

II

(Actos preparatórios)

COMISSÃO

Proposta de regulamento do Conselho que adapta pela sétima 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

(2002/C 126 E/01)

(Texto relevante para efeitos do EEE)

COM(2001) 698 final

(Apresentada pela Comissão em 30 de Novembro de 2001)

A COMISSÃO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado que institui a Comunidade Europeia,

Tendo em conta o 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 ⁽¹⁾, com a última redacção que lhe foi dada pelo Regulamento (CE) n.º 2135/98 ⁽²⁾, nomeadamente os seus artigos 17.º e 18.º,

Considerando o seguinte:

- (1) As especificações técnicas do anexo IB do Regulamento (CEE) n.º 3821/85 devem ser adaptadas ao progresso técnico, com particular atenção à segurança geral do sistema e à interoperabilidade entre o aparelho de controlo e os cartões de condutor.
- (2) A adaptação do aparelho requer igualmente uma adaptação do anexo II do Regulamento (CEE) n.º 3821/85, que define as marcas e os certificados de homologação.
- (3) O comité instituído pelo artigo 18.º do Regulamento (CE) n.º 3821/85 não emitiu parecer sobre as medidas constantes da proposta.
- (4) Em conformidade com o disposto no artigo 18.º, n.º 5, alínea b), a Comissão submete sem demora ao Conselho uma proposta sobre as disposições a tomar,

ADOPTOU O PRESENTE REGULAMENTO:

Artigo 1.º

O anexo do Regulamento (CE) n.º 2135/98 é substituído pelo anexo do presente regulamento.

Artigo 2.º

O anexo II do Regulamento (CEE) n.º 3821/85 é alterado do seguinte modo:

1. No capítulo I, n.º 1, o primeiro parágrafo é alterado do seguinte modo:
 - símbolo convencional «GR» relativo à Grécia é substituído por «23»;
 - símbolo convencional «IRL» relativo à Irlanda é substituído por «24»;
 - símbolo convencional «12» é acrescentado relativamente à Áustria;
 - símbolo convencional «17» é acrescentado relativamente à Finlândia;
 - símbolo convencional «5» é acrescentado relativamente à Suécia.
2. No capítulo I, n.º 1, o segundo parágrafo é alterado do seguinte modo:
 - A seguir a «folha», é inserida a expressão «ou do cartão tacográfico».
3. No capítulo I, o n.º 2 é alterado do seguinte modo:
 - A seguir a «folha de registo», é inserida a expressão «e em cada cartão tacográfico».
4. No capítulo II, é acrescentada ao título a expressão «PARA PRODUTOS CONFORMES AO ANEXO I».

⁽¹⁾ JO L 370 de 31.12.1985, p. 8.

⁽²⁾ JO L 274 de 9.10.1998, p. 1.

5. É aditado o seguinte capítulo III:

«III. CERTIFICADO DE HOMOLOGAÇÃO PARA PRODUTOS CONFORMES AO ANEXO I B

O Estado que tenha procedido a uma homologação concede ao requerente um certificado de homologação conforme ao modelo a seguir indicado. Para informar os outros Estados-Membros das homologações concedidas ou eventualmente revogadas, cada Estado-Membro utilizará cópias desse certificado.

CERTIFICADO DE HOMOLOGAÇÃO PARA PRODUTOS CONFORMES AO ANEXO I B

Designação do serviço competente:

Notificação relativa a (*):

- Homologação de
- Revogação da homologação de
- Modelo de aparelho de controlo
- Componente de aparelho de controlo (**)
- cartão de condutor
- cartão de oficina
- cartão de empresa
- cartão de controlador

Homologação n.º

1. Marca de fabrico ou marca comercial:
2. Nome do modelo:
3. Nome do fabricante:
4. Endereço do fabricante:
5. Apresentado para homologação para:
6. Laboratório(s):
7. Data e número do(s) ensaio(s):
8. Data da homologação:
9. Data da revogação da homologação:
10. Modelo com o qual o componente do aparelho de controlo se destina a ser utilizado:
11. Local:
12. Data:
13. Documentação descritiva anexa:

14. Observações (incluindo eventual oposição de carimbos)

.....
(assinatura)

(*) Assinalar a casa correspondente.

(**) Especificar o componente de que a notificação trata»

Artigo 3.º

O presente regulamento entra em vigor no vigésimo dia seguinte ao da sua publicação no *Jornal Oficial das Comunidades Europeias*.

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

ANEXO**«ANEXO I (B)****REQUISITOS DE CONSTRUÇÃO, DE ENSAIO, DE INSTALAÇÃO E DE INSPECÇÃO**

Numa preocupação de preservar a interoperabilidade (le terme "interoperacionalidade" existe aussi mais s'applique surtout à la radio-communication) dos suportes lógicos dos equipamentos definidos no presente anexo, determinadas siglas, termos ou expressões de programação informática foram mantidos no idioma original de redacção do texto, nomeadamente a língua inglesa. Algumas traduções literais foram no entanto incorporadas entre parênteses para mais informações sobre algumas dessas expressões, na mira de facilitar a compreensão.

