início do período de validade do certificado. A data de vigência do certificado é a data da criação do certificado.

9.3.2.7 Data de validade do certificado

CSM_149 A data de vigência do certificado indica a data e a hora de termo do período de validade do certificado.

9.3.2.8 Assinatura do certificado

CSM_150 A assinatura no certificado é criada sobre o corpo do certificado codificado, que inclui o marcador e o comprimento do corpo do certificado. O algoritmo de assinatura é ECDSA, conforme especificado em DSS, mediante utilização do algoritmo de hash ligado ao tamanho da chave da autoridade de assinatura, em conformidade com o CSM_50. O formato de assinatura deve ser simples, em conformidade com a Orientação Técnica TR-03111.

9.3.3 *Pedido de certificados*

CSM_151 Ao pedir um certificado, o requerente deve enviar à autoridade de certificação os seguintes dados:

— identificador de perfil do certificado pedido

— referência da autoridade de certificação a utilizar para a assinatura do certificado.

— chave pública a assinar

CSM_152 Num pedido de certificado à ERCA, para permitir que esta crie a referência do titular do novo certificado MSCA, a MSCA deve enviar os dados a seguir indicados, além dos que figuram no requisito CSM_151:

— código numérico da autoridade de certificação nacional (tipo de dados `NationNumeric`, definido no apêndice 1)

— código alfanumérico da autoridade de certificação nacional (tipo de dados `NationAlpha`, definido no apêndice 1)

— número de série de 1 byte que distingue as diferentes chaves da autoridade de certificação, caso sejam alteradas

— campo de dois bytes que contém informações adicionais específicas da autoridade de certificação

CSM_153 Num pedido de certificado a uma MSCA, para permitir que esta crie a referência do titular do novo certificado do equipamento, o fabricante do equipamento ou aparelho deve enviar os dados a seguir indicados, além dos que figuram no requisito CSM_151:

— identificador do tipo de equipamento, específico do fabricante

— se for conhecido (ver CSM_154), número de série do equipamento, único para o fabricante, para o tipo do equipamento e para o mês de fabrico; caso contrário, um identificador de pedido de certificado único

▼B

— mês e ano de fabrico do equipamento ou de pedido do certificado.

O fabricante assegura que estes dados estão corretos e que o certificado devolvido pela MSCA é inserido no equipamento a que se destina.

CSM_154 No caso de uma VU, o fabricante, quando pede um certificado, pode não conhecer o número de série específico do fabricante da VU ao qual se destinam o certificado e a chave privada associada. Se o conhecer, o fabricante da VU envia o número de série à MSCA. Se não o conhecer, o fabricante identifica cada pedido de certificado de forma única e envia o número de série do pedido de certificado à MSCA. O certificado obtido contém o número de série do pedido de certificado. Após a inserção do certificado numa VU específica, o fabricante comunica à MSCA a conexão entre o número de série do pedido de certificado e a identificação da VU.

10. AUTENTICAÇÃO MÚTUA E ENVIO SEGURO DE MENSAGENS ENTRE O CARTÃO E A VU

10.1. **Generalidades**

CSM_155 A um nível superior, a comunicação segura entre uma unidade-veículo e um cartão tacográfico baseia-se nos seguintes passos:

— Em primeiro lugar, cada parte demonstra à outra que possui um certificado de chave pública válido, assinado por uma autoridade de certificação do Estado-Membro. Por sua vez, o certificado de chave pública MSCA é assinado pela autoridade europeia de certificação de raiz. Este passo denomina-se «verificação da cadeia de certificados» e é pormenorizado na secção 10.2.

— Em segundo lugar, a unidade-veículo demonstra ao cartão que está de posse da chave privada correspondente à chave pública constante do certificado apresentado. Tal é feito através da assinatura de um número aleatório enviado pelo cartão. O cartão verifica a assinatura no número aleatório. Se esta verificação tiver êxito, a VU é autenticada. Este passo denomina-se «autenticação da VU» e é pormenorizado na secção 10.3.

— Em terceiro lugar, ambas as partes calculam, de modo independente, duas chaves de sessão AES que utilizam um algoritmo de concordância de chave assimétrica. Ao utilizar uma dessas chaves de sessão, o cartão cria um código de autenticação de mensagem (MAC) em alguns dados enviados pela VU. A VU verifica o MAC. Se esta verificação tiver êxito, o cartão é autenticado. Este passo denomina-se «autenticação do cartão» e é pormenorizado na secção 10.4.

— Em quarto lugar, a VU e o cartão utilizam as chaves de sessão acordadas para garantir a confidencialidade, a integridade e a autenticidade de todas as mensagens intercambiadas. Este passo denomina-se «envio seguro de mensagens» e é pormenorizado na secção 10.5.

CSM_156 O mecanismo descrito no requisito CSM_155 é acionado pela unidade-veículo sempre que o cartão for inserido numa das suas ranhuras para cartões.

▼B

10.2. **Verificação mútua da cadeia de certificados**

10.2.1 *Verificação da cadeia de certificados de cartão pela VU*

CSM_157 As unidades-veículo utilizam o protocolo descrito no esquema 4 para verificarem a cadeia de certificados dos cartões tacográficos.

Notas do esquema 4:

— Os certificados de cartão e as chaves públicas mencionados no esquema são os destinados à autenticação mútua. A secção 9.1.5 indica-os como Card_MA.

— Os certificados Card.CA e as chaves públicas mencionados no esquema são os destinados à assinatura dos certificados de cartão e estão indicados na CAR do certificado do cartão. A secção 9.1.3 indica-os como MSCA_Card.

— O certificado Card.CA.EUR mencionado no esquema é o certificado de raiz europeia indicado na CAR do certificado Card.CA.

— O certificado Card.Link mencionado no esquema é o certificado de ligação do cartão, caso exista. Em conformidade com a secção 9.1.2, trata-se de um certificado de ligação para um novo par de chaves de raiz europeia criado pela ERCA e assinado pela chave privada europeia anterior.

— O certificado Card.Link.EUR é o certificado de raiz europeia indicado na CAR do certificado Card.Link.

CSM_158 Conforme descrito no esquema 4, a verificação da cadeia de certificados dos cartões tem início com a inserção do cartão. A unidade-veículo lê a referência do titular do cartão (`cardExtendedSerialNumber`) a partir de EF ICC. Verifica se conhece o cartão, ou seja, se teve êxito na verificação da cadeia de certificados dos cartões no passado e a memorizou para referência futura. Em caso afirmativo e se o certificado do cartão ainda for válido, o processo continua, com a verificação da cadeia de certificados da VU. Caso contrário, a VU lê consecutivamente a partir do cartão o certificado MSCA_Card a utilizar para verificação do certificado do cartão, o certificado Card.CA.EUR a utilizar para verificação do certificado MSCA_Card e, possivelmente, o certificado de ligação, até localizar um certificado que conheça ou possa verificar. A VU utiliza então o certificado que conhece para verificar os certificados de cartão subjacentes que tenha lido a partir do cartão. Em caso de êxito, o processo continua com a verificação da cadeia de certificados da VU. Se não tiver êxito, a VU ignora o cartão.

▼B

Nota: Há três maneiras pelas quais a VU pode conhecer o certificado Card.CA.EUR:

— o certificado Card.CA.EUR é o mesmo que o certificado EUR da VU;

— o certificado Card.CA.EUR precede o certificado EUR da VU, e a VU continha este certificado já no momento da emissão (ver CSM_81);

— o certificado Card.CA.EUR sucede ao certificado EUR da VU, e a VU recebeu no passado, de outro cartão tacográfico, um certificado de ligação, que verificou e memorizou para referência futura.

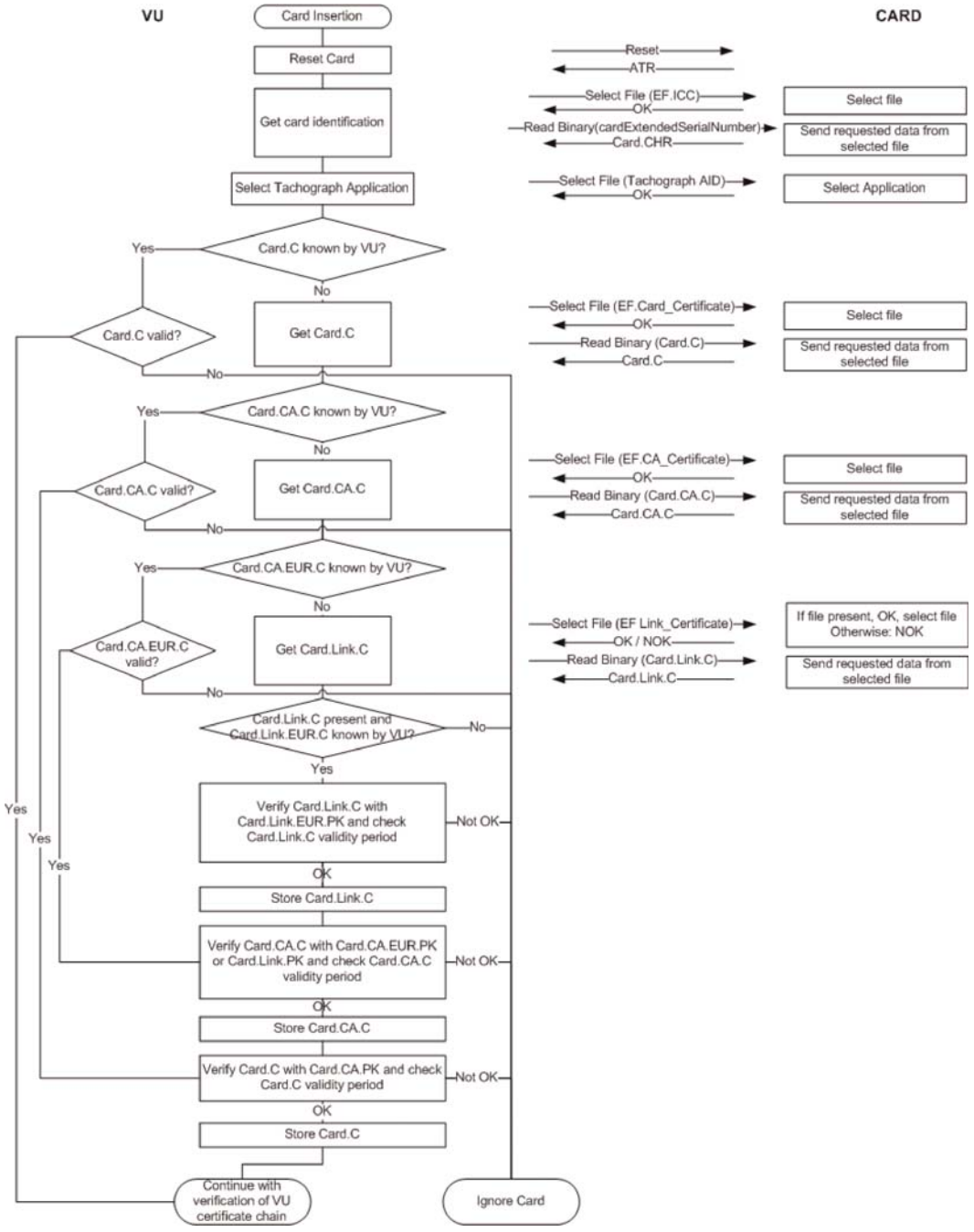
CSM_159 Conforme indica o esquema 4, assim que a VU tiver verificado a autenticidade e a validade de um certificado anteriormente desconhecido, pode memorizá-lo para referência futura, de tal forma que não precisa de verificar novamente a autenticidade se o certificado voltar a ser apresentado à VU. Em vez de memorizar todo o certificado, a VU pode optar por memorizar apenas o conteúdo do corpo, em conformidade com a secção 9.3.2.

CSM_160 A VU verifica a validade temporal de todos os certificados lidos a partir do cartão ou memorizados na sua memória e rejeita os certificados expirados. Para verificar a validade temporal de um certificado apresentado pelo cartão, a VU utiliza o seu relógio interno.

▼B

Esquema 4

Protocolo para a verificação da cadeia de certificado do cartão pela VU



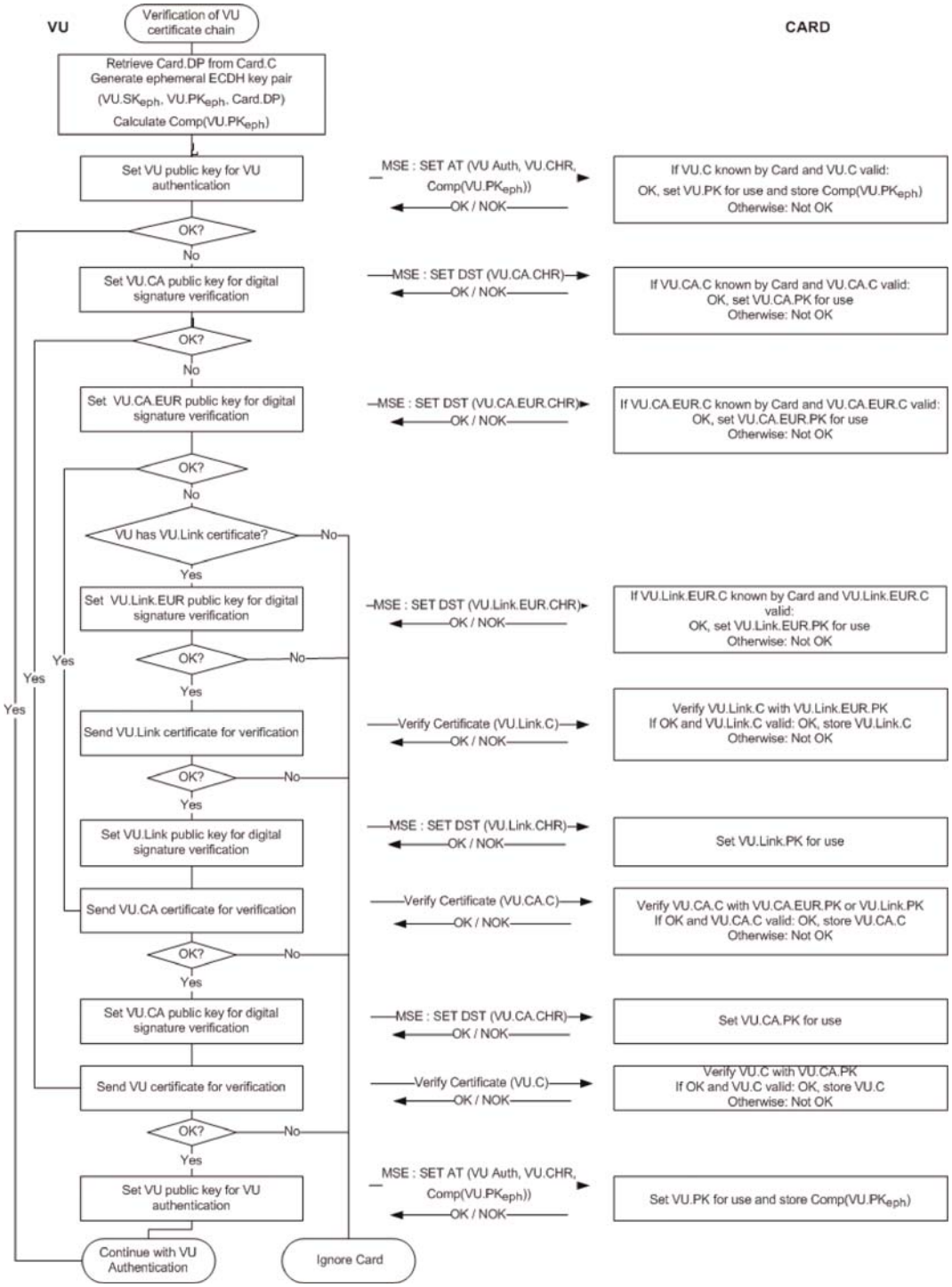
10.2.2 *Verificação da cadeia de certificado da VU pelo cartão*

CSM_161 Os cartões tacográficos utilizam o protocolo descrito no esquema 5 para a verificação da cadeia de certificados da VU.

▼B

Esquema 5

Protocolo para a verificação da cadeia de certificado da VU pelo cartão



Notas do esquema 5:

— Os certificados de VU e as chaves públicas mencionados no esquema são os destinados à autenticação mútua. A secção 9.1.4 indica-os como VU_MA.

▼B

— Os certificados VU.CA e as chaves públicas mencionados no esquema são os destinados à assinatura dos certificados da VU e do módulo GNSS externo. A secção 9.1.3 indica-os como MSCA_VU-EGF.

— O certificado VU.CA.EUR mencionado no esquema é o certificado de raiz europeia indicado na CAR do certificado VU.CA.

— O certificado VU.Link mencionado no esquema é o certificado de ligação da VU, caso exista. Em conformidade com a secção 9.1.2, trata-se de um certificado de ligação para um novo par de chaves de raiz europeia criado pela ERCA e assinado pela chave privada europeia anterior.

— O certificado VU.Link.EUR é o certificado de raiz europeia indicado na CAR do certificado VU.Link.

CSM_162 Conforme descrito no esquema 5, a verificação da cadeia de certificado da unidade-veículo tem início com a tentativa da unidade-veículo de definir a sua própria chave pública para utilização no cartão tacográfico. Se tal acontecer, significa que, no passado, o cartão verificou com êxito a cadeia de certificados da VU e memorizou o certificado da VU para referência futura. Neste caso, o certificado da VU é definido para utilização, e o processo continua, com a autenticação da VU. Se o cartão não conhecer o certificado da VU, esta deve apresentar consecutivamente o certificado VU.CA a utilizar para verificação do seu certificado de VU, o certificado VU.CA.EUR a utilizar para verificação do certificado VU.CA e, possivelmente, o certificado de ligação, a fim de localizar um certificado conhecido ou verificável pelo cartão. Se localizar um certificado, o cartão utiliza-o para verificar os certificados de VU subjacentes apresentados à VU. Em caso de êxito, a VU define finalmente a sua chave pública para utilização no cartão tacográfico. Se não tiver êxito, a VU ignora o cartão.

Nota: Há três maneiras pelas quais o cartão pode conhecer o certificado VU.CA.EUR:

— o certificado VU.CA.EUR é o mesmo que o certificado EUR do cartão

— o certificado VU.CA.EUR precede o certificado EUR do cartão, e o cartão continha este certificado já no momento da emissão (ver CSM_91)

— o certificado VU.CA.EUR sucede ao certificado EUR do cartão, e o cartão recebeu no passado, de outra unidade-veículo, um certificado de ligação, verificou-o e memorizou-o para referência futura.

CSM_163 A VU utiliza o comando MSE: Set AT para definir a sua chave pública para utilização no cartão tacográfico. Em conformidade com o apêndice 2, o comando contém uma indicação do mecanismo criptográfico que será utilizado com a chave definida. Este mecanismo é a autenticação da VU que utiliza o algoritmo ECDSA, em combinação com o algoritmo de hash ligado ao tamanho da chave do par de chaves VU_MA da VU, em conformidade com o requisito CSM_50.

▼B

CSM_164 O comando MSE: Set AT contém igualmente uma indicação do par de chaves efémeras que a VU utilizará durante a concordância de chave de sessão (ver secção 10.4). Por conseguinte, antes de enviar o comando MSE: Set AT, a VU cria um par de chaves ECC efémeras, para o que utiliza os parâmetros de domínio normalizados indicados no certificado do cartão. O par de chaves efémeras é indicado como ($VU.SK_{eph}$, $VU.PK_{eph}$, Card.DP). A VU recebe como identificação da chave da coordenada X do ponto público efémero ECDH. Trata-se da «representação compactada da chave pública» indicada como $Comp(VU.PK_{eph})$.

CSM_165 Se o comando MSE: Set AT tiver êxito, o cartão define o VU.PK indicado, para utilização posterior durante a autenticação do veículo, e memoriza temporariamente $Comp(VU.PK_{eph})$. Caso dois ou mais comandos MSE: Set AT com êxito sejam enviados antes de ser efetuada a concordância de chave de sessão, o cartão memoriza apenas o último $Comp(VU.PK_{eph})$ recebido.

CSM_166 O cartão verifica a validade temporal de todos os certificados apresentados pela VU ou referenciados pela VU, enquanto são memorizados na memória do cartão, e rejeita os certificados expirados.

CSM_167 Para verificar a validade temporal do certificado apresentado pela VU, cada cartão tacográfico memoriza internamente alguns dados que representam a hora atual. Estes dados não são diretamente atualizáveis por uma VU. Na emissão, a hora atual de um cartão deve ser igual à data de vigência do certificado Card_MA do cartão. Um cartão atualiza a sua hora se a data de vigência de um certificado «fonte de tempo válida» autêntico apresentado por uma VU for mais recente do que a hora atual do cartão. Nesse caso, o cartão define a sua hora atual para a data de vigência desse certificado. Como fonte de tempo válida, o cartão aceita apenas os seguintes certificados:

— Certificados de ligação ERCA da segunda geração

— Certificados MSCA da segunda geração

— Certificados de VU da segunda geração emitidos pelo mesmo país do próprio certificado dos cartões.

Nota: O último requisito implica que um cartão seja capaz de reconhecer a CAR do certificado de VU, ou seja, o certificado MSCA_VU-EGF. Este não será o mesmo que a CAR do seu próprio certificado, que é o certificado MSCA_Card.

CSM_168 Conforme indica o esquema 5, assim que o cartão tiver verificado a autenticidade e a validade de um certificado anteriormente desconhecido, pode memorizá-lo para referência futura, de tal modo que não precisa de verificar novamente a autenticidade do certificado se este voltar a ser-lhe

▼B

apresentado. Em vez de memorizar todo o certificado, o cartão pode optar por memorizar apenas o conteúdo do corpo, em conformidade com a secção 9.3.2.

10.3. **Autenticação da VU**

CSM_169 As unidades-veículo e os cartões utilizam o protocolo de autenticação da VU descrito no esquema 6 para autenticar a VU em relação ao cartão. A autenticação da VU permite que o cartão tacográfico verifique explicitamente se a VU é autêntica. Para isso, a VU utiliza a sua chave privada para assinar um desafio criado pelo cartão.

CSM_170 Ao lado do desafio do cartão, a VU inclui na assinatura a referência do titular do cartão retirada do certificado do cartão.

Nota: Garante-se assim que o cartão no qual a VU se autentica é o mesmo cuja cadeia de certificados a VU verificou anteriormente.

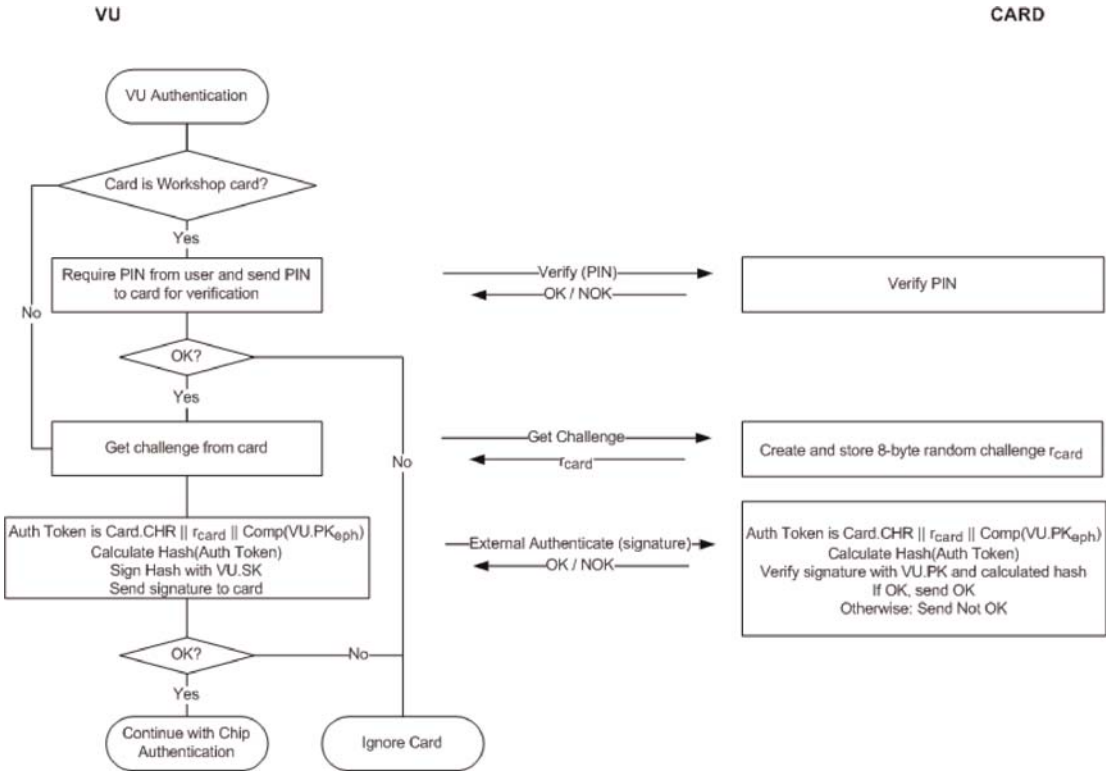
CSM_171 A VU inclui igualmente na assinatura o identificador da chave pública efémera Comp(VU.PK_{eph}) que a VU utiliza para configurar o envio seguro de mensagens durante o processo de autenticação de pastilha especificado na secção 10.4.

Nota: Garante-se assim que a VU com a qual o cartão comunica durante uma sessão de envio seguro de mensagens é a mesma que foi autenticada pelo cartão.

▼B

Esquema 6

Protocolo de autenticação da VU



CSM_172 Se, durante a sua autenticação, a VU enviar vários comandos GET CHALLENGE, o cartão devolve um novo desafio aleatório de 8 bytes, de cada vez, mas memoriza apenas o último desafio.

CSM_173 O algoritmo de assinatura utilizado pela VU para autenticação é ECDSA, em conformidade com DSS, que utiliza o algoritmo de hash ligado ao tamanho da chave do par de chaves VU_MA da VU, em conformidade com o requisito CSM_50. O formato de assinatura será simples, em conformidade com a Orientação Técnica TR-03111. A VU envia ao cartão a assinatura obtida.

CSM_174 Ao receber a assinatura da VU no comando EXTERNAL AUTHENTICATE, o cartão

— calcula o testemunho de autenticação mediante a concatenação Card.CHR, o desafio do cartão r_{card} e o identificador da chave pública efémera da VU Comp($VU.PK_{eph}$)

— calcula o hash sobre o testemunho de autenticação, que utiliza o algoritmo de hash ligado ao tamanho da chave do par de chaves VU_MA da VU, em conformidade com o requisito CSM_50

— verifica a assinatura da VU utilizando o algoritmo ECDSA em combinação com o VU.PK e o hash calculado.

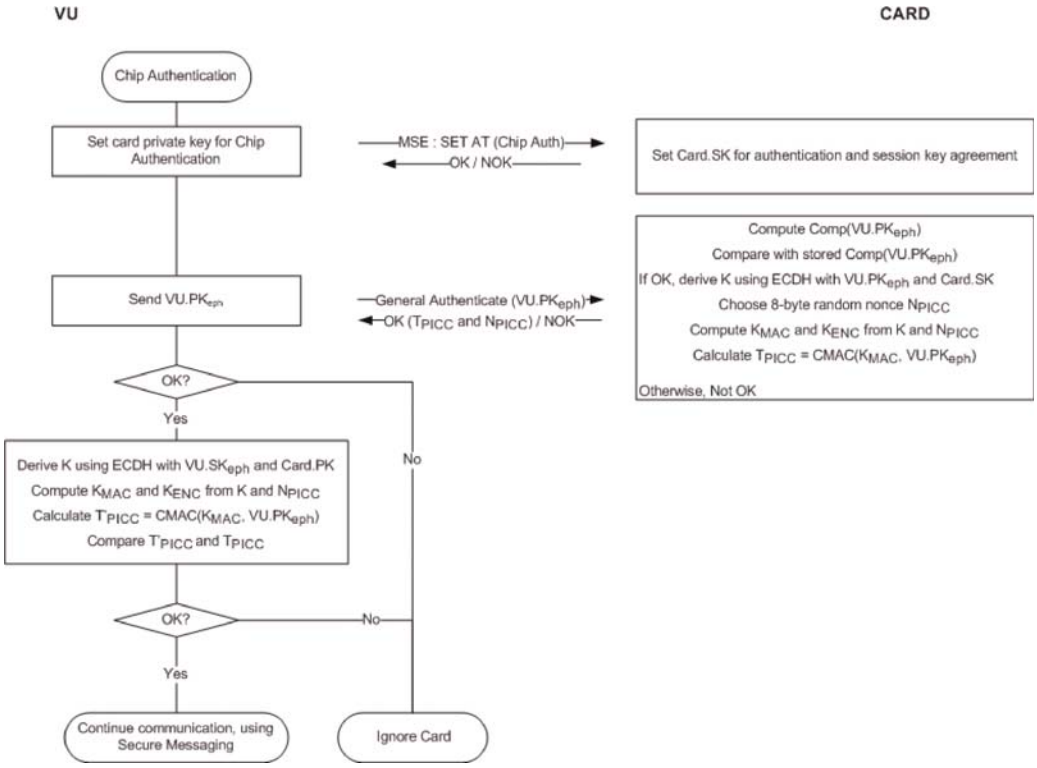
▼B

10.4. **Autenticação da pastilha e concordância de chave de sessão**

CSM_175 As unidades-veículo e os cartões utilizam o protocolo de autenticação da pastilha descrito no **esquema 7** para autenticar o cartão em relação à VU. A autenticação da pastilha permite que a unidade-veículo verifique explicitamente se o cartão é autêntico.

Esquema 7

Autenticação da pastilha e acordo de chave de sessão



CSM_176 A VU e o cartão tomam as seguintes medidas:

1. A unidade-veículo inicia o processo de autenticação da pastilha enviando o comando MSE: Set AT que indica «autenticação da pastilha utilizando o algoritmo ECDH que obtém um comprimento de chave de sessão AES ligado ao tamanho da chave do par de chaves Card_MA do cartão, em conformidade com o requisito CSM_50». A VU determina o tamanho da chave do par de chaves do cartão do certificado de cartão.

2. A VU envia para o cartão o ponto público $VU.PK_{eph}$ do seu par de chaves efémeras. Tal como explicado em CSM_164, a VU criou esse par de chaves efémeras antes da verificação da cadeia de certificado da VU. A VU enviou o identificador da chave pública efémera $Comp(VU.PK_{eph})$ para o cartão, que o memorizou.

▼B

3. O cartão calcula Comp($VU.PK_{eph}$) e compara o resultado com o valor memorizado de Comp($VU.PK_{eph}$).

4. O cartão calcula um k secreto, utilizando o algoritmo ECDH em combinação com a chave privada estática do cartão e a chave pública efémera da VU.

5. O cartão escolhe um valor de 8 bytes aleatórios N_{PICC} e utiliza-o para derivar duas chaves de sessão AES K_{MAC} e K_{ENC} de K (ver CSM_179).

6. Utilizando K_{MAC}, o cartão calcula um testemunho de autenticação sobre o identificador de chave pública efémera da VU: T_{PICC} = CMAC(K_{MAC}, $VU.PK_{eph}$). O cartão envia N_{PICC} e T_{PICC} para a unidade-veículo.

7. À semelhança do que o cartão fez no passo 4, a VU calcula um k secreto, utilizando o algoritmo ECDH em combinação com a chave pública estática do cartão e a chave privada efémera da VU.

8. A VU deriva chaves de sessão K_{MAC} e K_{ENC} de K e N_{PICC} (ver CSM_179).

9. A VU verifica o testemunho de autenticação T_{PICC}.

CSM_177 No passo 3, o cartão calcula Comp(VU.PKeph) como abcissa do ponto público em VU.PKeph.

CSM_178 Nos passos 4 e 7, o cartão e a unidade-veículo utilizam o algoritmo ECKA-EG definido na Orientação Técnica TR-03111.

CSM_179 Nos passos 5 e 8, o cartão e a unidade-veículo utilizam a função de derivação da chave para as chaves de sessão AES definidas na Orientação Técnica TR-03111, com as seguintes precisões e alterações:

— O valor do contador é '00 00 00 01' para K_{ENC} e '00 00 00 02' para K_{MAC}.

— O valor aleatório opcional *r* é utilizado e igual a N_{PICC}.

— Para derivar chaves AES de 128 bits, o algoritmo de hash a utilizar é SHA-256.

— Para derivar chaves AES de 192 bits, o algoritmo de hash a utilizar é SHA-384.

— Para derivar chaves AES de 256 bits, o algoritmo de hash a utilizar é SHA-512.

O comprimento das chaves de sessão (ou seja, o comprimento a que o hash é truncado) é ligado ao tamanho do par de chaves Card_MA, em conformidade com o requisito CSM_50.

▼B

CSM_180 Nos passos 6 e 9, o cartão e a unidade-veículo utilizam o algoritmo AES no modo CMAC, em conformidade com SP 800-38B. O comprimento de T_{PICC} está ligado ao comprimento das chaves de sessão AES, em conformidade com o requisito CSM_50.

10.5. **Envio seguro de mensagens**

10.5.1 *Generalidades*

CSM_181 Todos os comandos e respostas intercambiados entre uma unidade-veículo e um cartão tacográfico, após uma autenticação da pastilha com êxito e até ao fim da sessão, estão protegidos pelo envio seguro de mensagens.

CSM_182 Exceto quando da leitura de um ficheiro com condição de acesso SM-R-ENC-MAC-G2 (ver apêndice 2, secção 4), o envio seguro de mensagens é utilizado no modo «apenas autenticação», no qual é adicionada uma soma criptográfica de teste (a.k.a. MAC) a todos os comandos e respostas para garantir a autenticidade e a integridade das mensagens.

CSM_183 Ao ler dados de um ficheiro com condição de acesso SM-R--ENC-MAC-G2, o envio seguro de mensagens é utilizado no modo «encriptar depois autenticar», ou seja, os dados de resposta são encriptados primeiro para garantir a confidencialidade da mensagem, e em seguida é calculado um MAC sobre os dados encriptados formatados, para garantir a autenticidade e a integridade.

CSM_184 O envio seguro de mensagens utiliza AES, definido em AES, com as chaves de sessão K_{MAC} e K_{ENC} acordadas durante a autenticação da pastilha.

CSM_185 De modo a evitar ataques de reprodução, utiliza-se um número inteiro não assinado como o contador de sequências de envio (SSC). O tamanho do SSC é igual ao tamanho do bloco AES, ou seja, 128 bits. O SSC está no formato de primeiro MSB. O contador de sequências de envio é inicializado a zero (ou seja, '00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00') quando se iniciar o envio seguro de mensagens. O SSC aumenta sempre antes de ser criado um comando ou resposta APDU; ou seja, uma vez que o valor de início do SSC numa sessão SM é 0, no primeiro comando o valor do SSC será 1. O valor do SSC para a primeira resposta será 2.

CSM_186 No que se refere a encriptação de mensagens, utiliza-se K_{ENC} com AES no modo de funcionamento por cifragem progressiva (CBC), definido na norma ISO 10116, com um parâmetro intercalar $m = 1$ e um vetor de inicialização SV = E (K_{ENC}, SSC), ou seja, o valor atual do contador de sequências de envio encriptado com K_{ENC}.

CSM_187 Relativamente à autenticação de mensagens, utiliza-se K_{MAC} com AES no modo CMAC, em conformidade com SP 800-38B. O comprimento do MAC está ligado ao comprimento das chaves de sessão AES, em conformidade com o requisito CSM_50. O contador de sequências de envio estará incluído no MAC, prefixando-o antes da autenticação do datagrama.

▼B

10.5.2 *Estrutura do envio seguro de mensagens*

CSM_188 O envio seguro de mensagens faz uso apenas dos objetos de dados do envio seguro de mensagens (ver norma ISO 7816-4) enumerados no quadro 5. Estes objetos de dados serão utilizados em todas as mensagens, segundo a ordem especificada neste quadro.

Quadro 5

Objetos de dados do envio seguro de mensagens

Nome do objeto de dados	Marcador	Presença (O)brigatória, (C)ondicional ou (P)roibida:	
		Comandos	Respostas
Valor simples não codificado em BER-TLV	'81'	C	C
Valor simples codificado em BER-TLV, mas que não inclui SM DO	'B3'	C	C
Indicador de conteúdo de preenchimento seguido por criptograma, valor simples não codificado em BER-TLV	'87'	C	C
Le protegido	'97'	C	F
Estado de processamento	'99'	F	M
Soma criptográfica de teste	'8E'	M	M

Nota: Em conformidade com o apêndice 2, os cartões tacográficos podem aceitar os comandos READ BINARY e UPDATE BINARY com um byte INS ímpar (respetivamente, 'B1' e 'D7'). Estas variantes de comando são necessárias para ler e atualizar os ficheiros com 32 768 bytes ou mais. Caso se recorra a tal variante, utiliza-se um objeto de dados com o marcador 'B3' em vez de um objeto com marcador '81' (ver apêndice 2 para mais informações).

CSM_189 Todos os objetos de dados SM são codificados em DER TLV, em conformidade com a norma ISO 8825-1. Esta codificação resulta numa estrutura Marcador-Comprimento-Valor (TLV), nos seguintes termos:

Marcador: O marcador está codificado em um ou dois octetos e indica o conteúdo.

Comprimento: O comprimento é codificado como número inteiro não assinado, em um, dois ou três octetos, que resultam num comprimento máximo de 65 535 octetos. Utiliza-se o número mínimo de octetos.

Valor: O valor é codificado em zero ou mais octetos.

CSM_190 As APDU protegidas pelo envio seguro de mensagens são criadas do seguinte modo:

— O cabeçalho de comando é incluído no cálculo do MAC; por conseguinte, utiliza-se o valor '0C' para o CLA do byte de classe.

▼B

— Em conformidade com o apêndice 2, todos os bytes INS são pares, com a possível exceção de bytes INS ímpares para os comandos READ BINARY e UPDATE BINARY.

— O valor real de Lc é modificado para Lc após a aplicação do envio seguro de mensagens.

— O campo de dados é composto por objetos de dados SM.

— Na APDU de comando protegido, o novo byte Le é colocado no valor '00'. Se necessário, inclui-se um objeto de dados '97' no campo de dados, a fim de transmitir o valor original de Le.

CSM_191 Qualquer objeto de dados a encriptar é preenchido de acordo com a norma ISO 7816-4, mediante a utilização do indicador de conteúdo de preenchimento '01'. Relativamente ao cálculo do MAC, cada objeto de dados é igualmente preenchido em separado na APDU, de acordo com a norma ISO 7816-4.

Nota: O preenchimento para envio seguro de mensagens é efetuado sempre pelo nível de envio seguro de mensagens e não pelos algoritmos CMAC ou CBC.

Síntese e exemplos

Uma APDU de comando com envio seguro de mensagens aplicado terá a estrutura seguinte, consoante a caixa do comando não seguro correspondente (DO é objeto de dados):

Caixa 1:	CLA INS P1 P2 || Lc' || DO '8E' || Le
Caixa 2:	CLA INS P1 P2 || Lc' || DO '97' || DO'8E' || Le
Caixa 3 (byte INS par):	CLA INS P1 P2 || Lc' || DO '81' || DO'8E' || Le
Caixa 3 (byte INS ímpar):	CLA INS P1 P2 || Lc' || DO 'B3' || DO'8E' || Le
Caixa 4 (byte INS par):	CLA INS P1 P2 || Lc' || DO '81' || DO'97' || DO'8E' || Le
Caixa 4 (byte INS ímpar):	CLA INS P1 P2 || Lc' || DO 'B3' || DO'97' || DO'8E' || Le

onde Le = '00' ou '00 00', consoante se utilizem campos de comprimento curto ou campos de comprimento alargado (ver norma ISO 7816-4).

Uma APDU de resposta, com envio seguro de mensagens aplicado, tem a seguinte estrutura, consoante a caixa do comando não seguro correspondente (DO é objeto de dados):

Caixa 1 ou 3:	DO '99' || DO '8E' || SW1SW2
Caixa 2 ou 4 (byte INS par) com encriptação:	DO '81' || DO '99' || DO '8E' || SW1SW2
Caixa 2 ou 4 (byte INS par) sem encriptação:	DO '87' || DO '99' || DO '8E' || SW1SW2
Caixa 2 ou 4 (byte INS ímpar) sem encriptação:	DO 'B3' || DO '99' || DO '8E' || SW1SW2

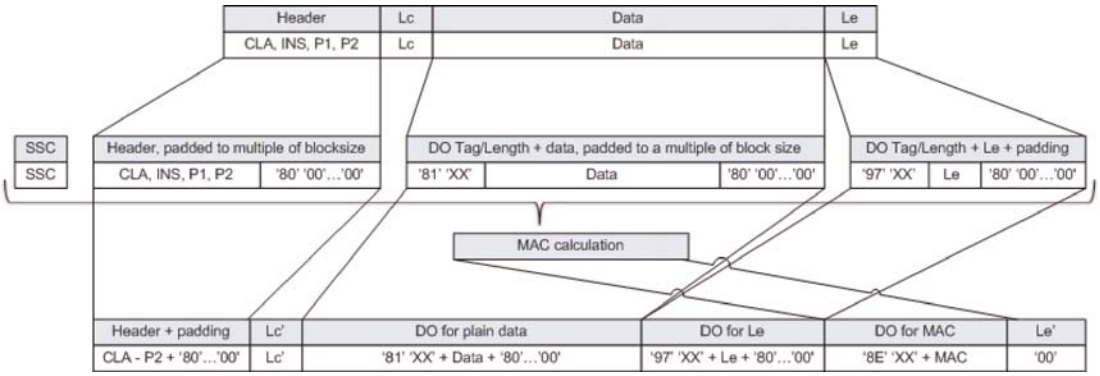
Nota: A caixa 2 ou 4 (byte INS ímpar) com encriptação nunca é utilizada na comunicação entre uma VU e um cartão.

▼B

Seguem-se três exemplos de transformações da APDU para comandos com código INS par. O esquema 8 apresenta uma APDU de comando da caixa 4 autenticada, o esquema 9 apresenta uma APDU de resposta da caixa 2/caixa 4 autenticada e o esquema 10 apresenta uma APDU de resposta da caixa 2/caixa 4 encriptada e autenticada.