I. DEFINIÇÕES

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

a) "Activação"

Fase no decurso da qual o aparelho de controlo se torna plenamente operacional e executa todas as funções, incluindo as de segurança.

A activação de um aparelho de controlo é feita por intermédio de um cartão de centro de ensaio, com introdução do correspondente código de identificação (PIN code).

b) "Autenticação"

Função destinada a estabelecer e verificar uma identidade alegada.

c) "Autenticidade"

Facto de determinada informação provir de uma parte cuja identidade pode ser verificada.

d) "Ensaio incorporado (BIT)"

Ensaio realizado a pedido. É accionado por efeito do operador ou de um mecanismo externo.

e) "Dia"

Um dia, das 0 às 24 horas. Todos os dias se reportam à hora UTC (hora universal coordenada).

f) "Calibração"

Actualização ou confirmação dos parâmetros do veículo a guardar na memória de dados e que compreendem a identificação (NIV, VRN e Estado-Membro de matrícula) e as características do veículo (w, k, l, medida do pneumático, ponto de regulação do eventual dispositivo de limitação da velocidade, UTC (hora universal coordenada no momento) e valor odométrico no momento.

A calibração de um aparelho de controlo é feita por intermédio de um cartão de centro de ensaio.

g) "Número do cartão"

Conjunto de 16 caracteres alfanuméricos que identificam inequivocamente um cartão tacográfico dentro de um Estado-Membro. O número do cartão inclui índice de série (eventual), índice de substituição e índice de renovação.

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

h) "Índice de série do cartão"

14.º carácter alfanumérico do número do cartão, destinado a distinguir os diversos cartões tacográficos atribuídos a um organismo ou a uma empresa que tenham direito a mais do que um. O organismo ou a empresa são identificados inequivocamente pelos primeiros 13 caracteres do número do cartão.

- i) **“Índice de renovação do cartão”**
- 16.º carácter alfanumérico do número do cartão tacográfico. Sobe uma unidade cada vez que o cartão é renovado.
- j) **“Índice de substituição do cartão”**
- 15.º carácter alfanumérico do número do cartão tacográfico. Sobe uma unidade cada vez que o cartão é substituído.
- k) **“Coeficiente característico do veículo”**
- Número indicativo do valor do sinal de saída emitido pela peça do veículo que faz a ligação entre ele e o aparelho de controlo (eixo ou veio de saída da caixa de velocidades), quando o veículo percorre a distância de 1 km medida nas condições normais de ensaio (ver secção VI.5). O coeficiente característico é expresso em impulsos por quilómetro ($w = \dots \text{imp/km}$).
- l) **“Cartão de empresa”**
- Cartão tacográfico emitido pelas autoridades de um Estado-Membro ao proprietário ou titular de um veículo equipado com aparelho de controlo.
- Este cartão identifica a empresa e permite visualizar, descarregar ou imprimir os dados que a empresa memorizou no aparelho de controlo por ela bloqueado.*
- m) **“Constante do aparelho de controlo”**
- Número indicativo do valor do sinal de entrada necessário para obter a indicação e o registo de uma distância percorrida de 1 km. Esta constante é expressa em impulsos por quilómetro ($k = \dots \text{imp/km}$).
- n) **“Tempo de condução contínua”⁽¹⁾**
- Somatório (calculado pelo aparelho de controlo) dos tempos de condução acumulados por um condutor desde o final da sua última AVAILABILITY (disponibilidade) ou BREAK/REST (pausa/repouso) ou desde o final do último período UNKNOWN (desconhecido)⁽²⁾ de 45 minutos ou mais (este pode ter sido cindido em vários períodos de 15 minutos ou mais). Os cálculos têm em conta, conforme necessário, actividades 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 ranhura.
- o) **“Cartão de controlador ou de controlo”**
- Cartão tacográfico emitido pelas autoridades de um Estado-Membro a uma autoridade nacional responsável pelo controlo.
- Este cartão identifica o organismo e, possivelmente, a pessoa responsável pelo controlo e permite acesso aos dados registados na memória ou nos cartões de condutor, para leitura, impressão e/ou descarregamento.*
- p) **“Tempo de pausa acumulado”⁽¹⁾**
- As pausas acumuladas no tempo de condução de um condutor são calculadas pelo aparelho de controlo como o somatório dos tempos de AVAILABILITY (disponibilidade), BREAK/REST (pausa/repouso) ou períodos UNKNOWN (desconhecidos)⁽²⁾ de 45 minutos ou mais, desde o final da sua última AVAILABILITY ou BREAK/REST ou desde o final do último período UNKNOWN⁽²⁾ de 45 minutos ou mais (este pode ter sido cindido em vários períodos de 15 minutos ou mais).
- Os cálculos têm em conta, conforme necessário, actividades 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.
- 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 electrónico de memorização de dados, incorporado no aparelho de controlo.

⁽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.

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

- r) **“Assinatura digital”**
- Dados apensos a um bloco de dados (ou transformação criptográfica do mesmo), os quais permitem ao receptor comprovar a autenticidade e a integridade do bloco.
- s) **“Descarregamento”**
- Cópia (conjuntamente com assinatura digital) de uma parte ou de um conjunto completo de dados memorizados na memória do veículo ou na memória do cartão de condutor.
- O descarregamento pode não alterar ou apagar dados memorizados.*
- t) **“Cartão de condutor”**
- Cartão tacográfico atribuído pelas autoridades de um Estado-Membro a um determinado condutor.
- Este cartão identifica o condutor e permite a memorização dos dados relativos às suas actividades.*
- u) **“Perímetro efectivo dos pneumáticos das rodas”**
- Média das distâncias percorridas por cada uma das rodas que fazem mover o veículo (rodas motoras) numa rotação completa. A medição destas distâncias deve ser feita nas condições normais de ensaio (ver secção VI.5) 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 devem ser aprovados por uma autoridade nacional competente.
- v) **“Incidente”**
- Operação anormal detectada pelo aparelho de controlo e que pode ter origem numa tentativa de fraude.
- w) **“Falha”**
- Operação anormal detectada pelo aparelho de controlo e que pode ter origem numa deficiência ou avaria do mesmo.
- x) **“Instalação”**
- Montagem do aparelho de controlo num veículo.
- y) **“Sensor de movimentos”**
- Peça do aparelho de controlo que emite um sinal representativo da velocidade do veículo e/ou da distância percorrida.
- z) **“Cartão não-válido”**
- Cartão no qual foi detectada uma falha, cuja autenticação inicial falhou, cuja data de início da validade não foi ainda alcançada ou cuja data de caducidade foi já ultrapassada.
- aa) **“Fora de âmbito”**
- Situação em que não é exigível a utilização do aparelho de controlo, nos termos do Regulamento (CEE) n.º 3820/85 do Conselho.
- bb) **“Excesso de velocidade”**
- 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 Directiva 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 ⁽²⁾.
- cc) **“Inspeção periódica”**
- Conjunto de operações destinadas a verificar se o aparelho de controlo funciona correctamente e se as suas características de regulação correspondem efectivamente aos parâmetros do veículo.

⁽¹⁾ Directiva 97/27/CE do Parlamento Europeu e do Conselho, de 22 Julho de 1997, relativa às massas e dimensões de determinadas categorias de veículos a motor e seus reboques e que altera a Directiva 70/156/CEE (JO L 233 de 25.8.1997, p. 1).

⁽²⁾ JO L 57 de 2.3.1992, p. 27.

- dd) **“Impressora”**
- Componente do aparelho de controlo que exhibe sob forma impressa os dados memorizados.
- ee) **“Aparelho de controlo”**
- Equipamento completo destinado a ser instalado a bordo dos veículos rodoviários para indicação, registo e memorização automáticos ou semi-automáticos dos dados sobre a marcha desses veículos, assim como sobre certos períodos de trabalho dos condutores.
- ff) **“Renovação”**
- Emissão de um novo cartão tacográfico quando o existente atinge a data de expiração da validade ou acusa defeito e é devolvido à autoridade emissora. A renovação implica sempre a certeza de não coexistirem dois cartões válidos.
- gg) **“Reparação”**
- Reparação de um sensor de movimentos ou de uma unidade-veículo, exigindo que se desligue a fonte de alimentação energética ou outros componentes do aparelho de controlo ou que se abra esse sensor ou essa unidade.
- hh) **“Substituição”**
- 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.
- ii) **“Certificação de segurança”**
- Processo destinado a certificar, por um organismo ITSEC ⁽¹⁾, se o aparelho (ou o componente) de controlo ou o cartão tacográfico em investigação cumprem os requisitos de segurança definidos no apêndice 10 (Objectivos Gerais de Segurança).
- jj) **“Auto-ensaio”**
- Ensaio realizado cíclica e automaticamente pelo aparelho de controlo, com vista a detectar falhas.
- kk) **“Cartão tacográfico”**
- Cartão inteligente destinado a ser utilizado com o aparelho de controlo, ao qual permite determinar a identidade (ou o grupo identificativo) do titular, bem como a transferência e a memorização de dados. Um cartão tacográfico pode pertencer a uma das seguintes categorias:
- cartão de condutor
 - cartão de controlador
 - cartão de centro de ensaio
 - cartão de empresa.
- ll) **“Homologação de tipo”**
- Processo destinado a certificar, por um Estado-Membro, se o aparelho (ou o componente) de controlo ou o cartão tacográfico em investigação cumprem o disposto no presente regulamento.
- mm) **“Medida do pneumático”**
- Designação das dimensões dos pneumáticos (rodas motoras externas), em conformidade com a Directiva 92/23/CEE ⁽²⁾.
- nn) **“Identificação do veículo”**
- Números identificativos: número de matrícula do veículo (VRN), com indicação do Estado-Membro de matrícula, e número de identificação do veículo (NIV) ⁽³⁾.