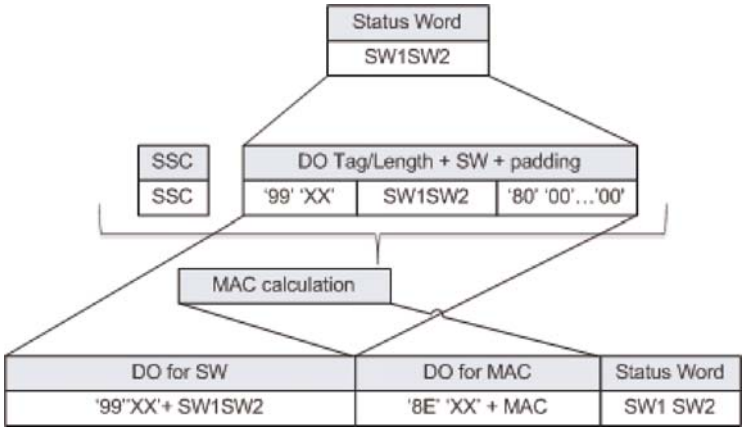
Esquema 8

Transformação de uma APDU de comando da caixa 4 autenticada



Esquema 9

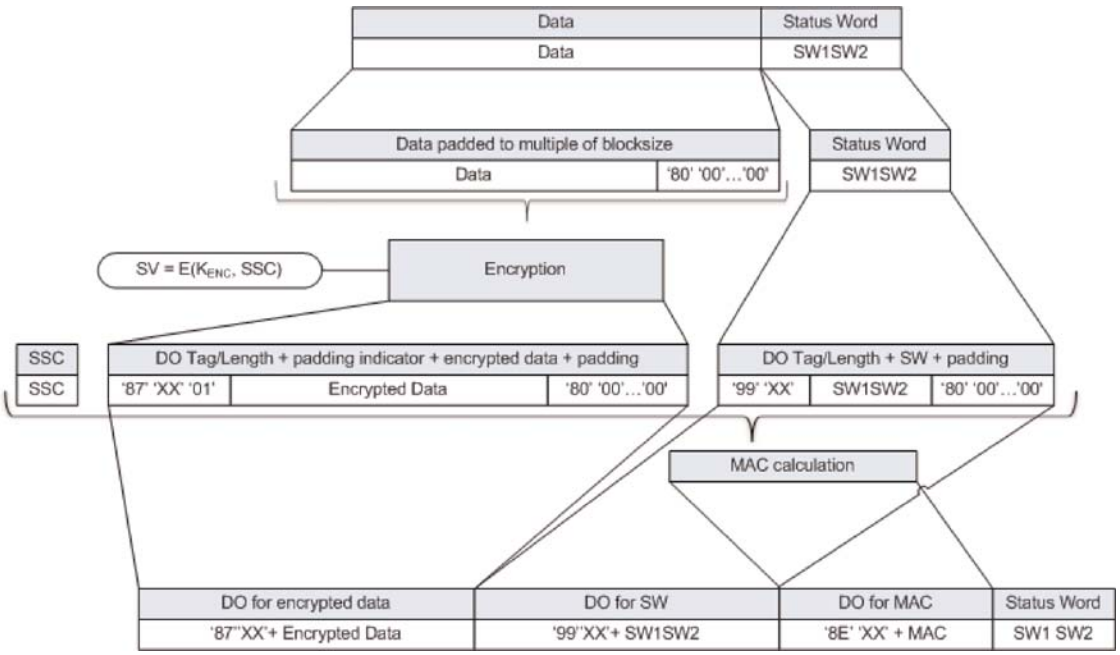
Transformação de uma APDU de resposta da caixa 2/ caixa 4 autenticada



▼B

Esquema 10

Transformação de uma APDU de resposta da caixa 2/ caixa 4 encriptada e autenticada



10.5.3 *Interrupção da sessão de envio seguro de mensagens*

CSM_192 A unidade-veículo interrompe uma sessão de envio seguro de mensagens contínua se e só se ocorrer uma das seguintes condições:

— recebe uma APDU de resposta simples

— deteta um erro de envio seguro de mensagens numa APDU de resposta:

  — está ausente um (esperado) objeto de dados do envio seguro de mensagens, está incorreta a ordem dos objetos de dados ou está incluído um objeto de dados desconhecido

  — está incorreto um objeto de dados do envio seguro de mensagens: por exemplo, o valor MAC está incorreto, a estrutura TLV está incorreta ou o indicador de preenchimento no marcador '87' não é igual a '01'

— o cartão envia um tipo de estado a indicar que detetou um erro SM (ver CSM_194)

— é atingido o limite para o número de comandos e respostas associados na sessão atual. Em relação a uma determinada VU, esse limite é definido pelo fabricante, tendo em conta os requisitos de segurança do equipamento informático utilizado, com um valor máximo de 240 comandos SM e respostas associadas por sessão.

▼B

CSM_193 O cartão tacográfico interrompe uma sessão de envio seguro de mensagens contínua se e só se ocorrer uma das seguintes condições:

— recebe uma APDU de comando simples

— deteta um erro de envio seguro de mensagens numa APDU de comando:

— está ausente um (esperado) objeto de dados do envio seguro de mensagens, está incorreta a ordem dos objetos de dados ou está incluído um objeto de dados desconhecido

— está incorreto um objeto de dados do envio seguro de mensagens: por exemplo, o valor MAC está incorreto ou a estrutura TLV está incorreta

— é desligado da energia elétrica ou reinicializado

— a VU seleciona uma aplicação no cartão

— a VU inicia o processo da sua autenticação

— é atingido o limite para o número de comandos e respostas associados na sessão atual. Em relação a um determinado cartão, esse limite é definido pelo fabricante, tendo em conta os requisitos de segurança do equipamento informático utilizado, com um valor máximo de 240 comandos SM e respostas associadas por sessão.

CSM_194 Em relação ao tratamento de erros SM por um cartão tacográfico:

— o cartão tacográfico responde com os bytes de estatuto '69 87' se estiverem ausentes alguns objetos de dados de envio seguro de mensagens numa APDU de comando, se estiver incorreta a ordem dos objetos de dados ou se estiverem incluídos objetos de dados desconhecidos

— o cartão tacográfico responde com bytes de estatuto '69 88' se um objeto de dados de envio seguro de mensagens estiver incorreto numa APDU de comando.

Em tal caso, os bytes de estatuto são devolvidos sem utilizar SM.

CSM_195 Se uma sessão de envio seguro de mensagens entre uma VU e um cartão tacográfico for interrompida, a VU e o cartão tacográfico:

— destroem as chaves de sessão memorizadas com segurança

— estabelecem imediatamente uma nova sessão de envio seguro de mensagens, conforme referido nas secções 10.2 a 10.5.

CSM_196 Se, por qualquer motivo, a VU decidir reiniciar a autenticação mútua em relação a um cartão inserido, o processo reinicia-se com a verificação da cadeia de certificado do cartão, conforme referido na secção 10.2, continuando como referido nas secções 10.2 a 10.5.

▼B

11. ACOPLAMENTO, AUTENTICAÇÃO MÚTUA E ENVIO SEGURO DE MENSAGENS DO MÓDULO GNSS EXTERNO COM A VU

11.1. **Generalidades**

CSM_197 O módulo GNSS utilizado por uma VU para determinar a sua posição pode ser interno (ou seja, incorporado na caixa da VU e não desmontável) ou externo. No primeiro caso, não há necessidade de uniformizar as comunicações internas entre o módulo GNSS e a VU, não se aplicando os requisitos do presente capítulo. No segundo caso, as comunicações entre a VU e o módulo GNSS externo são uniformizadas e protegidas, conforme descrito no presente capítulo.

CSM_198 A comunicação segura entre uma unidade-veículo e um módulo GNSS externo deve ter lugar do mesmo modo que a comunicação segura entre uma unidade-veículo e um cartão tacográfico, assumindo o módulo GNSS externo (EGF) o papel do cartão. Todos os requisitos do capítulo 10, relativos aos cartões tacográficos, são cumpridos por um EGF, tendo em conta os desvios, os esclarecimentos e os aditamentos do presente capítulo. Nomeadamente, a verificação mútua da cadeia de certificados, a autenticação da VU e a autenticação da pastilha são efetuadas conforme descrito nas secções 11.3 e 11.4.

CSM_199 A comunicação entre uma unidade-veículo e um EGF difere da comunicação entre uma unidade-veículo e um cartão, na medida em que, antes de poderem intercambiar dados com recurso a GNSS durante o funcionamento normal, uma VU e um EGF têm primeiro de ser acoplados numa oficina. O processo de acoplamento é descrito na secção 11.2.

CSM_200 Para a comunicação entre uma VU e um EGF, utilizam-se os comandos e respostas APDU baseados nas normas ISO 7816-4 e ISO 7816-8. A estrutura exata destas APDU é definida no apêndice 2 do presente anexo.

11.2. **Acoplamento da VU e do módulo GNSS externo**

CSM_201 O acoplamento da unidade-veículo com o EGF num veículo é efetuado por uma oficina. Apenas uma unidade-veículo e um EGF acoplados estão capacitados para comunicar durante o funcionamento normal.

CSM_202 O acoplamento de uma unidade-veículo e de um EGF só é possível se a unidade-veículo estiver em modo de calibração. O acoplamento deve ser iniciado pela unidade-veículo.

CSM_203 Uma oficina pode, a qualquer momento, reacoplar uma unidade-veículo a outro EGF ou ao mesmo EGF. Durante o reacoplamento, a VU destrói, de modo seguro, o certificado EGF_MA existente na sua memória e memoriza o certificado EGF_MA do EGF ao qual está a ser acoplada.

CSM_204 Uma oficina pode, a qualquer momento, reacoplar um módulo GNSS externo a outra VU ou à mesma VU. Durante o reacoplamento, o EGF destrói, de modo seguro, o certificado VU_MA existente na sua memória e memoriza o certificado VU_MA da VU à qual está a ser acoplado.

▼B

11.3. **Verificação mútua da cadeia de certificados**

11.3.1 *Generalidades*

CSM_205 A verificação mútua da cadeia de certificados entre uma VU e um EGF é efetuada por uma oficina e apenas durante o acoplamento da VU ao EGF. Durante o funcionamento normal de uma VU e um EGF acoplados, não se verificam certificados. Em vez disso, a VU e o FEG aprovam os certificados que memorizaram durante o acoplamento, após verificação da validade temporal desses certificados. Durante o funcionamento normal, a VU e o EGF não aprovam quaisquer outros certificados, de modo a proteger as comunicações entre a VU e o EGF.

11.3.2 *Durante o acoplamento VU-EGF*

CSM_206 Durante o acoplamento a um EGF, a unidade-veículo utiliza o protocolo descrito no esquema 4 (secção 10.2.1) para verificação da cadeia de certificados do módulo GNSS externo.

Notas do esquema 4 neste contexto:

— O controlo das comunicações está fora do âmbito do presente apêndice. No entanto, um EGF não é um cartão inteligente, pelo que, provavelmente, a VU não envia uma reinicialização para iniciar a comunicação nem recebe um ATR.

— Os certificados de cartão e as chaves públicas mencionados no esquema são interpretados como os certificados e chaves públicas do EGF para autenticação mútua. A secção 9.1.6 indica-os como EGF_MA.

— Os certificados Card.CA e as chaves públicas mencionados no esquema são interpretados como os certificados e chaves públicas de MSCA para assinatura de certificados EGF. A secção 9.1.3 indica-os como MSCA_VU-EGF.

— O certificado Card.CA.EUR mencionado no esquema é interpretado como o certificado de raiz europeia indicado na CAR do certificado MSCA_VU-EGF.

— O certificado Card.Link mencionado no esquema é interpretado como o certificado de ligação do EGF, caso exista. Em conformidade com a secção 9.1.2, trata-se de um certificado de ligação para um novo par de chaves de raiz europeia criado pela ERCA e assinado pela chave privada europeia anterior.

— O certificado Card.Link.EUR é o certificado de raiz europeia indicado na CAR do certificado Card.Link.

— Em vez de `cardExtendedSerialNumber`, a VU lê `sensorGNSSserialNumber`de EF ICC.

— Em vez de selecionar o AID do tacógrafo, a VU seleciona o AID EGF.

— «Ignorar cartão» deve ser interpretado como «Ignorar EGF».

▼B

CSM_207 Após verificar o certificado EGF_MA, a VU memoriza-o para utilização durante o funcionamento normal (ver secção 11.3.3).

CSM_208 Durante o acoplamento a uma VU, o módulo GNSS externo utiliza o protocolo descrito no esquema 5 (secção 10.2.2) para verificação da cadeia de certificados da VU.

Notas do esquema 5 neste contexto:

— A VU cria um novo par de chaves efémeras com recurso aos parâmetros de domínio no certificado EGF.

— Os certificados de VU e as chaves públicas mencionados no esquema são os destinados à autenticação mútua. A secção 9.1.4 indica-os como VU_MA.

— Os certificados VU.CA e as chaves públicas mencionados no esquema são os destinados à assinatura dos certificados da VU e do módulo GNSS externo. A secção 9.1.3 indica-os como MSCA_VU-EGF.

— O certificado VU.CA.EUR mencionado no esquema é o certificado de raiz europeia indicado na CAR do certificado VU.CA.

— O certificado VU.Link mencionado no esquema é o certificado de ligação da VU, caso exista. Em conformidade com a secção 9.1.2, trata-se de um certificado de ligação para um novo par de chaves de raiz europeia criado pela ERCA e assinado pela chave privada europeia anterior.

— O certificado VU.Link.EUR é o certificado de raiz europeia indicado na CAR do certificado VU.Link.

CSM_209 Em desvio do requisito CSM_167, um EGF utiliza a hora GNSS para verificação da validade temporal dos certificados apresentados.

CSM_210 Após verificar o certificado VU_MA, o módulo GNSS externo memoriza-o para utilização durante o funcionamento normal (ver secção 11.3.3).

11.3.3 *Durante o funcionamento normal*

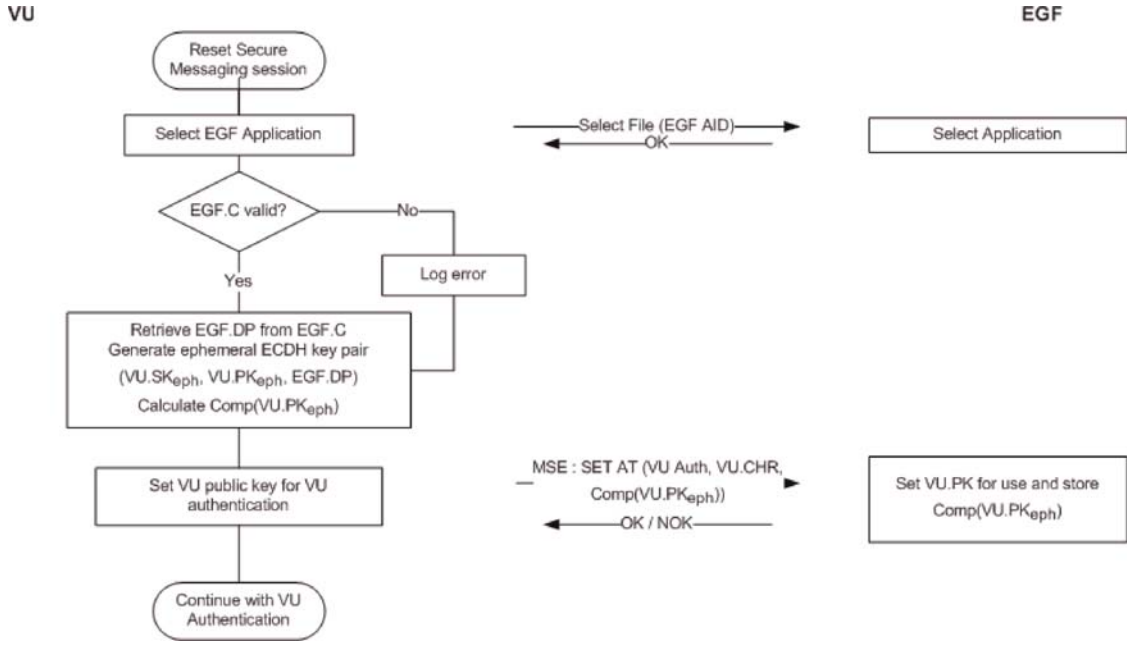
CSM_211 Durante o funcionamento normal, uma unidade-veículo e um EGF utilizam o protocolo descrito no esquema 11 para verificar a validade temporal dos certificados EGF_MA e VU_MA memorizados e para definir a chave pública VU_MA para autenticação subsequente da VU. Durante o funcionamento normal, não têm lugar verificações mútuas adicionais do certificado.

Importa lembrar que o esquema 11 consiste essencialmente nos primeiros passos apresentados no esquema 4 e no esquema 5. Importa lembrar ainda que, como um EGF não é um cartão inteligente, a VU provavelmente não envia uma reinicialização para iniciar a comunicação nem recebe um ATR. De qualquer modo, o controlo das comunicações está fora do âmbito do presente apêndice.

▼B

Esquema 11

Verificação mútua da validade temporal do certificado durante o funcionamento normal da VU com o EGF



CSM_212 Como mostra o esquema 11, se o certificado EGF_MA já não for válido, a unidade-veículo regista um erro. No entanto, a autenticação mútua, a concordância de chave e as comunicações subsequentes através do envio seguro de mensagens continuam normalmente.

11.4. **Autenticação da VU, autenticação da pastilha e concordância de chave de sessão**

CSM_213 A autenticação da VU, a autenticação da pastilha e a concordância de chave de sessão entre uma VU e um EGF ocorrem durante o acoplamento ou sempre que, durante o funcionamento normal, seja restabelecida uma sessão de envio seguro de mensagens. A VU e o EGF executam os processos descritos nas secções 10.3 e 10.4. Aplicam-se todos os requisitos constantes das presentes secções.

11.5. **Envio seguro de mensagens**

CSM_214 Todos os comandos e respostas intercambiados entre uma unidade-veículo e um módulo GNSS externo, após uma autenticação da pastilha com êxito e até ao fim da sessão, estão protegidos pelo envio seguro de mensagens no modo «apenas autenticação». Aplicam-se todos os requisitos da secção 10.5.

CSM_215 Se uma sessão de envio seguro de mensagens entre a VU e o EGF for interrompida, a VU estabelece imediatamente uma nova sessão de envio seguro de mensagens, conforme se descreve nas secções 11.3.3 e 11.4.

12. Emparelhamento e comunicações do sensor de movimentos com a VU

12.1. **Generalidades**

CSM_216 Durante o emparelhamento e o funcionamento normal, a unidade-veículo e o sensor de movimentos comunicam utilizando o protocolo de interface especificado na norma ISO 16844-3, com as alterações descritas no presente capítulo e na secção 9.2.1.

▼B

Nota: presume-se que os leitores deste capítulo estão familiarizados com o conteúdo da norma ISO 16844-3.

12.2. **Emparelhamento do sensor de movimentos com a VU, utilizando gerações de chaves diferentes**

Conforme explicado na secção 9.2.1, a chave de segurança do sensor de movimentos e todas as chaves associadas são substituídas periodicamente, o que pode conduzir a que, nos cartões de oficina, haja três chaves AES relativas ao sensor de movimentos $K_{M\text{-}WC}$ (de gerações de chaves consecutivas). De modo semelhante, pode haver nos sensores de movimentos até três encriptações de dados diferentes com recurso a AES (baseadas em gerações consecutivas da chave de segurança do sensor de movimentos K_M). Uma unidade-veículo contém apenas uma chave relativa ao sensor de movimentos $K_{M\text{-}VU}$.

CSM_217 A VU da segunda geração e o sensor de movimentos da segunda geração estão emparelhados do seguinte modo (comparar quadro 6 da norma ISO 16844-3):

1. O cartão de oficina da segunda geração é inserido na VU e a VU está ligada ao sensor de movimentos.

2. A VU lê todas as chaves $K_{M\text{-}WC}$ disponíveis do cartão de oficina, inspeciona os respetivos números de versão de chave e escolhe a que corresponde ao número de versão de chave da VU $K_{VU\text{-}M}$. Se no cartão de oficina não existir a correspondente chave $K_{M\text{-}WC}$, a VU interrompe o processo de emparelhamento e apresenta uma mensagem de erro apropriada ao titular do cartão de oficina.

3. A VU calcula a chave de segurança do sensor de movimentos K_M de $K_{M\text{-}VU}$ e $K_{M\text{-}WC}$, bem como a chave de identificação K_{ID} de K_M, em conformidade com a secção 9.2.1.

4. A VU envia a instrução para iniciar o processo de emparelhamento em relação ao sensor de movimentos, conforme consta da norma ISO 16844-3, e encripta o número de série que recebe do sensor de movimentos com a chave de identificação K_{ID}. A VU envia ao sensor de movimentos o número de série encriptado.

5. O sensor de movimentos faz corresponder o número de série encriptado consecutivamente com cada uma das encriptações do número de série que possui internamente. Se encontrar correspondência, a VU é autenticada. O sensor de movimentos regista a geração de K_{ID} utilizado pela VU e devolve a correspondente versão encriptada da sua chave de emparelhamento, ou seja, a encriptação criada com utilização da mesma geração de K_M.

6. A VU decifra a chave de emparelhamento utilizando K_M, cria uma chave de sessão K_S, encripta-a com a chave de emparelhamento e envia o resultado para o sensor de movimentos. O sensor de movimentos decifra K_S.

7. A VU reúne as informações de emparelhamento, conforme a norma ISO 16844-3 define, encripta as informações com a chave de emparelhamento e envia o resultado para o sensor de movimentos. O sensor de movimentos decifra as informações de emparelhamento.

8. O sensor de movimentos encripta as informações de emparelhamento recebidas com o K_S recebido e devolve-o à VU. A VU verifica se as informações de emparelhamento são as mesmas informações que enviou para o sensor de movimentos no passo anterior. Em caso afirmativo, prova-se que o sensor de movimentos utilizou o

▼B

mesmo K_S que a VU e, portanto, no passo 5 enviou a sua chave de emparelhamento encriptada com a geração correta de K_M. Assim, o sensor de movimentos é autenticado.

De salientar que os passos 2 e 5 são diferentes dos do processo uniformizado constante da norma ISO 16844-3. Os outros passos estão uniformizados.

Exemplo: Suponhamos que um emparelhamento ocorre no primeiro ano de validade do certificado ERCA (3) (ver esquema 2 na secção 9.2.1.2). Além disso,

— Suponhamos que o sensor de movimentos foi emitido no último ano de validade do certificado ERCA (1). Por conseguinte, conterá os seguintes dados e chaves:

  — $N_s[1]$: número de série encriptado com a geração 1 de K_{ID}

  — $N_s[2]$: número de série encriptado com a geração 2 de K_{ID}

  — $N_s[3]$: número de série encriptado com a geração 3 de K_{ID}

  — $K_P[1]$: chave de emparelhamento da geração 1 ([1]), encriptada com a geração 1 de K_M

  — $K_P[2]$: chave de emparelhamento da geração 2, encriptada com a geração 2 de K_M

  — $K_P[3]$: chave de emparelhamento da geração 3, encriptada com a geração 3 de K_M.

— Suponhamos que o cartão de oficina foi emitido no primeiro ano de validade do certificado ERCA (3). Por conseguinte, conterá a geração 2 e a geração 3 da chave $K_{M\text{-}WC}$.

— Suponhamos que a VU é uma VU da geração 2, que contém a geração 2 de $K_{M\text{-}VU}$.

Neste caso, acontecerá o seguinte nos passos 2 a 5:

— Passo 2: a VU lê a geração 2 e a geração 3 de $K_{M\text{-}WC}$ do cartão de oficina e inspeciona os respetivos números de versão.

— Passo 3: a VU combina a geração 2 de $K_{M\text{-}WC}$ com o seu $K_{VU\text{-}M}$ para calcular K_M e K_{ID}.

— Passo 4: a VU encripta o número de série que recebe do sensor de movimentos com K_{ID}.

— Passo 5: o sensor de movimentos compara os dados recebidos com $N_s[1]$ e não encontra correspondências. Em seguida, compara os dados com $N_s[2]$ e encontra uma correspondência. Conclui que a VU é uma VU da geração 2 e, por conseguinte, devolve $K_P[2]$.

([1]) De salientar que as chaves de emparelhamento da geração 1, da geração 2 e da geração 3 podem, na realidade, ser a mesma chave. Ou pode haver três chaves diferentes com comprimentos diferentes, conforme se explica no requisito CSM_117.

▼B

12.3. **Emparelhamento e comunicações do sensor de movimentos com a VU utilizando AES**

CSM_218 Em conformidade com o quadro 3 na secção 9.2.1, todas as chaves envolvidas no emparelhamento de uma unidade-veículo (da segunda geração) com um sensor de movimentos e nas comunicações subsequentes devem ser chaves AES, em vez de chaves de comprimento duplo TDES, nos termos da norma ISO 16844-3. Estas chaves AES podem ter um comprimento de 128, 192 ou 256 bits. Como o tamanho do bloco AES é de 16 bytes, o comprimento de uma mensagem encriptada é um múltiplo de 16 bytes, em comparação com 8 bytes para TDES. Além disso, algumas destas mensagens são utilizadas para transmitir chaves AES, cujo comprimento pode ser de 128, 192 ou 256 bits. Por conseguinte, o número de bytes de dados por instrução, constantes do quadro 5 da norma ISO 16844-3, é alterado como mostra o quadro 6:

Quadro 6

Número de bytes de dados de texto simples e encriptados por instrução definida na norma ISO 16844-3

Instruções	Pedido / resposta	Descrição dos dados	N.º de bytes de dados de texto simples, de acordo coma norma ISO 16844-3	N.º de bytes de dados de texto simples que utilizam chaves AES	N.º de bytes de dados encriptados ao utilizar chaves AES com comprimento em bits		
					128	192	256
10	Pedido	Dados de autenticação + número de ficheiro	8	8	16	16	16
11	Resposta	Dados de autenticação + conteúdo do ficheiro	16 ou 32, Consoante o ficheiro	16 ou 32, Consoante o ficheiro	16 / 32	16 / 32	16 / 32
41	Pedido	Número de série MoS	8	8	16	16	16
41	Resposta	Chave de emparelhamento	16	16 / 24 / 32	16	32	32
42	Pedido	Chave de sessão	16	16 / 24 / 32	16	32	32
43	Pedido	Informações do emparelhamento	24	24	32	32	32
50	Resposta	Informações do emparelhamento	24	24	32	32	32
70	Pedido	Dados de autenticação	8	8	16	16	16
80	Resposta	Valor do contador MoS + dados autenticados	8	8	16	16	16

CSM_219 As informações de emparelhamento enviadas nas instruções 43 (pedido da VU) e 50 (resposta MoS) são reunidas em conformidade com a secção 7.6.10 da norma ISO 16844-3, com exceção do algoritmo AES, que é utilizado em vez do algoritmo TDES no esquema de encriptação de dados de emparelhamento, resultando assim em duas encriptações AES e na adoção do preenchimento especificado no requisito CSM_220 para se adaptar ao tamanho do bloco AES. A chave K'_P para esta encriptação é criada da seguinte forma:

— Se a chave de emparelhamento K_P tiver 16 bytes de comprimento: $K'_P = K_P \text{ XOR } (N_s||N_s)$

▼B

— Se a chave de emparelhamento K_P tiver 24 bytes de comprimento: $K'_p = K_P$ XOR $(N_s||N_s||N_s)$

— Se a chave de emparelhamento K_P tiver 32 bytes de comprimento: $K'_p = K_P$ XOR $(N_s||N_s||N_s||N_s)$

onde N_s é o número de série do sensor de movimentos de 8 bytes.

CSM_220 Se o comprimento de dados de texto simples (que utiliza chaves AES) não for múltiplo de 16 bytes, utiliza-se o método de preenchimento 2, definido na norma ISO 9797-1.

Nota: Na norma ISO 16844-3, o número de bytes de dados de texto simples é sempre um múltiplo de 8, de tal modo que esse preenchimento não é necessário quando utiliza TDES. A definição de dados e mensagens constante da norma ISO 16844-3 não sofre alterações nesta parte do presente apêndice, exigindo, portanto, a aplicação de preenchimento.

CSM_221 Relativamente à instrução 11 e no caso de mais de um bloco de dados ter de ser encriptado, utiliza-se o modo de funcionamento por cifragem progressiva definido na norma ISO 10116, com um parâmetro intercalar $m = 1$. É a seguinte a IV a utilizar:

— Em relação à instrução 11: o bloco de autenticação de 8 bytes especificado na secção 7.6.3.3 da norma ISO 16844-3, com o método de preenchimento 2 definido na norma ISO 9797-1 (ver também secções 7.6.5 e 7.6.6 da norma ISO 16844-3).

— Em relação a todas as outras instruções nas quais são transferidos mais de 16 bytes, em conformidade com o quadro 6: '00' {16}, ou seja, 16 bytes com valor binário 0.

Nota: Como mostram as secções 7.6.5 e 7.6.6 da norma ISO 16844-3, quando o MoS encripta ficheiros de dados para inclusão na instrução 11, o bloco de autenticação é:

— utilizado como vetor de inicialização para a encriptação do modo CBC dos ficheiros de dados

— encriptado e incluído como primeiro bloco nos dados enviados à VU.

12.4. **Emparelhamento do sensor de movimentos com a VU, para diferentes gerações de aparelhos**

CSM_222 Conforme se explica na secção 9.2.1, o sensor de movimentos da segunda geração pode conter a encriptação dos dados de emparelhamento com recurso a TDES (definição na parte A do presente apêndice), que permite ao sensor de movimentos ser emparelhado com uma VU da primeira geração. Se for este o caso, a VU da primeira geração e o sensor de movimentos da segunda geração são emparelhados conforme descrito na parte A do presente apêndice e na norma ISO 16844-3. Relativamente ao processo de emparelhamento, pode utilizar-se um cartão de oficina tanto da primeira geração como da segunda.

Notas:

— Não é possível emparelhar uma VU da segunda geração com um sensor de movimentos da primeira geração.

▼B

— Não é possível utilizar um cartão de oficina da primeira geração para o acoplamento de uma VU da segunda geração a um sensor de movimentos.

13. SEGURANÇA PARA COMUNICAÇÕES À DISTÂNCIA POR DSRC

13.1. **Generalidades**

Em conformidade com o apêndice 14, uma VU cria regularmente dados relativos à monitorização tacográfica à distância (RTM) e envia-os ao sistema (interno ou externo) de comunicação à distância (RCF). O sistema de comunicação à distância tem a responsabilidade de enviar estes dados pela interface DSRC descrita no apêndice 14 ao interrogador à distância. O apêndice 1 prevê que os dados RTM são a concatenação de:

Carga útil encriptada do tacógrafo a encriptação em texto simples da carga útil do tacógrafo

Dados de segurança DSRC descrição adiante

O formato de dados em texto simples da carga útil do tacógrafo é especificado no apêndice 1 e descrito em pormenor no apêndice 14. A presente secção descreve a estrutura dos dados de segurança DSRC. A especificação formal é apresentada no apêndice 1.

CSM_223 Os dados `tachographPayload`de texto simples transmitidos pela VU a um sistema de comunicação à distância (se o RCF for externo à VU) ou da VU a um interrogador à distância pela interface DSRC (se o RCF for interno à VU) são protegidos no modo «encriptar depois autenticar», ou seja, os dados de carga útil do tacógrafo são encriptados primeiro para garantir a confidencialidade da mensagem e, posteriormente, é calculado um MAC para garantir a autenticidade e a integridade dos dados.

CSM_224 Os dados de segurança DSRC são constituídos pela concatenação dos seguintes elementos de dados, pela ordem indicada (ver também esquema 12):

Data e hora atuais	data e hora atuais da VU (tipo de dados `TimeReal`)
Contador	um contador de 3 bytes, ver CSM_225
Número de série da VU	o número de série da VU (tipo de dados `VuSerialNumber`)
Número de versão da chave de segurança DSRC	o número de versão de 1 byte da chave de segurança DSRC da qual derivaram as chaves DSRC específicas da VU (ver secção 9.2.2).
MAC	o MAC calculado sobre todos os bytes anteriores nos dados RTM.

CSM_225 O contador de 3 bytes nos dados de segurança DSRC está no formato de primeiro MSB. A primeira vez que uma VU calcula um conjunto de dados RTM após entrar em produção, fixa o valor do contador a 0. Sempre antes de calcular o próximo conjunto de dados RTM, a VU aumenta de 1 valor os dados do contador.

▼B

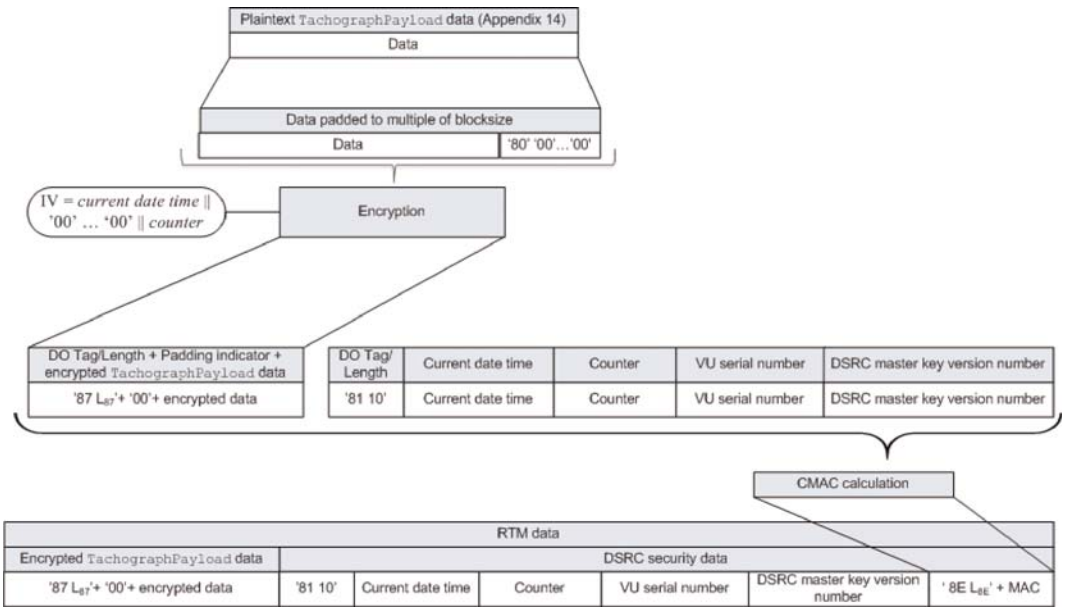
13.2. **Encriptação da carga útil do tacógrafo e criação de MAC**

CSM_226 Dado um elemento de dados de texto simples com tipo de dados `TachographPayload`, conforme descrição no apêndice 14, uma VU encripta esses dados do modo ilustrado no esquema 12: a chave DSRC da VU para encriptação $K\_VU_{DSRC}\_ENC$ (ver secção 9.2.2) é utilizada com AES no modo de funcionamento por cifragem progressiva (CBC), definido na norma ISO 10116, com um parâmetro intercalar $m = 1$. O vetor de inicialização é igual ao *IV = data e hora atual* || *'00 00 00 00 00 00 00 00'* || *contador*, onde *data e hora atual* e *contador* são especificados no requisito CSM_224. Os dados a encriptar são preenchidos utilizando o método 2 definido na norma ISO 9797-1.

CSM_227 A VU calcula o MAC nos dados de segurança DSRC como ilustra o esquema 12: o MAC é calculado sobre todos os bytes precedentes nos dados RTM, até o número de versão de chave de segurança DSRC, inclusive, e incluindo os marcadores e comprimentos dos objetos de dados. A VU utiliza a sua chave DSRC para autenticidade $K\_VU_{DSRC}\_MAC$ (ver secção 9.2.2) com o algoritmo AES no modo CMAC, em conformidade com SP 800--38B. O comprimento do MAC está ligado ao comprimento das chaves DSRC específicas da VU, em conformidade com o requisito CSM_50.

Esquema 12

Encriptação da carga útil do tacógrafo e criação do MAC



13.3. **Verificação e decifragem da carga útil do tacógrafo**

CSM_228 Quando um interrogador à distância recebe dados RTM de uma VU, envia-os todos para um cartão de controlo no campo de dados de um comando PROCESS DSRC MESSAGE, conforme descrito no apêndice 2. Logo:

▼B

1. O cartão de controlo inspeciona o número de versão da chave de segurança nos dados de segurança DSRC. Se o cartão de controlo não conhecer a chave de segurança DSRC indicada, devolve um erro especificado no apêndice 2 e interrompe o processo.

2. O cartão de controlo utiliza a chave de segurança DSRC indicada em combinação com o número de série da VU nos dados de segurança DSRC, para derivar as chaves DSRC específicas da VU K_VU_{DSRC}_ENC e K_VU_{DSRC}_MAC, em conformidade com o requisito CSM_124.

3. O cartão de controlo utiliza K_VU_{DSRC}_MAC para verificar o MAC nos dados de segurança DSRC, em conformidade com o requisito CSM_227. Se o MAC estiver incorreto, o cartão de controlo devolve um erro especificado no apêndice 2 e interrompe o processo.

4. O cartão de controlo utiliza K_VU_{DSRC}_ENC para decifrar a carga útil encriptada do tacógrafo, em conformidade com o requisito CSM_226. O cartão de controlo retira o preenchimento e devolve ao interrogador à distância os dados de carga útil decifrados do tacógrafo.

CSM_229 A fim de evitar ataques de reprodução, o interrogador à distância verifica a atualização dos dados RTM, verificando se as *data e hora atuais* nos dados de segurança DSRC não se desviam muito da hora atual do interrogador à distância.

Notas:

— Esta verificação exige que o interrogador à distância tenha uma fonte cronológica precisa e fiável.

— Como o apêndice 14 estabelece que a VU calcula um novo conjunto de dados RTM a cada 60 segundos e o relógio da VU pode desviar-se 1 minuto da hora real, o limite inferior para a atualização dos dados RTM é de 2 minutos. A atualização real a exigir depende igualmente da precisão do relógio do interrogador à distância.

CSM_230 Quando uma oficina verifica o funcionamento correto da funcionalidade DSRC de uma VU, envia todos os dados RTM recebidos da VU para um cartão de oficina no campo de dados de um comando PROCESS DSRC MESSAGE, conforme descrição no apêndice 2. O cartão de oficina realiza todas as verificações e ações especificadas no requisito CSM_228.

14. DESCARREGAMENTOS DE DADOS DE ASSINATURA E VERIFICAÇÃO DE ASSINATURAS

14.1. **Generalidades**

CSM_231 O equipamento dedicado inteligente (IDE) memoriza num ficheiro físico os dados recebidos de uma VU ou de um cartão durante uma sessão de descarregamento. Os dados podem ser memorizados num ESM (meio externo de memorização). Este ficheiro contém as assinaturas digitais em blocos de dados, em conformidade com o apêndice 7 e também os seguintes certificados (consultar secção 9.1):

▼B

— No caso de descarregamento de dados da VU:

— o certificado VU_Sign

— o certificado MSCA_VU-EGF que contém a chave pública a utilizar para a verificação do certificado VU-Sign

— No caso de descarregamento de dados do cartão:

— o certificado Card_Sign

— o certificado MSCA_Card que contém a chave pública a utilizar para a verificação do certificado Card-Sign

CSM_232 O IDE dispõe igualmente de:

— certificado de ligação que liga o último certificado EUR ao certificado EUR cujo período de validade o precede diretamente (se existir), no caso de utilizar um cartão de controlo para verificar a assinatura, como mostra o esquema 13;

— todos os certificados de raiz europeus válidos, no caso de verificar a própria assinatura.

Nota: o presente apêndice não especifica o método que o IDE utiliza para recuperar esses certificados.

14.2. **Criação da assinatura**

CSM_233 O algoritmo de assinatura para criação de assinaturas digitais em dados descarregados é ECDSA, em conformidade com DSS, que utiliza o algoritmo de hash ligado ao tamanho da chave da VU ou do cartão, em conformidade com o requisito CSM_50. O formato de assinatura é simples, em conformidade com a Orientação Técnica TR-03111.

14.3. **Verificação da assinatura**

CSM_234 Um IDE pode executar a verificação de uma assinatura em dados descarregados por si próprio ou utilizar um cartão de controlo para esse efeito. Caso utilize um cartão de controlo, a verificação da assinatura ocorre como mostra o esquema 13. Caso realize a verificação da própria assinatura, o IDE verifica a autenticidade e a validade de todos os certificados, na cadeia de certificado no ficheiro de dados e verifica a assinatura na sequência de dados do esquema de assinatura definido em DSS.

Notas do esquema 13:

— O equipamento que assinou os dados a analisar é designado EQT.

— Os certificados EQT e as chaves públicas mencionados no esquema são os destinados à assinatura, ou seja, VU_Sign ou Card_Sign.

— Os certificados EQT.CA e as chaves públicas mencionados no esquema são os destinados à assinatura dos certificados a VU ou de cartão, consoante o caso.

— O certificado EQT.CA.EUR mencionado no esquema é o certificado de raiz europeia indicado na CAR do certificado EQT.CA.

▼B

— O certificado EQT.Link mencionado no esquema é o certificado de ligação de EQT, caso exista. Em conformidade com a secção 9.1.2, trata-se de um certificado de ligação para um novo par de chaves de raiz europeia criado pela ERCA e assinado com a chave privada europeia anterior.

— O certificado EQT.Link.EUR é o certificado de raiz europeia indicado na CAR do certificado EQT.Link.

CSM_235 Para calcular o hash M enviado para o cartão de controlo no comando PSO:Hash, o IDE utiliza o algoritmo de hash ligado ao tamanho da chave da VU ou do cartão a partir do qual os dados são descarregados, em conformidade com o CSM_50.

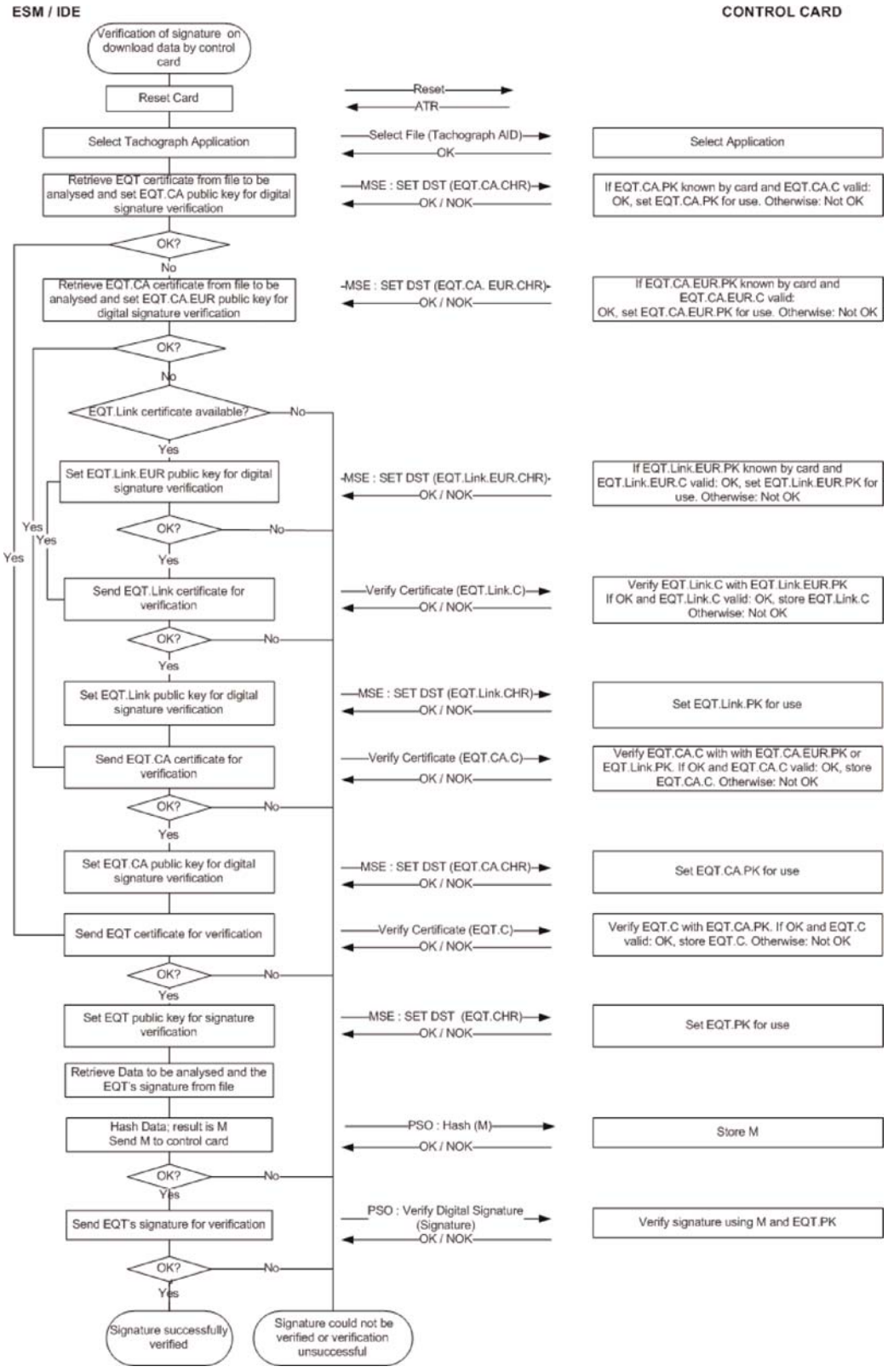
CSM_236 Para verificar a assinatura EQT, o cartão de controlo segue o esquema de assinatura definido em DSS.