⁽¹⁾ Recomendação 95/144/CE do Conselho, de 7 de Abril de 1995, relativa a critérios comuns de avaliação da segurança nas tecnologias da informação (JO L 93 de 26.4.1995, p. 27)

⁽²⁾ JO L 129 de 14.5.1992, p. 95.

⁽³⁾ Directiva 76/114/CEE de 18.12.1975 (JO L 24 de 30.1.1976, p. 1)

oo) “Unidade-veículo (VU)”

Aparelho de controlo, excluindo o sensor de movimentos e os cabos que o ligam. A unidade pode ser única ou consistir em diversas unidades distribuídas pelo veículo, sem prejuízo de cumprir os requisitos de segurança do presente regulamento.

pp) “Semana”

Intervalo utilizado pelo aparelho de controlo nos cálculos e que vai das 00h00 UTC de segunda-feira às 24h00 UTC de sábado.

qq) “Cartão de centro de ensaio”

Cartão tacográfico emitido pelas autoridades de um Estado-Membro ao fabricante ou instalador de um aparelho de controlo, ao fabricante do veículo ou ao centro de ensaio, homologados por esse Estado-Membro.

Este cartão identifica o titular e permite o ensaio, a calibração e/ou o descarregamento do aparelho de controlo.

II. CARACTERÍSTICAS GERAIS E FUNÇÕES DO APARELHO DE CONTROLO

000 Os veículos equipados com aparelhos de controlo que cumpram o disposto no presente anexo devem ter as funções de visualização da velocidade e de odómetro incorporadas no aparelho de controlo.

1. Características gerais

O aparelho de controlo tem por função registar, memorizar, exibir, imprimir e transmitir (ou dar saída a) os dados relativos às actividades do condutor.

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

002 A unidade-veículo inclui uma unidade de processamento, uma memória de dados, um relógio de tempo real, duas interfaces para cartões inteligentes (condutor e ajudante), uma impressora, um visor (ecrã de visualização), um alerta visual, um conector de calibração/d Descarregamento e os instrumentos para a introdução de dados por parte do utilizador.

O aparelho de controlo pode ser ligado a outros dispositivos por intermédio de conectores adicionais.

003 A inclusão de funções ou dispositivos, homologados ou não, no aparelho de controlo, ou a sua ligação a ele, não devem interferir, real ou potencialmente, com o seu funcionamento correcto nem com o disposto no regulamento.

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

004 O aparelho de controlo proporciona direitos de acesso selectivo 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 e em cartões tacográficos.

Este processo cumpre o disposto na Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados ⁽¹⁾.

2. Funções

005 O aparelho de controlo deve assegurar as seguintes funções:

- controlo da inserção e da retirada de cartões
- medição de velocidades e distâncias
- medição do tempo
- controlo das actividades do condutor
- controlo da situação de condução

⁽¹⁾ JO L 281 de 23.11.1995, p. 31.

- entradas efectuadas manualmente pelo condutor:
 - introdução do lugar de início e/ou final do período diário de trabalho
 - introdução manual das actividades do condutor
 - introdução de condições especiais
- gestão dos bloqueamentos da empresa
- vigilância das actividades de controlo
- detecção de incidentes e/ou falhas
- ensaios incorporados e auto-ensaios
- 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 de dados
- avisos ou alertas
- descarregamento de dados para meios externos
- transmissão (saída) de dados para dispositivos externos adicionais
- calibração
- ajustamento do tempo.

3. Modos de funcionamento

006 O aparelho de controlo deve possuir quatro modos de funcionamento:

- modo de operação
- modo de controlo
- modo de calibração
- modo de empresa.

007 O aparelho de controlo deve passar para os seguintes modos de funcionamento consoante os cartões tacográficos válidos inseridos nas correspondentes interfaces:

Modo de funcionamento		Ranhura do condutor				
		Cartão ausente	Cartão de condutor	Cartão de controlo	Cartão de centro de ensaio	Cartão de empresa
Ranhura do ajudante	Cartão ausente	Modo de operação	Modo de operação	Modo de controlo	Modo de calibração	Modo de empresa
	Cartão de condutor	Modo de operação	Modo de operação	Modo de controlo	Modo de calibração	Modo de empresa
	Cartão de controlo	Modo de controlo	Modo de controlo	Modo de controlo (*)	Modo de operação	Modo de operação
	Cartão de centro de ensaio	Modo de calibração	Modo de calibração	Modo de operação	Modo de calibração (*)	Modo de operação
	Cartão de empresa	Modo de empresa	Modo de empresa	Modo de operação	Modo de operação	Modo de empresa (*)

008

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

- 009 O aparelho de controlo ignora cartões não-válidos inseridos, a menos que seja possível visualizar, imprimir ou descarregar dados constantes de um cartão expirado.
- 010 Todas as funções enunciadas na secção II.22 devem ser operacionais em qualquer modo de funcionamento, com as seguintes excepções:
- a função de calibração é acessível unicamente em modo de calibração
 - a função de ajustamento do tempo é limitada quando não em modo de calibração
 - as funções de introdução manual pelo condutor são acessíveis unicamente em modo de operação ou de calibração
 - a função de gestão dos bloqueamentos da empresa é acessível unicamente em modo de empresa
 - a função de vigilância das actividades de controlo é operacional unicamente em modo de controlo
 - a função de descarregamento não é acessível em modo de operação (com excepção do previsto no requisito 150).
- 011 O aparelho de controlo pode transmitir (dar saída a) quaisquer dados para o visor, para a impressora ou para interfaces externas, com as seguintes excepções:
- em modo de operação, 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 caracteres discordantes (da esquerda para a direita)
 - em modo de empresa, a saída dos dados relativos ao condutor (requisitos 081, 084 e 087) só pode concretizar-se se se tratar de períodos não bloqueados por outra empresa (identificada pelos primeiros 13 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 8 dias anteriores.

4. Segurança

O dispositivo de segurança do sistema visa proteger a memória contra acesso e manipulação não autorizados dos dados, bem como detectar tentativas nesse sentido, proteger a integridade e a autenticidade dos dados intercambiados entre o sensor de movimentos e a unidade-veículo ou entre o aparelho de controlo e os cartões tacográficos e verificar a integridade e a autenticidade dos dados descarregados.

- 012 Para efeitos da segurança do sistema, o aparelho de controlo deve cumprir os requisitos especificados nos objectivos gerais de segurança do sensor de movimentos e da unidade-veículo (apêndice 10).

III. REQUISITOS DE CONSTRUÇÃO E DE FUNCIONAMENTO DO APARELHO DE CONTROLO

1. Controlo da inserção e da retirada de cartões

- 013 O aparelho de controlo controla as interfaces dos cartões, para detectar as inserções e retiradas dos mesmos.
- 014 O aparelho de controlo detecta se um cartão inserido é cartão tacográfico válido e, nessa eventualidade, identifica o tipo do cartão.
- 015 O aparelho de controlo deve ser concebido de modo a que os cartões tacográficos fiquem em posição fixa quando inseridos correctamente nas correspondentes interfaces.
- 016 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 acção positiva do utilizador.

2. Medição da velocidade e da distância

- 017 Esta função mede e fornece continuamente o valor odométrico correspondente à distância total percorrida pelo veículo.
- 018 Esta função deve medir e fornecer continuamente a velocidade do veículo.

019 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 detecta mais de 1 imp/seg durante pelo menos 5 segundos — caso contrário, o veículo é considerado parado.

Os dispositivos que exibem a velocidade (velocímetro) e a distância total (odómetro), 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).

2.1. *Medição da distância percorrida*

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

- acumulando quer os movimentos de avanço quer os de recuo,
- incluindo somente os movimentos de avanço.

021 O aparelho de controlo deve medir a distância de 0 a 9 999 999,9 km.

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

- $\pm 1\%$ antes da instalação
- $\pm 2\%$ durante a instalação e a inspecção periódica
- $\pm 4\%$ durante utilização.

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

2.2. *Medição da velocidade*

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

025 Para garantir uma tolerância máxima de ± 6 km/h na velocidade medida durante 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 efectuadas durante a instalação e a inspecção 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 uma velocidade constante).

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

025a A velocidade deve ser medida correctamente, cumprindo as tolerâncias normais, dentro de 2 segundos após ser consumada uma mudança de velocidade a uma aceleração até 2 m/s^2 .

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

3. *Medição do tempo*

027 Esta função deve medir permanentemente e fornecer sob formato digital a data e a hora UTC.

028 Os valores da data e da hora UTC são utilizados pelo aparelho de controlo como dados, para registo, impressão, intercâmbio, visualização, etc.

029 Para efeitos de visualização da hora local, deve ser possível modificar em saltos de meia hora o valor exibido.

030 A deriva de tempo deve situar-se dentro do intervalo ± 2 segundos por dia, em condições de homologação do tipo.

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

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

4. Controlo das actividades do condutor

- 033 Esta função deve acompanhar permanente e separadamente as actividades de um condutor e de um ajudante.
- 034 Actividades de condutor: DRIVING (condução), WORK (trabalho), AVAILABILITY (disponibilidade) ou BREAK/REST (pausa/repouso).
- 035 Deve ser possível ao condutor e/ou ao ajudante seleccionar manualmente WORK, AVAILABILITY ou BREAK/REST.
- 036 Com o veículo em movimento, é seleccionada automaticamente a actividade DRIVING para o condutor e a actividade AVAILABILITY para o ajudante.
- 037 Com o veículo parado, é seleccionada automaticamente a actividade WORK para o condutor.
- 038 A primeira mudança de actividade 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).
- 039 Esta função transmite as mudanças de actividade às funções de registo, com uma resolução de 1 minuto.
- 040 Se ocorrer uma actividade DRIVING dentro de um dado intervalo de 1 minuto, todo esse minuto será considerado DRIVING.
- 041 Se ocorrer uma actividade 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.
- 042 Dado um intervalo de 1 minuto que não seja considerado DRIVING nos termos do supradispuesto, todo esse intervalo será considerado como do mesmo tipo que a mais longa actividade contínua ocorrida dentro dele (ou a última de várias com a mesma duração).
- 043 Esta função deve também acompanhar permanentemente o tempo de condução contínua e o tempo acumulado de pausas do condutor.