Nota: O presente documento não especifica qualquer ação a empreender se uma assinatura num ficheiro de dados descarregados não puder ser verificada ou se a verificação não tiver êxito.

▼B

Esquema 13

Protocolo de verificação da assinatura num ficheiro de dados descarregados



▼B

Apêndice 12

POSICIONAMENTO BASEADO NO SISTEMA GLOBAL DE NAVEGAÇÃO POR SATÉLITE (GNSS)

ÍNDICE

1. INTRODUÇÃO

O presente apêndice estabelece os requisitos técnicos para os dados GNSS utilizados pela unidade-veículo, que incluem os protocolos a aplicar para garantir a transferência correta e segura de dados das informações de posicionamento.

Principais artigos do Regulamento (UE) n.º 165/2014 que motivam os presentes requisitos: «artigo 8.º — Registo da posição do veículo em certos pontos durante o período de trabalho diário», «artigo 10.º — Interface com sistemas de transporte inteligentes» e «artigo 11.º — Disposições pormenorizadas aplicáveis aos tacógrafos inteligentes».

▼B

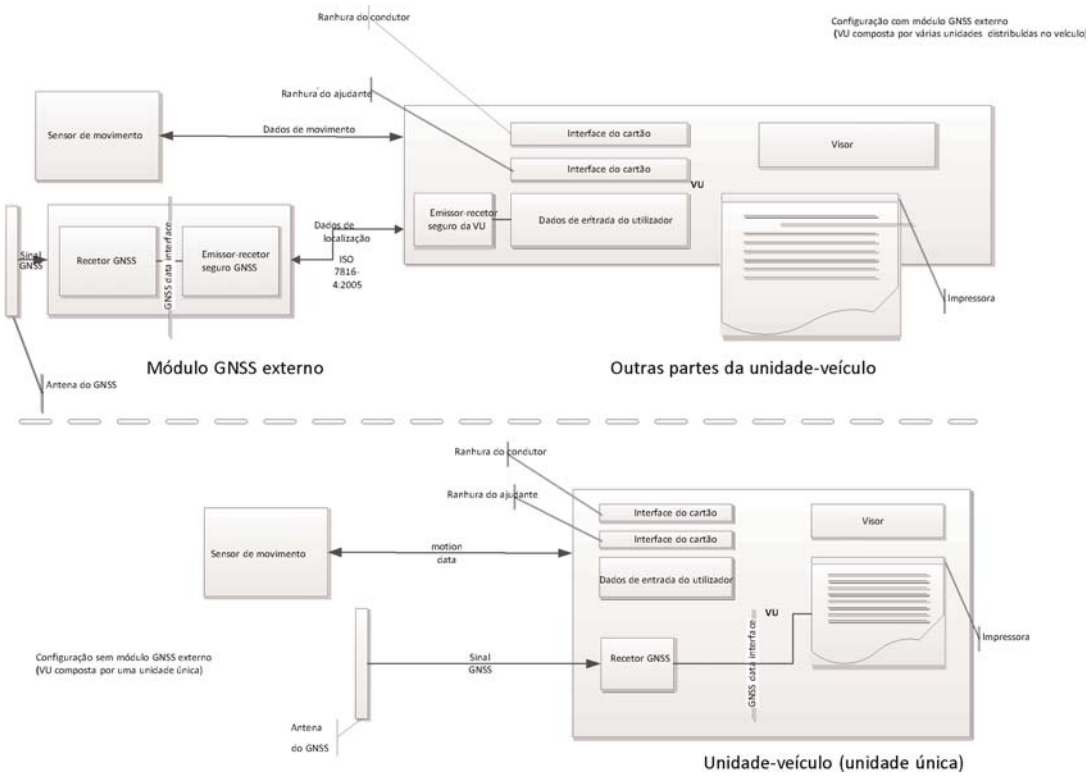
1.1. **Âmbito de aplicação**

GNS_1 A aplicação do artigo 8.º implica a recolha de dados de localização de, pelo menos, um GNSS pela unidade-veículo.

Conforme se vê na figura 1, a unidade-veículo pode ser com ou sem módulo GNSS externo:

Figura 1

Diversas configurações do recetor GNSS



1.2. **Acrónimos e notações**

No presente apêndice, utilizam-se os seguintes acrónimos:

DOP	Diluição de precisão
EGF	Ficheiro elementar do módulo GNSS
EGNOS	Serviço Europeu Complementar de Navegação Geoestacionária
GNSS	Sistema global de navegação por satélite
GSA	GPS DOP e satélites ativos
HDOP	Diluição de precisão horizontal
ICD	Documento de controlo da interface
NMEA	Associação Nacional de Eletrónica para Aplicações Marítimas

▼B

PDOP Diluição de precisão de posição

RMC Específico mínimo recomendado

SIS Sinal no espaço

HDOP Diluição de precisão vertical

VU Unidade-veículo

2. ESPECIFICAÇÕES DO RECETOR GNSS

Independentemente da configuração do tacógrafo inteligente, com ou sem módulo GNSS externo, o fornecimento de informações de posicionamento precisas e fiáveis é um elemento essencial do bom funcionamento do tacógrafo inteligente. Por conseguinte, convém exigir que este sistema seja compatível com os serviços prestados pelo Programa Galileo e pelo Serviço Europeu Complementar de Navegação Geoestacionária (EGNOS), conforme prevê o Regulamento (UE) n.º 1285/2013 do Parlamento Europeu e do Conselho ([1]). O sistema criado pelo Programa Galileo é um sistema autónomo mundial de navegação por satélite e o sistema criado pelo Programa EGNOS é um sistema regional de navegação por satélite que melhora a qualidade dos sinais do sistema de posicionamento global.

GNS_2 Os construtores devem assegurar que os recetores GNSS a bordo dos tacógrafos inteligentes são compatíveis com os serviços de posicionamento prestados pelos sistemas Galileo e EGNOS. Complementarmente, podem também optar por um sistema compatível com outros sistemas de navegação por satélite.

GNS_3 O recetor GNSS deve ter capacidade para aceitar a autenticação no serviço aberto Galileo quando esse serviço for disponibilizado pelo sistema Galileo e apoiado pelos fabricantes de recetores GNSS. Todavia, no caso dos tacógrafos inteligentes introduzidos no mercado antes de as anteriores condições estarem satisfeitas e desprovidos da capacidade de aceitar a autenticação do serviço aberto do Galileo, não é exigida reconversão.

3. FRASES NMEA

A presente secção descreve as frases NMEA utilizadas no funcionamento dos tacógrafos inteligentes e aplica-se à configuração dos tacógrafos inteligentes com ou sem módulo GNSS externo.

GNS_4 Os dados de localização baseiam-se nos dados GNSS específicos mínimos recomendados (RMC) da frase NMEA, que contém as informações de posição (latitude, longitude), as horas em formato UTC (hhmmss.ss) e a velocidade no solo em nós, mais valores adicionais.

Formato da frase RMC (segundo a norma NMEA V4.1):

([1]) Regulamento (UE) n.º 1285/2013 do Parlamento Europeu e do Conselho, de , relativo à im11 de dezembro de 2013 plantação e à exploração dos sistemas europeus de navegação por satélite e que revoga o Regulamento (CE) n.º 876/2002 do Conselho e o Regulamento (CE) n.º 683/2008 do Parlamento Europeu e do Conselho (JO L 347 de 20.12.2013, p. 1).

▼B

Figura 2

▼C2

Estrutura da frase RMC

1) Tempo (UTC)
2) Estatuto: A = posição válida, V = alerta
3) Latitude
4) N ou S
5) Longitude
6) E ou W
7) Velocidade no solo em nós
8) Trajeto corrigido, graus corretos
9) Data: ddmmaa
10) Variação magnética (graus)
11) E ou W
12) Soma de teste

▼B

O estatuto indica se o sinal GNSS está disponível. Enquanto o valor do estatuto não estiver fixado em A, os dados recebidos (por exemplo, relativos às horas, à latitude ou à longitude) não podem ser utilizados para registar a posição do veículo na VU.

A resolução da posição baseia-se no formato da frase RMC atrás descrita. A primeira parte dos campos 3) e 5) (os dois primeiros números) serve para representar os graus. O resto serve para representar os minutos, com três casas decimais. Portanto, a resolução é de 1/1000 de minuto ou 1/60000 de grau (porque um minuto é 1/60 de um grau).

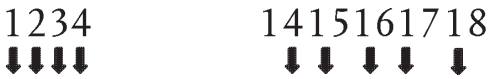
GNS_5 A unidade-veículo memoriza na sua base de dados as informações de posição relativas à latitude e à longitude, com uma resolução de 1/10 de minuto ou 1/600 de grau, conforme refere o apêndice 1 relativamente a GeoCoordinates de tipo.

A VU pode utilizar o comando GPS DOP e satélites ativos (GSA) para determinar e registar a disponibilidade e a exatidão do sinal. O comando HDOP é utilizado especialmente para fornecer uma indicação do nível de exatidão dos dados de localização registados (ver 4.2.2). A VU memoriza o valor da diluição de precisão horizontal (HDOP) calculado como o mínimo dos valores HDOP recolhidos nos sistemas GNSS disponíveis.

O Id do sistema GNSS indica GPS, Glonass, Galileo, Beidou ou Sistema de Aumento com recurso a Satélites (SBAS).

Figura 3

Estrutura da frase GSA



1) Modo de seleção
2) Modo
3) ID do 1.º satélite utilizado para determinar posição
4) ID do 2.º satélite utilizado para determinar posição

...

14) ID do 12.º satélite utilizado para determinar posição
15) PDOP em metros
16) HDOP em metros
17) VDOP em metros
18) Id do sistema GNSS
19) Soma de teste

▼B

Neste esquema, o modo (2) indica se não está disponível nenhuma determinação de posição (modo = 1) ou se está disponível uma determinação de posição para 2D (modo = 2) ou para 3D (modo = 3).

GNS_6 A frase *GSA* deve ser memorizada com o número de registo '06'.

GNS_7 O tamanho máximo das frases NMEA (por exemplo, RMC, GSA ou outras), que podem ser utilizadas para a calibragem do comando «ler registo» é de 85 bytes (ver quadro 1).

4. UNIDADE-VEÍCULO COM MÓDULO GNSS EXTERNO

4.1. **Configuração**

4.1.1 *Principais componentes e interfaces*

Nesta configuração, o recetor GNSS faz parte do módulo GNSS externo.

GNS_8 O módulo GNSS externo deve ser alimentado por uma interface de veículo específica.

GNS_9 O módulo GNSS externo tem os seguintes componentes (ver figura 4):

a) Um recetor GNSS comercial para fornecer os dados de posição, através da interface de dados GNSS. Por exemplo, a interface de dados GNSS pode ter a normalização NMEA V4.10, em que o recetor GNSS age como um transmissor e transmite frases NMEA ao emissor-recetor seguro GNSS na frequência de 1 Hz para o conjunto pré-definido de frases NMEA, que deve incluir pelo menos as frases RMC e GSA. A implementação da interface de dados GNSS é uma escolha dos fabricantes de módulos GNSS externos.

b) Um emissor-recetor (emissor-recetor seguro GNSS) com capacidade para servir a norma ISO/IEC 7816-4:2013 (ver 4.2.1), para comunicar com a unidade-veículo e servir a interface de dados GNSS para o recetor GNSS. A unidade é disponibilizada com uma memória destinada a memorizar os dados de identificação do recetor GNSS e do módulo GNSS externo.

c) Um sistema de invólucro com a função de deteção de adulteração, que envolve o recetor GNSS e o emissor-recetor seguro GNSS. A função de deteção de adulteração deve aplicar as medidas de proteção da segurança exigidas no perfil de proteção dos tacógrafos inteligentes.

d) Uma antena GNSS instalada no veículo e ligada ao recetor GNSS por meio do sistema de invólucro.

GNS_10 O módulo GNSS externo tem, pelo menos, as seguintes interfaces externas:

a) a interface para a antena GNSS instalada no camião, caso se utilize uma antena externa.

b) a interface para a unidade-veículo.

GNS_11 Na VU, o emissor-recetor seguro da VU é a outra extremidade das comunicações seguras com o emissor-recetor seguro GNSS e tem de obedecer à norma ISO/IEC 7816-4:2013 no que se refere à conexão com o módulo GNSS externo.

▼B

GNS_12 Para a camada física da comunicação com o módulo GNSS externo, a unidade-veículo deve obedecer à norma ISO/IEC 7816-12:2005 ou a outra norma compatível com a ISO/IEC 7816-4:2013 (ver 4.2.1).

4.1.2 *Estado do módulo GNSS externo no final da produção*

GNS_13 O módulo GNSS externo deve memorizar os seguintes valores, na memória não volátil do emissor-recetor seguro GNSS, quando este sai de fábrica:

— o par de chaves EGF_MA e o certificado correspondente

— o certificado MSCA_VU-EGF que contém a chave pública MSCA_VU-EGF.PK a utilizar para a verificação do certificado EGF_MA

— o certificado EUR que contém a chave pública EUR.PK a utilizar para a verificação do certificado MSCA_VU-EGF

— o certificado EUR cujo período de validade precede diretamente o período de validade do certificado EUR a utilizar para a verificação do certificado MSCA_VU-EGF, se existir

— o certificado de ligação que liga estes dois certificados EUR, se existir

— o número de série alargado do módulo GNSS externo

— o identificador do sistema operativo do módulo GNSS

— o número de homologação de tipo do módulo GNSS externo

— o identificador do componente de segurança do módulo GNSS externo.

4.2. **Comunicação entre o módulo GNSS externo e a unidade-veículo**

4.2.1 *Protocolo de comunicação*

GNS_14 O protocolo de comunicação entre o módulo GNSS externo e a unidade-veículo deve aceitar três funções:

1. recolha e distribuição de dados GNSS (por exemplo, posição, temporização, velocidade)

2. recolha dos dados de configuração do módulo GNSS externo

3. protocolo de gestão para aceitar o acoplamento, a autenticação mútua e a concordância de chave de sessão entre o módulo GNSS externo e a VU.

GNS_15 O protocolo de comunicação deve basear-se na norma ISO/IEC 7816-4:2013 em que o emissor-recetor seguro da VU desempenha o papel principal e o emissor-recetor seguro GNSS desempenha o papel secundário. A conexão física entre o módulo GNSS externo e a unidade-veículo tem por base a norma ISO/IEC 7816-12:2005 ou outra norma compatível com a ISO/IEC 7816-4:2013.

▼B

GNS_16 O protocolo de comunicação não aceita os campos de comprimento alargado.

GNS_17 O protocolo de comunicação estabelecido pela norma ISO 7816 (*-4:2013 e *-12:2005) entre o módulo GNSS externo e a VU deve ser definido como T=1.

GNS_18 Em relação às funções 1 — «recolha e distribuição de dados GNSS», 2 — «recolha dos dados de configuração do módulo GNSS externo» e 3 — «protocolo de gestão», o emissor-recetor seguro GNSS deve simular um cartão inteligente com uma arquitetura de sistema de ficheiros composta por um ficheiro principal (MF), um ficheiro de diretório (DF) com o identificador de aplicação especificado no apêndice 1, capítulo 6.2 (‘FF 44 54 45 47 4D’) e com três EF que possuem certificados e um ficheiro elementar único (EF.EGF) com identificador de ficheiro igual a ‘2F2F’, conforme consta do quadro 1.

GNS_19 O emissor-recetor seguro GNSS deve memorizar os dados provenientes do recetor GNSS e a configuração no EF.EGF. Trata-se de um ficheiro de registo linear de comprimento variável com um identificador igual a ‘2F2F’ em formato hexadecimal.

GNS_20 O emissor-recetor seguro GNSS deve utilizar uma memória para guardar os dados capazes de executar, pelo menos, 20 milhões de ciclos de escrita/leitura. À parte este aspeto, a conceção e a aplicação internas do emissor-recetor seguro GNSS são deixadas ao critério dos fabricantes.

O mapeamento de números e dados de registo consta do quadro 1. De referir que há quatro frases GSA para os quatro sistemas de satélite e para o sistema de aumento com recurso a satélites (SBAS).

GNS_21 A estrutura do ficheiro é dada no quadro 1. Relativamente às condições de acesso (ALW, NEV, SM-MAC), ver apêndice 2, capítulo 3.5.

Quadro 1

▼C2

Estrutura do ficheiro

		Condições de acesso		
Ficheiro	ID do ficheiro	Leitura	Atualização	Encriptado
MF	3F00			
EF.ICC	0002	ALW	NEV (pela VU)	Não
DF do módulo GNSS	0501	ALW	NEV	Não
EF EGF_MACertificate	C100	ALW	NEV	Não
EF CA_Certificate	C108	ALW	NEV	Não
EF Link_Certificate	C109	ALW	NEV	Não
EF.EGF	2F2F	SM-MAC	NEV (pela VU)	Não

▼C2

Ficheiro/elemento de dados	N.º de registo	Dimensões (bytes)		Valores por defeito
		Mín.	Máx.	
MF		552	1 031	
EF.ICC				
sensorGNSSSerialNumber		8	8	
DF GNSS Facility		*612*	*1 023*	
EF EGF_MACertificate		*204*	*341*	
EGFCertificate		204	341	{00..00}
EF CA_Certificate		*204*	*341*	
MemberStateCertificate		204	341	{00..00}
EF Link_Certificate		*204*	*341*	
LinkCertificate		204	341	{00..00}
EF.EGF				
Frase NMEA RMC	«01»	85	85	
1.ª frase NMEA GSA	«02»	85	85	
2.ª frase NMEA GSA	«03»	85	85	
3.ª frase NMEA GSA	«04»	85	85	
4.ª frase NMEA GSA	«05»	85	85	
5.ª frase NMEA GSA	«06»	85	85	
Número de série alargado do módulo GNSS externo, definido no apêndice 1 como SensorGNSSSerialNumber.	«07»	8	8	
Identificador do sistema operativo do emissor-recetor seguro GNSS, definido no apêndice 1 como SensorOSIdentifier.	«08»	2	2	
Número de homologação de tipo do módulo GNSS externo, definido no apêndice 1 como SensorExternalGNSSApprovalNumber.	«09»	16	16	
Identificador do componente de segurança do módulo GNSS externo, definido no apêndice 1 como SensorExternalGNSSSCIdentifier	«10»	8	8	
RFU — Reservado para futura utilização	De «11» a «FD»			

▼B

4.2.2 *Transferência segura de dados GNSS*

GNS_22 A transferência segura de dados de posição GNSS é autorizada apenas nas seguintes condições:

1. O processo de acoplamento foi concluído, conforme descreve o apêndice 11 (Mecanismos comuns de segurança).

▼B

2. A autenticação mútua periódica e a concordância de chave de sessão entre a VU e o módulo GNSS externo, também descritas no apêndice 11 (Mecanismos comuns de segurança), foram executadas na frequência indicada.

GNS_23 Com uma periodicidade de T segundos, em que T é um valor inferior ou igual a 10, salvo se ocorrer o acoplamento ou a autenticação mútua e a concordância de chave de sessão, a VU pede ao módulo GNSS externo a informação de posição segundo a seguinte sequência:

1. A VU pede dados de localização ao módulo GNSS externo, bem como dados de diluição de precisão (à frase GSA NMEA). O emissor-recetor seguro da VU utiliza o comando SELECT e READ RECORD(S) (norma ISO/IEC 7816-4:2013) no modo apenas de autenticação do envio seguro de mensagens descrito no apêndice 11, secção 11.5, com o identificador de ficheiro «2F2F» e o número RECORD igual a «01» para a frase RMC NMEA e '02', '03', '04', '05', '06' para a frase GSA NMEA.

2. Os dados recebidos relativos à última localização são memorizados no EF com identificador '2F2F' e os registos descritos no quadro 1, no emissor-recetor seguro GNSS, dado que este recebe dados NMEA com a frequência de, pelo menos, 1 Hz proveniente do recetor GNSS por meio da interface de dados GNSS.

3. O emissor-recetor seguro GNSS envia a resposta ao emissor-recetor seguro da VU utilizando a mensagem de resposta APDU no modo apenas de autenticação do envio seguro de mensagens descrito no apêndice 11, secção 11.5.

4. O emissor-recetor seguro da VU verifica a autenticidade e a integridade da resposta recebida. Se o resultado for positivo, os dados de localização são transferidos para o processador da VU por meio da interface de dados GNSS.

5. O processador da VU verifica os dados recebidos extraindo a informação (por exemplo, latitude, longitude, hora) da frase RMC NMEA. A frase RMC NMEA inclui a informação se a posição for válida. Se a posição não for válida, os dados de localização ainda não estão disponíveis e não podem ser utilizados para registar a posição do veículo. Se a posição for válida, o processador da VU extrai também os valores de HDOP de frases GSA NMEA e calcula o valor médio nos sistemas de satélite disponíveis (ou seja, quando a determinação de posição está disponível).

6. O processador da VU memoriza a informação recebida e processada, como latitude, longitude, hora e velocidade, na VU, segundo formato definido no apêndice 1 (Dicionário de dados) como GeoCoordinates, juntamente com o valor de HDOP calculado como o mínimo dos valores HDOP recolhidos nos sistemas GNSS disponíveis.

▼B

4.2.3 *Estrutura do comando Read Record*

▼C2

A presente secção descreve em pormenor a estrutura do comando Read Record (ler registo). O envio seguro de mensagens (modo «apenas autenticação») é adicionado conforme descrito no apêndice 11 (Mecanismos comuns de segurança).

▼B

GNS_24 O comando deve aceitar o modo apenas de autenticação do envio seguro de mensagens (ver apêndice 11).

GNS_25 Mensagem de comando

▼C2

Byte	Comprimento	Valor	Descrição
CLA	1	«0Ch»	Pedido envio seguro de mensagens
INS	1	«B2h»	Ler registo (Read Record)
P1	1	«XXh»	Número de registo («00» refere-se ao registo atual)
P2	1	«04h»	Ler registo com o número indicado em P1
Le	1	«XXh»	Comprimento dos dados esperados. Número de bytes a ler

▼B

GNS_26 O registo referenciado em P1 torna-se o registo atual.

Byte	Comprimento	Valor	Descrição
#1-#X	X	'XX..XXh'	Dados lidos
SW	2	'XXXXh'	Palavras de estatuto (SW1, SW2)

— Se o comando tiver êxito, o emissor-recetor seguro GNSS devolve '**9000**'.

— Se o ficheiro atual não for orientado para o registo, o emissor-recetor seguro GNSS devolve '**6981**'.

— Se o comando for utilizado com P1 = '00', mas não houver nenhum EF atual, o emissor-recetor seguro GNSS devolve **'6986'** (comando não permitido).

— Se o registo não for encontrado, o emissor-recetor seguro GNSS devolve '**6A 83**'.

— Se o módulo GNSS externo tiver detetado adulteração, deve devolver as palavras de estatuto '**66 90**'.

GNS_27 O emissor-recetor seguro GNSS deve aceitar os comandos de tacógrafo da geração 2 a seguir indicados, especificados no apêndice 2:

Comando	Referência
Select	Apêndice 2, capítulo 3.5.1
Read Binary	Apêndice 2, capítulo 3.5.2
Get Challenge	Apêndice 2, capítulo 3.5.4
PSO: Verify Certificate	Apêndice 2, capítulo 3.5.7
External Authenticate	Apêndice 2, capítulo 3.5.9
General Authenticate	Apêndice 2, capítulo 3.5.10
MSE:SET	Apêndice 2, capítulo 3.5.11

▼B

4.3. **Acoplamento, autenticação mútua e concordância de chave de sessão do módulo GNSS externo com a unidade-veículo**

O acoplamento, a autenticação mútua e a concordância de chave de sessão do módulo GNSS externo com a unidade-veículo são descritos no apêndice 11 (Mecanismos comuns de segurança), capítulo 11.

4.4. **Tratamento de erros**

Esta secção descreve como são abordadas e registadas na VU as condições de erro potenciais do módulo GNSS externo.

4.4.1 *Erro de comunicação com o módulo GNSS externo*

GNS_28 Se não conseguir comunicar com o módulo GNSS externo acoplado durante mais de 20 minutos seguidos, a VU cria e regista um incidente do tipo EventFaultType com o valor de enumeração '53'H *Falha de comunicação GNSS externo* e com o período de tempo definido para a hora atual. O incidente só será criado se se verificarem as duas condições seguintes: a) o tacógrafo inteligente não está no modo de calibração; b) o veículo está em movimento. Neste contexto, desencadeia-se um erro de comunicação quando o emissor-recetor seguro da VU não recebe mensagem de resposta após uma mensagem de pedido descrita em 4.2.

4.4.2 *Violação da integridade física do módulo GNSS externo*

GNS_29 Se o módulo GNSS externo tiver sido violado, o emissor-recetor seguro GNSS apaga toda a sua memória, incluindo material criptográfico. Conforme descrito em GNS_25 e GNS_26, a VU deteta adulteração se a resposta tiver estatuto '6690'. A VU cria então um incidente do tipo EventFaultType com o valor de enumeração *'55'H deteção de adulteração de GNSS*.

4.4.3 *Ausência de informação sobre a posição do recetor GNSS*

GNS_30 Se o emissor-recetor seguro GNSS não receber dados do recetor GNSS durante mais de 3 horas seguidas, o emissor-recetor seguro GNSS cria uma mensagem de resposta para o comando READ RECORD com número RECORD igual a '01', com um campo de dados de 12 bytes, todos definidos para 0xFF. Após a receção da mensagem de resposta com este valor do campo de dados, a VU cria e regista um incidente do tipo EventFaultType com o valor de enumeração '52'H *falha do recetor GNSS externo* com um período de tempo igual ao valor atual da hora apenas se se verificarem as duas condições seguintes: a) o tacógrafo inteligente não está no modo de calibração; b) o veículo está em movimento.

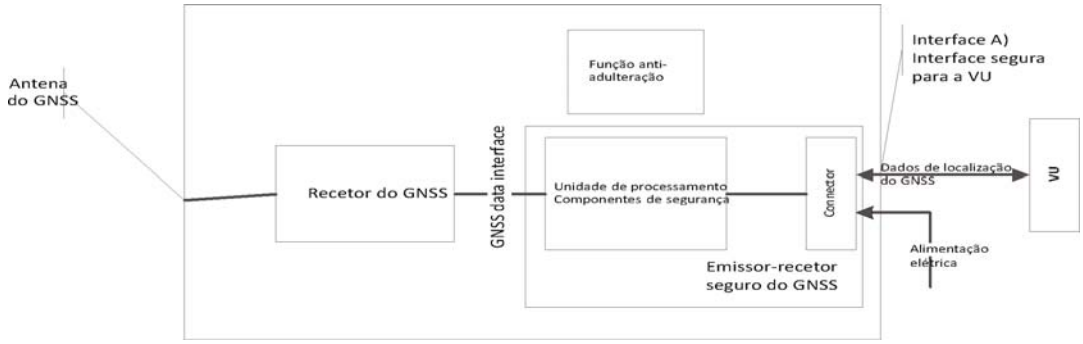
4.4.4 *Expiração do certificado do módulo GNSS externo*

GNS_31 Se detetar que o certificado EGF utilizado para autenticação mútua já não é válido, a VU cria e regista uma falha do aparelho de controlo de typeEventFaultType com o valor de enumeração *'56'H certificado do módulo GNSS Externo expirado* com um período de tempo igual ao valor atual da hora. A VU continua a utilizar os dados de posição GNSS recebidos.

▼B

Figura 4

Esquema do módulo GNSS externo



5. UNIDADE-VEÍCULO SEM MÓDULO GNSS EXTERNO

5.1. **Configuração**

Na presente configuração, o recetor GNSS está no interior da unidade-veículo, conforme consta da figura 1.

GNS_32 O recetor GNSS funciona como transmissor e transmite frases NMEA ao processador da VU, que funciona como ouvinte, com uma frequência de 1/10 Hz ou mais rápida para o conjunto pré-definido de frases NMEA, que deve incluir, pelo menos, as frases RMC e GSA.

GNS_33 A antena GNSS externa instalada no veículo ou a antena GNSS interna devem estar ligadas à VU.

5.2. **Tratamento de erros**

5.2.1 *Ausência de informação sobre a posição do recetor GNSS*

GNS_34 Se não receber dados do recetor GNSS durante mais de 3 horas seguidas, a VU cria e regista um incidente do tipo EventFaultType com o valor de enumeração '51'H *falha do recetor GNSS interno* com um período de tempo igual ao valor atual da hora apenas se se verificarem as duas condições seguintes: a) o tacógrafo inteligente não está no modo de calibração; b) o veículo está em movimento.

6. CONFLITO DE TEMPO GNSS

Se detetar uma discrepância de mais de 1 minuto entre o tempo da função de medição do tempo da unidade-veículo e o tempo proveniente do recetor GNSS, a VU regista um incidente do tipo EventFaultType com o valor de enumeração *'0B'H conflito de tempo (GNSS versus relógio interno da VU)*. Este incidente é registado juntamente com o valor do relógio interno da unidade-veículo e surge juntamente com um ajustamento automático do tempo. Após a produção de um incidente de conflito de tempo, a VU não verifica a discrepância de tempo para as 12 horas seguintes. Este incidente não se produz se não tiver sido detetado qualquer sinal GNSS válido pelo recetor GNSS nos últimos 30 dias. No entanto, quando a informação da posição do recetor GNSS estiver novamente disponível, efetuar-se-á o ajustamento automático do tempo.

▼B

7. CONFLITO RELATIVO AO MOVIMENTO DO VEÍCULO

GNS_35 A VU desencadeia e regista um incidente do tipo «conflito relativo ao movimento do veículo» (ver requisito 84 no presente anexo) com um período de tempo igual ao valor atual da hora, caso a informação de movimento calculada com base no sensor de movimento seja contrariada por informação de movimento calculada com base no recetor GNSS ou com base no módulo GNSS externo. Para detetar tais contradições, utiliza-se o valor mediano das diferenças de velocidade entre estas fontes, conforme a seguir se especifica:

— no máximo de 10 em 10 segundos, calcula-se o valor absoluto da diferença entre a velocidade do veículo, estimada com base no GNSS, e a estimada com base no sensor de movimento

— para calcular o valor mediano, devem utilizar-se todos os valores calculados num intervalo de tempo que inclua os últimos cinco minutos de movimento

— o valor mediano é calculado como média de 80 % dos valores remanescentes, depois de se eliminarem os mais elevados em valor absoluto.

O incidente «conflito relativo ao movimento do veículo» é desencadeado se o valor mediano for superior a 10 km/h durante cinco minutos contínuos de movimento do veículo. Podem utilizar-se, a título facultativo, outras fontes independentes para deteção de movimentos do veículo, para se obter uma deteção mais fiável das manipulações do tacógrafo. (Nota: recorre-se ao valor mediano relativo aos últimos 5 minutos para atenuar o risco de medições discrepantes e de valores transitórios). Este incidente não se produz nas condições seguintes: a) durante uma travessia de batelão/comboio; b) quando a informação de posição do recetor GNSS não está disponível; c) enquanto se estiver em modo de calibração.

▼B

Apêndice 13

INTERFACE ITS

ÍNDICE

1. INTRODUÇÃO

O presente apêndice especifica a conceção e os procedimentos a seguir a fim de implementar a interface com sistemas de transporte inteligentes (ITS), conforme estipula o artigo 10.º do Regulamento (UE) n.º 165/2014 («*o Regulamento*»).

Nos termos do *Regulamento*, os tacógrafos dos veículos podem ser equipados com interfaces normalizadas que permitam a um dispositivo externo utilizar, em modo operacional, os dados registados ou produzidos pelo tacógrafo, desde que se verifiquem as seguintes condições:

a) a interface não afeta a autenticidade nem a integridade dos dados do tacógrafo

b) a interface respeita as disposições pormenorizadas do artigo 11.º do Regulamento;

c) só depois de o condutor a que os dados se referem ter dado o seu consentimento de modo verificável, o dispositivo externo ligado à interface tem acesso aos dados pessoais, incluindo os dados de geoposicionamento.

2. ÂMBITO DE APLICAÇÃO

O presente apêndice visa especificar de que modo as aplicações alojadas em dispositivos externos podem obter dados (*os dados*) de um tacógrafo através de uma conexão Bluetooth®.

Os dados disponíveis através desta interface são descritos no anexo 1 do presente documento. Esta interface não proíbe a implantação de outras interfaces (por exemplo, através de CANbus) para a transmissão dos dados da VU a outras unidades de processamento do veículo.

▼B

O presente apêndice especifica:

— *Os dados* disponíveis através da interface ITS

— O perfil Bluetooth® utilizado para transferir os dados

— Os procedimentos de descarregamento e pedido e a sequência das operações

— O mecanismo de emparelhamento entre o tacógrafo e o dispositivo externo

— O mecanismo de consentimento disponível para o condutor

Para esclarecimento, o presente anexo não especifica:

— O funcionamento e a gestão da recolha dos *dados* na VU (a especificar noutras secções do *Regulamento* ou então tratar-se-á de uma função de conceção de produto)

— A forma de apresentação dos dados recolhidos para aplicações alojadas no dispositivo externo

— Disposições de segurança de dados sobre o que fornece o Bluetooth® (como encriptação) relativamente ao conteúdo dos *dados* (a especificar noutras secções do *Regulamento* [Apêndice 10 — Mecanismos comuns de segurança])

— Os protocolos Bluetooth® utilizados pela interface ITS.

2.1. **Acrónimos, definições e notações**

No presente apêndice utilizam-se os seguintes acrónimos e definições, que lhe são específicos:

a comunicação	intercâmbio de informações/dados entre uma unidade principal (ou seja, os tacógrafos) e uma unidade externa, pela interface ITS, através do Bluetooth®.
os dados	os conjuntos de dados especificados no anexo 1.
o regulamento	Regulamento (UE) n.º 165/2014 do Parlamento Europeu e do Conselho, de 4 de fevereiro de 2014, relativo à utilização de tacógrafos nos transportes rodoviários, que revoga o Regulamento (CEE) n.º 3821/85 do Conselho relativo à introdução de um aparelho de controlo no domínio dos transportes rodoviários e que altera o Regulamento (CE) n.º 561/2006 do Parlamento Europeu e do Conselho relativo à harmonização de determinadas disposições em matéria social no domínio dos transportes rodoviários
BR	taxa de base (Basic Rate)
EDR	taxa de dados melhorada (Enhanced Data Rate)
GNSS	sistema global de navegação por satélite (Global Navigation Satellite System)
IRK	chave de resolução de identidade (Identity Resolution Key)
ITS	sistema de transporte inteligente (Intelligent Transport System)
LE	baixo consumo energético (Low Energy)
PIN	número de identificação pessoal (Personal Identification Number)
PUC	código de desbloqueio pessoal (Personal Unblocking Code)
SID	identificador de serviço (Service Identifier)
SPP	perfil de porta-série (Serial Port Profile)

▼B

SSP	emparelhamento simples seguro (Secure Simple Pairing)
TRTP	parâmetro de pedido de transferência (Transfer Request Parameter)
TREP	parâmetro de resposta de transferência (Transfer Response Parameter)
VU	unidade-veículo (Vehicle Unit)

3. REGULAMENTOS E NORMAS DE REFERÊNCIA

A especificação definida no presente apêndice refere-se à totalidade ou a partes dos regulamentos e normas a seguir indicados (e deles depende). Nas cláusulas do presente apêndice especificam-se as normas pertinentes ou as cláusulas pertinentes das normas. Em caso de contradição, prevalecem as cláusulas do presente apêndice.

Os regulamentos e as normas de referência no presente apêndice são:

— Regulamento (UE) n.º 165/2014 do Parlamento Europeu e do Conselho, de 4 de fevereiro de 2014, relativo à utilização de tacógrafos nos transportes rodoviários, que revoga o Regulamento (CEE) n.º 3821/85 do Conselho relativo à introdução de um aparelho de controlo no domínio dos transportes rodoviários e que altera o Regulamento (CE) n.º 561/2006 do Parlamento Europeu e do Conselho relativo à harmonização de determinadas disposições em matéria social no domínio dos transportes rodoviários.

— Regulamento (CE) n.º 561/2006 do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativo à harmonização de determinadas disposições em matéria social no domínio dos transportes rodoviários, que altera os Regulamentos (CEE) n.º 3821/85 e (CE) n.º 2135/98 do Conselho e revoga o Regulamento (CEE) n.º 3820/85 do Conselho.

— ISO 16844 — 4: Road vehicles — Tachograph systems — Part 4: Can interface

— ISO 16844 — 7: Road vehicles — Tachograph systems — Part 7: Parameters

— Bluetooth® — Serial Port Profile — V1.2

— Bluetooth® — Versão principal 4.2

— NMEA 0183 V4.1 protocol

4. PRINCÍPIOS DE FUNCIONAMENTO DA INTERFACE

4.1. **Condições prévias para a transferência de dados através da interface ITS**

A VU tem a responsabilidade de manter atualizados e guardar os dados a memorizar na VU, sem qualquer envolvimento da interface ITS. O meio pelo qual se consegue este procedimento é interno à VU, está especificado em outras partes do Regulamento e não é especificado no presente apêndice.

4.1.1 *Dados fornecidos através da interface ITS*

A VU tem a responsabilidade de atualizar os dados que estarão disponíveis através da interface ITS, a uma frequência determinada nos procedimentos da VU, sem qualquer envolvimento da interface ITS. Os dados da VU são utilizados como base para preencher e atualizar os *dados,* estando os meios pelos quais tal é conseguido especificados em outras partes do *Regulamento* ou, se não existir essa especificação, trata-se de uma função de conceção do produto, não estando especificado no presente apêndice.

▼B

4.1.2 *Conteúdo dos dados*

O conteúdo dos *dados* é o especificado no anexo 1 do presente apêndice.

4.1.3 *Aplicações ITS*

As aplicações ITS utilizam os dados disponibilizados através da interface ITS para, por exemplo, otimizar a gestão de atividades de condutor, respeitando o Regulamento, detetar eventuais falhas do tacógrafo ou utilizar os dados GNSS. A especificação das aplicações não cabe no âmbito de aplicação do presente apêndice.

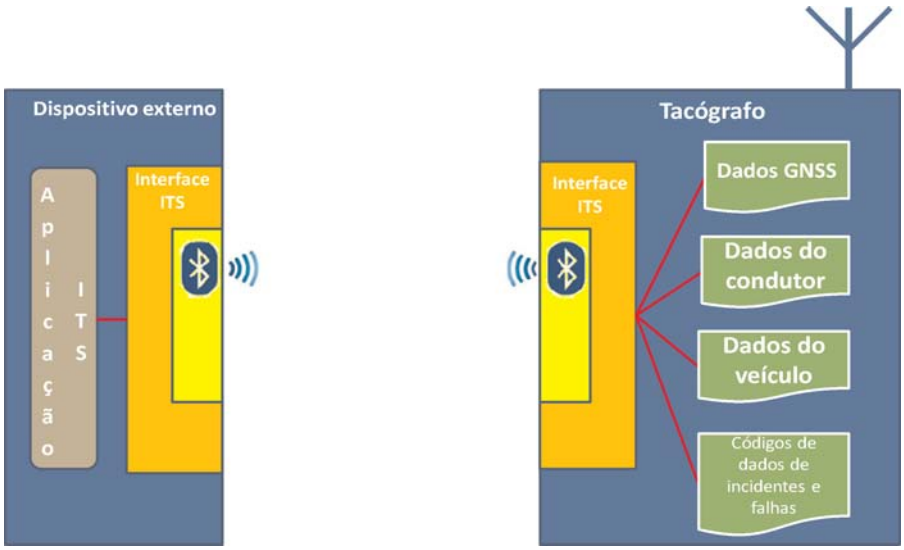
4.2. **Tecnologia da comunicação**

O intercâmbio dos *dados* utilizando a interface ITS é realizado através de uma interface Bluetooth® compatível através da versão 4.2 ou posterior. O Bluetooth® opera na banda (ISM) não licenciada, industrial, científica e médica de 2,4 a 2,485 GHz. O Bluetooth® 4.2 oferece privacidade reforçada e mecanismos de segurança e aumenta a velocidade e a fiabilidade da transferência de dados. Para efeitos desta especificação, utiliza-se o rádio Bluetooth® de classe 2 com alcance até 10 metros. Para mais informações sobre Bluetooth® 4.2: www.bluetooth.com (https://www.bluetooth.org/en-us/specification/adopted-specifications?_ga=1.215147412.2083380574.1435305676).

A *comunicação* deve ser estabelecida com o aparelho de comunicação após a conclusão de um processo de emparelhamento por um dispositivo autorizado. Dado que Bluetooth® está a utilizar um modelo principal/secundário (senhor/escravo) para controlar quando e onde os dispositivos podem enviar dados, o tacógrafo desempenhará o papel de senhor, enquanto o dispositivo externo será o escravo.

Quando um dispositivo externo surge no alcance da VU, pela primeira vez, pode iniciar-se o processo de emparelhamento Bluetooth® (ver também o anexo 2). Os dispositivos partilham os respetivos endereços, nomes, perfis e chave secreta comum, que lhes permite conectarem-se sempre que futuramente se juntarem. Uma vez concluído este passo, o dispositivo externo é aprovado e fica em condições de iniciar pedidos de descarregamento de dados do tacógrafo. Não se prevê adicionar mecanismos de encriptação além dos proporcionados por Bluetooth®. No entanto, se forem necessários outros mecanismos de segurança, tal será feito em conformidade com o apêndice 10 — Mecanismos comuns de segurança.

A imagem que se segue descreve o princípio geral de comunicação.



▼B

Deve utilizar-se o perfil SPP (Serial Port Profile) de Bluetooth® para a transferência de dados da VU para o dispositivo externo.

4.3. **Autorização do PIN**

Por motivos de segurança, a VU deve impor um sistema de autorização de código PIN separado do emparelhamento por Bluetooth. Todas as VU devem ser capazes de criar códigos PIN para fins de autenticação, compostos por quatro dígitos, pelo menos. Sempre que um dispositivo externo emparelhar com a VU, tem de fornecer o código PIN correto antes de receber quaisquer dados.

A inserção correta do PIN resulta na colocação do dispositivo na lista de permissões (lista branca), a qual deve memorizar, pelo menos, 64 dispositivos emparelhados com a VU em questão.