5. Controlo da situação de condução

- 044 Esta função deve acompanhar permanente e automaticamente a situação da condução.
- 045 A situação de condução CREW (tripulação) é seleccionada quando dois cartões válidos de condutor são inseridos no aparelho de controlo. Em qualquer outro caso, é seleccionada a situação de condução SINGLE (elemento só).

6. Entradas efectuadas manualmente pelos condutores

6.1. Introdução do lugar de início e/ou de final do período diário de trabalho

- 046 Esta função permite introduzir os lugares em que se iniciam ou concluem os períodos diários de trabalho de um condutor e/ou de um ajudante.
- 047 Os lugares são definidos como o país e, quando igualmente pertinente, a região.
- 048 No momento em que um cartão de condutor (ou de centro de ensaio) é retirado, o aparelho de controlo pede que o condutor (ou ajudante) introduza um "lugar no qual termina o período de trabalho diário".
- 049 O aparelho de controlo deve permitir também que este pedido seja ignorado.
- 050 Sem cartão ou em momentos em que não haja inserção ou retirada de cartão, deve continuar a ser possível introduzir lugares de início e/ou final do período de trabalho diário.

6.2. Introdução manual das actividades dos condutores

- 050a Ao ser inserido um cartão de condutor (ou de centro de ensaio), e somente nessa situação, o aparelho de controlo:
- recorda ao titular do cartão a data e a hora da última retirada do cartão e
 - pede ao titular do cartão que assinale se a inserção representa uma continuação do período de trabalho diário em curso.

O aparelho de controlo deve permitir ao titular do cartão ignorar o pedido, responder positivamente ou responder negativamente:

- Caso o titular do cartão ignore o pedido, o aparelho de controlo pedir-lhe-á que introduza um “lugar no qual se inicia o período de trabalho diário”, permitindo embora que este pedido seja ignorado. O local introduzido é registado na memória de dados e no cartão tacográfico e associado à hora de inserção do cartão.
- Caso o titular do cartão responda positiva ou negativamente, o aparelho de controlo convidá-lo-á a introduzir manualmente as actividades, com as respectivas datas e horas de início e de final, unicamente entre WORK, AVAILABILITY e BREAK/REST, incluídas exclusivamente dentro do período que vai da última retirada até à presente inserção, e sem permitir a mútua sobreposição dessas actividades. Este processo desenrola-se do seguinte modo:
 - Caso o titular do cartão responda positivamente ao pedido, o aparelho de controlo convidá-lo-á a introduzir manualmente e por ordem cronológica as actividades relativas ao período que vai da última retirada até à presente inserção. O processo termina quando o tempo de final de uma actividade introduzida manualmente coincidir com o tempo de inserção do cartão.
 - Caso o titular do cartão responda negativamente ao pedido:
 - O aparelho de controlo convidá-lo-á a introduzir manualmente e por ordem cronológica as actividades desde o tempo de retirada do cartão até ao tempo de final do correspondente período de trabalho diário (ou das actividades relativas ao veículo em questão, caso o período de trabalho diário continue numa folha de registo). Antes de permitir ao titular do cartão introduzir manualmente cada actividade, o aparelho de controlo convidá-lo-á a assinalar se o tempo de final da última actividade registada representa o final de um anterior período de trabalho (ver nota *infra*).

Nota: Caso o titular do cartão não declare quando terminou o anterior período de trabalho e introduza manualmente uma actividade cujo tempo de final coincida com o tempo de inserção do cartão, o aparelho de controlo:

- considerará que o período de trabalho diário terminou no tempo de início do primeiro período de REST (repouso) — ou do primeiro período UNKNOWN (desconhecido) que reste — depois da retirada do cartão ou no tempo da retirada do cartão se não tiver sido introduzido nenhum período de repouso (e se não restar nenhum período UNKNOWN),
- considerará que o tempo de início (ver *infra*) coincide com o tempo de inserção do cartão,
- seguirá os passos que a seguir se referem.
- Então, se o tempo de final do correspondente período de trabalho não coincidir com o tempo da retirada do cartão, ou se não tiver sido introduzido nesse momento nenhum lugar de final do período de trabalho diário, o aparelho de controlo convidará o titular do cartão a “confirmar ou introduzir o lugar no qual terminou o período de trabalho diário” (permitindo embora que este pedido seja ignorado). O local introduzido é registado (apenas no cartão tacográfico e apenas se for distinto do eventualmente introduzido no momento da retirada do cartão) e associado ao tempo de final do período de trabalho diário.
- Então, o aparelho de controlo convidará o titular do cartão a “introduzir um tempo de início” do período de trabalho diário em curso (ou das actividades associadas ao veículo em questão, no caso de o titular do cartão ter previamente utilizado uma folha de registos durante esse período) e pedir-lhe-á um “lugar no qual se inicia o período de trabalho diário” (permitindo embora que este pedido seja ignorado). O local introduzido é registado no cartão tacográfico e associado àquele tempo de início. Se este coincidir com o tempo de inserção do cartão, o local é também registado na memória de dados.
- Então, se este tempo de início não coincidir com o tempo de inserção do cartão, o aparelho de controlo convidará o titular do cartão a introduzir actividades manualmente e por ordem cronológica, desde este tempo de início até ao tempo de inserção do cartão. O processo termina quando o tempo de final de uma actividade introduzida manualmente coincidir com o tempo de inserção do cartão.
- O aparelho de controlo permitirá então que o titular do cartão modifique actividades introduzidas manualmente, até à validação por selecção de um comando específico, inviabilizando a partir daí tais modificações.
- Se não se lhes seguir a introdução de actividades, estas respostas ao pedido inicial serão interpretadas pelo aparelho de controlo como se o titular do cartão tivesse ignorado o pedido.

Ao longo de todo este processo, o aparelho de controlo tem períodos limitados de espera pelas entradas:

- Se durante 1 minuto não houver interacção com a interface homem/máquina do aparelho (com eventual aviso visual e possivelmente sonoro ao cabo de 30 segundos) ou
- se for retirado o cartão ou for inserido outro cartão de condutor (ou de centro de ensaio) ou
- logo que o veículo entre em movimento,

o aparelho de controlo valida as entradas já efectuadas.

6.3. *Introdução de condições especiais*

050b 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)

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 for inserido ou retirado um cartão de condutor.

7. *Gestão dos bloqueamentos da empresa*

- 051 Esta função deve permitir que a gestão dos bloqueamentos efectuados por uma empresa restrinja a si o acesso aos dados em modo de empresa.
- 052 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).
- 053 Os bloqueamentos só em tempo real podem ser desencadeados (lock-in) ou cessados (lock-out).
- 054 A cessação do bloqueamento (lock-out) só será possível à empresa que o tiver desencadeado (lock-in) (identificada pelos primeiros 13 algarismos do número do respectivo cartão de empresa).
- 055 O bloqueamento cessará automaticamente (lock-out) se outra empresa desencadear um bloqueamento (lock-in).
- 055a No caso de uma empresa desencadear um bloqueamento (lock-in) quando o bloqueamento anterior era para a mesma empresa, assumir-se-á então que o bloqueamento anterior não foi “cessado” e ainda está “desencadeado”.

8. *Vigilância das actividades de controlo*

- 056 Esta função deve vigiar as actividades DISPLAYING (visualização), PRINTING (impressão), VU (unidade-veículo) e DOWNLOADING (descarregamento) do cartão, em modo de controlo.
- 057 Esta função deve vigiar também as actividades 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”.

9. *Detecção de incidentes e/ou falhas*

058 Esta função deve detectar os seguintes incidentes e/ou falhas:

9.1. *Incidente “inserção de cartão não-válido”*

059 Este incidente produz-se quando é inserido um cartão não-válido e/ou quando expira o prazo de validade de um cartão inserido.

9.2. Incidente “conflito de cartões”

- 060 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				
		Cartão ausente	Cartão de condutor	Cartão de controlo	Cartão de centro de ensaio	Cartão de empresa
Ranhura do ajudante	Cartão ausente					
	Cartão de condutor				X	
	Cartão de controlo			X	X	X
	Cartão de centro de ensaio		X	X	X	X
	Cartão de empresa			X	X	X

9.3. Incidente “sobreposição de tempos”

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

9.4. Incidente “condução sem cartão adequado”

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

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

9.5. Incidente “inserção de cartão durante a condução”

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

9.6. Incidente “última sessão de cartão encerrada incorrectamente”

- 064 Este incidente produz-se quando, na inserção de um cartão, o aparelho de controlo detecta que, apesar do disposto na secção III.1, a anterior sessão não foi encerrada correctamente (cartão retirado antes de nele terem sido registados todos os dados importantes). Este incidente só será produzido por cartões de condutor e de centro de ensaio.

9.7. Incidente “excesso de velocidade”

- 065 Este incidente produz-se em situações de excesso de velocidade.

9.8. Incidente “interrupção da alimentação energética”

- 066 Este incidente produz-se, fora do modo de calibração, se a alimentação energética do sensor de movimentos e/ou da unidade-veículo for interrompida durante mais de 200 milissegundos. 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 accionar este incidente.

9.9. Incidente “erro nos dados de movimento”

- 067 Este incidente produz-se em caso de interrupção no 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.

9.10. Incidente “tentativa de violação da segurança”

- 068 Este incidente produz-se, fora do modo de calibração, perante qualquer outro incidente que afecte a segurança do sensor de movimentos e/ou da unidade-veículo, conforme consta dos objectivos gerais de segurança destes componentes.

9.11. “Falha do cartão”

- 069 Esta falha ocorre se se verificar algum defeito no cartão durante o funcionamento.