Não introduzir o código PIN correto três vezes consecutivas faz com que o dispositivo seja temporariamente colocado na lista de proibições (lista negra). Enquanto estiver na lista de proibições, todas as novas tentativas do dispositivo serão rejeitadas. Não introduzir o código PIN correto três novas vezes consecutivas resulta numa maior duração do tempo de proibição (ver quadro 1). A introdução do código PIN correto restaura a duração da proibição e o número de tentativas. O esquema 1 do anexo 2 representa o diagrama sequencial de uma tentativa de validação do PIN.

Quadro 1

Duração da proibição, dependente do número de falhas consecutivas de introdução do código PIN correto

Número de falhas consecutivas	Duração da proibição
3	30 segundos
6	5 minutos
9	1 hora
12	24 horas
15	Permanente

Não introduzir o código PIN correto quinze vezes (5 × 3) consecutivas coloca a unidade ITS permanentemente na lista de proibições. Apenas a introdução do código PUC correto reverterá esta proibição permanente.

O código PUC é composto por oito dígitos e fornecido pelo fabricante juntamente com a VU. Não introduzir o código PUC correto dez vezes consecutivas coloca a unidade ITS definitivamente na lista de proibições.

Embora o fabricante pode oferecer a possibilidade de alterar o código PIN, diretamente através da VU, o código PUC não é alterável. A alteração do código PIN, quando possível, requer a introdução do código PIN atual diretamente na VU.

Note-se que todos os dispositivos memorizados na lista de permissões serão mantidos até à sua remoção manual pelo utilizador (por exemplo, através da interface homem-máquina da VU ou por outros meios). Deste modo, podem ser retiradas da lista de permissões as unidades ITS perdidas ou roubadas. Qualquer unidade ITS que fique fora do alcance da conexão Bluetooth durante mais de 24 horas é também retirada automaticamente da lista de permissões da VU e tem de apresentar novamente o código PIN correto quando a conexão for restabelecida.

▼B

O formato das mensagens entre a interface da VU e a VU não é fornecido, mas deixado ao critério do fabricante. O fabricante assegura, porém, que o formato de mensagem entre a unidade ITS e a interface da VU é respeitado (ver especificações ASN.1).

Todos os pedidos de dados devem, por conseguinte, estar em conformidade com a verificação adequada da credencial do remetente antes de qualquer forma de tratamento. O esquema 2 do anexo 2 representa o diagrama sequencial para este procedimento. Todos os dispositivos da lista de proibições recebem uma rejeição automática; os dispositivos não constantes da lista de proibições nem da lista de permissões recebem um pedido de PIN que têm de atender antes de reenviar o respetivo pedido de dados.

4.4. **Formato das mensagens**

Todas as mensagens intercambiadas entre a unidade ITS e a interface da VU são formatadas com uma estrutura em três partes: cabeçalho, composto por um byte-alvo (TGT), um byte-fonte (SRC) e um byte de comprimento (LEN).

O campo de dados é composto por um byte de identificador de serviço (SID) e bytes de dados em quantidade variável (255 no máximo).

O byte soma de teste é o módulo 256 da série soma de 1 byte de todos os bytes da mensagem, excluindo o próprio CS.

A mensagem é Big Endian.

Quadro 2

Formato geral das mensagens

Cabeçalho			Campo de dados					Soma de teste
TGT	SRC	LEN	SID	TRTP	CC	CM	DATA	CS
3 bytes			Máx. 255 bytes					1 byte

Cabeçalho

TGT e SRC: o ID dos dispositivos-alvo (TGT) e dos dispositivos-fonte (SRC) da mensagem. A interface da VU terá o ID por defeito «EE». Este ID não pode ser alterado. A unidade ITS utiliza o ID por defeito «A0» para a sua primeira mensagem da sessão de comunicação. A interface da VU deve, em seguida, atribuir um ID único à unidade ITS e informá-la deste ID para futuras mensagens durante a sessão.

O byte LEN só considera a parte «DATA» do campo de dados (ver quadro 2), estando implícitos os quatro primeiros bytes.

A interface da VU confirma a autenticidade do remetente da mensagem pelo cruzamento da sua própria IDList com os dados Bluetooth, verificando se a unidade ITS enumerada no ID fornecido está atualmente no alcance da conexão Bluetooth.

Campo de dados

Além do SID, o campo de dados deve conter igualmente outros parâmetros: um parâmetro de pedido de transferência (TRTP) e bytes de contador.

▼B

Se os dados que têm de ser executados forem demasiado longos em relação ao espaço disponível numa mensagem, serão divididos em várias submensagens. Cada submensagem deve ter os mesmos cabeçalho e SID, mas conterá um contador de 2 bytes, contra-corrente (CC) e contador de máx. (CM), para indicar o número da submensagem. Para efeitos de verificar erros e interromper, o dispositivo de receção acusa cada uma das submensagens. O dispositivo de receção pode aceitar a submensagem, pedir a sua retransmissão, pedir o recomeço ao dispositivo de receção ou interromper a transmissão.

Deve ser dado o valor 0xFF a CC e CM, se não forem utilizados.

▼C2

Por exemplo, a mensagem

CABEÇALHO	SID	TRTP	CC	CM	DATA	CS
3 bytes	Comprimento superior a 255 bytes					1 byte

é transmitida da seguinte forma:

CABEÇALHO	SID	TRTP	01	n	DATA	CS
3 bytes	255 bytes					1 byte

CABEÇALHO	SID	TRTP	02	n	DATA	CS
3 bytes	255 bytes					1 byte

…

CABEÇALHO	SID	TRTP	N	N	DATA	CS
3 bytes	Máx. 255 bytes					1 byte

▼B

O quadro 3 contém as mensagens que a VU e a unidade ITS serão capazes de intercambiar. O conteúdo de cada parâmetro é dado em números hexadecimais. Para maior clareza, CC e CM não estão representados no quadro (ver *supra* o formato completo).

Quadro 3

Conteúdo pormenorizado da mensagem

Mensagem	Cabeçalho			DADOS			Soma de teste
	TGT	SRC	LEN	SID	TRTP	DATA	
RequestPIN	*ITSID*	EE	00	01	FF		
SendITSID	*ITSID*	EE	01	02	FF	*ITSID*	
SendPIN	EE	*ITSID*	04	03	FF	4*INTEGER (0..9)	
PairingResult	*ITSID*	EE	01	04	FF	BOOLEAN (T/F)	
SendPUC	EE	*ITSID*	08	05	FF	8*INTEGER (0..9)	

▼B

Mensagem	Cabeçalho			DADOS			Soma de teste
	TGT	SRC	LEN	SID	TRTP	DATA	
BanLiftingResult	*ITSID*	EE	01	06	FF	BOOLEAN (T/F)	
RequestRejected	*ITSID*	EE	08	07	FF	Hora	
RequestData							
standardTachData	EE	*ITSID*	01	08	01		
personalTachData	EE	*ITSID*	01	08	02		
gnssData	EE	*ITSID*	01	08	03		
standardEventData	EE	*ITSID*	01	08	04		
personalEventData	EE	*ITSID*	01	08	05		
standardFaultData	EE	*ITSID*	01	08	06		
manufacturerData	EE	*ITSID*	01	08	07		
ResquestAccepted	*ITSID*	EE	Len	09	TREP	Dados	
DataUnavailable							
Dados indisponíveis	*ITSID*	EE	02	0A	TREP	10	
Dados pessoais não partilhados	*ITSID*	EE	02	0A	TREP	11	
NegativeAnswer							
Rejeição geral	*ITSID*	EE	02	0B	SID Req	10	
Serviço não compatível	*ITSID*	EE	02	0B	SID Req	11	
Subfunção não compatível	*ITSID*	EE	02	0B	SID Req	12	
Comprimento de mensagem incorreto	*ITSID*	EE	02	0B	SID Req	13	
Condições incorretas ou erro de sequência do pedido	*ITSID*	EE	02	0B	SID Req	22	
Pedido fora do alcance	*ITSID*	EE	02	0B	SID Req	31	
Resposta pendente	*ITSID*	EE	02	0B	SID Req	78	
Incompatibilidade ITSID	*ITSID*	EE	02	0B	SID Req	FC	
ITSID não encontrado	*ITSID*	EE	02	0B	SID Req	FB	

RequestPIN (SID 01)

Esta mensagem é emitida pela interface da VU se uma unidade ITS que não conste da lista de proibições nem da lista de permissões enviar um pedido de dados.

▼B

SendITSID (SID 02)

Esta mensagem é emitida pela interface da VU sempre que um novo dispositivo enviar um pedido. Este dispositivo deve utilizar o ID por defeito «A0» antes de ser atribuído um ID único para a sessão de comunicação.

SendPIN (SID 03)

Esta mensagem é emitida pela unidade ITS para que passe a constar da lista de permissões da interface da VU. O conteúdo desta mensagem é um INTEGER 4 entre os códigos 0 e 9.

PairingResult (SID 04)

Esta mensagem é emitida pela interface da VU para informar a unidade ITS se o código PIN que enviou estava correto. O conteúdo desta mensagem é um BOOLEAN com o valor «True» se o código PIN estiver correto e «False» caso contrário.

SendPUC (SID 05)

Esta mensagem é emitida pela unidade ITS para levantar uma sanção da lista de proibições da interface da VU. O conteúdo desta mensagem é um INTEGER 8 entre os códigos 0 e 9.

BanLiftingResult (SID 06)

Esta mensagem é emitida pela interface da VU para informar a unidade ITS se o código PUC que enviou estava correto. O conteúdo desta mensagem é um BOOLEAN com o valor «True» se o código PUC estiver correto e «False» caso contrário.

RequestRejected (SID 07)

Esta mensagem é emitida pela interface da VU como resposta a qualquer mensagem da unidade ITS constante da lista de proibições, com exceção de «SendPUC». A mensagem deve conter o tempo restante da unidade ITS na lista de proibições, seguindo o formato de sequência «Time», definido no anexo 3.

RequestData (SID 08)

Esta mensagem de acesso aos dados é emitida pela unidade ITS. O tipo de dados necessário é indicado por um parâmetro de pedido de transferência (TRTP) de um byte. Existem vários tipos de dados:

— standardTachData (TRTP 01): dados disponíveis do tacógrafo, classificados como não pessoais

— personalTachData (TRTP 02): dados disponíveis do tacógrafo, classificados como pessoais

— gnssData (TRTP 03): dados GNSS, sempre pessoais

— standardEventData (TRTP 04): dados de incidentes registados, classificados como não-pessoais

— personalEventData (TRTP 05): dados de incidentes registados, classificados como pessoais

— standardFaultData (TRTP 06): falhas registadas, classificadas como não-pessoais

— manufacturerData (TRTP 07): dados disponibilizados pelo fabricante.

▼B

Ver anexo 3 do presente apêndice para mais informações sobre o conteúdo de cada tipo de dados.

Ver apêndice 12 para mais informações sobre o formato e o conteúdo dos dados GNSS.

Ver anexos 1B e 1C para mais informações sobre o código de dados de incidentes e falhas.

ResquestAccepted (SID 09)

Esta mensagem é emitida pela interface da VU, caso tenha sido aceite uma mensagem «RequestData» da unidade ITS. Esta mensagem contém um TREP de 1 byte, que é o byte TRTP da mensagem RequestData associada, e todos os dados do tipo pedido.

DataUnavailable (SID 0A)

Esta mensagem é emitida pela interface da VU se, por um determinado motivo, os dados pedidos não estiverem disponíveis para enviar a uma unidade ITS constante da lista de permissões. A mensagem contém um TREP de 1 byte que é o TRTP dos dados pedidos e um código de erro de 1 byte especificado no quadro 3. São os seguintes os códigos disponíveis:

— Dados indisponíveis (10): A interface da VU não pode aceder aos dados da VU por motivos não especificados.

— Dados pessoais não partilhados (11): A unidade ITS tenta recuperar dados pessoais quando não são partilhados.

NegativeAnswer (SID 0B)

Estas mensagens são emitidas pela interface da VU se um pedido não puder ser concluído por qualquer outro motivo que não a indisponibilidade dos dados. Normalmente, estas mensagens são o resultado de um mau formato de pedido (comprimento, SID, ITSID...), mas não se limitam a isso. O TRTP no campo de dados contém o SID do pedido. O campo de dados contém um código que identifica o motivo da resposta negativa. São os seguintes os códigos disponíveis:

— Rejeição geral (código: 10)

— A ação não pode ser executada por um motivo não mencionado abaixo nem na secção (inserir número de secção *DataUnavailable*).

— Serviço não compatível (código: 11)

— O SID dos pedidos não é compreendido.

— Subfunção não compatível (código: 12)

— O TRTP dos pedidos não é compreendido. Pode estar, por exemplo, em falta ou fora dos valores aceites.

— Comprimento de mensagem incorreto (código: 13)

— O comprimento da mensagem recebida está errado (incompatibilidade entre o byte LEN e o comprimento real da mensagem).

— Condições incorretas ou erro de sequência do pedido (código: 22)

— O serviço requerido não está ativo ou a sequência das mensagens de pedido não está correta.

— Pedido fora do alcance (código: 33)

▼B

— O registo do parâmetro de pedido (campo de dados) não é válido.

— Resposta pendente (código: 78)

— A ação pedida não pode ser concluída a tempo e a VU não está preparada para aceitar outro pedido.

— Incompatibilidade *ITSID* (código: FB)

— O SRC *ITSID* não corresponde ao dispositivo associado, após comparação com as informações de Bluetooth.

— *ITSID* não encontrado (código: FC)

— O SRC *ITSID* não está associado a nenhum dispositivo.

As linhas 1 a 72 (**FormatMessageModule**) do código ASN.1 do anexo 3 especificam o formato de mensagem, descrito no quadro 3. Indicam-se abaixo mais pormenores sobre o conteúdo das mensagens.

4.5. **Consentimento do condutor**

Todos os dados disponíveis estão classificados como dados-padrão ou dados pessoais. Os dados pessoais são acessíveis apenas se o condutor tiver consentido que os seus dados pessoais do tacógrafo passem da rede do veículo para aplicações de terceiros.

O consentimento do condutor é dado quando, à primeira inserção de um cartão de condutor ou cartão de oficina desconhecido da unidade-veículo naquele momento, o titular do cartão é convidado a manifestar o seu consentimento para a saída de dados pessoais relacionados com o tacógrafo através da interface ITS opcional (ver também o anexo 1C, ponto 3.6.2).

O estado de consentimento (ativado/desativado) é registado na memória do tacógrafo.

No caso de vários condutores, são partilhados com a interface ITS apenas os dados pessoais relativos aos condutores que deram o seu consentimento. Por exemplo, se houver dois condutores no veículo, e apenas o primeiro tiver aceitado partilhar os seus dados pessoais, os dados relativos ao segundo condutor não serão partilhados.

4.6. **Recuperação de dados-padrão**

O esquema 3 do anexo 2 representa os diagramas sequenciais de um pedido válido enviado pela unidade ITS para aceder aos dados-padrão. A unidade ITS está devidamente inserida na lista de permissões e não está a pedir dados pessoais, não sendo necessária verificação adicional. Os diagramas consideram que já foi seguido o procedimento adequado ilustrado no esquema 2 do anexo 2. Podem ser equiparados à caixa cinza *REQUEST TREATMENT* do esquema 2.

De entre os dados disponíveis, consideram-se os dados-padrão:

— standardTachData (TRTP 01)

— StandardEventData (TRTP 04)

— standardFaultData (TRTP 06)

4.7. **Recuperação de dados pessoais**

O esquema 4 do anexo 2 representa o diagrama sequencial para o procedimento de pedido de dados pessoais. Como foi referido anteriormente, a interface da VU só envia dados pessoais se o condutor tiver dado o seu consentimento explícito (ver também 4.5). Caso contrário, o pedido tem de ser rejeitado automaticamente.

▼B

De entre os dados disponíveis, consideram-se pessoais os seguintes:

— personalTachData (TRTP 02)

— gnssData (TRTP 03)

— personalEventData (TRTP 05)

— manufacturerData (TRTP 07)

4.8. **Recuperação de dados de incidentes e falhas**

As unidades ITS devem poder pedir dados de incidentes que contenham a lista de todos os incidentes imprevistos. Esses dados são considerados dados-padrão ou dados pessoais (ver anexo 3). O conteúdo de cada incidente está de acordo com a documentação fornecida no anexo 1 do presente apêndice.

▼B

ANEXO 1

LISTA DE DADOS DISPONÍVEIS ATRAVÉS DA INTERFACE ITS

Dados	Fonte	►C2 Classificação dos dados (pessoal/não pessoal) ◄
VehicleIdentificationNumber	Unidade-veículo	**não pessoal**
CalibrationDate	Unidade-veículo	**não pessoal**
T instant velocidadeTachographVehicleSpeed	Unidade-veículo	pessoal
Seletor do condutor Driver1WorkingState	Unidade-veículo	pessoal
Driver2WorkingState	Unidade-veículo	pessoal
Limiar de Velocidade detetado DriveRecognize	Unidade-veículo	**não pessoal**
Dia de semana Driver1TimeRelatedStates	Cartão de conductor	pessoal
Driver2TimeRelatedStates	Cartão de conductor	pessoal
DriverCardDriver1	Unidade-veículo	**não pessoal**
DriverCardDriver2	Unidade-veículo	**não pessoal**
OverSpeed	Unidade-veículo	pessoal
TimeDate	Unidade-veículo	**não pessoal**
HighResolutionTotalVehicleDistance	Unidade-veículo	**não pessoal**
ServiceComponentIdentification	Unidade-veículo	**não pessoal**
ServiceDelayCalendarTimeBased	Unidade-veículo	**não pessoal**
Driver1Identification	Cartão de conductor	pessoal
Driver2Identification	Cartão de conductor	pessoal
NextCalibrationDate	Unidade-veículo	**não pessoal**
Driver1ContinuousDrivingTime	Cartão de conductor	pessoal
Driver2ContinuousDrivingTime	Cartão de conductor	pessoal
Driver1CumulativeBreakTime	Cartão de conductor	pessoal
Driver2CumulativeBreakTime	Cartão de conductor	pessoal
Driver1CurrentDurationOfSelectedActivity	Cartão de conductor	pessoal
Driver2CurrentDurationOfSelectedActivity	Cartão de conductor	pessoal
SpeedAuthorised	Unidade-veículo	**não pessoal**
TachographCardSlot1	Cartão de conductor	**não pessoal**
TachographCardSlot2	Cartão de conductor	**não pessoal**
Driver1Name	Cartão de conductor	pessoal
Driver2Name	Cartão de conductor	pessoal

▼B

Dados	Fonte	►C2 Classificação dos dados (pessoal/não pessoal) ◄
OutOfScopeCondition	Unidade-veículo	**não pessoal**
ModeOfOperation	Unidade-veículo	**não pessoal**
Driver1CumulatedDrivingTimePreviousAndCurrentWeek	Cartão de conductor	pessoal
Driver2CumulatedDrivingTimePreviousAndCurrentWeek	Cartão de conductor	pessoal
EngineSpeed	Unidade-veículo	pessoal
RegisteringMemberState	Unidade-veículo	**não pessoal**
VehicleRegistrationNumber	Unidade-veículo	**não pessoal**
Driver1EndOfLastDailyRestPeriod	Cartão de conductor	pessoal
Driver2EndOfLastDailyRestPeriod	Cartão de conductor	pessoal
Driver1EndOfLastWeeklyRestPeriod	Cartão de conductor	pessoal
Driver2EndOfLastWeeklyRestPeriod	Cartão de conductor	pessoal
Driver1EndOfSecondLastWeeklyRestPeriod	Cartão de conductor	pessoal
Driver2EndOfSecondLastWeeklyRestPeriod	Cartão de conductor	pessoal
Driver1CurrentDailyDrivingTime	Cartão de conductor	pessoal
Driver2CurrentDailyDrivingTime	Cartão de conductor	pessoal
Driver1CurrentWeeklyDrivingTime	Cartão de conductor	pessoal
Driver2CurrentWeeklyDrivingTime	Cartão de conductor	pessoal
Driver1TimeLeftUntilNewDailyRestPeriod	Cartão de conductor	pessoal
Driver2TimeLeftUntilNewDailyRestPeriod	Cartão de conductor	pessoal
Driver1CardExpiryDate	Cartão de conductor	pessoal
Driver2CardExpiryDate	Cartão de conductor	pessoal
Driver1CardNextMandatoryDownloadDate	Cartão de conductor	pessoal
Driver2CardNextMandatoryDownloadDate	Cartão de conductor	pessoal
TachographNextMandatoryDownloadDate	Unidade-veículo	**não pessoal**
Driver1TimeLeftUntilNewWeeklyRestPeriod	Cartão de conductor	pessoal
Driver2TimeLeftUntilNewWeeklyRestPeriod	Cartão de conductor	pessoal
Driver1NumberOfTimes9hDailyDrivingTimesExceeded	Cartão de conductor	pessoal
Driver2NumberOfTimes9hDailyDrivingTimesExceeced	Cartão de conductor	pessoal

▼B

Dados	Fonte	►C2 Classificação dos dados (pessoal/não pessoal) ◄
Driver1CumulativeUninterruptedRestTime	Cartão de conductor	pessoal
Driver2CumulativeUninterruptedRestTime	Cartão de conductor	pessoal
Driver1MinimumDailyRest	Cartão de conductor	pessoal
Driver2MinimumDailyRest	Cartão de conductor	pessoal
Driver1MinimumWeeklyRest	Cartão de conductor	pessoal
Driver2MinimumWeeklyRest	Cartão de conductor	pessoal
Driver1MaximumDailyPeriod	Cartão de conductor	pessoal
Driver2MaximumDailyPeriod	Cartão de conductor	pessoal
Driver1MaximumDailyDrivingTime	Cartão de conductor	pessoal
Driver2MaximumDailyDrivingTime	Cartão de conductor	pessoal
Driver1NumberOfUsedReducedDailyRestPeriods	Cartão de conductor	pessoal
Driver2NumberOfUsedReducedDailyRestPeriods	Cartão de conductor	pessoal
Driver1RemainingCurrentDrivingTime	Cartão de conductor	pessoal
Driver2RemainingCurrentDrivingTime	Cartão de conductor	pessoal
Posição GNSS	Unidade-veículo	pessoal

2) DADOS GNSS CONTÍNUOS, DISPONÍVEIS APÓS CONSENTIMENTO DO CONDUTOR

Ver apêndice 12 — GNSS.

3) CÓDIGOS DE INCIDENTE, DISPONÍVEIS SEM CONSENTIMENTO DO CONDUTOR

Incidente	Regras de memorização	Dados a registar por cada incidente
Inserção de cartão não válido	— os 10 incidentes mais recentes	— data e hora do incidente — tipo, número, Estado-Membro emissor e geração do cartão que causa o incidente — número de incidentes similares nesse dia
Conflito de cartões	— os 10 incidentes mais recentes	— data e hora do início do incidente — data e hora do final do incidente — tipo, número, Estado-Membro emissor e geração dos dois cartões que causam o conflito
Última sessão de cartão encerrada incorretamente	— os 10 incidentes mais recentes	— data e hora de inserção do cartão — tipo, número, Estado-Membro emissor e geração do cartão — dados da última sessão, conforme leitura do cartão: — data e hora de inserção do cartão — VRN, Estado-Membro de matrícula e geração da VU

▼B

Incidente	Regras de memorização	Dados a registar por cada incidente
Interrupção da alimentação energética (2)	— o incidente mais longo de cada um dos últimos 10 dias de ocorrência — os 5 incidentes mais longos dos últimos 365 dias	— data e hora do início do incidente — data e hora do final do incidente — tipo, número, Estado-Membro emissor e geração de qualquer cartão inserido no início e/ou no final do incidente — número de incidentes similares nesse dia
Erro de comunicação com o sistema de comunicação à distância	— o incidente mais longo de cada um dos últimos 10 dias de ocorrência — os 5 incidentes mais longos dos últimos 365 dias	— data e hora do início do incidente — data e hora do final do incidente — tipo, número, Estado-Membro emissor e geração de qualquer cartão inserido no início e/ou no final do incidente — número de incidentes similares nesse dia
Ausência de informações sobre a posição do recetor GNSS	— o incidente mais longo de cada um dos últimos 10 dias de ocorrência — os 5 incidentes mais longos dos últimos 365 dias	— data e hora do início do incidente — data e hora do final do incidente — tipo, número, Estado-Membro emissor e geração de qualquer cartão inserido no início e/ou no final do incidente — número de incidentes similares nesse dia
Erro nos dados de movimento	— o incidente mais longo de cada um dos últimos 10 dias de ocorrência — os 5 incidentes mais longos dos últimos 365 dias	— data e hora do início do incidente — data e hora do final do incidente — tipo, número, Estado-Membro emissor e geração de qualquer cartão inserido no início e/ou no final do incidente — número de incidentes similares nesse dia
Conflito relativo ao movimento do veículo	— o incidente mais longo de cada um dos últimos 10 dias de ocorrência — os 5 incidentes mais longos dos últimos 365 dias	— data e hora do início do incidente — data e hora do final do incidente — tipo, número, Estado-Membro emissor e geração de qualquer cartão inserido no início e/ou no final do incidente — número de incidentes similares nesse dia
Tentativas de violação da segurança	os 10 incidentes mais recentes por tipo de incidente	— data e hora do início do incidente — data e hora do final do incidente (se pertinente) — tipo, número, Estado-Membro emissor e geração de qualquer cartão inserido no início e/ou no final do incidente — tipo de incidente

▼B

Incidente	Regras de memorização	Dados a registar por cada incidente
Conflito de tempo	— o incidente mais longo de cada um dos últimos 10 dias de ocorrência — os 5 incidentes mais longos dos últimos 365 dias	— data e hora do aparelho de controlo — data e hora GNSS — tipo, número, Estado-Membro emissor e geração de qualquer cartão inserido no início e/ou no final do incidente — número de incidentes similares nesse dia

4) CÓDIGOS DE INCIDENTE DISPONÍVEIS COM CONSENTIMENTO DO CONDUTOR

Incidente	Regras de memorização	Dados a registar por cada incidente
Condução sem cartão adequado	— o incidente mais longo de cada um dos últimos 10 dias de ocorrência — os 5 incidentes mais longos dos últimos 365 dias	— data e hora do início do incidente — data e hora do final do incidente — tipo, número, Estado-Membro emissor e geração de qualquer cartão inserido no início e/ou no final do incidente — número de incidentes similares nesse dia
Inserção de cartão durante condução	— o último incidente de cada um dos últimos 10 dias de ocorrência	— data e hora do incidente — tipo, número, Estado-Membro emissor e geração do cartão — número de incidentes similares nesse dia
Excesso de velocidade (1)	— o incidente mais grave (ou seja, o caso de velocidade média mais elevada) de cada um dos últimos 10 dias de ocorrência — um dos 5 incidentes mais graves dos últimos 365 dias — o primeiro incidente desde a última calibração	— data e hora do início do incidente — data e hora do final do incidente — velocidade máxima medida durante o incidente — velocidade média (aritmética) medida durante o incidente — tipo, número, Estado-Membro emissor e geração do cartão de condutor (quando aplicável) — número de incidentes similares nesse dia

5) CÓDIGOS DE DADOS DE FALHA DISPONÍVEIS SEM CONSENTIMENTO DO CONDUTOR

Falha	Regras de memorização	Dados a registar por cada falha
Falhas do cartão	— as 10 falhas mais recentes de cartão de condutor	— data e hora do início da falha — data e hora do final da falha — tipo, número, Estado-Membro emissor e geração do cartão
Falhas do aparelho de controlo	— as 10 falhas mais recentes por tipo de falha — a primeira falha ocorrida desde a última calibração	— data e hora do início da falha — data e hora do final da falha — tipo de falha — tipo, número, Estado-Membro emissor e geração de qualquer cartão inserido no início e/ou no final da falha

▼B

Esta falha ocorre em consequência de qualquer das seguintes, fora do modo de calibração:

— Falha interna da VU

— Falha da impressora

— Falha do visor

— Falha do descarregamento

— Falha do sensor

— Falha do recetor GNSS ou do módulo GNSS externo

— Falha do sistema de comunicação à distância

6) INCIDENTES E FALHAS ESPECÍFICOS DO FABRICANTE, SEM CONSENTIMENTO DO CONDUTOR

Incidente ou falha	Regras de memorização	Dados a registar por cada incidente
A definir pelo fabricante	A definir pelo fabricante	A definir pelo fabricante

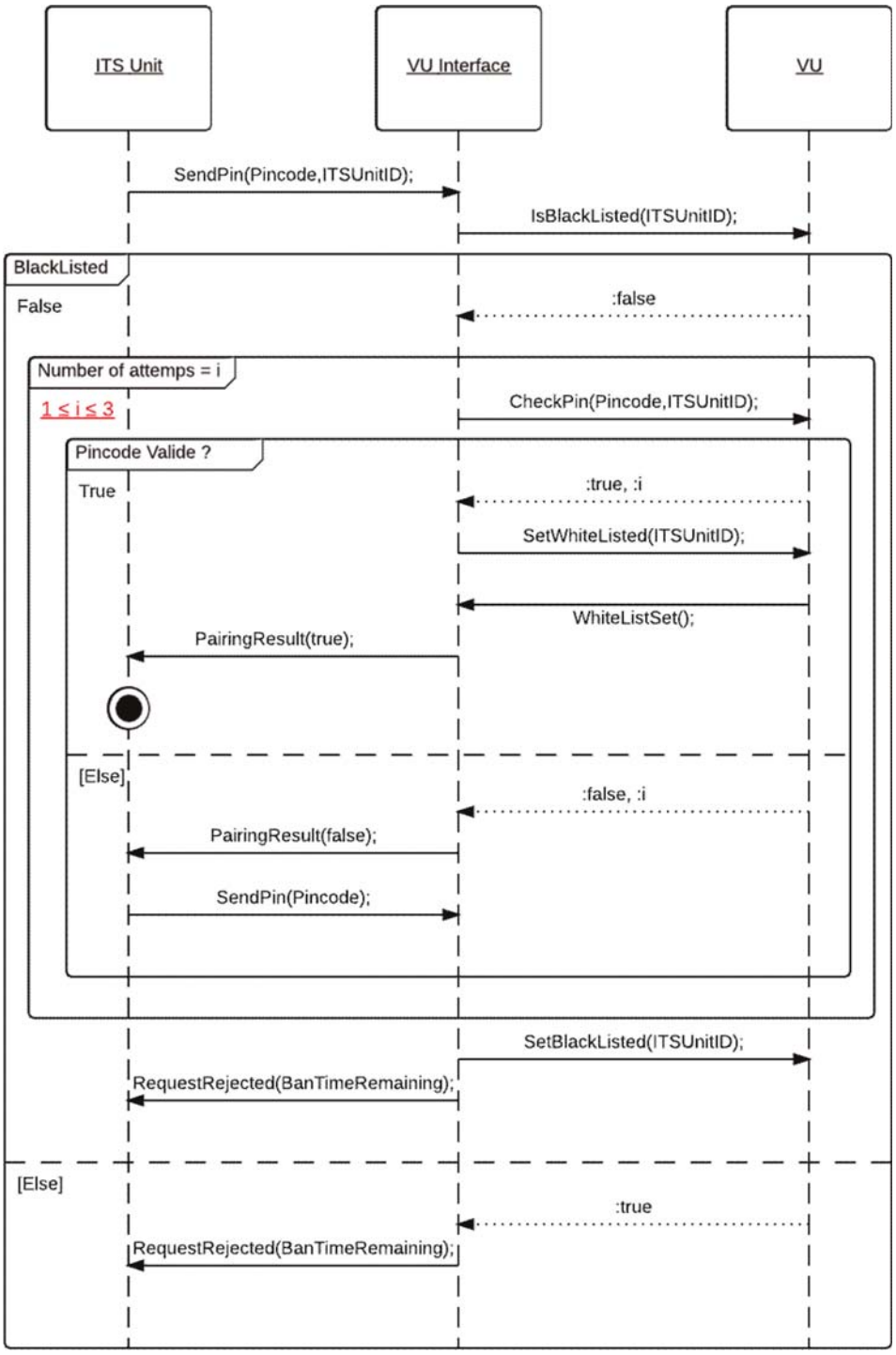
▼B

ANEXO 2

DIAGRAMAS SEQUENCIAIS DE INTERCÂMBIOS DE MENSAGENS COM A UNIDADE ITS

Esquema 1

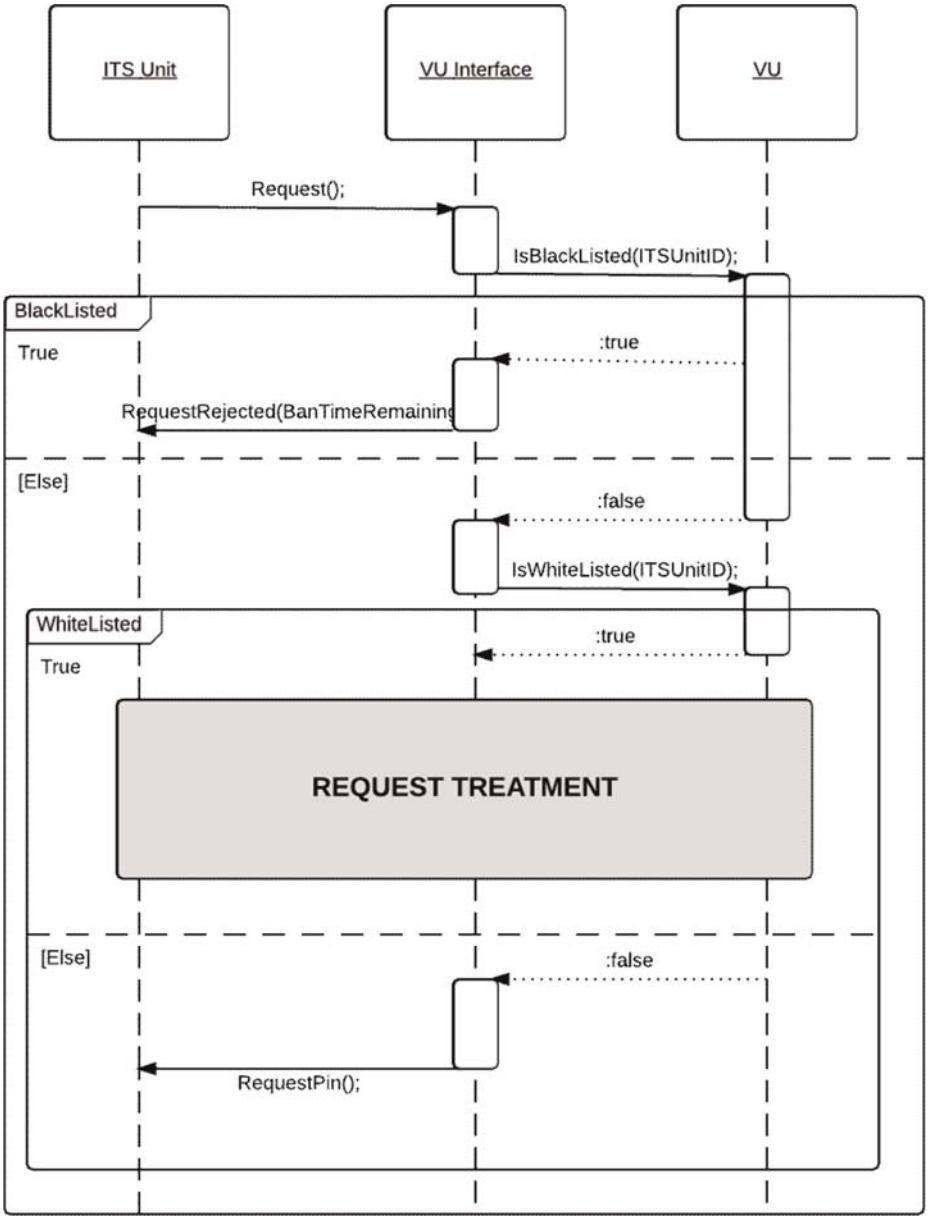
Diagrama sequencial para tentativa de validação do PIN



▼B

Esquema 2

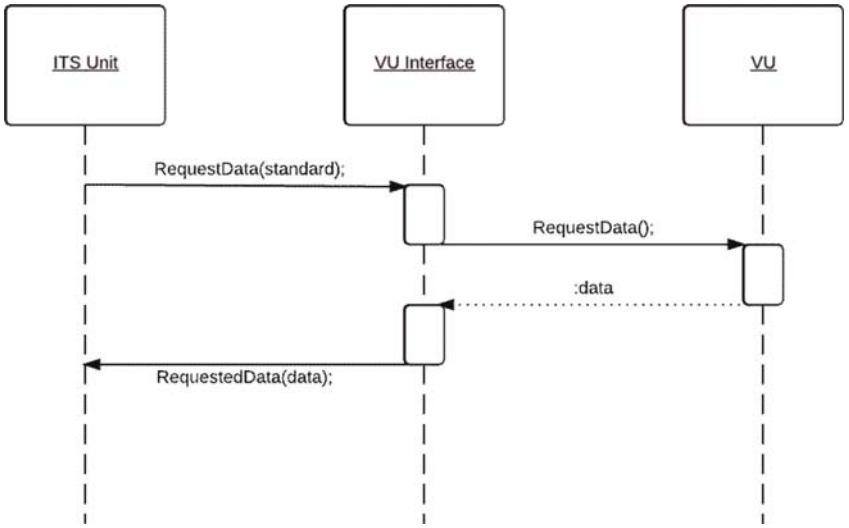
Diagrama sequencial para verificação de autorização da unidade ITS



▼B

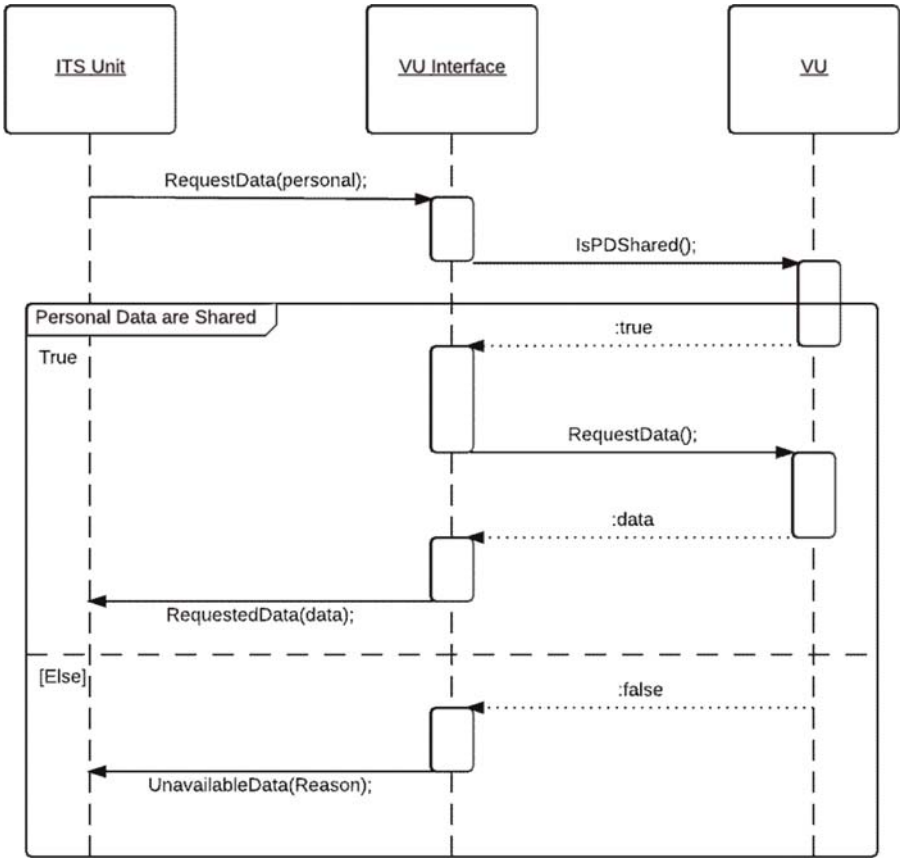
Esquema 3

Diagrama sequencial para processar um pedido de dados classificados como não-pessoais (após acesso com PIN correto)



Esquema 4

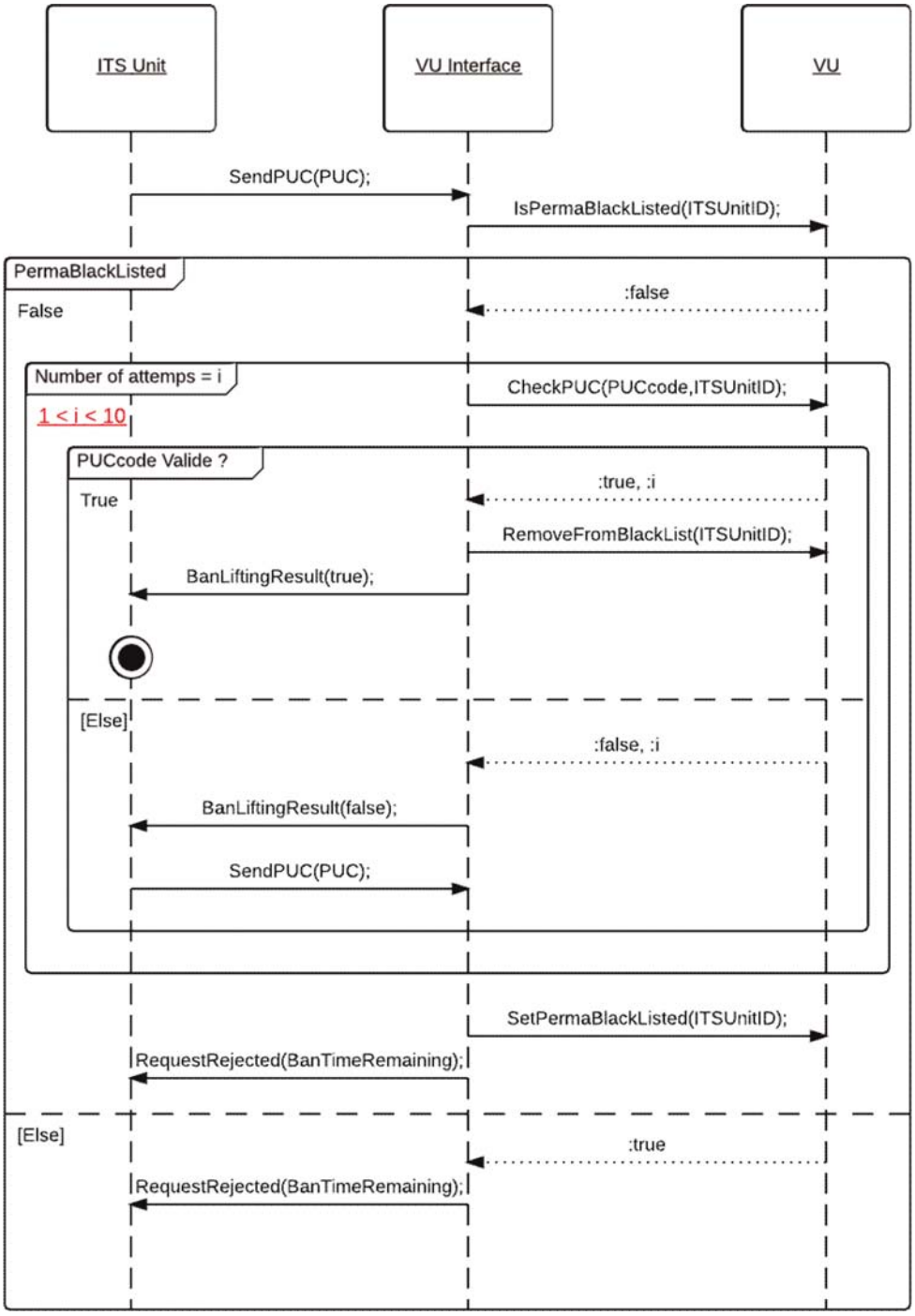
Diagrama sequencial para processar um pedido de dados classificados como pessoais (após acesso com PIN correto)



▼B

Esquema 5

Diagrama sequencial para tentativa de validação do PUC



▼B

ANEXO 3

ASN.1 SPECIFICATIONS

```
FormatMessageModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
EXPORTS ;
IMPORTS SendPIN, SendPUC, PairingResult, RequestPIN, RequestRejected,
        BanLiftingResult FROM PINPUCDataFieldsModule
        RequestAccepted,RequestData, DataUnavailable FROM
        RequestDataFieldsModule
        SendITSID, NegativeAnswer FROM OtherDataFieldsModule;

      CompleteMessage ::=SEQUENCE{
            header Header,
            data DataField,
            checksum Checksum
      }

      ----------------
      --HEADER TYPES--
      ----------------


      Header::=SEQUENCE{
            tgt IDList,
            src IDList,
            len BIT STRING (1..255)
      }

      vuID BIT STRING ::= 'EE'H
      IDList ::=CHOICE{
            vu BIT STRING (vuID),
            itsUnits SEQUENCE OF BIT STRING,
                  --Default hex Value:A0, redefined after first message exchange--
                  --Each ID will be linked to the Bluetooth ID of the device--
            ...
      }

      --------------------
      --DATAFIELDS TYPES--
      --------------------
      DataField ::=SEQUENCE{
            sid BIT STRING,
            trtp BIT STRING,
            subMBytes SubMessageBytes,
            dataField Content,
            ...
      }

      SubMessageBytes ::= SEQUENCE{
            currentSubM BIT STRING,
            totalSubM BIT STRING
      }

      Content ::= CHOICE{
            requestPIN RequestPIN,
            sendITSID SendITSID,
            sendPin SendPIN,
```

▼B

```
55                pairRslt PairingResult,
56                sendPUC SendPUC,
57                banlift BanLiftingResult,
58                requestRejected RequestRejected,
59                requestData RequestData,
60                requestOK RequestAccepted,
61                dataUnavailable DataUnavailable,
62                negAns NegativeAnswer
63          }
64
65          ------------------
66          --CHECKSUM TYPES--
67          ------------------
68
69          Checksum ::= SEQUENCE{
70                --SHA2 checksum
71          }
72    END
73
```

▼B

```
PINPUCDataFieldsModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
EXPORTS SendPIN, SendPUC, PairingResult, RequestPIN, RequestRejected,
BanLiftingResult;
IMPORTS ;

      ----------
      ---Utils--
      ----------

      PUC ::= SEQUENCE (SIZE(8)) OF
      INTEGER (SIZE(0..9))

      PIN ::=      SEQUENCE (SIZE(4)) OF
            INTEGER (SIZE(0..9))

      -------------------------
      --Messages From ITS Unit--
      -------------------------

      SendPIN {PIN:pin} ::= SEQUENCE {
            sid BIT STRING ('03'H),
            pin PIN (pin)
      }

      SendPUC {PUC:puc} ::= SEQUENCE {
            sid BIT STRING ('05'H),
            puc PUC (puc)
      }
      --------------------
      --Messages From VU--
      --------------------

      PairingResult ::= SEQUENCE{
            sid BIT STRING ('04'H),
            result BOOLEAN
      }

      RequestPIN {MType:receivedRequest}::= SEQUENCE{
            sid BIT STRING ('01'H)
      }

      RequestRejected ::= SEQUENCE{
            sid BIT STRING ('07'H),
            banTimeRemaining GeneralizedTime, --PermaBan == 1k years-- }

      BanLiftingResult ::= SEQUENCE{
            sid BIT STRING ('06'H),
            result BOOLEAN
      }
END
```

▼B

```
RequestDataFields DEFINITIONS AUTOMATIC TAGS ::= BEGIN
	EXPORTS RequestAccepted,RequestData, DataUnavailable ;
	IMPORTS StandardEvent, PersonalEvent, StandardFault FROM EventsModule;

	------------------
	---From ITS Unit--
	------------------
	RequestData ::= SEQUENCE{
		sid BIT STRING ('08'H),
		requestedData DataTypeCode,
		...
	}

	-----------
	--From VU--
	-----------
	RequestAccepted ::=SEQUENCE{
		sid BIT STRING ('09'H),
		trtp DataTypeCode,
		dataSheet CHOICE{
			standardData StandardTachDataContent,
			personalData PersonalTachDataContent,
			gnss GNSSDataContent,
			standardEvent StandardEventContent,
			personalEvent PersonalEventContent,
			standardFault StandardFaultContent,
			manufacturerdata ManufacturerDataContent,
			...
		}
	}

	DataTypeCode ::=CHOICE{
		standardTachData BIT STRING ('01'H),
		personalTachData BIT STRING ('02'H),
		gnssData BIT STRING ('03'H),
		standardEventData BIT STRING ('04'H),
		personalEventData BIT STRING ('05'H),
		standardFaultData BIT STRING ('06'H),
		manufacturerData BIT STRING ('07'H),
		...
	}

	DataUnavailable ::=SEQUENCE{
		sid BIT STRING ('0A'H),
		trtp DataTypeCode,
		reason UnavailableDataCodes
	}

	UnavailableDataCodes ::= CHOICE{
		noDataAvailable BIT STRING ('10'H),
		personalDataNotShared BIT STRING ('11'H),
		...
	}
	---------------------------
	--Complete Tachograph Data--
	---------------------------
	--The format of the data was taken from the ISO16844-7 norm, more information
available in this ISO document–

```

▼B

```
Time ::= SEQUENCE{
       seconds INTEGER (0..59.75), --increment: 0.25s--
       minutes INTEGER (0..59), --increment: 1min--
       hours INTEGER (0..23), --increment: 1h--
       day INTEGER (0.25.. 31.75), --increment: 0.25d--
       month INTEGER (1..12), --increment: 1month--
       year INTEGER (1985..2235), --increment: 1year--
       locMinOffset INTEGER (-59..59), --increment: 1min--
       locHouroffset INTEGER (-23..23)--increment: 1h--
}

Date ::= SEQUENCE{
       month INTEGER (1..12), --increment: 1month--
       day INTEGER (0.25.. 31.75), --increment: 0.25d--
       year INTEGER (1985..2235) --increment: 1year--
}

DriverName ::=SEQUENCE{
       codePageSurname UTF8String, --See ISO/IEC 8859--
       surname UTF8String,
       codePageFirstname UTF8String, --See ISO/IEC 8859--
       firstname UTF8String,
}

-------------------
--Message Content--
-------------------

StandardTachDataContent ::= SEQUENCE{
       trtp DataTypeCode (DataTypeCode.&standardTachData),
       personal BOOLEAN (FALSE),
       data StandardTachyDataSheet,
}

PersonalTachDataContent ::= SEQUENCE{
       trtp DataTypeCode (DataTypeCode.&personalTachData),
       personal BOOLEAN (TRUE),
       data PersonalTachyDataSheet
}

GNSSDataContent ::= SEQUENCE{
       trtp DataTypeCode (DataTypeCode.&gnssData),
       personal BOOLEAN (TRUE),
       data GNSSDataSheet
}

StandardEventContent ::= SEQUENCE{
       trtp DataTypeCode (DataTypeCode.&standardEventData),
       personal BOOLEAN (FALSE),
       data StandardEventDataSheet
}

PersonalEventContent ::= SEQUENCE{
       trtp DataTypeCode (DataTypeCode.&personalEventData),
       personal BOOLEAN (TRUE),
       data PersonalEventDataSheet
}

StandardFaultContent ::= SEQUENCE{
```

▼B

```
243                trtp DataTypeCode (DataTypeCode.&standardFaultData),
244                personal BOOLEAN (FALSE),
245                data StandardFault
246          }
247
248          ManufacturerDataContent ::= SEQUENCE{
249                trtp DataTypeCode (DataTypeCode.&manufacturerData),
250                personal BOOLEAN (TRUE),
251                ...
252          }
253
254          ---------------
255          --DATA SHEETS--
256          ---------------
257
258          --Data sheet format follows ISO 16844-7.--
259          StandardTachyDataSheet ::= SEQUENCE{
260                vin UTF8String (SIZE(17)),
261                calibrationDate Date,
262                driveRecognize INTEGER (2 UNION 12),
263                driverCardDriver1 INTEGER (2 UNION 12),
264                driverCardDriver2 INTEGER (2 UNION 12),
265                timeDate Time,
266                highResolutionTotalVehicleDistance INTEGER (0..21055406), --increment:
267    5m--
268                serviceComponentIdentification INTEGER (0..255),
269                serviceDelayCalendarTimeBased INTEGER (-125..125), --increment: 1week-
270    -
271                nextCalibrationDate Date,
272                speedAuthorised INTEGER (0..250.996), --increment 1/256km/h--
273                tachographCardSlot1 INTEGER (0..4...), --Maximum 250--
274                tachographCardSlot2 INTEGER (0..4...), --Maximum 250--
275                outOfScopeCondition INTEGER(2 UNION 12),
276                modeOfOperation INTEGER (0..4...), --Maximum 250--
277                registeringMemberState UTF8String,
278          vehicleRegistrationNumber SEQUENCE {
279                      codePageVRN INTEGER (0..255),
280                      vrn OCTET STRING (SIZE(13)),
281                },
282                tachographNextMandatoryDownloadDate Date,
283                ...
284          }
285
286          PersonalTachyDataSheet ::= SEQUENCE{
287                tachographVehicleSpeed INTEGER (0..250.996), --increment 1/256km/h--
288                driver1WorkingState INTEGER (2 UNION 12 UNION 102 UNION 112 UNION 1002
289    UNION 1012...),
290                driver2WorkingState INTEGER (2 UNION 12 UNION 102 UNION 112 UNION 1002
291    UNION 1012...),
292
293                driver1TimeRelatedStates INTEGER(2 UNION 12 UNION 102 UNION 112 UNION
294    1002 UNION
295                                                 1012 UNION 1102 UNION 1112 UNION
296    10002 UNION 10012 UNION
297                                                 10102 UNION 10112 UNION 11002 UNION
298    11012...),
299                driver2TimeRelatedStates INTEGER(2 UNION 12 UNION 102 UNION 112 UNION
300    1002 UNION
```

▼B

```
                                                    1012 UNION 1102 UNION 1112 UNION
10002 UNION 10012 UNION
                                                    10102 UNION 10112 UNION 11002 UNION
11012...),

              overSpeed INTEGER (2 UNION 12),
              driver1Identification INTEGER (SIZE(19)), --TODO NEED FURTHER SPECS
FROM TACHO REGULATION--
              driver2Identification INTEGER (SIZE(19)), --TODO NEED FURTHER SPECS
FROM TACHO REGULATION--
              driver1ContinuousDrivingTime INTEGER (0.. 64255), --increment: 1min--
              driver2ContinuousDrivingTime INTEGER (0.. 64255), --increment: 1min--
              driver1CurrentDurationOfSelectedActivity INTEGER (0.. 64255), --
increment: 1min--
              driver2CurrentDurationOfSelectedActivity INTEGER (0.. 64255), --
increment: 1min--
              driver1Name DriverName,
              driver2Name DriverName,
              driver1CumulatedDrivingTimePreviousAndCurrentWeek INTEGER (0.. 64255),
--increment: 1min--
              driver2CumulatedDrivingTimePreviousAndCurrentWeek INTEGER (0.. 64255),
--increment: 1min--
              engineSpeed INTEGER(0..8031.875), --increment: 0,125r/min--
              driver1EndOfLastDailyRestPeriod Time,
              driver2EndOfLastDailyRestPeriod Time,
              driver1EndOfLastWeeklyRestPeriod Time,
              driver2EndOfLastWeeklyRestPeriod Time,
              driver1EndOfSecondLastWeeklyRestPeriod Time,
              driver2EndOfSecondLastWeeklyRestPeriod Time,
              driver1CurrentDailyDrivingTime INTEGER (0.. 64255), --increment: 1min-
-
              driver2CurrentDailyDrivingTime INTEGER (0.. 64255), --increment: 1min-
-
              driver1CurrentWeeklyDrivingTime INTEGER (0.. 64255), --increment:
1min--
              driver2CurrentWeeklyDrivingTime INTEGER (0.. 64255), --increment:
1min--
              driver1TimeLeftUntilNewDailyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
              driver2TimeLeftUntilNewDailyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
              driver1CardExpiryDate Date,
              driver2CardExpiryDate Date,
              driver1CardNextMandatoryDownloadDate Date,
              driver2CardNextMandatoryDownloadDate Date,
              driver1TimeLeftUntilNewWeeklyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
              driver2TimeLeftUntilNewWeeklyRestPeriod INTEGER (0.. 64255), --
increment: 1min--
              driver1NumberOfTimes9hDailyDrivingTimesExceeded INTEGER (0..13),
              driver2NumberOfTimes9hDailyDrivingTimesExceeced INTEGER (0..13),
              driver1CumulativeUninterruptedRestTime INTEGER (0.. 64255), --
increment: 1min--
              driver2CumulativeUninterruptedRestTime INTEGER (0.. 64255), --
increment: 1min--
              driver1MinimumDailyRest INTEGER (0.. 64255), --increment: 1min--
              driver2MinimumDailyRest INTEGER (0.. 64255), --increment: 1min--
              driver1MinimumWeeklyRest INTEGER (0.. 64255), --increment: 1min--
              driver2MinimumWeeklyRest INTEGER (0.. 64255), --increment: 1min--
```

▼B

```
360                driver1MaximumDailyPeriod INTEGER (0..250), --increment: 1h--
361                driver2MaximumDailyPeriod INTEGER (0..250), --increment: 1h--
362                driver1MaximumDailyDrivingTime INTEGER (910 UNION 1010),
363                driver2MaximumDailyDrivingTime INTEGER (910 UNION 1010),
364                driver1NumberOfUsedReducedDailyRestPeriods INTEGER (0..13),
365                driver2NumberOfUsedReducedDailyRestPeriods INTEGER (0..13),
366                driver1RemainingCurrentDrivingTime INTEGER (0.. 64255), --increment:
367    1min--
368                driver2RemainingCurrentDrivingTime INTEGER (0.. 64255), --increment:
369    1min--
370                ...
371          }
372
373          GNSSDataSheet ::=  SEQUENCE {
374          gnssPosition GeoCoordinates
375                --See Appendix 1 for definition of GeoCoordinates--
376          }
377
378          StandardEventDataSheet ::= SEQUENCE{
379                events SEQUENCE OF StandardEvent
380          }
381
382          PersonalEventDataSheet ::= SEQUENCE{
383                events SEQUENCE OF PersonalEvent
384          }
385    END
386
387    EventsModule DEFINITIONS AUTOMATIC TAGS ::= BEGIN
388          EXPORTS ALL;
389          IMPORTS NationAlpha FROM Appendix1; --See Appendix 1 for more information
390    about NationAlpha--
391
392                SecurityBreachEvent ::=SEQUENCE{
393                      --See Annex 1B for more information--
394                }
395
396                RecordingEquipmentFaultType ::= SEQUENCE{
397                      --See Annex 1B for more information--
398                }
399
400                StandardEvent::= CHOICE{
401                      insertionInvalidCard InsertionOfANonValidCard,
402                      cardConflict CardConflict,
403                      timeOverlap TimeOverlap,
404                      previousSessionNotClosed LastCardSessionNotCorrectlyClosed,
405                      overSpeeding OverSpeeding,
406                      powerSupplyInterruption PowerSupplyInterruption,
407                      comErrorWithRemoteFacility
408    CommunicationErrorWithTheRemoteCommunicationFacility,
409                      absenceGNSSPosition
410    AbsenceOfPositionInformationFromGNSSReceiver,
411                      positionDataError PositionDataError,
412                      motionDataError MotionDataError,
413                      vehicleMotionConflict VehicleMotionConflict,
414                      securityBreachAttempt SecurityBreachAttempt,
415                      timeConflict TimeConflict,
416                      ...
417                }
418
```

▼B

```
PersonalEvent ::= CHOICE{
      lackOfAppropriateCard DrivingWithoutAnAppropriateCard,
      cardInsertionWhileDriving CardInsertionWhileDriving,
      overSpeeding OverSpeeding,
      ...
}

StandardFault ::= CHOICE{
      cardFault CardFault,
      recordingEquipementFault RecordingEquipmentFault,
...
}

---------------
--EVENTS LIST--
---------------

InsertionOfANonValidCard::=SEQUENCE{
      beginDate GeneralizedTime,
      endDate GeneralizedTime,
      carsdType SEQUENCE OF UTF8String,
      cardsNumber SEQUENCE OF INTEGER,
      issuingMemberState SEQUENCE OF NationAlpha,
      cardsGeneration SEQUENCE OF INTEGER
}

CardConflict ::= SEQUENCE{
      beginDate GeneralizedTime,
      endDate GeneralizedTime,
      carsdType SEQUENCE OF UTF8String,
      cardsNumber SEQUENCE OF INTEGER,
      issuingMemberState SEQUENCE OF NationAlpha,
      cardsGeneration SEQUENCE OF INTEGER
}

TimeOverlap ::=SEQUENCE{
      beginDate GeneralizedTime,
      endDate GeneralizedTime,
      carsdType SEQUENCE OF UTF8String,
      cardsNumber SEQUENCE OF INTEGER,
      issuingMemberState SEQUENCE OF NationAlpha,
      cardsGeneration SEQUENCE OF INTEGER,
      numberSimilarEvent INTEGER
}

DrivingWithoutAnAppropriateCard ::= SEQUENCE{
      beginDate GeneralizedTime,
      endDate GeneralizedTime,
      carsdType SEQUENCE OF UTF8String,
      cardsNumber SEQUENCE OF INTEGER,
      issuingMemberState SEQUENCE OF NationAlpha,
      cardsGeneration SEQUENCE OF INTEGER,
      numberOfSimilarEvent INTEGER
}

CardInsertionWhileDriving ::= SEQUENCE{
      date GeneralizedTime,
      carsdType SEQUENCE OF UTF8String,
      cardsNumber SEQUENCE OF INTEGER,
```

▼B

```
478                     issuingMemberState SEQUENCE OF NationAlpha,
479                     numberOfSimilarEvents INTEGER
480             }
481
482             LastCardSessionNotCorrectlyClosed ::=SEQUENCE{
483                     beginDate GeneralizedTime,
484                     endDate GeneralizedTime,
485                     carsdType SEQUENCE OF UTF8String,
486                     cardsNumber SEQUENCE OF INTEGER,
487                     issuingMemberState SEQUENCE OF NationAlpha,
488                     cardsGeneration SEQUENCE OF INTEGER,
489                     oldSession SEQUENCE{
490                             beginDate GeneralizedTime,
491                             endDate GeneralizedTime,
492                             vrn UTF8String,
493                             issuingMemberState NationAlpha,
494                             cardsGeneration INTEGER,
495                     }
496             }
497
498             OverSpeeding ::=SEQUENCE{
499                     beginDate GeneralizedTime,
500                     endDate GeneralizedTime,
501                     maximumSpeed INTEGER,
502                     averageSpeed INTEGER,
503                     cardType UTF8String,
504                     cardNumber INTEGER,
505                     issuingMemberState NationAlpha,
506                     cardGeneration INTEGER,
507                     numberOfSimilarEvents INTEGER
508             }
509
510             PowerSupplyInterruption ::=SEQUENCE{
511                     beginDate GeneralizedTime,
512                     endDate GeneralizedTime,
513                     carsdType SEQUENCE OF UTF8String,
514                     cardsNumber SEQUENCE OF INTEGER,
515                     issuingMemberState SEQUENCE OF NationAlpha,
516                     cardsGeneration SEQUENCE OF INTEGER,
517                     numberOfSimilarEvent INTEGER
518             }
519
520             CommunicationErrorWithTheRemoteCommunicationFacility ::=SEQUENCE{
521                     beginDate GeneralizedTime,
522                     endDate GeneralizedTime,
523                     carsdType SEQUENCE OF UTF8String,
524                     cardsNumber SEQUENCE OF INTEGER,
525                     issuingMemberState SEQUENCE OF NationAlpha,
526                     cardsGeneration SEQUENCE OF INTEGER,
527                     numberOfSimilarEvent INTEGER
528             }
529
530             AbsenceOfPositionInformationFromGNSSReceiver ::= SEQUENCE{
531                     beginDate GeneralizedTime,
532                     endDate GeneralizedTime,
533                     carsdType SEQUENCE OF UTF8String,
534                     cardsNumber SEQUENCE OF INTEGER,
535                     issuingMemberState SEQUENCE OF NationAlpha,
536                     cardsGeneration SEQUENCE OF INTEGER,
```

▼B

```
537                     numberOfSimilarEvent INTEGER
538             }
539
540             PositionDataError ::= SEQUENCE{
541                     beginDate GeneralizedTime,
542                     endDate GeneralizedTime,
543                     carsdType SEQUENCE OF UTF8String,
544                     cardsNumber SEQUENCE OF INTEGER,
545                     issuingMemberState SEQUENCE OF NationAlpha,
546                     cardsGeneration SEQUENCE OF INTEGER,
547                     numberOfSimilarEvent INTEGER
548             }
549
550             MotionDataError ::= SEQUENCE{
551                     beginDate GeneralizedTime,
552                     endDate GeneralizedTime,
553                     carsdType SEQUENCE OF UTF8String,
554                     cardsNumber SEQUENCE OF INTEGER,
555                     issuingMemberState SEQUENCE OF NationAlpha,
556                     cardsGeneration SEQUENCE OF INTEGER,
557                     numberOfSimilarEvent INTEGER
558             }
559
560             VehicleMotionConflict ::= SEQUENCE{
561                     beginDate GeneralizedTime,
562                     endDate GeneralizedTime,
563                     carsdType SEQUENCE OF UTF8String,
564                     cardsNumber SEQUENCE OF INTEGER,
565                     issuingMemberState SEQUENCE OF NationAlpha,
566                     cardsGeneration SEQUENCE OF INTEGER,
567                     numberOfSimilarEvent INTEGER
568             }
569
570             SecurityBreachAttempt ::= SEQUENCE{
571                     beginDate GeneralizedTime,
572                     endDate GeneralizedTime OPTIONAL,
573                     carsdType SEQUENCE OF UTF8String,
574                     cardsNumber SEQUENCE OF INTEGER,
575                     issuingMemberState SEQUENCE OF NationAlpha,
576                     numberOfSimilarEvent INTEGER,
577                     typeOfEvent SecurityBreachEvent
578             }
579
580
581             TimeConflict ::= SEQUENCE{
582                     beginDate GeneralizedTime,
583                     endDate GeneralizedTime,
584                     carsdType SEQUENCE OF UTF8String,
585                     cardsNumber SEQUENCE OF INTEGER,
586                     issuingMemberState SEQUENCE OF NationAlpha,
587                     cardsGeneration SEQUENCE OF INTEGER,
588                     numberOfSimilarEvent INTEGER
589             }
590
591             ---------------
592             --FAULTS LIST--
593             ---------------
594
595             CardFault ::= SEQUENCE{
```

▼B

```
596                     beginDate GeneralizedTime,
597                     endDate GeneralizedTime,
598                     carsdType SEQUENCE OF UTF8String,
599                     cardsNumber SEQUENCE OF INTEGER,
600                     issuingMemberState SEQUENCE OF NationAlpha,
601                     cardsGeneration SEQUENCE OF INTEGER,
602             }
603
604             RecordingEquipmentFault ::= SEQUENCE{
605                     beginDate GeneralizedTime,
606                     endDate GeneralizedTime,
607                     faultType RecordingEquipmentFaultType,
608                     carsdType SEQUENCE OF UTF8String,
609                     cardsNumber SEQUENCE OF INTEGER,
610                     issuingMemberState SEQUENCE OF NationAlpha,
611                     cardsGeneration SEQUENCE OF INTEGER,
612             }
613 END
```

▼B

Apêndice 14.

FUNÇÃO DE COMUNICAÇÃO À DISTÂNCIA

ÍNDICE

▼B

1 INTRODUÇÃO

Este apêndice especifica a conceção e os procedimentos a seguir a fim de implementar a função de comunicação à distância («a comunicação»), conforme estipula o artigo 9.º do Regulamento (UE) n.º 165/2014 («o Regulamento»).

DSC_1 O Regulamento (UE) n.º 165/2014 determina que o tacógrafo deve estar equipado com uma função de comunicação à distância que permita aos agentes das autoridades de controlo lerem informações dos tacógrafos de veículos em circulação, mediante equipamentos de interrogação à distância (leitor de comunicações de deteção rápida à distância [REDCR]), especialmente equipamentos de interrogação de conexão sem fios que utilizam interfaces de comunicações dedicadas de curto alcance (DSRC) CEN 5,8 GHz.

Importa compreender que esta função se destina a servir apenas como um pré-filtro, de modo a selecionar veículos para uma inspeção aprofundada, e não substitui o processo de inspeção formal, determinado pelo Regulamento (UE) n.º 165/2014 (cf. considerando 9 deste regulamento, nos termos do qual a comunicação à distância entre o tacógrafo e as autoridades responsáveis pelo controlo rodoviário facilita controlos de estrada seletivos).

DSC_2 Os *dados* são intercambiados por meio da *comunicação*, que será uma ligação com recurso a comunicações sem fios DSRC de 5,8 GHz compatíveis com o presente apêndice, ensaiada em relação aos parâmetros pertinentes da norma EN 300 674-1 {Electromagnetic compatibility and Radio spectrum Matters (ERM); Road Transport and Traffic Telematics (RTTT); Dedicated Short Range Communication (DSRC) transmission

▼B

equipment (500 kbit/s / 250 kbit/s) operating in the 5,8 GHz Industrial, Scientific and Medical (ISM) band; Part 1: General characteristics and test methods for Road Side Units (RSU) and On -Board Units (OBU)}.

DSC_3 A *comunicação* deve ser estabelecida com o equipamento de comunicação apenas quando tal for solicitado pelo equipamento da autoridade de controlo competente, mediante a utilização de meios de radiocomunicação compatíveis (*leitor de comunicações de deteção rápida à distância [REDCR]*).

DSC_4 Os *dados* devem estar protegidos, para garantir a integridade.

DSC_5 «Só as autoridades responsáveis pelo controlo autorizadas a controlar as infrações ao Regulamento (CE) n.º 561/2006 e ao Regulamento (UE) n.º 165/2014 e as oficinas terão acesso aos *dados* comunicados, na medida em que for necessário para verificar o correto funcionamento do tacógrafo».

DSC_6 Durante a *comunicação*, são intercambiados apenas os *dados* estritamente necessários para a realização de controlos de estrada seletivos a veículos com tacógrafos eventualmente manipulados ou indevidamente utilizados.

DSC_7 A integridade e a segurança dos *dados* obtêm-se protegendo os *dados* na unidade-veículo (VU) e passando pelo meio de comunicação à distância sem fios DSRC de 5,8 GHz apenas os dados de carga útil segura e os dados relacionados com a segurança (ver 5.4.4), o que significa que somente os agentes autorizados das autoridades de controlo competentes dispõem dos meios para compreender os dados transmitidos pela *comunicação* e para verificar a sua autenticidade (ver apêndice 11 — Mecanismos comuns de segurança).

DSC_8 Os *dados* contêm um período de tempo para o momento da sua última atualização.

DSC_9 O conteúdo dos dados de segurança deve ser conhecido apenas e sob o controlo das autoridades de controlo competentes e pelas partes com as quais essas autoridades partilham esta informação. O referido conteúdo está fora do âmbito das disposições da *comunicação* que é objeto do presente apêndice, com a ressalva de que a *comunicação* prevê a transferência de um pacote de dados de segurança com cada pacote de dados de carga útil.

DSC_10 A mesma arquitetura e os mesmos equipamentos devem poder ser utilizados para adquirir outros conceitos de dados (como a pesagem a bordo) utilizando a arquitetura aqui especificada.

DSC_11 Para esclarecimento, em conformidade com o disposto no Regulamento (UE) n.º 165/2014 (artigo 7.º), os dados relativos à identidade do condutor não devem ser divulgados através da *comunicação*.

2 ÂMBITO DE APLICAÇÃO

O presente apêndice destina-se a especificar de que modo os agentes das autoridades de controlo competentes utilizam uma comunicação sem fios DSRC 5,8 GHz específica para obter à distância dados (*os dados*) provenientes de um veículo visado, a qual identifica a eventual violação do

▼B

Regulamento (UE) n.º 165/2014 por este veículo e assinala a necessidade de o mandar parar, com vista a uma investigação mais aprofundada.

Segundo o Regulamento (UE) n.º 165/2014, os dados recolhidos devem limitar-se (ou ser relativos) aos dados que identificam uma potencial infração, na aceção do seu artigo 9.º.

Neste cenário, o tempo disponível para a comunicação é limitado, porque a *comunicação* é orientada e com uma conceção de curto alcance. Além disso, os mesmos meios de comunicação destinados à monitorização tacográfica à distância (RTM) podem ser igualmente utilizados pelas autoridades de controlo para outras aplicações (como os pesos e as dimensões máximos dos veículos pesados de mercadorias, definidos na Diretiva (UE) 2015/719) e essas operações podem ser distintas ou sequenciais, ao critério das autoridades de controlo competentes.

O presente apêndice especifica:

— O equipamento de comunicações, procedimentos e protocolos a utilizar para a *comunicação*

— As normas e regulamentos a que o equipamento de rádio deve obedecer

— A apresentação dos *dados* no equipamento de *comunicação*

— Os procedimentos de descarregamento e pedido e a sequência das operações

— Os *dados* a transferir

— A potencial interpretação dos *dados* transferidos através da *comunicação*

— As disposições destinadas aos dados de segurança relativos à *comunicação*

— A disponibilidade dos *dados* para as autoridades de controlo competentes

— O modo como o *leitor de comunicações de deteção rápida à distância* pode pedir diferentes conceitos de dados sobre a carga e a frota

Para esclarecimento, o presente apêndice não especifica:

— O funcionamento e a gestão da recolha dos *dados* na VU (que serão uma função da conceção do produto, salvo se especificadas noutras partes do Regulamento (UE) n.º 165/2014)

— A forma de apresentação dos dados recolhidos para o agente das autoridades de controlo, nem os critérios a utilizar por essas autoridades para decidirem quais os veículos a mandar parar (que serão uma função da conceção do produto, salvo se especificados noutras partes do Regulamento (UE) n.º 165/2014 ou uma decisão política das autoridades de controlo competentes). Para esclarecimento: a *comunicação* disponibiliza os *dados* apenas às autoridades de controlo competentes, para que estas possam tomar decisões informadas

▼B

— Disposições de segurança dos dados (como a encriptação) relativamente ao conteúdo dos *dados* (especificadas no apêndice 11 — Mecanismos comuns de segurança)

— Pormenores de conceitos de dados diferentes de RTM que podem ser obtidos utilizando a mesma arquitetura e o mesmo equipamento

— Pormenor do comportamento e da gestão entre VU e a DSRC-VU, nem o comportamento na DSRC-VU (exceto para fornecer os *dados*, quando um REDCR os pedir).

3 ACRÓNIMOS, DEFINIÇÕES E NOTAÇÕES

No presente apêndice utilizam-se os seguintes acrónimos e definições, que lhe são específicos:

antena	Dispositivo elétrico que converte energia elétrica em ondas de rádio e vice-versa, utilizado em combinação com um transmissor ou um recetor de rádio. Em funcionamento, um transmissor de rádio fornece uma corrente elétrica oscilante com uma frequência de rádio aos terminais da antena, e a antena irradia a energia da corrente sob a forma de ondas eletromagnéticas (ondas de rádio). Na receção, uma antena interceta alguma da energia de uma onda eletromagnética, a fim de produzir uma pequena tensão nos seus terminais, que é aplicada a um recetor para ser amplificada
comunicação	Intercâmbio de informações/dados entre uma *DSRC-REDCR* e uma DSRC-VU, de acordo com a secção 5, numa relação de principal-secundário, para obter os *dados*
dados	Dados seguros de formato definido (ver 5.4.4), pedidos pela *DSRC--REDCR* e fornecidos à *DSRC--REDCR* pela *DSRC-VU* através de uma ligação DSRC 5,8 GHz, definida em 5
Regulamento (UE) n.º 165/2014	Regulamento (UE) n.º 165/2014 do Parlamento Europeu e do Conselho, de 4 de fevereiro de 2014, relativo à utilização de tacógrafos nos transportes rodoviários, que revoga o Regulamento (CEE) n.º 3821/85 do Conselho relativo à introdução de um aparelho de controlo no domínio

▼B

	dos transportes rodoviários e que altera o Regulamento (CE) n.º 561/2006 do Parlamento Europeu e do Conselho relativo à harmonização de determinadas disposições em matéria social no domínio dos transportes rodoviários
AID	Identificador de uma aplicação
BLE	Baixo consumo energético do Bluetooth
BST	Quadro de serviço de baliza
CIWD	Inserção de cartão durante a condução
CRC	Controlo de redundâncias cíclicas
DSC (n)	Identificador de um pedido de apêndice DSRC específico
DSRC	Comunicações dedicadas de curto alcance
DSRC-REDCR	DSRC–Leitor de comunicações de deteção rápida à distância
DSRC-VU	DSRC–Unidade-veículo (módulo de «comunicação de deteção rápida à distância», definido no anexo 1C)
DWVC	Condução sem cartão válido
EID	Identificador de elemento
LLC	Controlo de ligação lógica
LPDU	LLC Unidade de dados de protocolo
OWS	Sistema de pesagem a bordo
PDU	Unidade de dados de protocolo
REDCR	Leitor de comunicação de deteção rápida à distância (equipamento definido no anexo 1C)
RTM	Monitorização tacográfica à distância
SM-REDCR	Módulo de segurança do leitor de comunicação de deteção rápida à distância
TARV	Aplicações telemáticas para veículos regulamentados (série das normas ISO 15638)

▼B

VU	Unidade-veículo
VUPM	Memória de carga útil da unidade-veículo
VUSM	Módulo de segurança da unidade-veículo
VST	Quadro de serviço do veículo
WIM	Peso em movimento
WOB	Peso a bordo

A especificação definida no presente apêndice refere-se à totalidade ou a partes dos regulamentos e normas a seguir indicados e deles depende. O clausulado do presente apêndice especifica as normas pertinentes ou cláusulas pertinentes das normas. Em caso de contradição, prevalecem as cláusulas do presente apêndice. Em caso de contradição sem que esteja claramente determinada qualquer especificação no presente apêndice, prevalece a aplicação da Recomendação ERC 70-03 (com ensaio em função dos parâmetros adequados da norma EN 300 674-1), seguindo-se, por ordem decrescente de preferência, as normas EN 12795, EN 12253, EN 12834 e EN 13372, n.os 6.2, 6.3, 6.4 e 7.1.

Regulamentos e normas de referência no presente apêndice:

[1] Regulamento (UE) n.º 165/2014 do Parlamento Europeu e do Conselho, de 4 de fevereiro de 2014, relativo à utilização de tacógrafos nos transportes rodoviários, que revoga o Regulamento (CEE) n.º 3821/85 do Conselho relativo à introdução de um aparelho de controlo no domínio dos transportes rodoviários e que altera o Regulamento (CE) n.º 561/2006 do Parlamento Europeu e do Conselho relativo à harmonização de determinadas disposições em matéria social no domínio dos transportes rodoviários.

[2] Regulamento (CE) n.º 561/2006 do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativo à harmonização de determinadas disposições em matéria social no domínio dos transportes rodoviários, que altera os Regulamentos (CEE) n.º 3821/85 e (CE) n.º 2135/98 do Conselho e revoga o Regulamento (CEE) n.º 3820/85 do Conselho.

[3] ERC 70-03 CEPT: ECC Recommendation 70-03: Relating to the Use of Short Range Devices (SRD)

[4] ISO 15638-9 Intelligent transport systems — Framework for cooperative telematics applications for regulated commercial freight vehicles (TARV).

[5] EN 300 674-1: Electromagnetic compatibility and Radio spectrum Matters (ERM); Road Transport and Traffic Telematics (RTTT); Dedicated Short Range Communication (DSRC) transmission equipment (500 kbit/s / 250 kbit/s) operating in the 5,8 GHz Industrial, Scientific and Medical (ISM) band; Part 1: General characteristics and test methods for Road Side Units (RSU) and On-Board Units (OBU).

[6] EN 12253: Road transport and traffic telematics — Dedicated short-range communication — Physical layer using microwave at 5,8 GHz.

▼B

[7] EN 12795: Road transport and traffic telematics — Dedicated short-range communication — Data link layer: medium access and logical link control.

[8] EN 12834: Road transport and traffic telematics — Dedicated short-range communication — Application layer.

[9] EN 13372: Road transport and traffic telematics — Dedicated short-range communication — Profiles for RTTT applications

[10] ISO 14906: Electronic fee collection — Application interface definition for dedicated short- range communication

4 CENÁRIOS OPERACIONAIS

4.1 **Panorâmica**

O Regulamento (UE) n.º 165/2014 apresenta cenários específicos e controlados nos quais deve ser utilizada a *comunicação.*

Cenários compatíveis:

«Communication Profile 1: Roadside inspection using a short range wireless communication Remote Early Detection Communication Reader instigating a physical roadside inspection (master-:-slave)

Reader Profile 1a: via a hand aimed or temporary roadside mounted and aimed Remote Early Detection Communication

Reader Profile 1b: via a vehicle mounted and directed Remote Early Detection Communication Reader».

4.1.1 *Condições prévias para a transferência de dados através da interface DSRC 5,8 GHz*

NOTA: A fim de compreender o contexto das condições prévias o leitor é mencionado no esquema 14.3 infra.

4.1.1.1 Dados detidos pela VU

DSC_12 A VU tem a responsabilidade de manter atualizados de 60 em 60 segundos e de guardar os dados a memorizar na VU, sem qualquer envolvimento da função de comunicação DSRC. O meio pelo qual se consegue este procedimento é interno à VU, está especificado no Regulamento (UE) n.º 165/2014 e no anexo 1C, secção 3.19 («*Comunicação à distância para controlos de estrada seletivos*») e não é especificado no presente apêndice.

4.1.1.2 Dados fornecidos ao módulo DSRC-VU

DSC_13 A VU tem a responsabilidade de atualizar os dados (os *dados*) tacográficos DSRC sempre que os dados memorizados na VU sejam atualizados em intervalos determinados em 4.1.1.1 (DSC_12), sem qualquer envolvimento da função de comunicação DSRC.

DSC_14 Os dados da VU são utilizados como base para preencher e atualizar os *dados,* estando os meios pelos quais tal é conseguido especificados no anexo 1C, secção 3.19 («*Comunicação à distância para controlos de estrada seletivos*») ou, se não existir essa especificação, trata-se de uma função de conceção do produto, que o presente apêndice não especifica. Relativamente à conceção da conexão entre o módulo DSRC-VU e a VU, consultar a secção 5.6.

▼B

4.1.1.3 Conteúdo dos dados

DSC_15 O conteúdo e o formato dos *dados* devem ser tais que, uma vez decifrados, são estruturados e disponibilizados na forma e no formato especificados na secção 5.4.4 do presente apêndice (estruturas de dados).

4.1.1.4 Apresentação dos dados

DSC_16 Os *dados*, tendo sido mantidos atualizados com frequência, de acordo com os procedimentos previstos em 4.1.1.1, devem ser protegidos antes da apresentação à *DSRC-VU* e apresentados como valor de conceito de dados seguros, para memorização temporária na *DSRC-VU* como a versão atual dos *dados.* Estes dados são transferidos do *VUSM* para o *VUPM* da função DSRC. O *VUSM* e *VUPM* são funções e não necessariamente entidades físicas. A forma de instanciação física para executar essas funções será uma questão de conceção do produto, salvo especificação noutras partes do Regulamento (UE) n.º 165/2014.

4.1.1.5 Dados de segurança

DSC_17 Os dados de segurança (*securityData*), compreendendo os dados exigidos pelo *REDCR* para concluir a sua capacidade de decifrar os *dados*, são fornecidos conforme define o apêndice 11 (Mecanismos comuns de segurança) e apresentados como valores de conceito de dados, para memorização temporária na *DSRC-VU* como a versão atual de *securityData,* na forma definida na secção 5.4.4. do presente apêndice.

4.1.1.6 Dados VUPM disponíveis para transferência através da interface DSRC

DSC_18 O conceito dos dados que devem estar sempre disponíveis na VUPM de função DSRC para transferência imediata, a pedido do *REDCR*, é definido na secção 5.4.5 relativamente a especificações completas do módulo ASN.1.

Panorâmica geral do perfil de comunicação 1

Este perfil abrange o caso em que um agente das autoridades de controlo competentes utiliza um leitor de comunicações de deteção rápida à distância (interfaces DSRC de 5,8 GHz em aplicação da Recomendação ERC 70-03 e ensaiadas em relação aos parâmetros pertinentes da norma EN 300 674-1, conforme refere a secção 5) (o *REDCR*) para identificar à distância um veículo que está em possível violação do disposto no *Regulamento (UE) n.º 165/2014.* Uma vez identificado, o agente das autoridades de controlo competentes que está a controlar a interrogação decide se o veículo deve ser parado.

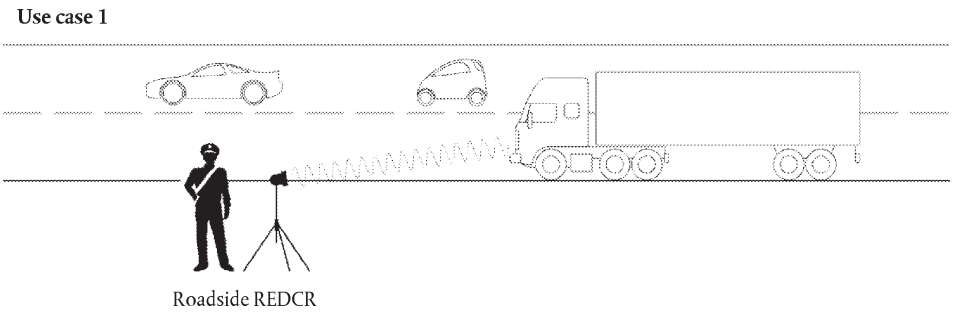
4.1.2 *Perfil 1a: através de um leitor de comunicações de deteção rápida à distância apontado manualmente ou montado e apontado temporariamente à estrada*

Neste caso de utilização, o agente das autoridades de controlo competentes está postado na berma da estrada e segura um *REDCR* manual de mira, montado no tripé ou outro equipamento portátil semelhante, a partir da berma da estrada, na direção do centro do para-brisas do veículo visado. A interrogação é feita com recurso a interfaces DSRC de 5,8 GHz, em aplicação da Recomendação ERC 70-03, e ensaiada em relação aos parâmetros pertinentes da norma EN 300 674-1, conforme refere a secção 5 (ver esquema 14.1 — Caso de utilização 1).

▼B

Esquema 14.1

Caso de utilização 1: interrogação de estrada com recurso a DSRC de 5,8 GHz

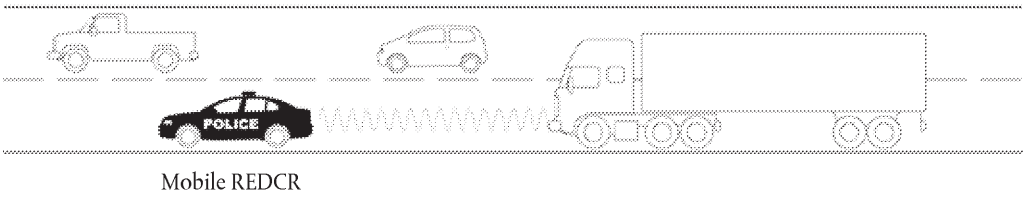


4.1.3 *Perfil 1b: através de um leitor de comunicações de deteção rápida à distância (REDCR) montado num veículo e direcionado*

Neste caso de utilização, o agente das autoridades de controlo competentes está postado dentro de um veículo em movimento e segura um *REDCR* manual de mira, portátil a partir do veículo, em direção ao centro do para-brisas do veículo visado, ou o *REDCR* está montado no interior ou no veículo de modo a apontar em direção ao centro do para-brisas do veículo visado quando o veículo do leitor de comunicações de deteção rápida à distância está numa posição particular pertinente para o veículo visado (por exemplo, diretamente em frente num fluxo de tráfego). A interrogação é feita com recurso a interfaces DSRC de 5,8 GHz em aplicação da Recomendação ERC 70-03 e ensaiada em relação aos parâmetros pertinentes da norma EN 300 674-1, conforme refere a secção 5 (ver esquema 14.2 — Caso de utilização 2).

Esquema 14.2

Caso de utilização 2: interrogação com base em veículo, com recurso a DSRC de 5,8 GHz



4.2 **Segurança/integridade**

Para tornar possível verificar a autenticidade e a integridade dos dados descarregados através da comunicação à distância, os *dados* seguros são verificados e decifrados em conformidade com o apêndice 11 (Mecanismos comuns de segurança).

5 CONCEÇÃO E PROTOCOLOS DA COMUNICAÇÃO À DISTÂNCIA

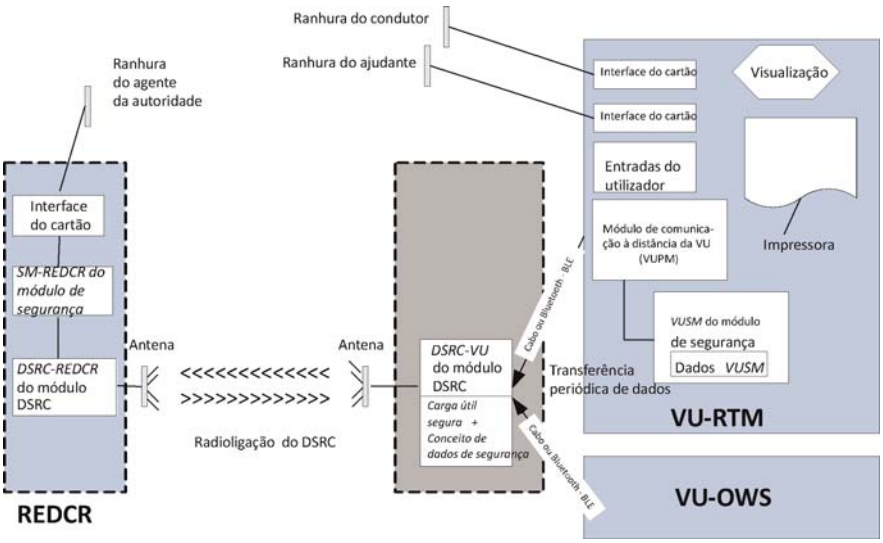
5.1 **Conceção**

A conceção da função de comunicação à distância no tacógrafo inteligente é apresentada e descrita no esquema 14.3.

▼B

Esquema 14.3

Conceção da função de comunicação à distância



DSC_19 As funções que se seguem localizam-se na VU:

— Módulo de Segurança (*VUSM*). Esta função, presente na VU, é responsável pela proteção dos *dados* que se transmitem da *DSRC-VU* ao agente das autoridades de controlo competentes, através da comunicação à distância.

— Os dados protegidos são memorizados na memória VUSM. Em intervalos determinados em 4.1.1.1 (DSC_12), a VU encripta e reabastece o conceito RTMdata (que compreende dados de carga útil e valores de conceito de dados de segurança determinados no presente apêndice), detido na memória de DSRC-VU. O funcionamento do módulo de segurança está definido no apêndice 11 (Mecanismos comuns de segurança) e fora do âmbito de aplicação do presente apêndice, com a ressalva de que é necessário fornecer atualizações ao módulo de comunicação da VU sempre que os dados VUSM mudarem.

— A comunicação entre a VU e a DSRC-VU pode ser uma comunicação por cabo ou uma comunicação de baixo consumo energético do Bluetooth (BLE), e a localização física da DSRC-VU pode estar integrada na antena (no para-brisas do veículo), pode ser interna à VU ou localizar-se algures entre os dois.

— A DSRC-VU deve ter uma fonte fiável de energia permanentemente disponível. O meio pelo qual a energia lhe é fornecida é uma decisão de conceção.

— A memória da DSRC-VU deve ser não-volátil, para que os dados sejam mantidos mesmo quando a ignição do veículo está desligada.

— Se a comunicação entre a VU e a DSRC-VU for efetuada através de BLE e a fonte de energia for uma bateria não recarregável, a fonte de energia da DSRC-VU deve ser substituída a cada inspeção periódica e o fabricante do equipamento DSRC-VU deve ser responsável por garantir

▼B

que a alimentação elétrica é adequada para durar de uma inspeção periódica à seguinte, mantendo o acesso normal aos dados por um REDCR durante todo o período, sem falhas nem interrupções.

— Módulo de «memória de carga útil» VU RTM (*VUPM*). Esta função, presente na VU, é responsável por fornecer e atualizar os *dados*. O conteúdo dos *dados* («Tachograph-Payload») está definido em 5.4.4/5.4.5 e é atualizado no intervalo determinado em 4.1.1.1 (DSC_12).

— DSRC-VU. Esta é a função, no interior ou ligada à antena e em comunicação com a VU através de uma ligação com fios ou sem fios (BLE), que mantém os dados atuais (*VUPM-dados*) e gere a resposta a uma interrogação no meio de comunicação DSRC de 5,8 GHz. A desconexão do módulo DSCR ou interferências durante o funcionamento normal do veículo com o funcionamento do módulo DSRC devem ser interpretadas como violação do Regulamento (UE) n.º 165/2014.

— Módulo de segurança (REDCR) (*SM-REDCR*) é a função utilizada para decifrar e verificar a integridade dos dados provenientes da VU. O meio pelo qual tal é conseguido está determinado no apêndice 11 (Mecanismos comuns de segurança) e não está definido no presente apêndice.

— A função do módulo DSRC (REDCR) (*DSRC-REDCR*) compreende um emissor-recetor de 5,8 GHz e *software* associado (permanente e não-permanente) que gere a *comunicação* com a *DSRC-VU* em conformidade com o presente apêndice.

— A *DSRC-REDCR* interroga a *DSRC-VU* do veículo visado e obtém os *dados* (*VUPM-dados* atuais do veículo visado), através da ligação DSRC e processa e memoriza os dados recebidos na sua *SM-REDCR*.

— A antena DSRC-VU deve ser posicionada num local onde otimize a comunicação DSRC entre o veículo e a antena do lado da estrada (em geral, sensivelmente no centro do para-brisas do veículo). Nos veículos ligeiros, é adequada a parte superior do para-brisas.

— Em frente ou próximo da antena, não deve haver objetos metálicos (por exemplo, crachás, autocolantes, película antirreflexo, tiras, para-sóis, escovas do limpa-para-brisas em repouso) que possam interferir com a comunicação.

— A antena deve ser montada de modo que a sua visão seja aproximadamente paralela à superfície da estrada.

▼B

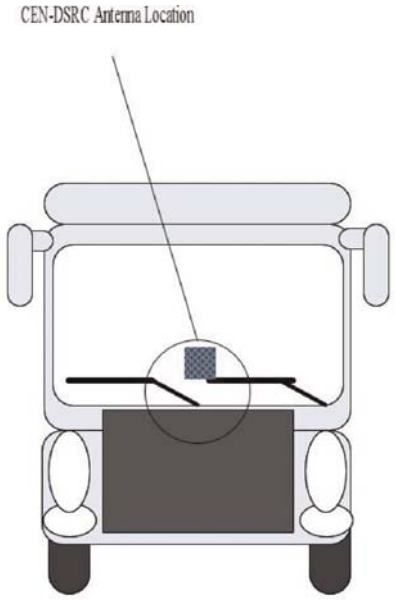
DSC_20 A antena e a comunicação devem funcionar nos termos da ERC 70-03, ensaiadas em relação aos parâmetros pertinentes da norma EN 300 674-1, conforme refere a secção 5. A antena e a comunicação podem pôr em prática técnicas de atenuação do risco de interferência sem fios descritas no relatório ECC 228, utilizando, por exemplo, filtros na comunicação CEN DSRC 5,8 GHz.

DSC_21 A antena DSRC deve estar ligada ao módulo DSRC-VU diretamente no módulo montado ou junto ao para-brisas ou através de um cabo dedicado construído de maneira a dificultar desconexão ilegal. Desconexão ou interferências com o funcionamento da antena constituem violações do Regulamento (UE) n.º 165/2014. Ocultação deliberada ou outra forma de impacto negativo no desempenho operacional da antena deve ser interpretada como violação do Regulamento (UE) n.º 165/2014.

DSC_22 O fator forma da antena não está definido e deve ser uma decisão comercial, desde que a DSRC-VU montada satisfaça os requisitos de conformidade definidos na secção 5. A antena é posicionada conforme determinado em DSC_19 e demonstrado no esquema 14.4 (linha oval) e aceita eficientemente os casos de utilização descritos em 4.1.2 e 4.1.3.

Esquema 14.4

Exemplo de posicionamento da antena DSRC de 5,8 GHz no para-brisas dos veículos regulamentados



O fator forma do *REDCR* e da respetiva antena pode variar de acordo com as circunstâncias do leitor (montado em tripé, porte manual, montado no veículo, etc.) e com o *modus operandi* aplicado pelo agente das autoridades de controlo.

A função de exibição e/ou notificação é utilizada para apresentar ao agente das autoridades de controlo os resultados da função de comunicação à distância. A exibição pode ser fornecida num ecrã, como resultado impresso, sinal de áudio ou combinação das notificações. A forma dessa exibição e/ou notificação depende dos agentes das autoridades de controlo e da conceção do equipamento, não estando especificada no presente apêndice.

▼B

DSC_23 O fator de conceção e forma do *REDCR* deve ser uma função de conceção comercial, em aplicação da Recomendação ERC 70-03 e das especificações de conceção e desempenho definidas no presente apêndice (secção 5.3.2), proporcionando assim a máxima flexibilidade de mercado para conceber e fornecer equipamentos e cobrir os cenários específicos de interrogação de qualquer autoridade de controlo competente.

DSC_24 O fator conceção e forma da *DSRC-VU* e o seu posicionamento dentro ou fora da VU deve ser uma função de conceção comercial, em aplicação da Recomendação ERC 70-03 e das especificações de conceção e desempenho definidas no presente apêndice (secção 5.3.2) e nesta cláusula (5.1)

DSC_25 No entanto, a *DSRC-VU* deve ser razoavelmente capaz de aceitar valores de conceito de dados de outro equipamento inteligente de veículos por meio de uma conexão-padrão da indústria aberta e protocolos (por exemplo, de equipamento de pesagem a bordo), desde que os conceitos de dados sejam identificados por identificadores de aplicação/nomes de ficheiros conhecidos e únicos. Por outro lado, as instruções de funcionamento desses protocolos devem ser disponibilizadas à Comissão Europeia e disponibilizadas, sem custos, aos fabricantes dos equipamentos relevantes.

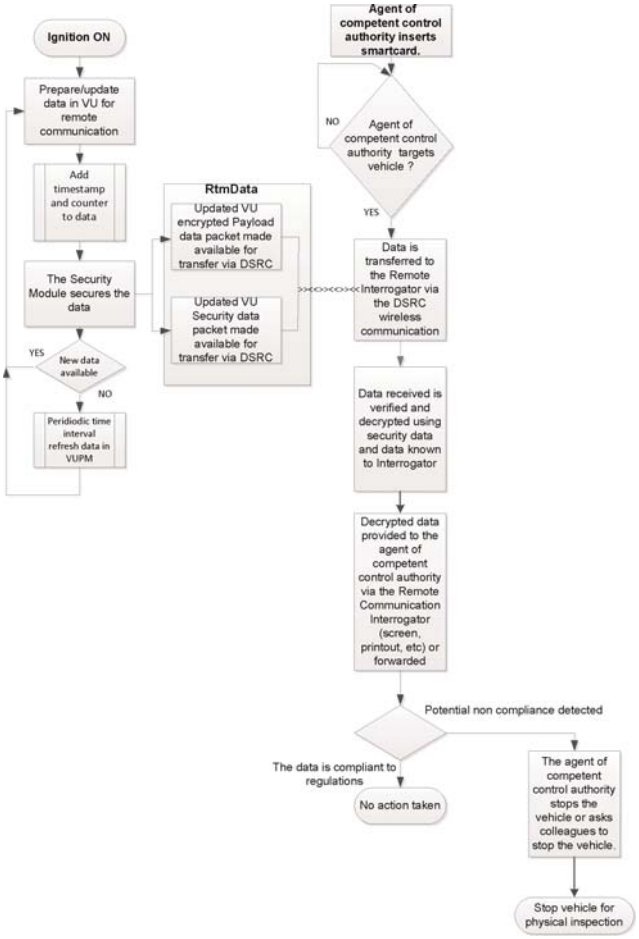
5.2 **Fluxo de trabalho**

5.2.1 *Operações*

O fluxo de trabalho das operações está representado no esquema 14.5.

Esquema 14.5

Fluxo de trabalho para a função de comunicação à distância



▼B

Descrevem-se seguidamente as fases:

a. Com o veículo em funcionamento (ignição ligada), o tacógrafo fornece dados à função da VU. A função da VU prepara os *dados* para a função de comunicação à distância (encriptada) e atualiza o *VUPM* guardado na memória da *DSRC-VU* (conforme definição em 4.1.1.1--4.1.1.2). Os *dados* recolhidos devem ser formatados conforme determinado em 5.4.4-5.4.5.

b. Sempre que os *dados* são atualizados, o período de tempo definido no conceito de dados de segurança é atualizado.

c. A função *VUSM* protege os dados em conformidade com os procedimentos previstos no apêndice 11.

d. Sempre que são atualizados (ver 4.1.1.1-4.1.1.2), os *dados* são transferidos para a *DSRC-VU*, onde substituem todos os dados anteriores, para que esses dados atualizados (os *dados)* estejam sempre disponíveis, no caso de uma interrogação por um *REDCR*. Se forem fornecidos pela VU à DSRC-VU, os *dados* devem ser identificáveis pelo nome de ficheiro *RTMData* ou pelos identificadores ApplicationID e Attribute.

e. Se um agente de controlo quiser designar um veículo e recolher os correspondentes *dados*, deve, em primeiro lugar, inserir o seu cartão inteligente no *REDCR* para permitir a *comunicação* e para permitir que o *SM-REDCR* verifique a sua autenticidade e decifre os dados.

f. O agente da autoridade de controlo competente designa um veículo e pede os dados através da comunicação à distância. O *REDCR* abre uma sessão da interface DSRC de 5,8 GHz com a *DSRC-VU* do veículo visado e pede os *dados*. Os *dados* são transferidos para *o REDCR* através do sistema de comunicações sem fios como um DSRC Attribute utilizando o serviço de Application GET definido em 5.4. O Attribute contém os valores encriptados de dados de carga útil e os dados de segurança DSRC.

g. Os dados são analisados pelo equipamento *REDCR* e fornecidos ao agente da autoridade de controlo competente.

h. O agente da autoridade de controlo competente utiliza os dados para o auxiliar a decidir se deve ou não parar o veículo para uma inspeção pormenorizada, ou pedir a outro agente da autoridade de controlo competente para parar o veículo.

5.2.2 *Interpretação dos dados recebidos através da comunicação DSRC*

DSC_26 Os dados recebidos através da interface de 5,8 GHz devem transportar o significado e a importação definidos nas secções 5.4.4 e 5.4.5 e apenas esse significado e essa importação, e devem estar compreendidos nos objetivos neles definidos. Em conformidade com o Regulamento (UE) n.º 165/2014, os *dados* apenas devem ser utilizados para fornecer informações

▼B

pertinentes à autoridade de controlo competente com vista a auxiliar os agentes na determinação de qual o veículo que deve ser parado para inspeção física, sendo posteriormente destruídos, conforme estipula o artigo 9.º do Regulamento (UE) n.º 165/2014.

5.3 **Parâmetros da interface física DSRC para comunicação à distância**

5.3.1 *Restrições de localização*

DSC_27 A interrogação à distância de veículos com recurso à interface SRC de 5,8 GHz não deve ser utilizada a menos de 200 metros de um pórtico operacional DSRC de 5,8 GHz.

5.3.2 *Parâmetros de ligação descendente e ascendente*

DSC_28 O equipamento utilizado na monitorização tacográfica à distância deve estar conforme e em aplicação da Recomendação ERC 70-03 e dos parâmetros definidos nos quadros 14.1 e 14.2 abaixo.

DSC_29 Além disso, para garantir a compatibilidade com os parâmetros operacionais dos outros sistemas DSRC de 5,8 GHz normalizados, o equipamento utilizado na monitorização tacográfica à distância deve estar em conformidade com os parâmetros das normas EN 12253 e EN 13372.

A saber:

Quadro 14.1

▼C2

Parâmetros de ligação descendente

Ponto	Parâmetro	Valor(es)	Observação
D1	Frequências de ligação descendente	O REDCR pode utilizar quatro alternativas: 5,7975 GHz 5,8025 GHz 5,8075 GHz 5,8125 GHz	No limite de ERC 70-03. As frequências de ligação podem ser selecionadas pelo responsável do sistema de controlo rodoviário e não têm de ser conhecidas a nível de DSRC-VU (conforme EN 12253 e EN 13372)
D1a (*)	Tolerância das frequências de ligação	No limite de ± 5 ppm	(conforme EN 12253)
D2 (*)	Máscara espetral de emissão da RSU (REDCR)	No limite de ERC 70-03. O REDCR deve corresponder à classe B,C definida na norma EN 12253. Não há mais requisitos específicos no presente anexo.	Parâmetro utilizado para controlar interferências entre interrogadores nas proximidades (cf. definição nas normas EN 12253 e EN 13372)
D3	OBU (DSRC-VU) Gama mínima de frequências	Entre 5,795 e 5,815 GHz	(conforme EN 12253)
D4 (*)	P.I.R.E. máxima	No limite de ERC 70-03 (sem autorizações) e da regulamentação nacional Máximo + 33 dBm	(conforme EN 12253)

▼C2

Ponto	Parâmetro	Valor(es)	Observação
D4a	Máscara angular P.I.R.E.	Conforme especificação declarada e publicada do projetista do interrogador	(conforme EN 12253)
D5	Polarização	Circular no sentido retrógrado	(conforme EN 12253)
D5a	Polarização cruzada	XPD: No eixo de visão: (REDCR) RSU t ≥ 15 dB (DSRC-VU) OBU r ≥ 10 dB Na zona – 3 dB: (REDCR) RSU t ≥ 10 dB (DSRC-VU) OBU r ≥ 6 dB	(conforme EN 12253)
D6 (*)	Modulação	Modulação de amplitude a dois níveis	(conforme EN 12253)
D6a (*)	Índice de modulação	0,5 … 0,9	(conforme EN 12253)
D6b	Padrão do olho	≥ 90 % (tempo)/≥ 85 % (amplitude)	
D7 (*)	Codificação de dados	FM0 O bit «1» só tem transições no início e no fim do intervalo. Em comparação com o bit «1», o bit «0» tem uma transição suplementar no meio do intervalo.	(conforme EN 12253)
D8 (*)	Débito de bits	500 kBit/s	(conforme EN 12253)
D8a	Tolerância do relógio de bits	Melhor do que ± 100 ppm	(conforme EN 12253)
D9 (*)	Taxa de erro de bits (B.E.R.) para a comunicação	$\leq 10^{-6}$ se a potência incidente na OBU (DSRC-VU) se situar na gama dada por [D11a — D11b].	(conforme EN 12253)
D10	Sinal que aciona a OBU (DSRC-VU)	A OBU (DSRC-VU) é acionada ao receber uma cadeia com 11 ou mais octetos (incluindo preâmbulo)	Não é necessária nenhuma estrutura especial de acionamento. A DSRC-VU pode ser acionada ao receber uma cadeia com menos de 11 octetos (conforme EN 12253)
D10a	Tempo máximo de arranque	≤ 5 ms	(conforme EN 12253)
D11	Zona de comunicação	Espaço dentro do qual se atinge um B.E.R. correspondente a D9a	(conforme EN 12253)
D11a (*)	Limite de potência para comunicação (superior)	– 24dBm	(conforme EN 12253)

▼C2

Ponto	Parâmetro	Valor(es)	Observação
D11b (*)	Limite de potência para comunicação (inferior)	Potência incidente: – 43 dBm (eixo de visão) – 41 dBm [entre – 45° e + 45°, corresponde ao plano paralelo à superfície da estrada quando a DSRC-VU é instalada posteriormente no veículo (Azimuth)]	(conforme EN 12253) Requisito alargado a ângulos horizontais até ± 45°, atendendo aos casos de utilização definidos no presente anexo
D12 (*)	Nível da potência de corte da DSRC-VU	– 60 dBm	(conforme EN 12253)
D13	Preâmbulo	O preâmbulo é obrigatório	(conforme EN 12253)
D13a	Comprimento e estrutura do preâmbulo	16 bits ± 1 bit «1» codificado em FM0	(conforme EN 12253)
D13b	Forma de onda do preâmbulo	Sequência alternante de nível baixo e nível elevado, com 2 μs de duração de impulso Tolerância dada por D8a	(conforme EN 12253)
D13c	Bits residuais	A RSU (REDCR) é autorizada a emitir um máximo de 8 bits depois do sinal de fim. A OBU (DSRC-VU) não é obrigada a ter em conta estes bits suplementares.	(conforme EN 12253)

(*) — Parâmetros de ligação descendente sujeitos a ensaios de conformidade segundo a norma EN 300 674-1

▼B

Quadro 14.2

▼C2

Parâmetros de ligação ascendente

Item	Parâmetro	Valor(es)	Observação
U1 (*)	Frequências de subligação	A OBU (DSRC-VU) deve comportar 1,5 MHz e 2,0 MHz A RSU (REDCR) deve comportar 1,5 MHz ou 2,0 MHz ou ambos. U1-0: 1,5 MHz U1-1: 2,0 MHz	A seleção da frequência de subligação (1,5 MHz ou 2,0 MHz) depende do perfil EN 13372 selecionado.
U1a (*)	Tolerância das frequências de subligação	No intervalo ± 0,1 %	(conforme EN 12253)
U1b	Utilização de bandas laterais	Mesmos dados em ambos os lados	(conforme EN 12253)
U2 (*)	Máscara espetral de emissão da OBU (DSRC-VU)	Conforme EN12253 1) Potência extrabanda: ver ETSI EN 300674-1	(conforme EN 12253)

▼C2

Item	Parâmetro	Valor(es)	Observação
		2) Potência intrabanda: [U4a] dBm a 500 kHz 3) Emissão noutro qualquer canal ascendente: U2(3)-1 = – 35 dBm a 500 kHz	
U4a (*)	P.I.R.E. máxima — banda lateral única (eixo de visão)	Duas opções: U4a-0: – 14 dBm U4a-1: – 21 dBm	Conforme especificação declarada e publicada do projetista do equipamento
U4b (*)	P.I.R.E. máxima — banda lateral única (35°)	Duas opções: — Não aplicável — – 17dBm	Conforme especificação declarada e publicada do projetista do equipamento
U5	Polarização	Circular no sentido retrógrado	(conforme EN 12253)
U5a	Polarização cruzada	XPD: Eixo de visão: (REDCR) RSU r ≥ 15 dB (DSRC-VU) OBU t ≥ 10 dB Na zona – 3 dB: (REDCR) RSU r ≥ 10 dB (DSRC-VU) OBU t ≥ 6 dB	(conforme EN 12253)
U6	Modulação de subligação	2-PSK Dados codificados sincronizados com a subligação: Transições de dados codificados coincidem com transições de subligação	(conforme EN 12253)
U6b	Ciclo de funcionamento	Ciclo de funcionamento: 50 % ± α, α ≤ 5 %	(conforme EN 12253)
U6c	Modulação em ligação	Multiplicação da subligação modulada pela ligação	(conforme EN 12253)
U7 (*)	Codificação de dados	NRZI (sem transição no início do bit «1», com transição no início do bit «0», sem transição no interior do bit)	(conforme EN 12253)
U8 (*)	Débito de bits	250 kbit/s	(conforme EN 12253)
U8a	Tolerância do relógio de bits	No intervalo ± 1 000 ppm	(conforme EN 12253)
U9	Taxa de erro de bits (B.E.R.) para a comunicação	$\leq 10^{-6}$	(conforme EN 12253)

▼C2

Item	Parâmetro	Valor(es)	Observação
U11	Zona de comunicação	Espaço dentro do qual está situada a DSRC-VU, de modo tal que as suas emissões são recebidas pelo REDCR com uma B.E.R. inferior à dada por U9a	(conforme EN 12253)
U12a (*)	Ganho de conversão (limite inferior)	1 dB para cada banda lateral Abertura angular: circularmente simétrica entre o eixo de visão e ± 35° [entre – 45° e + 45°, corresponde ao plano paralelo à superfície da estrada quando a DSRC-VU é instalada posteriormente no veículo (Azimuth)]	No caso de ângulos horizontais até ± 45°, a abertura é maior do que a especificada, atendendo aos casos de utilização definidos no presente anexo
U12b (*)	Ganho de conversão (limite superior)	10 dB para cada banda lateral	Para cada banda lateral dentro de um cone circular em torno de um eixo de visão com um ângulo de ± 45°, a abertura é menor do que a especificada
U13	Preâmbulo	O preâmbulo é obrigatório	(conforme EN 12253)
U13a	Comprimento e estrutura do preâmbulo	32 a 36 μs, modulado com subligação apenas; depois, 8 bits «0» codificados em NRZI	(conforme EN 12253)
U13b	Bits residuais	A DSRC-VU é autorizada a emitir um máximo de 8 bits depois do sinal de fim. A RSU (REDCR) não é obrigada a ter em conta estes bits suplementares.	(conforme EN 12253)

(*) — Parâmetros de ligação ascendente sujeitos a ensaios de conformidade segundo a norma EN 300 674-1

▼B

5.3.3 *Conceção das antenas*

5.3.3.1 Antena REDCR

DSC_30 A conceção da antena *REDCR* deve ser uma função de conceção comercial, a operar dentro dos limites definidos na secção 5.3.2, adaptados para otimizar o desempenho de leitura do *DSRC-REDCR* com a finalidade específica e as circunstâncias de leitura nas quais o *REDCR* foi concebido para funcionar.

5.3.3.2 Antena da VU

DSC_31 A conceção da antena *DSRC-VU* deve ser uma função de conceção comercial, a operar dentro dos limites definidos na secção 5.3.2, adaptados para otimizar o desempenho de leitura do *DSRC-REDCR* com a finalidade específica e as circunstâncias de leitura nas quais o *REDCR* foi concebido para funcionar.

▼B

DSC_32 A antena da VU deve ser fixada ou aproximada ao para-brisas dianteiro do veículo, conforme especificado na secção 5.1.

DSC_33 No ambiente de ensaio de uma oficina (ver secção 6.3), uma antena da DSRC-VU, colocada conforme descrito em 5.1, deve ligar-se com êxito a uma comunicação de ensaio-padrão e proporcionar uma transação RTM bem-sucedida, conforme definido no presente apêndice, a uma distância de 2 a 10 metros, melhor do que 99 % das vezes, com uma média superior a 1 000 interrogações de leitura.

5.4 **Requisitos de protocolo DSRC para RTM**

5.4.1 *Panorâmica*

DSC_34 O protocolo de transação para descarregamento dos *dados* através da ligação da interface DSRC de 5,8 GHz deve cumprir as etapas que se seguem (esta secção descreve um fluxo de transação em condições ideais, sem retransmissões nem interrupções de comunicação).

NOTA: A finalidade da fase de inicialização (etapa 1) é estabelecer a comunicação entre o *REDCR* e as DSRC-VU que entraram na área de transação da DSRC de 5,8 GHz (principal-secundário) mas ainda não estabeleceram comunicação com o *REDCR*, e notificar os processos da aplicação.

— **Etapa 1** — Inicialização. O *REDCR* envia uma estrutura que contém um «quadro de serviço de baliza» (BST), que inclui os identificadores de aplicação (AID) na lista de serviço que aceita. Na aplicação RTM será simplesmente o serviço com o valor AID = 2 (carga e frota). A *DSRC-VU* avalia o BST recebido e responde (ver adiante) com a lista das aplicações aceites no domínio carga e frota, ou não responde se nenhum for aceite. Se o *REDCR* não oferecer AID=2, a DSRC-VU não responde ao *REDCR*.

— **Etapa 2** — A *DSRC-VU* envia uma estrutura que contém um pedido de atribuição de janela privada.

— **Etapa 3** — O *REDCR* envia uma estrutura que contém um pedido de atribuição de janela privada.

— **Etapa 4** — A *DSRC-VU* utiliza a janela privada atribuída para enviar uma estrutura que contém o seu quadro de serviço do veículo (VST). Este VST inclui uma lista de todas as instanciações de aplicação diferentes que esta *DSRC-VU* aceita no âmbito de AID=2. As diferentes instanciações devem ser identificadas por meio de EID de geração exclusiva, cada um associado a um valor do parâmetro Application Context Mark que indica a aplicação e a norma aceites.

— **Etapa 5** — Em seguida, o *REDCR* analisa o VST oferecido e termina a ligação (RELEASE), uma vez que não está interessado em nada do que o VST tem para oferecer (ou seja, está a receber um VST de uma *DSRC-VU* que não aceita a transação RTM) ou, se receber um VST adequado, inicia uma instanciação da aplicação.

▼B

— **Etapa 6** — Para que tal aconteça, o *REDCR* deve enviar uma estrutura que contém um comando de recuperação dos dados RTM, identificando a instanciação da aplicação RTM por meio da especificação do identificador correspondente à instanciação da aplicação RTM (conforme especificado pela *DSRC-VU* no VST) e atribui uma janela privada.

— **Etapa 7** — A *DSRC-VU* utiliza a janela privada atribuída recentemente para enviar uma estrutura que contém o identificador tratado correspondente à instanciação da aplicação RTM conforme previsto no VST, seguido pelo atributo *RtmData* (elemento de carga útil + elemento de segurança).

— **Etapa 8** — Se houver vários serviços pedidos, o valor «n» é alterado para o número de referência de serviço seguinte e o processo é repetido.

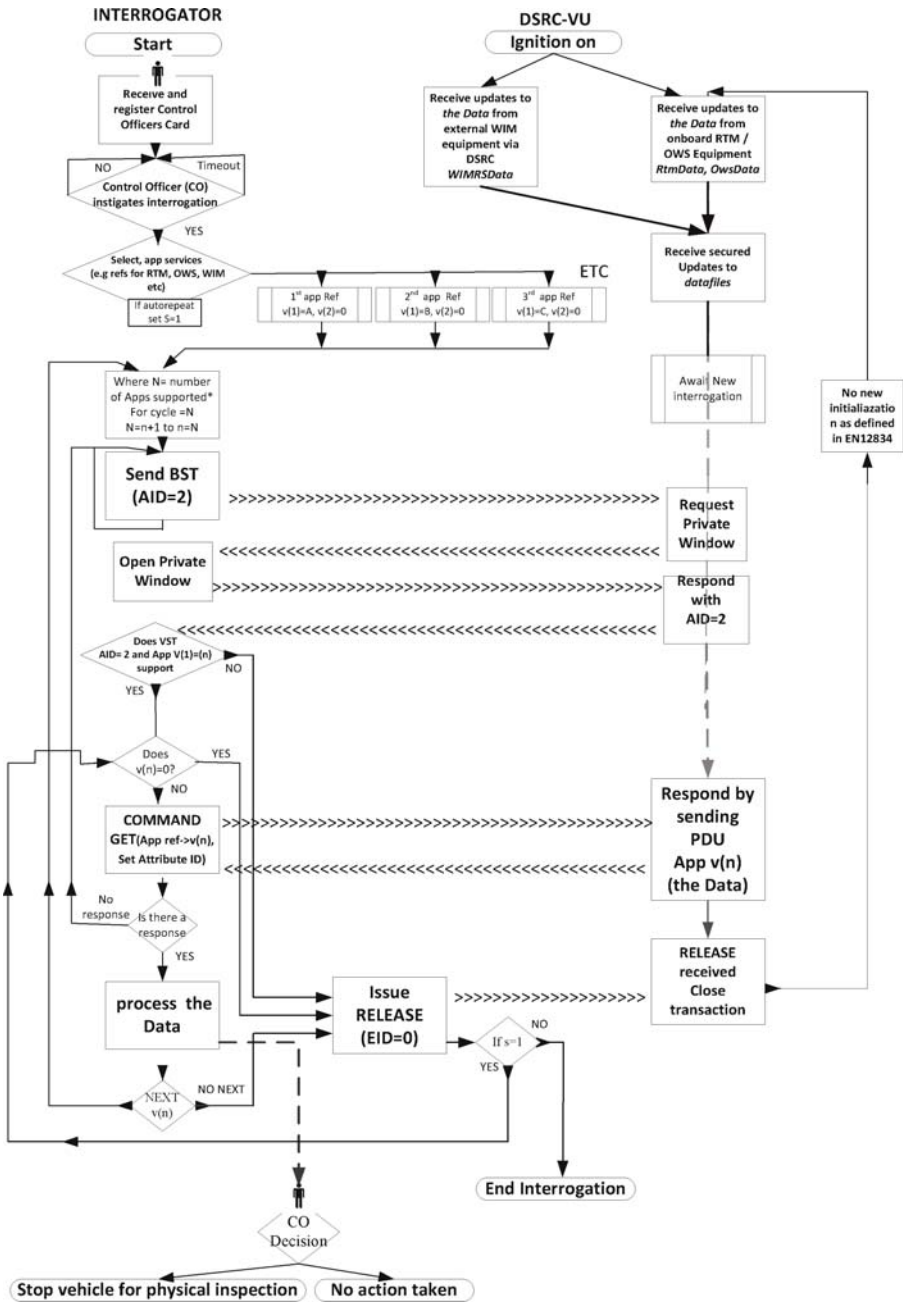
— **Etapa 9** — O *REDCR* confirma a receção dos dados, enviando uma estrutura que contém um comando RELEASE para a *DSRC-VU* terminar a sessão OU, se não tiver conseguido validar uma receção bem sucedida do LDPU, volta à etapa 6.

Ver no esquema 14.6 uma imagem do protocolo de transação.

▼B

Esquema 14.6

RTM acima do fluxo de processo DSRC de 5,8 GHz



5.4.2 *Comandos*

DSC_35 Os comandos que se seguem são as únicas funções utilizadas numa fase de transação RTM:

— **INITIALISATION.request**: comando emitido a partir do REDCR sob a forma de uma transmissão com a definição de aplicações que o REDCR aceita.

— **INITIALISATION.response**: resposta da DSRC-VU que confirma a conexão e contém uma lista de instâncias de aplicações aceites com características e informações sobre como tratá-las (EID).

▼B

— **GET.request**: comando emitido do *REDCR* para a *DSRC-VU*, que especifica a instanciação da aplicação a tratar por meio de um EID definido, recebido no VST, instruindo a *DSRC-VU* para enviar o atributo selecionado com os *dados*. O objetivo do comando GET é que o *REDCR* obtenha os *dados* da *DSRC-VU*.

— **GET.response**: resposta da DSRC-VU que contém *os dados* pedidos.

— **ACTION.request ECHO**: comando que instrui a *DSRC-VU* para devolver os dados da *DSRC-VU* para o *REDCR*. O objetivo do comando ECHO é autorizar as oficinas ou unidades de ensaio de homologações de tipo a testar se a ligação DSRC funciona sem necessidade de acesso a credenciais de segurança.

— **ACTION.response ECHO**: resposta da DSRC VU no comando ECHO.

— **EVENT_REPORT.request RELEASE**: comando que dá instrução à *DSRC-VU* de que a transação está finalizada. O objetivo do comando RELEASE é terminar a sessão com a *DSRC-VU*. Ao receber o comando RELEASE, a *DSRC-VU* não responde a mais nenhumas interrogações no âmbito da conexão atual. De salientar que, segundo a norma EN 12834, uma DSRC-VU não se ligará duas vezes ao mesmo interrogador, a menos que tenha estado fora da área de comunicação durante 255 segundos ou se a ID da baliza do interrogador for alterada.

5.4.3 *Sequência de comandos de interrogação*

DSC_36 Do ponto de vista da sequência de comando e resposta, a transação é descrita da seguinte forma:

▼C2

Sequência	Emissor		Recetor	Descrição	Ação
1	REDCR	>	DSRC-VU	Inicialização da ligação de comunicação — Pedido	REDCR difunde BST
2	*DSRC-VU*	>	REDCR	*Inicialização da ligação de comunicação — Resposta*	*Se BST comportar AID = 2, DSRC-VU pede atribuição de janela privada*
3	REDCR	>	DSRC-VU	Atribui janela privada	Envia estrutura que contém atribuição de janela privada
4	*DSRC-VU*	>	*REDCR*	*Envia VST*	*Envia estrutura que inclui VST*
5	REDCR	>	DSRC-VU	Envia GET.request relativo a dados contidos no atributo para EID específico	
6	*DSRC-VU*	>	*REDCR*	*Envia GET.response com o atributo pedido para o EID específico*	*Envia atributo (RTMData, OWSData…) com os dados para o EID específico*

▼C2

Sequência	Emissor		Recetor	Descrição	Ação
7	REDCR	>	DSRC-VU	Envia GET.request relativo a dados de outro atributo (se pertinente)	
8	*DSRC-VU*	>	*REDCR*	*Envia GET.response com o atributo pedido*	*Envia atributo com os dados para o EID específico*
9	REDCR	>	DSRC-VU	Acusa receção dos dados	Envia comando RELEASE que encerra a transação
10	*DSRC-VU*			*Encerra transação*	

▼B

Nas cláusulas 5.4.7 e 5.4.8 é definido um exemplo de sequência e conteúdos de transação das estruturas intercambiadas.

5.4.4 *Estruturas de dados*

DSC_37 A estrutura semântica dos *dados*, quando passados através da interface DSRC de 5,8 GHz, deve ser compatível com o descrito no presente apêndice. O modo como esses dados estão estruturados é especificado na presente cláusula.

DSC_38 A carga útil (dados RTM) é composta pela concatenação de:

1. Dados EncryptedTachographPayload: trata-se da encriptação da TachographPayload definida em ASN.1, na secção 5.4.5. O método de encriptação é descrito no apêndice 11;

2. DSRCSecurityData, especificado no apêndice 11.

DSC_39 Os dados RTM são tratados como RTM Attribute = 1 e são transferidos no RTM container =10.

DSC_40 A marca de contexto RTM identificador da parte normalizada aceite na série das normas TARV (RTM corresponde à parte 9).

A definição do módulo ASN.1 para os dados DSRC na aplicação RTM é definida como se segue:

▼B

```
TarvRtm {iso(1) standard(0) 15638 part9(9) version1(1)}
DEFINITIONS AUTOMATIC TAGS
::= BEGIN
IMPORTS
-- Imports data attributes and elements from EFC which are used for RTM
LPN
FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

-- Imports function parameters from the EFC Application Interface Definition
SetMMIRq
FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

-- Imports the L7 DSRCData module data from the EFC Application Interface Definition
Action-Request, Action-Response, ActionType, ApplicationList, AttributeIdList, AttributeList,
Attributes,
BeaconID, BST, Dsrc-EID, DSRCApplicationEntityID, Event-Report-Request, Event-Report- Response,
EventType, Get-Request, Get-Response, Initialisation-Request, Initialisation-Response,
ObeConfiguration, Profile, ReturnStatus, Time, T-APDUs, VST
FROM EfcDsrcGeneric {iso(1) standard(0) 14906 generic(1) version5(5)};


-- Definitions of the RTM functions:
RTM-InitialiseComm-Request ::= BST
RTM-InitialiseComm-Response::= VST
RTM-DataRetrieval-Request::= Get-Request (WITH COMPONENTS {fill (SIZE(1)), eid, accessCredentials ABSENT,iid
ABSENT,  attrIdList})
RTM-DataRetrieval-Response::= Get-Response {RtmContainer} (WITH COMPONENTS {..., eid, iid ABSENT})
RTM-TerminateComm::= Event-Report-Request {RtmContainer}(WITH COMPONENTS {mode (FALSE), eid (0),
eventType (0)})

RTM-TestComm-Request::= Action-Request {RtmContainer} (WITH COMPONENTS {..., eid (0), actionType
(15), accessCredentials ABSENT, iid ABSENT})

RTM-TestComm-Response::= Action-Response {RtmContainer} (WITH COMPONENTS {..., fill (SIZE(1)), eid
(0), iid ABSENT})

-- Definitions of the RTM attributes:
RtmData ::= SEQUENCE {
      encryptedTachographPayload OCTET STRING (SIZE(67)) (CONSTRAINED BY { -- calculated encrypting
TachographPayload as per Appendix 11 --}),
      DSRCSecurityData OCTET STRING
      }
TachographPayload ::= SEQUENCE {
            tp15638VehicleRegistrationPlate LPN -- Vehicle Registration Plate as per EN 15509.
            tp15638SpeedingEvent            BOOLEAN,  -- 1= Irregularities in speed (see Annex 1C)
            tp15638DrivingWithoutValidCard  BOOLEAN,     -- 1= Invalid card usage (see Annex 1C)
            tp15638DriverCard               BOOLEAN,-- 0= Indicates a valid driver card  (see Annex 1C)
            tp15638CardInsertion            BOOLEAN, -- 1= Card insertion while driving (see Annex 1C)
            tp15638MotionDataError          BOOLEAN, -- 1= Motion data error (see Annex 1C)
            tp15638VehicleMotionConflict    BOOLEAN, -- 1= Motion conflict (see Annex 1C)
            tp156382ndDriverCard            BOOLEAN, -- 1= Second driver card inserted (see Annex 1C)
            tp15638CurrentActivityDriving   BOOLEAN, -- 1= other activity selected;
                                                      -- 0= driving selected
            tp15638LastSessionClosed        BOOLEAN, -- 1= improperly, 0= properly, closed
            tp15638PowerSupplyInterruption  INTEGER (0..127), -- Supply interrupts in the last 10 days
            tp15638SensorFault              INTEGER (0..255),-- eventFaultType as per data dictionary
-- All subsequent time related types as defined in Annex 1C.
            tp15638TimeAdjustment           INTEGER(0..4294967295), -- Time of the last time adjustment
            tp15638LatestBreachAttempt      INTEGER(0..4294967295), -- Time of last breach attempt
            tp15638LastCalibrationData      INTEGER(0..4294967295), -- Time of last calibration data
            tp15638PrevCalibrationData      INTEGER(0..4294967295), -- Time of previous calibration data
            tp15638DateTachoConnected       INTEGER(0..4294967295), -- Date tachograph connected
            tp15638CurrentSpeed             INTEGER (0..255), -- Last current recorded speed
            tp15638Timestamp                INTEGER(0..4294967295) -- Timestamp of current record[2]
            }
Rtm-ContextMark ::= SEQUENCE {
  standardIdentifier    StandardIdentifier, -- identifier of the TARV part and its version

  RtmCommProfile          INTEGER {
                                C1 (1),
                                C2 (2)
                                } (0..255) DEFAULT 1
  }
RtmTransferAck ::= INTEGER {
                Ok (1),
                NoK (2)
                } SIZE (1..255)
```

▼B

```
StandardIdentifier ::= OBJECT IDENTIFIER
RtmContainer ::= CHOICE {
        integer                     [0]    INTEGER,
        bitstring                   [1]    BIT STRING,
        octetstring                 [2]    OCTET STRING (SIZE (0..127, ...)),
        universalString             [3]    UniversalString,
        beaconId                    [4]    BeaconID,
        t-apdu                      [5]    T-APDUs,
        dsrcApplicationEntityId     [6]    DSRCApplicationEntityID,
        dsrc-Ase-Id                 [7]    Dsrc-EID,
        attrIdList                  [8]    AttributeIdList,
        attrList                    [9]    AttributeList{RtmContainer},
        rtmData                     [10]   RtmData,
        rtmContextmark              [11]   Rtm-ContextMark,
        reserved12                  [12]   NULL,
        reserved13                  [13]   NULL,
        reserved14                  [14]   NULL,
        time                        [15]   Time,
-- values from 16 to 255 reserved for ISO/CEN usage
        }}

END
```

5.4.5 *Elementos de RtmData, ações realizadas e definições*

DSC_41 Os valores de dados a calcular pela VU e utilizados para atualizar os dados seguros na DSRC-VU devem ser calculados de acordo com as regras definidas no quadro 14.3:

Quadro 14.3

▼C2

Elementos de RtmData, ações realizadas e definições

(1) Elemento de dados RTM	(2) Ação realizada pela VU		(3) Definição de dados ASN.1
RTM1 **Placa de matrícula do veículo**	A VU fixa o valor do elemento de dados RTM1 *tp15638VehicleRegistrationPlate* a partir do valor registado do tipo de dados *VehicleRegistrationIdentification* definido no apêndice 1	Placa de matrícula do veículo expressa sob a forma de uma cadeia de caracteres	`tp15638VehicleRegstrationPlate LPN,` `-- Placa de matrícula do veículo importada de ISO 14906 com a limitação especificada em EN 15509, que é uma SEQUENCE na qual o código do país é seguido de um indicador alfabético e do número da placa propriamente dito, sempre com 14 octetos (com zeros de enchimento, se necessário), pelo que o comprimento de tipo EN 15509 é sempre de 17 octetos, dos quais 14 correspondem ao número "real" da placa.`
RTM2 **Incidente «Excesso de velocidade»**	A VU gera um valor booliano para o elemento de dados RTM2 tp15638SpeedingEvent. O valor de tp15638SpeedingEvent é calculado pela VU a partir do número de incidentes «excesso de velocidade» registados na VU durante os últimos 10 dias de ocorrência (cf. definição no anexo 1C).	1 (TRUE) — indica irregularidades de velocidade durante os últimos 10 dias de ocorrência	`tp15638speedingEvent BOOLEAN,`

▼C2

(1) Elemento de dados RTM	(2) Ação realizada pela VU		(3) Definição de dados ASN.1
	Se houver pelo menos um tp15638SpeedingEvent durante os últimos 10 dias de ocorrência, o valor de tp15638SpeedingEvent é fixado em TRUE (verdadeiro). DE CONTRÁRIO, se não houver incidentes durante os últimos 10 dias de ocorrência, o tp15638SpeedingEvent fixado em FALSE (falso).		
RTM3 **Condução sem cartão válido**	A VU gera um valor booliano para o elemento de dados RTM3 tp15638DrivingWithoutValidCard. A VU atribui o valor True à variável tp15638DrivingWithoutValidCard se, durante os últimos 10 dias de ocorrência, os dados da VU tiverem registado pelo menos um incidente «condução sem cartão válido» (cf. definição no anexo 1C). DE CONTRÁRIO, se não houver tais incidentes durante os últimos 10 dias de ocorrência, a variável tp15638DrivingWithoutValidCard é fixada em FALSE.	1 (TRUE) = indica utilização de cartão inválido	`tp15638DrivingWithoutValidCard BOOLEAN,`
RTM4 **Cartão de condutor válido**	A VU gera um valor booliano para o elemento de dados RTM4 tp15638DriverCard com base nos dados armazenados na VU e definidos no apêndice 1. Se não estiver presente um cartão de condutor válido, a VU fixa a variável em TRUE DE CONTRÁRIO, se estiver presente um cartão de condutor válido, a VU fixa a variável em FALSE	0 (FALSE) = indica um cartão de condutor válido	`tp15638DriverCard BOOLEAN,`
RTM5 **Inserção de cartão durante a condução**	A VU gera um valor booliano para o elemento de dados RTM5. A VU atribui o valor TRUE à variável tp15638CardInsertion se, durante os últimos 10 dias de ocorrência, os dados da VU tiverem registado pelo menos um incidente «inserção de cartão durante a condução» (cf. definição no anexo 1C). DE CONTRÁRIO, se não houver tais incidentes durante os últimos 10 dias de ocorrência, a variável tp15638CardInsertion é fixada em FALSE.	1 (TRUE) = indica inserção de cartão durante a condução durante os últimos 10 dias de ocorrência	`tp15638CardInsertion BOOLEAN,`
RTM6 **Erro nos dados de movimento**	A VU gera um valor booliano para o elemento de dados RTM6. A VU atribui o valor TRUE à variável tp15638MotionDataError se, durante os últimos 10 dias de ocorrência, os dados da VU tiverem registado pelo menos um incidente «erro nos dados de movimento» (cf. definição no anexo 1C). DE CONTRÁRIO, se não houver tais incidentes durante os últimos 10 dias de ocorrência, a variável tp15638MotionDataError é fixada em FALSE.	1 (TRUE) = indica erro nos dados de movimento durante os últimos 10 dias de ocorrência	`tp15638motionDataError BOOLEAN,`

▼C2

(1) Elemento de dados RTM	(2) Ação realizada pela VU		(3) Definição de dados ASN.1
RTM7 **Conflito relativo ao movimento do veículo**	A VU gera um valor booliano para o elemento de dados RTM7. A VU atribui o valor TRUE à variável tp15638vehicleMotionConflict se, durante os últimos 10 dias de ocorrência, os dados da VU tiverem registado pelo menos um incidente do tipo «conflito relativo ao movimento do veículo» (valor “0A”H). DE CONTRÁRIO, se não houver incidentes durante os últimos 10 dias de ocorrência, a variável tp15638vehicleMotionConflict é fixada em FALSE.	1 (TRUE) = indica conflito relativo ao movimento durante os últimos 10 dias de ocorrência	`tp15638vehicleMotionConflict BOOLEAN,`
RTM8 **Segundo cartão de condutor**	A VU gera um valor booliano para o elemento de dados RTM8 com base no anexo 1C («Dados relativos à atividade de condutor», CREW e CO-DRIVER). Se estiver presente um segundo cartão de condutor válido, a VU fixa a variável em TRUE. DE CONTRÁRIO, se não estiver presente um segundo cartão de condutor válido, a VU fixa a variável em FALSE.	1 (TRUE) = indica inserção de um segundo cartão de condutor	`tp156382ndDriverCard BOOLEAN,`
RTM9 **Atividade em curso**	A VU gera um valor booliano para o elemento de dados RTM9. Se a atividade em curso for registada na VU como outra atividade que não «DRIVING» (cf. definição no anexo 1C), a VU fixa a variável em TRUE. DE CONTRÁRIO, se a atividade em curso for registada na VU como «DRIVING», a VU fixa a variável em FALSE.	1 (TRUE) = outra atividade selecionada; 0 (FALSE) = selecionada condução	`tp15638currentActivityDriving BOOLEAN`
RTM10 **Encerramento da última sessão**	A VU gera um valor booliano para o elemento de dados RTM10. Se a última sessão de cartão não tiver sido corretamente encerrada (cf. definição no anexo 1C), a VU fixa a variável em TRUE. DE CONTRÁRIO, se a última sessão de cartão tiver sido corretamente encerrada, a VU fixa a variável em FALSE.	1 (TRUE) = encerramento incorreto 0 (FALSE) = encerramento correto	`tp15638lastSessionClosed BOOLEAN`
RTM11 **Interrupção da alimentação energética**	A VU gera um valor configurado por um número inteiro para o elemento de dados RTM11. A VU atribui à variável tp15638PowerSupplyInterruption um valor igual à mais longa interrupção de fornecimento de energia, na aceção do artigo 9.º do Regulamento (UE) n.º 165/2014, do tipo «nterrupção da alimentação energética» (cf. definição no anexo 1C).	— Número de interrupções da alimentação energética durante os últimos 10 dias de ocorrência	`tp15638powerSupplyInterruption INTEGER (0..127),`

▼C2

(1) Elemento de dados RTM	(2) Ação realizada pela VU		(3) Definição de dados ASN.1
	DE CONTRÁRIO, se não tiver havido incidentes de interrupção da alimentação energética durante os últimos 10 dias de ocorrência, o valor do inteiro é fixado em 0.		
RTM12 **Falha do sensor**	A VU gera um valor configurado por um número inteiro para o elemento de dados RTM12. A VU atribui à variável sensorFault o valor de: — 1, se, durante os últimos 10 dias, tiver sido registado um incidente do tipo «falha do sensor» “35”H; — 2, se, durante os últimos 10 dias, tiver sido registado um incidente do tipo «falha do recetor GNSS» (quer interno quer externo, com os valores de enumeração “51”H ou “52”H); — 3, se, durante os últimos 10 dias, tiver sido registado um incidente do tipo «falha de comunicação do módulo GNSS externo “53”H»; — 4, se, durante os últimos 10 dias de ocorrência, tiverem sido registadas falhas do sensor e falhas do recetor GNSS; — 5, se, durante os últimos 10 dias de ocorrência, tiverem sido registadas falhas do sensor e falhas de comunicação do módulo GNSS externo; — 6, se, durante os últimos 10 dias de ocorrência, tiverem sido registadas falhas do recetor GNSS e falhas de comunicação do módulo GNSS externo; — 7, se, durante os últimos 10 dias de ocorrência, tiverem sido registadas no sensor falhas dos três tipos. DE CONTRÁRIO, a VU atribui o valor 0 se não tiverem sido registados incidentes durante os últimos 10 dias de ocorrência.	— falha do sensor: um octeto (cf. dicionário de dados)	`tp15638SensorFault INTEGER (0..255),`
RTM13 **Ajustamento do tempo**	A VU gera um valor configurado por um número inteiro (timeReal, do apêndice 1) para o elemento de dados RTM13, com base na presença de dados relativos ao ajustamento do tempo (cf. definição no anexo 1C). A VU atribui o valor do momento em que ocorreu o último incidente de ajustamento do tempo. DE CONTRÁRIO, se não houver nos dados da VU nenhum incidente «ajustamento do tempo» (cf. definição no anexo 1C), a VU fixa o valor 0.	Momento do último ajustamento do tempo	`tp15638TimeAdjustment INTEGER(0..4294967295),`
RTM14 **Tentativa de violação da segurança**	A VU gera um valor configurado por um número inteiro (timeReal, do apêndice 1) para o elemento de dados RTM14, com base na presença de um incidente «tentativa de violação da segurança» (cf. definição no anexo 1C). A VU atribui o valor do momento em que ocorreu o último incidente de tentativa de violação da segurança registado pela VU.	Momento da última tentativa de violação da segurança — Valor por defeito = 0x00FF	`tp15638LatestBreachAttempt INTEGER(0..4294967295),`

▼C2

(1) Elemento de dados RTM	(2) Ação realizada pela VU		(3) Definição de dados ASN.1
	DE CONTRÁRIO, se não houver nos dados da VU nenhum incidente «tentativa de violação da segurança» (cf. definição no anexo 1C), a VU fixa o valor 0x00FF.		
RTM15 **Última calibração**	A VU gera um valor configurado por um número inteiro (timeReal, do apêndice 1) para o elemento de dados RTM15, com base na presença de dados de uma última calibração (cf. definição no anexo 1C). A VU fixa o valor do momento das duas últimas calibrações (RTM15 e RTM16), definidas em VuCalibrationData no apêndice 1. A VU fixa o valor de RTM15 como sendo o timeReal da última calibração registada.	Momento dos dados da última calibração	`tp15638LastCalibrationData INTEGER(0..4294967295),`
RTM16 **Calibração anterior**	A VU gera um valor configurado por um número inteiro (timeReal, do apêndice 1) para o elemento de dados RTM16 do registo da calibração que precede imediatamente a última. DE CONTRÁRIO, se não tiver havido calibração anterior, a VU fixa o valor de RTM16 como sendo 0.	Momento dos dados da calibração anterior	`tp15638PrevCalibrationData INTEGER(0..4294967295),`
RTM17 **Data de ligação do tacógrafo**	A VU gera um valor configurado por um número inteiro (timeReal, do apêndice 1) para o elemento de dados RTM17. A VU fixa o valor do momento da sua instalação inicial. A VU extrai estes dados dos VuCalibrationData (apêndice 1) nos vuCalibrationRecords, com CalibrationPurpose igual a “03”H	Data de ligação do tacógrafo	`tp15638DateTachoConnected INTEGER(0..4294967295),`
RTM18 **Velocidade atual**	A VU gera um valor configurado por um número inteiro para o elemento de dados RTM18. A VU fixa o valor de RTM16 como sendo a última velocidade atual registada no momento da última atualização dos RtmData.	Última velocidade atual registada	`tp15638CurrentSpeed INTEGER (0..255),`
RTM19 **Período de tempo**	A VU gera um valor configurado por um número inteiro (timeReal, do apêndice 1) para o elemento de dados RTM19. A VU fixa o valor de RTM19 como sendo o momento da última atualização dos RtmData.	Período de tempo do registo TachographPayload atual	`tp15638Timestamp INTEGER(0..4294967295),`

▼B

5.4.6 *Mecanismo de transferência de dados*

DSC_42 Os dados de carga útil definidos anteriormente são pedidos pelo REDCR após a fase de inicialização e, consequentemente, transmitidos pela *DSRC-VU* na janela atribuída. O comando GET é utilizado pelo REDCR para recuperar dados.

▼B

DSC_43 Relativamente a todos os intercâmbios DSRC, os dados devem ser codificados utilizando PER (regras de codificação compactadas).

5.4.7 *Descrição pormenorizada de transação DSRC*

DSC_44 A inicialização é realizada de acordo com DSC_44 a DSC_48 e quadros 14.4-14.9. Na fase de inicialização, o REDCR começa a enviar uma estrutura que contém um BST (quadro de serviço de baliza) nos termos das normas EN 12834 e EN 13372, 6.2, 6.3, 6.4 e 7.1, com as configurações especificadas no quadro 14.4:

Quadro 14.4

▼C2

Inicialização — Configurações da estrutura BST

Campo	Configurações
Link Identifier	Endereço de difusão
BeaconId	Conforme EN 12834
Time	Conforme EN 12834
Profile	Sem extensão — utilizar 0 ou 1
MandApplications	Sem extensão, EID não presente, parâmetro não presente, AID = 2 Freight&Fleet
NonMandApplications	Não presente
ProfileList	Sem extensão, número de perfis na lista = 0
Fragmentation header	Sem fragmentação
Layer 2 settings	PDU de comando, comando UI

▼B

No quadro 14.5 que se segue é apresentado um exemplo prático das configurações especificadas no quadro 14.4, com uma indicação de codificações de bits.

Quadro 14.5

▼C2

Inicialização — Exemplo do conteúdo da estrutura BST

N.º do octeto	Atributo/campo	Bits no octeto	Descrição
1	FLAG	0111 1110	Sinal (bandeira) de início
2	Broadcast ID	1111 1111	Endereço de difusão
3	MAC Control Field	1010 0000	PDU de comando
4	LLC Control field	0000 0011	Comando UI

▼C2

N.º do octeto	Atributo/campo	Bits no octeto	Descrição
5	Fragmentation header	1xxx x001	Sem fragmentação
6	BST	1000	Pedido de inicialização
	SEQUENCE {		
	OPTION indicator BeaconID SEQUENCE { ManufacturerId INTEGER (0..65535)	0	Aplicações NonMand não presentes
		xxx	Identificador do fabricante
7		xxxx xxxx	
8		xxxx x	
	IndividualID INTEGER (0..134217727)	xxx	ID de 27 bits disponível para o fabricante
9		xxxx xxxx	
10		xxxx xxxx	
11	}	xxxx xxxx	
12	Time INTEGER (0..4294967295)	xxxx xxxx	Tempo real UNIX de 32 bits
13		xxxx xxxx	
14		xxxx xxxx	
15		xxxx xxxx	
16	Profile INTEGER (0..127,…)	0000 0000	Sem extensão. Perfil de exemplo 0
17	MandApplications SEQUENCE (SIZE(0..127, …)) OF {	0000 0001	Sem extensão, número de mandApplications = 1
18	SEQUENCE {		
	OPTION indicator	0	EID não presente
	OPTION indicator	0	Parâmetro não presente
	AID DSRCApplicationEntityID}}	00 0010	Sem extensão. AID = 2 Freight&Fleet

▼C2

N.º do octeto	Atributo/campo	Bits no octeto	Descrição
19	ProfileList SEQUENCE (0..127,…) OF Profile}	0000 0000	Sem extensão, número de perfis na lista = 0
20	FCS	xxxx xxxx	Sequência de verificação da estrutura
21		xxxx xxxx	
22	Flag	0111 1110	Sinal (bandeira) de terminação

▼B

DSC_45 Ao receber um BST, a *DSRC-VU* necessita da atribuição de uma janela privada, especificada pelas normas EN 12795 e EN 13372, cláusula 7.1.1, sem configurações RTM específicas. O quadro 14.6 apresenta um exemplo de codificação de bits:

Quadro 14.6

▼C2

Inicialização — Conteúdos da estrutura de pedido de atribuição de janela privada

N.º do octeto	Atributo/campo	Bits no octeto	Descrição
1	FLAG	0111 1110	Sinal (bandeira) de início
2	Private LID	xxxx xxxx	Endereço de ligação da DSRC-VU específica
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	0110 0000	Pedido de atribuição de janela privada
7	FCS	xxxx xxxx	Sequência de verificação da estrutura
8		xxxx xxxx	
9	Flag	0111 1110	Sinal (bandeira) de terminação

▼B

DSC_46 O REDCR responde mediante a atribuição de uma janela privada, conforme especificado pelas normas EN 12795 e EN 13372, cláusula 7.1.1, sem configurações RTM específicas.

O quadro 14.7 apresenta um exemplo de codificação de bits.

Quadro 14.7

▼C2

Inicialização — Conteúdos da estrutura de atribuição de janela privada

N.º do octeto	Atributo/campo	Bits no octeto	Descrição
1	FLAG	0111 1110	Sinal (bandeira) de início
2	Private LID	xxxx xxxx	Endereço de ligação da DSRC-VU específica
3		xxxx xxxx	

▼C2

N.º do octeto	Atributo/campo	Bits no octeto	Descrição
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	0010 s000	Atribuição de janela privada
7	FCS	xxxx xxxx	Sequência de verificação da estrutura
8		xxxx xxxx	
9	Flag	0111 1110	Sinal (bandeira) de terminação

▼B

DSC_47 Ao receber a atribuição de janela privada, a *DSRC-VU* envia o seu VST (quadro de serviço de veículo), conforme definido nas normas EN 12834 e EN 13372, 6.2, 6.3, 6.4 e 7.1, com as configurações especificadas no quadro 14.8, utilizando a janela de transmissão atribuída.

Quadro 14.8

▼C2

Inicialização — Configurações da estrutura VST

Campo	Configurações
Private LID	Conforme EN 12834
VST parameters	Fill = 0. Em seguida, por cada aplicação compatível: EID presente, parâmetro presente, AID = 2, EID tal como gerado pela OBU
Parameter	Sem extensão. Contém a marca de contexto RTM
ObeConfiguration	O campo opcional ObeStatus pode estar presente, mas não deve ser utilizado pelo REDCR
Fragmentation header	Sem fragmentação
Layer 2 settings	PDU de comando, comando UI

▼B

DSC_48 A *DSRC-VU* aceita a aplicação «Carga e Frota», identificada pelo identificador de aplicação «2». Podem ser aceites outros identificadores de aplicação, mas não estão presentes neste VST, dado que o BST exige apenas AID = 2. O campo «aplicações» contém uma lista das instâncias de aplicação aceites na *DSRC-VU*. Para cada instanciação de aplicação é atribuída a referência à norma adequada, constituída por uma marca Rtm Context, que é composta por um IDENTIFICADOR DE OBJETO que representa a norma a que se refere, a sua parte (9 para RTM) e, eventualmente, a sua versão, além de um EID que é criado pela DSRC-VU e associado a essa instância de aplicação.

No quadro 14.9 que se segue é apresentado um exemplo prático das configurações especificadas no quadro 14.8, com uma indicação de codificações de bits.

▼B

Quadro 14.9

▼C2

Inicialização — Exemplo de conteúdos da estrutura VST

N.º do octeto	Atributo/campo	Bits no octeto	Descrição
1	FLAG	0111 1110	Sinal (bandeira) de início
2	Private LID	xxxx xxxx	Endereço de ligação da DSRC-VU específica
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1100 0000	PDU de comando
7	LLC Control field	0000 0011	Comando UI
8	Fragmentation header	1xxx x001	Sem fragmentação
9	VST SEQUENCE {	1001	Resposta de inicialização
	Fill BIT STRING (SIZE(4))	0000	Não utilizado; fixado em 0
10	Profile INTEGER (0..127,…) Applications SEQUENCE OF {	0000 0000	Sem extensão; perfil de exemplo 0
11		0000 0001	Sem extensão, 1 aplicação
12	SEQUENCE {		
	OPTION indicator	1	EID presente
	OPTION indicator	1	Parâmetro presente
	AID DSRCApplicationEntityID	00 0010	Sem extensão; AID = 2 Freight&Fleet
13	EID Dsrc-EID	xxxx xxxx	Definido na OBU; identifica a instância de aplicação
14	Parameter Container {	0000 0010	Sem extensão; escolha de contentor = 02; cadeia de octetos
15		0000 1000	Sem extensão; comprimento da marca de contexto RTM = 8

▼C2

N.º do octeto	Atributo/campo	Bits no octeto	Descrição
16	Rtm-ContextMark::= SEQUENCE { StandardIdentifier standardIdentifier	0000 0110	Identificador de objeto da norma seguida (parte e versão). Exemplo: ISO (1) Standard (0) TARV (15638) part9(9) Version1 (1). O primeiro octeto é 06H, o identificador de objeto. O segundo octeto é 06H, o seu comprimento. Os 6 octetos subsequentes codificam o identificador de objeto do exemplo. Nota: apenas um elemento da sequência está presente (o elemento opcional RtmCommProfile está omisso).
17		0000 0110	
18		0010 1000	
19		1000 0000	
20		1111 1010	
21		0001 0110	
22		0000 1001	
23		0000 0001	
24	ObeConfiguration Sequence {		
	OPTION indicator		ObeStatus não presente
	EquipmentClass INTEGER (0..32767)	xxx xxxx	
25		xxxx xxxx	
26	ManufacturerId INTEGER (0..65535)	xxxx xxxx	Identificador de fabricante para a DSRC-VU, conforme registo ISO 14816
27		xxxx xxxx	
28	FCS	xxxx xxxx	Sequência de verificação da estrutura
29		xxxx xxxx	
30	Flag	0111 1110	Sinal (bandeira) de terminação

▼B

DCS_49 O REDCR lê os dados emitindo um comando GET, em conformidade com o comando GET definido nas normas EN 13372, 6.2, 6.3, 6.4, e EN 12834, com as configurações especificadas no quadro 14.10.

Quadro 14.10

▼C2

Apresentação — Configurações da estrutura de pedido GET

Campo	Configurações
Invoker Identifier (IID)	Não presente
Link Identifier (LID)	Endereço de ligação da DSRC-VU específica
Chaining	Não
Element Identifier (EID)	Conforme especificação na VST. Sem extensão

▼C2

Campo	Configurações
Access Credentials	Não
AttributeIdList	Sem extensão, 1 atributo, AttributeID = 1 (RtmData)
Fragmentation	Não
Layer2 settings	PDU de comando, comando ACn solicitado

▼B

O quadro 14.11 mostra um exemplo da leitura dos dados RTM.

Quadro 14.11

▼C2

Apresentação — Exemplo de estrutura de pedido Get

N.º do octeto	Atributo/campo	Bits no octeto	Descrição
1	FLAG	0111 1110	Sinal (bandeira) de início
2	Private LID	xxxx xxxx	Endereço de ligação da DSRC-VU específica
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1010 s000	PDU de comando
7	LLC Control field	n111 0111	Comando ACn solicitado, bit n
8	Fragmentation header	1xxx x001	Sem fragmentação
9	Get.request SEQUENCE {	0110	Pedido Get
	OPTION indicator	0	Credenciais de acesso não presentes
	OPTION indicator	0	IID não presente
	OPTION indicator	1	AttributeIdList presente
	Fill BIT STRING(SIZE (1))	0	Fixado em 0
10	EID INTEGER(0..127,…)	xxxx xxxx	O EID da instância de aplicação RTM, conforme especificação na VST. Sem extensão
11	AttributeIdList SEQUENCE OF { AttributeId}}	0000 0001	Sem extensão, número de atributos = 1
12		0000 0001	AttributeId = 1, RtmData. Sem extensão
13	FCS	xxxx xxxx	Sequência de verificação da estrutura
14		xxxx xxxx	
15	Flag	0111 1110	Sinal (bandeira) de terminação

▼B

DSC_50 Ao receber o comando Get Request, a *DSRC-VU*, envia uma resposta Get com os dados pedidos, em conformidade com o Get response definido nas normas EN 13372, 6.2, 6.3, 6.4, e EN 12834, com configurações conforme especificado no quadro 14.12.

Quadro 14.12

▼C2

Apresentação — Configurações da estrutura de resposta Get

Campo	Configurações
Invoker Identifier (IID)	Não presente
Link Identifier (LID)	Conforme EN 12834
Chaining	Não
Element Identifier (EID)	Conforme especificação na VST
Access Credentials	Não
Fragmentation	Não
Layer2 settings	PDU de resposta. Resposta disponível e comando aceite. Comando ACn

▼B

O quadro 14.13 mostra um exemplo da leitura dos dados RTM.

Quadro 14.13

▼C2

Apresentação — Exemplo de conteúdos da estrutura de resposta

N.º do octeto	Atributo/campo	Bits no octeto	Descrição
1	FLAG	0111 1110	Sinal (bandeira) de início
2	Private LID	xxxx xxxx	Endereço de ligação da DSRC-VU específica
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1101 0000	PDU de resposta
7	LLC Control field	n111 0111	Resposta disponível, comando ACn bit n
8	LLC Status field	0000 0000	Resposta disponível e comando aceite
9	Fragmentation header	1xxx x001	Sem fragmentação
10	Get.response SEQUENCE {	0111	Obter resposta

▼C2

N.º do octeto	Atributo/campo	Bits no octeto	Descrição
	OPTION indicator	0	IID não presente
	OPTION indicator	1	Lista de atributos presente
	OPTION indicator	0	Estatuto de devolução não presente
	Fill BIT STRING(SIZE(1))	0	Não utilizado
11	EID INTEGER(0..127,…)	xxxx xxxx	A responder da aplicação RTM Instance. Sem extensão,
12	AttributeList SEQUENCE OF {	0000 0001	Sem extensão, número de atributos = 1
13	Attributes SEQUENCE { AttributeId	0000 0001	Sem extensão, AttributeId = 1 (RtmData)
14	AttributeValue CONTAINER {	0000 1010	Sem extensão, escolha de contentor = 10_{10}
15		kkkk kkkk	RtmData
16		kkkk kkkk	
17		kkkk kkkk	
…		…	
n	}}}}	kkkk kkkk	
n+1	FCS	xxxx xxxx	Sequência de verificação da estrutura
n+2		xxxx xxxx	
n+3	Flag	0111 1110	Sinal (bandeira) de terminação

▼B

DSC_51 O REDCR encerra a conexão mediante a emissão de um comando EVENT_REPORT, RELEASE conforme às normas EN 13372, 6.2, 6.3, 6.4, e EN 12834, 7.3.8, sem configurações RTM específicas. O quadro 14.14 mostra um exemplo de codificação de bits do comando RELEASE.

Quadro 14.14

▼C2

Terminação — Conteúdo da estrutura de terminação da ligação EVENT_REPORT

N.º do octeto	Atributo/campo	Bits no octeto	Descrição
1	FLAG	0111 1110	Sinal (bandeira) de início
2	Private LID	xxxx xxxx	Endereço de ligação da DSRC-VU específica
3		xxxx xxxx	
4		xxxx xxxx	

▼C2

N.º do octeto	Atributo/campo	Bits no octeto	Descrição
5		xxxx xxxx	
6	MAC Control field	1000 s000	A estrutura contém um comando LPDU
7	LLC Control field	0000 0011	Comando UI
8	Fragmentation header	1xxx x001	Sem fragmentação
9	EVENT_REPORT.request SEQUENCE {	0010	EVENT_REPORT (Release)
	OPTION indicator	0	Credenciais de acesso não presentes
	OPTION indicator	0	Parâmetro de incidente: não presente
	OPTION indicator	0	IID não presente
	Mode BOOLEAN	0	Não se espera resposta
10	EID INTEGER (0..127,…)	0000 0000	Sem extensão, EID = 0 (System)
11	EventType INTEGER (0..127,…)}	0000 0000	Tipo de incidente: 0 = Release
12	FCS	xxxx xxxx	Sequência de verificação da estrutura
13		xxxx xxxx	
14	Flag	0111 1110	Sinal (bandeira) de terminação

▼B

DSC_52 Não se prevê que a *DSRC-VU* responda ao comando Release. A comunicação é, pois, encerrada.

5.4.8 *Descrição de transação de ensaio DSRC*

DSC_53 Conforme definido no apêndice 11 (Mecanismos comuns de segurança), é necessário realizar ensaios completos que incluam a proteção dos dados, por pessoas autorizadas com acesso a procedimentos de segurança, utilizando o comando GET normal atrás definido.

DSC_54 Devem ser realizados ensaios de colocação em serviço e inspeção periódica que exijam conteúdo de dados decifrados, conforme especificado no apêndice 11 (Mecanismos comuns de segurança) e no apêndice 9 (Relação dos ensaios mínimos exigidos para homologação de tipo).

No entanto, a comunicação DSRC básica pode ser ensaiada pelo comando ECHO. Esses ensaios podem ser necessários aquando da colocação em serviço, numa inspeção periódica, ou de qualquer outra forma por exigência da autoridade de controlo competente ou do Regulamento (UE) n.º 165/2014 (ver secção 6).

▼B

DSC_55 De modo a efetuar este ensaio de comunicação básico, o comando ECHO é emitido pelo REDCR durante uma sessão, ou seja, depois de uma fase de inicialização ter sido concluída com êxito. A sequência de interações é, desta forma, semelhante à de uma interrogação:

— Etapa 1 — *O REDCR* envia um «quadro de serviço de baliza» (BST), que inclui os identificadores de aplicação (AID) na lista de serviço que aceita. Nas aplicações RTM será simplesmente o serviço com o valor AID = 2.

A *DSRC-VU* avalia o BST recebido e sempre que identificar que o BST está a pedir Freight&Fleet (AID = 2), a *DSRC-VU* responde. Se *o REDCR* não oferecer AID=2, a *DSRC-VU* desliga a sua transação com *o REDCR*.

— Etapa 2 — *A DSRC-VU* envia um pedido de atribuição de janela privada.

— Etapa 3 — O REDCR envia uma atribuição de janela privada.

— Etapa 4 — A *DSRC-VU* utiliza a janela privada atribuída para enviar o seu quadro de serviço do veículo (VST). Este VST inclui uma lista de todas as instanciações de aplicação diferentes que esta *DSRC-VU* aceita no âmbito de AID=2. As diferentes instanciações devem ser identificadas por meio de EID exclusivos, cada um associado a um valor do parâmetro que indica a instância da aplicação que é aceite.

— Etapa 5 — Em seguida, *o REDCR* analisa o VST oferecido, e termina a ligação (RELEASE), uma vez que não está interessado em nada do que o VST tem para oferecer (ou seja, está a receber um VST de uma *DSRC-VU* que não é uma RTM VU) ou, se receber um VST adequado, inicia uma instanciação da aplicação.

— Etapa 6 — O *REDCR* emite um comando (ECHO) à *DSRC-VU* específica e atribui uma janela privada.

— Etapa 7 — A *DSRC-VU* utiliza a janela privada atribuída recentemente para enviar uma estrutura de resposta ECHO.

Os quadros que se seguem apresentam um exemplo prático de uma sessão de intercâmbio ECHO.

DSC_56 A inicialização é realizada de acordo com a secção 5.4.7 (DSC_44 — DSC_48) e com os quadros 14.4 a 14.9.

DSC_57 O REDCR emite um comando ACTION, ECHO conforme com a norma ISO 14906, contendo 100 octetos de dados e sem configurações específicas de RTM. O quadro 14.15 mostra o conteúdo da estrutura enviada pelo REDCR.

▼B

Quadro 14.15

▼C2

Exemplo de estrutura de pedido de ação ECHO

N.º do octeto	Atributo/campo	Bits no octeto	Descrição
1	FLAG	0111 1110	Sinal (bandeira) de início
2	Private LID	xxxx xxxx	Endereço de ligação da DSRC-VU específica
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1010 s000	PDU de comando
7	LLC Control field	n111 0111	Comando ACn solicitado, bit n
8	Fragmentation header	1xxx x001	Sem fragmentação
9	ACTION.request SEQUENCE {	0000	Pedido de ação (ECHO)
	OPTION indicator	0	Credenciais de acesso não presentes
	OPTION indicator	1	Parâmetro de ação presente
	OPTION indicator	0	IID não presente
	Mode BOOLEAN	1	Espera-se resposta
10	EID INTEGER (0..127,…)	0000 0000	Sem extensão, EID = 0 (System)
11	ActionType INTEGER (0..127,…)	0000 1111	Sem extensão. Tipo de ação: pedido ECHO
12	ActionParameter CONTAINER {	0000 0010	Sem extensão, escolha de contentor = 2
13		0110 0100	Sem extensão. Comprimento da cadeia = 100 octetos
14		xxxx xxxx	Dados a reenviar
…		…	
113	}}	xxxx xxxx	
114	FCS	xxxx xxxx	Sequência de verificação da estrutura
115		xxxx xxxx	
116	Flag	0111 1110	Sinal (bandeira) de terminação

▼B

DSC_58 Ao receber o pedido ECHO, a *DSRC-VU* envia uma resposta ECHO de 100 octetos de dados, refletindo o comando recebido, de acordo com a norma ISO 14906, sem configurações específicas de RTM. O quadro 14.16 mostra um exemplo de codificação do nível de bit.

Quadro 14.16

▼C2

Inicialização — Exemplo de estrutura de resposta de ação ECHO

N.º do octeto	Atributo/campo	Bits no octeto	Descrição
1	FLAG	0111 1110	Sinal (bandeira) de início
2	Private LID	xxxx xxxx	Endereço de ligação da DSRC-VU específica
3		xxxx xxxx	
4		xxxx xxxx	
5		xxxx xxxx	
6	MAC Control field	1101 0000	PDU de resposta
7	LLC Control field	n111 0111	Comando ACn, bit n
8	LLC status field	0000 0000	Resposta disponível
9	Fragmentation header	1xxx x001	Sem fragmentação
10	ACTION.response SEQUENCE {	0001	Resposta de ACTION (ECHO)
	OPTION indicator	0	IID não presente
	OPTION indicator	1	Parâmetro de resposta presente
	OPTION indicator	0	Estatuto de devolução não presente
	Fill BIT STRING (SIZE (1))	0	Não utilizado
11	EID INTEGER (0..127,…)	0000 0000	Sem extensão, EID = 0 (System)
12	ResponseParameter CONTAINER {	0000 0010	Sem extensão, escolha de contentor = 2
13		0110 0100	Sem extensão. Comprimento da cadeia = 100 octetos
14		xxxx xxxx	Dados reenviados
…		…	
113	}}	xxxx xxxx	
114	FCS	xxxx xxxx	Sequência de verificação da estrutura
115		xxxx xxxx	
116	Flag	0111 1110	Sinal (bandeira) de terminação

▼B

5.5 **Apoio à Diretiva (UE) 2015/719**

5.5.1 *Panorâmica*

DSC_59 Em cumprimento da Diretiva (UE) 2015/719, relativa aos pesos e dimensões máximos dos veículos pesados de mercadorias, o protocolo de transação para descarregamento de dados OWS através da ligação da interface DSRC de 5,8 GHz é o mesmo utilizado para os dados RTM (ver 5.4.1). A única diferença é que o identificador de objeto relativo à norma TARV se refere à norma ISO 15638 (TARV), parte 20, relativa a WOB/OWS.

5.5.2 *Comandos*

DSC_60 Os comandos utilizados para uma transação OWS são os mesmos utilizados numa transação RTM.

5.5.3 *Sequência de comandos de interrogação*

DSC_61 A sequência de comando de interrogação para os dados OWS é a mesma que para os dados RTM.

5.5.4 *Estruturas de dados*

DSC_62 A carga útil (dados OWS) é composta pela concatenação de

1. dados EncryptedOwsPayload: trata-se da encriptação de OwsPayload definida em ASN.1, na secção 5.5.5. O método de encriptação deve ser o mesmo aprovado para o RtmData, que é especificado no apêndice 11;

2. DSRCSecurityData, calculado com os mesmos algoritmos aprovados para o RtmData, que é especificado no apêndice 11.

▼B

5.5.5 *Módulo ASN.1 para a transação OWS DSRC*

DSC_63 O módulo ASN.1 para os dados DSRC na aplicação RTM é definido do seguinte modo:

```
TarvOws {iso(1) standard(0) 15638 part20(20)
version1(1)} DEFINITIONS AUTOMATIC TAGS
::= BEGIN
IMPORTS
-- Imports data attributes and elements from EFC which are used for OWS
LPN
FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

-- Imports function parameters from the EFC Application Interface Definition
SetMMIRq
FROM EfcDsrcApplication {iso(1) standard(0) 14906 application(0) version5(5)}

-- Imports the L7 DSRCData module data from the EFC Application Interface Definition
Action-Request, Action-Response, ActionType, ApplicationList, AttributeIdList, AttributeList,
Attributes,
BeaconID, BST, Dsrc-EID, DSRCApplicationEntityID, Event-Report-Request, Event-Report- Response,
EventType, Get-Request, Get-Response, Initialisation-Request, Initialisation-Response,
ObeConfiguration, Profile, ReturnStatus, Time, T-APDUs, VST
FROM EfcDsrcGeneric {iso(1) standard(0) 14906 generic(1) version5(5)};

-- Definitions of the OWS functions:
OWS-InitialiseComm-Request ::= BST
OWS-InitialiseComm-Response::= VST
OWS-DataRetrieval-Request::= Get-Request (WITH COMPONENTS {fill (SIZE(1)), eid, accessCredentials
ABSENT, iid ABSENT, attrIdList})
OWS-DataRetrieval-Response::= Get-Response {OwsContainer} (WITH COMPONENTS {..., eid, iid ABSENT})
OWS-TerminateComm::= Event-Report-Request {OwsContainer}(WITH COMPONENTS {mode (FALSE), eid (0),
eventType (0)})
OWS-TestComm-Request::= Action-Request {OwsContainer} (WITH COMPONENTS {..., eid (0), actionType
(15), accessCredentials ABSENT, iid ABSENT})
OWS-TestComm-Response::= Action-Response {OwsContainer} (WITH COMPONENTS {..., fill (SIZE(1)), eid
(0), iid ABSENT})

-- Definitions of the OWS attributes:
OwsData :: = SEQUENCE {
     encryptedOwsPayload OCTET STRING (SIZE(51)) (CONSTRAINED BY { -- calculated encrypting
OwsPayload as per Appendix 11 --}),
     DSRCSecurityData OCTET STRING
     }
OwsPayload :: = SEQUENCE {
           tp15638VehicleRegistrationPlate LPN -- Vehicle Registration Plate as per EN 15509.
           recordedWeight INTEGER (0..65535),           -- 0= Total measured weight of the  heavy
goods vehicle                                                          -- with 10 Kg
resolution.
           axlesConfiguration OCTET STRING SIZE (3),     -- 0= 20 bits allowed for the number
                                                                  -- of axles for 10 axles.
           axlesRecordedWeight OCTET STRING SIZE (20),   -- 0= Recorded Weight for each axle
                                                                  -- with 10 Kg resolution.
           tp15638Timestamp              INTEGER(0..4294967295)      -- Timestamp of current record
     }

Ows-ContextMark ::= SEQUENCE {
 standardIdentifier    StandardIdentifier, -- identifier of the TARV part and its version
     }

StandardIdentifier ::= OBJECT IDENTIFIER
 OwsContainer ::= CHOICE {
     integer                    [0]    INTEGER,
     bitstring                  [1]    BIT STRING,
     octetstring                [2]    OCTET STRING (SIZE (0..127, ...)),
     universalString            [3]    UniversalString,
     beaconId                   [4]    BeaconID,
     t-apdu                     [5]    T-APDUs,
     dsrcApplicationEntityId    [6]    DSRCApplicationEntityID,
     dsrc-Ase-Id                [7]    Dsrc-EID,
     attrIdList                 [8]    AttributeIdList,
     attrList                   [9]    AttributeList{RtmContainer},
     reserved10                 [10]   NULL,
     OwsContextmark             [11]   Ows-ContextMark,
     OwsData                    [12]   OwsData,
     reserved13                 [13]   NULL,
     reserved14                 [14]   NULL,
     time                       [15]   Time,
-- values from 16 to 255 reserved for ISO/CEN usage
     }}

END
```

▼B

5.5.6 *Elementos de OwsData, ações realizadas e definições*

Os elementos de OwsData são definidos em cumprimento da Diretiva (UE) 2015/719, relativa aos pesos e dimensões máximos dos veículos pesados de mercadorias. Seu significado:

— recordedWeight representa o peso total medido do veículo pesado com uma resolução de 10 kg, conforme definido na norma EN ISO 14906. Por exemplo, um valor de 2 500 representa um peso de 25 toneladas.

— axlesConfiguration representa a configuração do veículo pesado como número de eixos. A configuração é definida com a máscara de 20 bits (aumentado a partir da norma EN ISO 14906).

Uma máscara de 2 bits representa a configuração de um eixo com o seguinte formato:

— 00B significa que o valor está «indisponível», porque o veículo não tem equipamento para tomar o peso no eixo.

— 01B significa que o eixo não está presente.

— 10B significa que o eixo está presente e que o peso foi calculado e recolhido e é fornecido no campo axlesRecordedWeight.

— O valor 11B é reservado para utilizações futuras.

Os quatro últimos bits estão reservados para utilizações futuras.

Número de eixos										
Número de eixos no trator			Número de eixos no reboque							
00/01/ 10/11	00/01/ 10/11	00/01/ 10/11	00/01/ 10/11	00/01/ 10/11	00/01/ 10/11	00/01/ 10/11	00/01/ 10/11	00/01/ 10/11	00/01/ 10/11	RFU (4 bits)

— axlesRecordedWeight representa o peso específico registado para cada eixo com uma resolução de 10 kg. Utilizam-se dois octetos para cada eixo. Por exemplo, um valor de 150 representa um peso de 1 500 kg.

Os outros tipos de dados são definidos em 5.4.5.

5.5.7 *Mecanismos de transferência de dados*

DSC_64 O mecanismo de transferência de dados para dados OWS entre o interrogador e o módulo DSRC no veículo deve ser igual para dados RTM (ver 5.4.7).

DSC_65 A transferência de dados entre a plataforma de recolha de dados dos pesos máximos e o módulo DSRC no veículo deve ser baseado na conexão física, nas interfaces e no protocolo definidos na secção 5.6.

5.6 **Transferência de dados entre a DSRC-VU e a VU**

5.6.1 *Conexão física e interfaces*

DSC_66 A conexão entre a *VU* e a *DSRC-VU* pode ser por cabo físico ou por comunicação sem fios de curto alcance com base em Bluetooth v4.0 BLE.

▼B

DSC_67 Independentemente da escolha da conexão física e interface, devem ser satisfeitos os seguintes requisitos:

DSC_68 a) A fim de que possam ser contratados fornecedores diferentes para o fornecimento de VU e DSRC-VU e, na verdade, diferentes lotes de DSRC-VU, a conexão entre a VU e a DSRC-VU deve ser uma conexão-padrão aberta. A VU deve conectar-se à DSRC-VU

i) utilizando um cabo fixo de pelo menos 2 m ou um conector H11 Straight DIN 41612 — conector macho homologado de 11 pinos — da DSRC-VU para corresponder a um conector fêmea homologado DIN/ISO semelhante do dispositivo da VU,

ii) utilizando baixo consumo energético do Bluetooth (BLE),

iii) utilizando uma conexão homologada pelas normas ISO 11898 ou SAE J1939;

DSC_69 b) A definição das interfaces e da conexão entre a VU e DSRC-VU tem de aceitar (isto é, tem de ser compatível com) os comandos do protocolo de aplicação definidos na secção 5.6.2 e

DSC_70 c) A VU e a DSRC-VU têm de aceitar (isto é, têm de ser compatíveis com) a operação de transferência de dados através da conexão, no que respeita ao desempenho e à alimentação energética.

5.6.2 *Protocolo de aplicação*

DSC_71 O protocolo de aplicação entre o módulo de comunicação à distância da VU e a DSRC-VU é responsável por transferir periodicamente os dados de comunicação à distância da VU para a DSRC.

DSC_72 Identificam-se a seguir os principais comandos:

1. Inicialização da ligação de comunicação — pedido

2. Inicialização da ligação de comunicação — resposta

3. Envio de dados com identificador da aplicação RTM e carga útil definida pelos dados RTM

4. Reconhecimento dos dados

5. Terminação da ligação de comunicação — pedido

6. Terminação da ligação de comunicação — resposta

DSC_73 Em ASN1.0, os comandos anteriores podem ser definidos como:

▼B

```
Remote Communication DT Protocol DEFINITIONS ::= BEGIN

     RCDT-Communication Link Initialization - Request ::= SEQUENCE {
          LinkIdentifier INTEGER
     }

     RCDT-Communication Link Initialization - Response::= SEQUENCE {
          LinkIdentifier INTEGER,
          answer         BOOLEAN
     }

          RCDT- Send Data ::=
          SEQUENCE { LinkIdentifier
          INTEGER, DataTransactionId
          INTEGER, RCDTData
          SignedTachographPayload
     }

          RCDT Data Acknowledgment ::
          SEQUENCE { LinkIdentifier
          INTEGER, DataTransactionId
          INTEGER,
          answer         BOOLEAN
     }

          RCDT-Communication Link Termination - Request ::= SEQUENCE {
          LinkIdentifier INTEGER
     }

          RCDT-Communication Link Termination - Response::= SEQUENCE {
          LinkIdentifier INTEGER,
          answer         BOOLEAN
     }

End
```

DSC_74 A descrição dos comandos e parâmetros é a seguinte:

— RCDT-Communication Link Initialization – Request : utilizado para inicializar a ligação de comunicação. O comando é enviado pela VU à DSRC-VU. O LinkIdentifier é definido pela VU e comunicado à DSRC-VU para rastrear uma ligação de comunicação específica

(*Nota:* destina-se a aceitar ligações futuras e outros módulos/aplicações, como a pesagem a bordo).

— RCDT-Communication Link Initialization – Response : utilizado pela DSRC-VU para fornecer a resposta do pedido de inicialização da ligação de comunicação. O comando é enviado pela DSRC-VU à VU. O comando fornece o resultado da inicialização como resposta = 1 (êxito) ou = 0 (falha).

DSC_75 A inicialização da ligação de comunicação deve ser efetuada apenas após a instalação e a calibração e após estar ligado o arranque do motor/VU.

▼B

— RCDT-Send Data: utilizado para, através da VU, enviar o RCDTData assinado (ou seja, os *dados de comunicação à distância*) à DSRC-VU. Os dados são enviados de 60 em 60 segundos. O parâmetro DataTransactionId identifica a transmissão específica de dados. O LinkIdentifier é igualmente utilizado para garantir que a ligação adequada está correta.

— RCDT-Data Acknowledgment: enviado pela DSRC--VU para fornecer o retorno à VU sobre a receção dos dados de um comando RCDT-Send Dataidentificado pelo parâmetro DataTransactionId. O parâmetro de resposta é = 1 (êxito) ou = 0 (falha). Se uma VU receber mais do que três respostas iguais a 0 ou não receber RCDT Data Acknowledgment para um RCDT- Send Data específico enviado anteriormente com um DataTransactionId específico, cria e regista um incidente.

— RCDT-Communication Link Termination requesté enviado pela VU à DSRC-VU para encerrar uma ligação para um LinkIdentifier específico.

DSC_76 Ao reiniciar a DSRC-VU ou uma VU, todas as ligações de comunicação existentes devem ser removidas, dado poderem existir ligações «penduradas» devido ao desligamento repentino de uma VU.

— RCDT-Communication Link Termination – Response: enviado pela DSRC-VU à VU para confirmar o pedido de terminação da ligação pela VU para o LinkIdentifier específico.

5.7 **Tratamento de erros**

5.7.1 *Memorização e comunicação dos dados na DSRC-VU*

DSC_77 Os *dados* devem ser fornecidos, já protegidos, pela função *VUSM* à *DSRC-VU*. O *VUSM* verifica se os dados registados na *DSRC-VU* foram registados corretamente. O registo e a comunicação de erros na transferência de dados da *VU* para a memória da *DSRC-VU* são registados com o tipo EventFaultType e o valor de enumeração definido como falha de comunicação '62'H módulo de comunicação à distância juntamente com o período de tempo.

DSC_78 A *VU* mantém um ficheiro identificado por um nome exclusivo facilmente identificável pelos inspetores, para fins de registo de «falhas de comunicação interna da VU».

DSC_79 Se o VUPM tentar obter dados da VU do módulo de segurança (para passar ao VU-DSRC), mas não o fizer, regista a falha com o tipo EventFaultType e o valor de enumeração definido como falha de comunicação *'62'H módulo de comunicação à distância*, juntamente com o período de tempo. O

▼B

fracasso da comunicação é detetado quando uma mensagem RCDT Data Acknowledgment não é recebida para o correspondente (ou seja, com o mesmo DataTransactionId nas mensagens nas mensagens) RCDT Send Data durante mais de três vezes consecutivas.

5.7.2 *Erros de comunicações sem fios*

DSC_80 O tratamento de erros de comunicação deve ser coerente com o disposto nas normas DSRC correspondentes, nomeadamente EN 300 674-1, EN 12253, EN 12795 e EN 12834 e os parâmetros adequados da norma EN 13372.

5.7.2.1 *Erros de encriptação e assinatura*

DSC_81 Os erros de assinatura e de encriptação devem ser tratados conforme definido no apêndice 11 (Mecanismos comuns de segurança) e não estão presentes nas mensagens de erro associadas à transferência de dados DSRC.

5.7.2.2 *Registo de erros*

O meio DSRC é uma comunicação sem fios dinâmica num ambiente de condições atmosféricas e de interferência incertas, particularmente nas combinações «REDCR portátil» e «veículo em movimento» presentes nesta aplicação. É, por conseguinte, necessário verificar a diferença entre uma «falha de leitura» e uma situação de «erro». Numa transação através de uma interface sem fios, é comum a falha de leitura e, normalmente, a consequência é voltar a tentar, ou seja, voltar a transmitir o BST e tentar novamente a sequência, que, na maioria das circunstâncias, leva a uma conexão de comunicação e transferência de dados com êxito, exceto se o veículo visado se mover para fora do alcance durante o tempo necessário para retransmitir (uma instância de «leitura» «com êxito» pode ter envolvido várias tentativas e repetições).

A falha de leitura pode ter múltiplas causas: as antenas não estão devidamente emparelhadas (falha de «pontaria»); uma das antenas está blindada (pode ser deliberado, mas pode igualmente dever-se à presença física de outro veículo); há interferência do rádio, especialmente de cerca de 5,8 GHz Wi-Fi ou outras comunicações sem fios de acesso público; há interferência do radar ou condições atmosféricas adversas (por exemplo, durante um temporal); ou simples movimento para fora do alcance da comunicação DSRC. Pela sua natureza, as instâncias individuais de falhas de leitura não podem ser registadas, simplesmente porque a comunicação não aconteceu.

No entanto, se o agente da autoridade de controlo competente tiver como alvo um veículo e tentar interrogar a sua *DSRC-VU*, mas sem obter êxito na transferência de dados, esta falha pode ter ocorrido devido a adulteração deliberada e, por conseguinte, o agente precisa de um meio para registar a falha e avisar os seus colegas a jusante de que pode haver uma violação. Os colegas podem, desta forma, parar o veículo e realizar uma inspeção física. No entanto, como não ocorreu nenhuma comunicação com êxito, o DSRC-VU não pode fornecer dados sobre a falha. Essa comunicação deve, por conseguinte, ser uma função de conceção de equipamento REDCR.

Tecnicamente, «falha de leitura» é diferente de «erro». Neste contexto, um «erro» é a aquisição de um valor errado.

▼B

Os dados transferidos para a *DSRC-VU* são fornecidos já protegidos, pelo que devem ser verificados pelo fornecedor dos dados (ver 5.4).

Os dados transferidos posteriormente através da interface aérea são verificados através de controlos de redundância cíclica ao nível das comunicações. Se o CRC validar, os dados estão corretos. Se o CRC não validar, os dados são retransmitidos. A probabilidade de os dados poderem passar com êxito por um CRC, de modo incorreto, é estatisticamente muito improvável, pelo que pode ser descartada.

Se o CRC não validar e não houver tempo para retransmitir e receber os dados corretos, o resultado não será um erro, mas uma instanciação de um tipo específico de falha de leitura.

O único dado de «falha» significativo que pode ser registado é o número de iniciações com êxito, das transações que ocorrem, que não resultam numa transferência bem sucedida de dados para o REDCR.

DSC_82 Por conseguinte, o *REDCR* regista, com período de tempo, o número de ocasiões em que a fase de «inicialização» de uma interrogação DSRC for bem sucedida, mas a transação termina antes de os *dados* terem sido recuperados com êxito pelo REDCR. Estes dados estarão disponíveis para o agente da autoridade de controlo competente e serão memorizados na memória do equipamento REDCR. Os meios pelos quais tal é obtido terão a ver com a conceção do produto ou a especificação de uma autoridade de controlo competente.

O único dado de «erro» significativo que pode ser registado é o número de ocasiões em que o REDCR não decifra os *dados* recebidos. No entanto, deve referir-se que tal é relativo apenas à eficiência do *software* REDCR. Tecnicamente, os dados podem ser decifrados, mas não fazem sentido semântico.

DSC_83 Por conseguinte, o *REDCR* regista, com período de tempo, o número de ocasiões em que a decifragem dos dados recebidos através da interface DSRC foi tentada mas falhou.

6 ENSAIOS DE COLOCAÇÃO EM SERVIÇO E DE INSPEÇÃO PERIÓDICA PARA A FUNÇÃO DE COMUNICAÇÃO À DISTÂNCIA

6.1 **Geral**

DSC_84 Estão previstos dois tipos de ensaios para a função de comunicação à distância:

1) Ensaio ECHO para validar o *DSRC-REDCR* >>-:-<*DSRC-VU sem fios* canal de comunicação.

2) Ensaio de segurança integral para garantir que um cartão de oficina é capaz de aceder a conteúdo de dados assinado e encriptado criado pela VU e transmitido através do canal de comunicação sem fios.

6.2 **ECHO**

A presente cláusula contém disposições especificamente para testar apenas se o *DSRC-REDCR* >>-:-<*DSRC-VU* está funcionalmente ativo.

▼B

O objetivo do comando ECHO é autorizar as oficinas ou unidades de ensaio de homologações de tipo a testar se a ligação DSRC funciona sem necessidade de acesso a credenciais de segurança. Por conseguinte, o equipamento do dispositivo de teste só tem de ser capaz de inicializar uma comunicação DSRC (envio de um BST com AID = 2) e enviar o comando ECHO; presumindo que o DSRC está a trabalhar, receberá a resposta ECHO (ver 5.4.8 para mais informações). Presumindo que recebe corretamente esta resposta, a ligação DSRC (*DSRC-REDCR* >>-:-<*DSRC-VU*) pode ser validada como funcionando corretamente.

6.3 **Ensaios para validar o conteúdo de dados seguro**

DSC_85 Este ensaio é executado para validar o fluxo de dados de segurança integral. Este ensaio requer um leitor de ensaio DSRC. O leitor de ensaio DSRC executa a mesma função e é aplicado com as mesmas especificações do leitor utilizado pelas forças da lei (autoridade de controlo competente), com a diferença de que, para autenticar o utilizador do leitor de ensaio DSRC, deve ser utilizado um cartão de oficina, e não um cartão de controlo. O ensaio pode ser executado após a ativação inicial de um tacógrafo inteligente ou no final do procedimento de calibração. Após a ativação, a unidade-veículo deve criar e comunicar ao DSRC-VU os dados de deteção rápida protegidos.

DSC_86 O pessoal da oficina tem de posicionar o leitor de ensaio DSRC a uma distância entre 2 e 10 metros à frente do veículo.

DSC_87 De seguida, o pessoal da oficina insere um cartão de oficina no leitor de ensaio DSRC para pedir a interrogação dos dados de deteção rápida à unidade-veículo. Após uma interrogação com êxito, o pessoal da oficina acede aos dados recebidos para garantir que foi validada com êxito, em termos de integridade, e decifrada.

▼B

Apêndice 15

MIGRAÇÃO: GESTÃO DA COEXISTÊNCIA DE GERAÇÕES DE APARELHOS

ÍNDICE

1. DEFINIÇÕES

Para efeitos do presente apêndice, entende-se por:

Sistema tacográfico inteligente*:* conforme definição no presente anexo (capítulo 1: definição bbb);

Sistema tacográfico da primeira geração*:* conforme definição no presente regulamento (artigo 2.º: definição 1);

Sistema tacográfico da segunda geração*:* conforme definição no presente regulamento (artigo 2.º: definição 7);

Data de produção*:* conforme definição no presente anexo (capítulo 1: definição ccc);

Equipamento dedicado inteligente (IDE)*:* equipamento utilizado para executar a descarga de dados, conforme definição no apêndice 7 do presente anexo.

2. DISPOSIÇÕES GERAIS

2.1. **Síntese da transição**

O preâmbulo do presente anexo sumariza a transição entre os sistemas tacográficos da primeira e da segunda gerações.

Além do disposto no presente preâmbulo:

— os sensores de movimento da primeira geração não são interoperáveis com as unidades-veículo da segunda geração

— os sensores de movimento da segunda geração começarão a ser instalados nos veículos em simultâneo com as unidades-veículo da segunda geração

▼B

— os equipamentos de descarregamento de dados e de calibração terão de evoluir, para se tornarem compatíveis com a utilização de ambas as gerações de aparelhos de controlo e cartões tacográficos.

2.2. **Interoperabilidade entre VU e cartões**

Entende-se que os cartões tacográficos da primeira geração são interoperáveis com as unidades-veículo da primeira geração (em conformidade com o anexo 1B do presente regulamento), ao passo que os cartões tacográficos da segunda geração são interoperáveis com as unidades-veículo da segunda geração (em conformidade com o anexo 1C do presente regulamento). Aplicam-se, além disso, os requisitos *infra*.

MIG_001 Salvo o disposto nos requisitos MIG_004 e MIG_005, os cartões tacográficos da primeira geração podem continuar a ser utilizados em unidades-veículo da segunda geração até ao termo da sua validade. Porém, os titulares dos cartões podem pedir a sua substituição por cartões tacográficos da segunda geração, logo que disponíveis.

MIG_002 As unidades-veículo da segunda geração devem poder utilizar qualquer cartão válido inserido da primeira geração, de condutor, de controlo ou de empresa.

MIG_003 Esta capacidade pode ser suprimida definitivamente por oficinas, para que nas referidas unidades-veículo deixem de ser aceites cartões tacográficos da primeira geração, mas somente depois de a Comissão Europeia lançar um procedimento no sentido de as oficinas o fazerem (por exemplo, durante cada inspeção periódica do tacógrafo).

MIG_004 Nas unidades-veículo da segunda geração só é possível utilizar cartões de oficina da segunda geração.

MIG_005 Para determinar o modo de funcionamento, as unidades-veículo da segunda geração atendem apenas ao tipo dos cartões válidos inseridos, independentemente da geração a que estes correspondam.

MIG_006 Os cartões tacográficos válidos da segunda geração devem poder ser utilizados em unidades-veículo da primeira geração, exatamente como os cartões tacográficos da primeira geração do mesmo tipo.

2.3. **Interoperabilidade entre VU e MS**

Entende-se que os sensores de movimento da primeira geração são interoperáveis com as unidades-veículo da primeira geração, ao passo que os sensores de movimento da segunda geração são interoperáveis com as unidades-veículo da segunda geração. Aplicam-se, além disso, os requisitos *infra*.

MIG_007 Não é possível emparelhar nem utilizar unidades-veículo da segunda geração com sensores de movimento da primeira geração.

MIG_008 Os sensores de movimento da segunda geração podem ser emparelhados e utilizados com unidades-veículo quer apenas da segunda geração quer de ambas as gerações.

2.4. **Interoperabilidade entre unidades-veículo, cartões tacográficos e equipamento de descarregamento de dados**

MIG_009 O equipamento de descarregamento de dados pode ser utilizado com unidades-veículo e cartões tacográficos quer apenas de uma geração quer de ambas as gerações.

▼B

2.4.1 *Descarregamento direto do cartão pelo IDE*

MIG_010 Os dados são descarregados pelo IDE a partir de cartões tacográficos de uma dada geração inseridos nos seus leitores de cartões, utilizando os mecanismos de segurança e o protocolo de descarregamento de dados dessa geração, sendo que os dados descarregados terão o formato definido para a mesma geração.

MIG_011 Para permitir o controlo de condutores por autoridades não pertencentes à UE, é também possível descarregar cartões de condutor (e de oficina) da segunda geração, exatamente do mesmo modo que os cartões de condutor (e de oficina) da primeira geração. Esse descarregamento inclui:

— EF, `IC` e `ICC` não assinados

— EF (primeira geração) `Card_Certificate` e `CA_Certificate` não assinados

— os outros EF de dados da aplicação (dentro do DF `TACHO`) solicitados pelo protocolo de descarregamento do cartão da primeira geração; esta informação deve ser protegida com uma assinatura digital, de acordo com os mecanismos de segurança da primeira geração

O descarregamento não inclui EF de dados da aplicação presentes apenas em cartões de condutor (e de oficina) da segunda geração (EF de dados da aplicação dentro do DF `TACHO_G2`).

2.4.2 *Descarregamento do cartão através de uma unidade-veículo*

MIG_012 Os dados são descarregados de um cartão da segunda geração inserido numa unidade-veículo da primeira geração que utiliza o protocolo de descarregamento de dados da primeira geração. O cartão responde aos comandos da unidade-veículo exatamente do mesmo modo que um cartão da primeira geração, e os dados descarregados têm o mesmo formato que os dados descarregados de um cartão da primeira geração.

MIG_013 Os dados são descarregados de um cartão da primeira geração inserido numa unidade-veículo da segunda geração que utiliza o protocolo de descarregamento de dados definido no apêndice 7 do presente anexo. A unidade-veículo envia comandos ao cartão exatamente do mesmo modo que uma unidade-veículo da primeira geração, e os dados descarregados devem respeitar o formato definido para cartões da primeira geração.

2.4.3 *Descarregamento da unidade-veículo*

MIG_014 Os dados são descarregados de unidades-veículo da segunda geração que utilizam mecanismos de segurança da segunda geração e o protocolo de descarregamento de dados definido no apêndice 7 do presente anexo.

MIG_015 Para permitir o controlo de condutores por autoridades não pertencentes à UE e o descarregamento de dados da unidade-veículo por oficinas não pertencentes à UE, existe a opção de descarregar dados de unidades-veículo da segunda geração que utilizam os mecanismos de segurança da primeira geração e o protocolo de descarregamento de dados da primeira geração. Os dados descarregados devem ter o mesmo formato que os dados descarregados de uma unidade-veículo da primeira geração. Esta funcionalidade pode ser selecionada por meio de comandos no menu.

▼B

2.5. **Interoperabilidade entre VU e aparelhos de calibração**

MIG_016 Os aparelhos de calibração devem poder executar a calibração de uma dada geração de tacógrafo, utilizando o protocolo de calibração dessa geração. Os aparelhos de calibração podem ser utilizados com tacógrafos quer apenas de uma geração quer de ambas as gerações.

3. PRINCIPAIS ETAPAS DURANTE O PERÍODO ANTERIOR À DATA DE PRODUÇÃO

MIG_017 Os certificados e chaves de ensaio devem ser disponibilizados aos fabricantes **30 meses** (pelo menos) antes da data de produção.

MIG_018 Os ensaios de interoperabilidade, se solicitados pelos fabricantes, devem estar prontos a ter início **15 meses** (pelo menos) antes da data de produção.

MIG_019 Os certificados e chaves oficiais devem ser disponibilizados aos fabricantes **12 meses** (pelo menos) antes da data de produção.

MIG_020 Os Estados-Membros devem poder emitir cartões de oficina da segunda geração **3 meses** (pelo menos) antes da data de produção.

MIG_021 Os Estados-Membros devem poder emitir todos os tipos de cartões tacográficos da segunda geração **1 mês** (pelo menos) antes da data de produção.

4. DISPOSIÇÕES PARA O PERÍODO APÓS A DATA DE PRODUÇÃO

MIG_022 Após a data de produção, os Estados-Membros emitirão apenas cartões tacográficos da segunda geração.

MIG_023 Os fabricantes de unidades-veículo ou de sensores de movimento poderão produzir unidades-veículo ou sensores de movimento da primeira geração enquanto este equipamento for utilizado no terreno, de modo a que os componentes com defeito possam ser substituídos.

MIG_024 Os fabricantes de unidades-veículo ou de sensores de movimento poderão solicitar e obter a manutenção da homologação de tipos já homologados de unidades-veículo ou de sensores de movimento da primeira geração.

▼B

Apêndice 16.

ADAPTADOR PARA VEÍCULOS DAS CATEGORIAS M1 E N1

ÍNDICE

1. ABREVIATURAS E REFERÊNCIAS

1.1. **Abreviaturas**

A DEFINIR a definir

VU unidade-veículo

1.2. **Normas de referência**

ISO 16844-3 Road vehicles — Tachograph systems — Part 3: Motion sensor interface

2. CARACTERÍSTICAS GERAIS E FUNÇÕES DO ADAPTADOR

2.1. **Descrição geral do adaptador**

ADA_001 O adaptador deve fornecer permanentemente a uma VU a ele ligada dados securizados representativos da velocidade de circulação do veículo e da distância por ele percorrida.

O adaptador destina-se unicamente aos veículos que têm de ser equipados com aparelhos de controlo na aceção do presente regulamento.

▼B

O adaptador deve ser instalado e utilizado apenas nos veículos correspondentes à definição yy («adaptador») do anexo IC, onde não seja mecanicamente possível instalar outro tipo de sensor de movimentos que, por outro lado, cumpre o disposto no presente anexo e nos seus apêndices 1 a 16.

O adaptador não pode ter uma interface mecânica com partes móveis do veículo; deve, sim, ser ligado aos impulsos velocidade/distância gerados por sensores integrados ou interfaces alternativas.

ADA_002 Deve colocar-se um sensor de movimentos de tipo homologado (em conformidade com o disposto no anexo IC, ponto 8, «Homologação de tipo dos aparelhos de controlo e dos cartões tacográficos») na caixa do adaptador, que incluirá também um dispositivo conversor para induzir os impulsos de entrada no sensor de movimentos incorporado. Por sua vez, o sensor de movimentos incorporado deve ser ligado à VU, para que a interface entre a VU e o adaptador cumpra os requisitos da norma ISO 16844-3.

2.2. **Funções**

ADA_003 Funções do adaptador:

— estabelecer uma interface com os impulsos de entrada de velocidade e adaptá-los

— induzir os impulsos de entrada no sensor de movimentos incorporado

— todas as funções do sensor de movimentos incorporado, fornecendo à VU dados de movimento securizados

2.3. **Segurança**

ADA_004 Ao adaptador não pode ser concedida a certificação de segurança correspondente ao objetivo genérico de segurança do sensor de movimentos, definido no apêndice 10 do presente anexo. Em vez disso, aplicam-se-lhe os requisitos de segurança especificados no ponto 4.4 do presente apêndice.

3. REQUISITOS APLICÁVEIS AO APARELHO DE CONTROLO QUANDO ESTÁ INSTALADO UM ADAPTADOR

Neste capítulo e nos seguintes, explicam-se os requisitos do presente anexo quando é utilizado um adaptador. Os números dos requisitos do anexo IC figuram entre parêntesis retos.

ADA_005 O aparelho de controlo de um veículo equipado com adaptador deve cumprir integralmente o disposto no presente anexo, salvo indicação em contrário neste apêndice.

ADA_006 Quando é instalado um adaptador, o aparelho de controlo inclui os cabos, o adaptador (incluindo um sensor de movimentos) e uma VU [01].

ADA_007 A função de deteção de incidentes e/ou falhas do aparelho de controlo é alterada nos seguintes termos:

— O incidente «interrupção da alimentação energética» é desencadeado pela VU, fora do modo de calibração, no caso de uma interrupção superior a 200 milésimos de segundo na alimentação elétrica do sensor de movimentos incorporado [79]

▼B

— O incidente «erro nos dados de movimento» é desencadeado pela VU em caso de interrupção no fluxo normal de dados entre o sensor de movimentos incorporado e a VU e/ou em caso de erro na integridade ou na autenticação de dados durante o intercâmbio destes entre o sensor de movimentos incorporado e a VU [83]

— O incidente «tentativa de violação da segurança» é desencadeado pela VU na eventualidade de qualquer outro incidente que afete a segurança do sensor de movimentos incorporado, fora do modo de calibração [85]

— A «falha do aparelho de controlo» é desencadeada pela VU, fora do modo de calibração, na eventualidade de qualquer falha do sensor de movimentos incorporado [88].

ADA_008 As falhas do adaptador detetáveis pelo aparelho de controlo são as relacionadas com o sensor de movimentos incorporado [88].

ADA_009 A função de calibração da VU deve permitir emparelhar automaticamente o sensor de movimentos incorporado e a VU [202, 204].

4. REQUISITOS DE CONSTRUÇÃO E FUNCIONAMENTO DO ADAPTADOR

4.1. **Estabelecer uma interface com os impulsos de entrada de velocidade e adaptá-los**

ADA_011 A interface do adaptador para entrada de dados deve aceitar impulsos de frequência representativos da velocidade de circulação do veículo e da distância por ele percorrida. Características elétricas dos impulsos de entrada: *A definir pelo fabricante*. A interface correta dos dados do adaptador para o veículo, se for caso disso, será viabilizada por ajustamentos acessíveis apenas ao fabricante do adaptador e à oficina homologada que o instala.

ADA_012 Se for caso disso, a interface dos dados do adaptador deve poder multiplicar ou dividir os impulsos de frequência de entrada da velocidade por um fator fixo, para adaptar o sinal a um valor na gama do fator k definida pelo presente anexo (4 000 a 25 000 impulsos/km). Esse fator fixo só pode ser programado pelo fabricante do adaptador e pela oficina homologada que o instala.

4.2. **Induzir os impulsos de entrada no sensor de movimentos incorporado**

ADA_013 Os impulsos de entrada, eventualmente adaptados conforme atrás se especificou, são induzidos no sensor de movimentos incorporado, de modo a que cada impulso de entrada seja detetado pelo sensor.

4.3. **Sensor de movimentos incorporado**

ADA_014 O sensor de movimentos incorporado deve ser estimulado pelos impulsos induzidos, podendo assim gerar dados que representam com precisão o movimento do veículo, como se tivesse uma interface mecânica com uma parte móvel do veículo.

ADA_015 Para identificar o adaptador, a VU deve utilizar os dados de identificação do sensor de movimentos incorporado [95].

▼B

ADA_016 Os dados da instalação armazenados no sensor de movimentos incorporado devem ser considerados como representando os dados da instalação do adaptador [122].

4.4. **Requisitos de segurança**

ADA_017 A caixa do adaptador deve ser projetada de modo a impossibilitar a sua abertura. Deve ser selada, de modo a permitir detetar facilmente tentativas de fraude física (por exemplo, através de inspeção visual — ver ADA_035). Os selos devem cumprir os mesmos requisitos dos selos dos sensores de movimentos [398 a 406].

ADA_018 Deve ser impossível remover do adaptador o sensor de movimentos incorporado sem quebrar o(s) selo(s) da caixa do adaptador ou o selo entre o sensor e a caixa do adaptador (ver ADA_034).

ADA_019 O adaptador deve assegurar que os dados de movimento só possam ser processados e derivados a partir dos dados de entrada do adaptador.

4.5. **Características de desempenho**

ADA_020 O adaptador deve ser plenamente funcional no intervalo de temperatura definido pelo fabricante.

ADA_021 O adaptador deve ser plenamente funcional no intervalo de humidade de 10 % a 90 % [214].

ADA_022 O adaptador deve ser protegido contra sobretensão elétrica, inversão da polaridade da sua fonte de alimentação e curtos-circuitos [216].

ADA_023 O adaptador deve ainda:

— reagir a um campo magnético que perturbe a deteção do movimento do veículo; nessas circunstâncias, a unidade-veículo regista e memoriza falhas do sensor [88]

— ou dispor de um elemento de deteção que esteja protegido contra campos magnéticos ou lhes seja imune [217].

ADA_024 O adaptador deve cumprir o disposto na regulamentação internacional ONU ECE R10, relativa à compatibilidade eletromagnética, e deve ser protegido contra descargas eletrostáticas e contra transitórios [218].

4.6. **Materiais**

ADA_025 O adaptador deve atingir o grau de proteção *(a determinar pelo fabricante, dependendo da posição da instalação)* [220, 221].

ADA_026 A caixa do adaptador deve ser de cor amarela.

4.7. **Marcações**

ADA_027 Ao adaptador deve ser afixada uma placa descritiva, com os seguintes elementos:

— nome e endereço do fabricante do adaptador

— número dado pelo fabricante e ano de fabrico do adaptador

— marca de homologação do tipo do adaptador ou do tipo do aparelho de controlo, incluindo o adaptador

— data de instalação do adaptador

▼B

— número de identificação do veículo no qual foi instalado o adaptador.

ADA_028 A placa descritiva deve também indicar os seguintes elementos (se não forem legíveis do exterior no sensor de movimentos incorporado):

— nome do fabricante do sensor de movimentos incorporado

— número dado pelo fabricante e ano de fabrico do sensor de movimentos incorporado

— marca de homologação do sensor de movimentos incorporado.

5. INSTALAÇÃO DO APARELHO DE CONTROLO QUANDO É UTILIZADO UM ADAPTADOR

5.1. **Instalação**

ADA_029 Os adaptadores só podem ser instalados por fabricantes de veículos ou por oficinas homologadas, autorizadas a instalar, ativar e calibrar tacógrafos digitais e tacógrafos inteligentes.

ADA_030 A oficina homologada que instala o adaptador ajusta a interface de entrada de dados e seleciona o fator de divisão do sinal de entrada (se for caso disso).

ADA_031 A oficina homologada que instala o adaptador sela a caixa do adaptador.

ADA_032 O adaptador deve ser colocado o mais próximo possível da parte do veículo que fornece os impulsos de entrada.

ADA_033 Os cabos que fornecem energia elétrica ao adaptador devem ser de cor vermelha (polo positivo) e negra (terra).

5.2. **Selagem**

ADA_034 Requisitos aplicáveis à selagem:

— a caixa do adaptador deve ser selada (ver ADA_017)

— a caixa do sensor incorporado deve ser selada à caixa do adaptador, a menos que seja impossível remover o sensor sem quebrar o(s) selo(s) da caixa do adaptador (ver ADA_018)

— a caixa do adaptador deve ser selada ao veículo

— a ligação entre o adaptador e o equipamento que fornece os seus impulsos de entrada deve ser selada em ambos os extremos (na medida do razoavelmente possível).

6. VERIFICAÇÕES, INSPEÇÕES E REPARAÇÕES

6.1. **Controlos periódicos**

ADA_035 Quando se utiliza um adaptador, cada inspeção periódica do aparelho de controlo (entendendo-se por inspeções periódicas as que cumprem os requisitos [409] a [413] do anexo 1C) deve incluir as seguintes verificações:

— se o adaptador exibe a devida marca de homologação de tipo

— se estão intactos os selos colocados no adaptador e nas suas ligações

▼B

— se o adaptador foi instalado conforme indica a placa de instalação

— se o adaptador foi instalado conforme a especificação do técnico responsável e/ou do fabricante do veículo

— se é autorizada a montagem de um adaptador no veículo inspecionado.

ADA_036 Estas inspeções devem incluir a calibração e a substituição de todos os selos, qualquer que seja o seu estado.

7. HOMOLOGAÇÃO DE TIPO DO APARELHO DE CONTROLO QUANDO É UTILIZADO UM ADAPTADOR

7.1. **Aspetos gerais**

ADA_037 Quando for sujeito à homologação de tipo, o aparelho de controlo deve estar completo, com o adaptador [425].

ADA_038 Qualquer adaptador pode ser sujeito a homologação de tipo autonomamente ou como componente de um aparelho de controlo.

ADA_039 Esta homologação de tipo deve incluir ensaios de funcionalidade que envolvam o adaptador. Os resultados positivos de cada um destes ensaios devem ser declarados por certificados correspondentes [426].

7.2. **Certificado de funcionalidade**

ADA_040 Ao fabricante só será passado o certificado de funcionalidade do adaptador ou do aparelho de controlo que inclui adaptador se tiverem êxito os seguintes ensaios de funcionalidade mínimos:

N.º	Ensaio	Descrição	Requisitos correlatos
1.	**Exame administrativo**		
1.1	Documentação	Adequação da documentação do adaptador	
2.	**Inspeção visual**		
2.1.	Conformidade do adaptador com a documentação		
2.2.	Identificação/marcações do adaptador		ADA_027, ADA_028
2.3	Materiais do adaptador		[219] a [223] ADA_026
2.4.	Selagem		ADA_017, ADA_018, ADA_034
3.	**Ensaios de funcionalidade**		
3.1	Indução dos impulsos de velocidade no sensor de movimentos incorporado		ADA_013

▼B

N.º	Ensaio	Descrição	Requisitos correlatos
3.2	Estabelecer uma interface com os impulsos de entrada de velocidade e adaptá-los		ADA_011, ADA_012
3.3	Precisão da medição de movimentos		[30] a [35], [217]
4.	**Ensaios ambientais**		
4.1	Resultados dos ensaios do fabricante	Resultados dos ensaios ambientais do fabricante	ADA_020, ADA_021, ADA_022, ADA_024
5.	**Ensaios de compatibilidade eletromagnética**		
5.1	Emissões radiadas e suscetibilidade	Verificação da conformidade com a Diretiva 2006/28/ /CE	ADA_024
5.2	Resultados dos ensaios do fabricante	Resultados dos ensaios ambientais do fabricante	ADA_024

▼C1

ANEXO II

MARCA E CERTIFICADO DE HOMOLOGAÇÃO

I. MARCA DE HOMOLOGAÇÃO

1. Composição da marca de homologação:

a) um retângulo, no interior do qual se coloca a letra «e», seguida de uma letra ou de um número distintivo do país que tenha concedido a homologação, segundo as seguintes convenções:

Bélgica	6
Bulgária	34
República Checa	8
Dinamarca	18
Alemanha	1
Estónia	29
Irlanda	24
Grécia	23
Espanha	9
França	2
Croácia	25
Itália	3
Chipre	CY
Letónia	32
Lituânia	36
Luxemburgo	13
Hungria	7
Malta	MT
Países Baixos	4
Áustria	12
Polónia	20
Portugal	21
Roménia	19
Eslovénia	26
Eslováquia	27
Finlândia	17
Suécia	5
Reino Unido	11

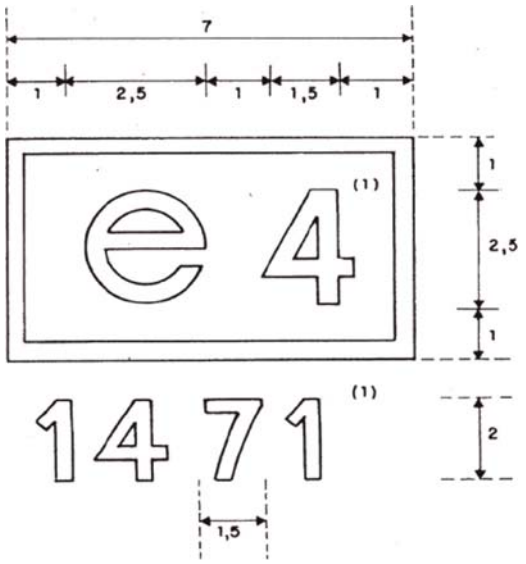
e

b) o número de homologação, correspondente ao número do certificado de homologação atribuído ao protótipo do aparelho de controlo ou à folha de registo ou correspondente ao número do cartão tacográfico, colocado na proximidade daquele retângulo.

▼C1

2. A marca de homologação é aposta na chapa sinalética de cada aparelho, em cada folha de registo e em cada cartão tacográfico. Deve ser indelével e conservar-se sempre bem legível.

3. As dimensões da marca de homologação, a seguir representada graficamente ([1]), são expressas em milímetros. Trata-se de dimensões mínimas. A relação de proporcionalidade entre as dimensões deve ser respeitada.



([1]) Valores meramente a título de orientação.

▼C1

II. CERTIFICADO DE HOMOLOGAÇÃO PARA TACÓGRAFOS ANALÓGICOS

O Estado-Membro que tiver procedido a uma homologação deve conceder ao requerente um certificado de homologação, conforme o modelo a seguir indicado. Para informar outros Estados-Membros das homologações concedidas ou eventualmente revogadas, os Estados-Membros devem utilizar cópias do certificado.

CERTIFICADO DE HOMOLOGAÇÃO

Nome da autoridade competente .....

Comunicação referente a ([1]):

— homologação de um modelo de aparelho de controlo

— revogação da homologação de um modelo de aparelho de controlo

— homologação de um modelo de folha de registo

— revogação da homologação de um modelo de folha de registo

N.º de homologação:

.....

1. Marca de fabrico ou comercial .....

2. Denominação do modelo .....

3. Nome do fabricante .....

4. Endereço do fabricante .....

5. Data da apresentação para homologação .....

6. Laboratório de ensaios .....

7. Data e número de ensaios .....

8. Data da homologação .....

9. Data da revogação da homologação .....

10. Modelo(s) de aparelho(s) de controlo no(s) qual(is) a folha se destina a ser utilizada

11. Lugar .....

12. Data .....

13. Documentos descritivos em anexo .....

14. Observações (incluindo a posição dos selos, se for caso disso)

(assinatura)

([1]) Riscar o que não interessa.

▼C1

III. CERTIFICADO DE HOMOLOGAÇÃO PARA TACÓGRAFOS DIGITAIS

O Estado-Membro que tiver procedido a uma homologação deve conceder ao requerente um certificado de homologação, conforme o modelo a seguir indicado. Para informar outros Estados-Membros das homologações concedidas ou eventualmente revogadas, os Estados-Membros devem utilizar cópias do certificado.

CERTIFICADO DE HOMOLOGAÇÃO PARA TACÓGRAFOS DIGITAIS

Nome da autoridade competente .....

Comunicação referente a ([1]):

☐ homologação de: ☐ revogação da homologação de:

☐ modelo de aparelho de controlo

☐ componente de aparelho de controlo ([2])

☐ cartão de condutor

☐ cartão de oficina

☐ cartão de empresa

☐ cartão de controlador

N.º de homologação:

.....

1. Marca de fabrico ou marca comercial .....
2. Nome do modelo .....
3. Nome do fabricante .....
4. Endereço do fabricante .....
5. Data da apresentação para homologação .....
6. Laboratório(s) .....
7. Data e número do relatório de ensaio .....
8. Data da homologação .....
9. Data da revogação da homologação .....
10. Modelo de aparelho(s) de controlo no(s) qual(is) o componente se destina a ser utilizado
11. Lugar .....
12. Data .....
13. Documentos descritivos em anexo .....
14. Observações (incluindo a posição dos selos, se for caso disso)

(assinatura)

([1]) Assinalar os quadrados pertinentes.
([2]) Especificar o componente a que se refere a comunicação.

▼C1

IV. CERTIFICADO DE HOMOLOGAÇÃO PARA TACÓGRAFOS INTELIGENTES

O Estado-Membro que tiver procedido a uma homologação deve conceder ao requerente um certificado de homologação, conforme o modelo a seguir indicado. Para informar outros Estados-Membros das homologações concedidas ou eventualmente revogadas, os Estados-Membros devem utilizar cópias do certificado.

CERTIFICADO DE HOMOLOGAÇÃO PARA TACÓGRAFOS INTELIGENTES

Nome da autoridade competente .....

Comunicação referente a ([1]):

☐ homologação de: ☐ revogação da homologação de:

☐ modelo de aparelho de controlo

☐ componente de aparelho de controlo ([2])

☐ cartão de condutor

☐ cartão de oficina

☐ cartão de empresa

☐ cartão de controlador

N.º de homologação:

.....

1. Marca de fabrico ou marca comercial .....
2. Nome do modelo .....
3. Nome do fabricante .....
4. Endereço do fabricante .....
5. Data da apresentação para homologação .....
6. a) Laboratório de ensaio para certificação de funcionalidade .....
   b) Laboratório de ensaio para certificação de segurança .....
   c) Laboratório de ensaio para certificação de interoperabilidade .....
7. a) Data e número do certificado de funcionalidade .....
   b) Data e número de certificado de segurança … .....
8. Data da homologação .....
9. Data da revogação da homologação .....
10. Modelo de aparelho(s) de controlo no(s) qual(is) o componente se destina a ser utilizado
11. Lugar .....
12. Data .....
13. Documentos descritivos em anexo .....
14. Observações (incluindo a posição dos selos, se for caso disso)

(assinatura)

([1]) Assinalar os quadrados pertinentes.
([2]) Especificar o componente a que se refere a comunicação.