9.12. “Falha do aparelho de controlo”

- 070 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

10. Ensaios incorporados e auto-ensaio

- 071 O aparelho de controlo deve detectar automaticamente falhas, por meio de auto-ensaio e de ensaios incorporados, em conformidade com a seguinte tabela:

Subconjunto a ensaiar	Auto-ensaio	Ensaio incorporado
Software (suporte lógico)		Integridade
Memória de dados	Acesso	Acesso, integridade de dados
Interfaces dos cartões	Acesso	Acesso
Teclado		Verificação manual
Impressora	(ao critério do fabricante)	Impressão
Visor		Verificação visual
Descarregamento (executado só durante o descarregamento)	Funcionamento correcto	
Sensor	Funcionamento correcto	Funcionamento correcto

11. Leitura da memória de dados

- 072 O aparelho de controlo deve poder ler quaisquer dados memorizados na sua memória.

12. Registo e memorização de dados na memória

Para efeitos desta secção:

- Define-se “365 dias” como 365 dias de actividade média do condutor num veículo. A actividade 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 actividade. 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 actividade.
- Os tempos são registados com uma resolução de 1 minuto, salvo especificação diversa.
- Os valores odométricos são registados com uma resolução de 1 km.
- As velocidades são registadas com uma resolução de 1 km/h.

- 073 Os dados memorizados na memória não devem ser afectados por um corte exterior na alimentação energética inferior a 12 meses, em condições de homologação.
- 074 O aparelho de controlo deve poder registar e memorizar implícita ou explicitamente na sua memória os seguintes dados:
- 12.1. Dados de identificação do aparelho**
- 12.1.1. *Dados de identificação da unidade-veículo*
- 075 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
 - número da versão do suporte lógico
 - data de instalação da versão do suporte lógico
 - ano de fabrico do aparelho
 - número de homologação.
- 076 Os dados de identificação da unidade-veículo são registados e memorizados definitivamente pelo seu fabricante, com excepção dos relativos ao suporte lógico e do número de homologação, os quais podem ser modificados na eventualidade de uma reclassificação do suporte lógico.
- 12.1.2. *Dados de identificação do sensor de movimentos*
- 077 O sensor de movimentos deve poder memorizar na sua memória os seguintes dados de identificação:
- nome do fabricante
 - número da peça
 - número de série
 - número de homologação
 - identificador incorporado do componente de segurança (p.ex., número de chip/processador interno)
 - identificador do sistema operativo (p.ex., número da versão do suporte lógico).
- 078 Os dados de identificação do sensor de movimentos são registados e memorizados definitivamente nele pelo seu fabricante.
- 079 A unidade-veículo deve poder registar e memorizar na sua memória os seguintes dados emparelhados de identificação do sensor de movimentos:
- número de série
 - número de homologação
 - primeira data de emparelhamento.
- 12.2. Elementos de segurança**
- 080 O sensor de movimentos deve poder memorizar os seguintes elementos de segurança:
- chave pública europeia
 - certificado do Estado-Membro
 - certificado do equipamento
 - chave privada do equipamento.
- Os elementos de segurança do aparelho de controlo são inseridos nele pelo fabricante da unidade-veículo.
- 12.3. Dados relativos à inserção e à retirada de cartões de condutor**
- 081 Por cada ciclo de inserção e retirada de um cartão de condutor ou de centro de ensaio, 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 data e a hora da inserção do cartão
- o valor odométrico 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 odométrico 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
 - data e hora da retirada do cartão
- um indicador ou bandeira em como, no momento da inserção do cartão, o titular efectuou ou não a introdução manual de actividades.

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

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

12.4. *Dados relativos à actividade de condutor*

084 O aparelho de controlo deve registar e memorizar na sua memória de dados qualquer mudança na actividade do condutor ou do ajudante, qualquer mudança na situação da condução e/ou qualquer inserção ou retirada de um cartão de condutor ou de centro de ensaio:

- situação da condução: CREW, SINGLE
- ranhura: DRIVER (condutor principal), CO-DRIVER (ajudante)
- situação do cartão na ranhura correspondente: INSERTED (inserido), NOT INSERTED (não inserido) (ver nota)
- actividade: DRIVING, AVAILABILITY, WORK, BREAK/REST
- data e hora da mudança.

Nota: Por INSERTED entende-se que se encontra inserido na ranhura um cartão válido de condutor ou de centro de ensaio. Por NOT INSERTED entende-se o contrário, ou seja, que na ranhura não se encontra inserido nenhum cartão válido de condutor ou de centro de ensaio (p.ex., não foi inserido nenhum cartão ou o inserido é de empresa).

Nota: Dados relativos à actividade introduzidos manualmente por um condutor não são registados na memória.

085 A memória deve poder guardar durante pelo menos 365 dias os dados relativos à actividade do condutor.

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

12.5. *Lugares de início e/ou final dos períodos de trabalho diário*

087 O aparelho de controlo deve registar e memorizar na sua memória de dados a entrada do condutor ou do ajudante no lugar onde tem início e/ou final um período de trabalho diário:

- conforme o caso, número e Estado-Membro emissor do cartão do condutor ou do ajudante,
- data e hora da entrada (ou data e hora relativas à entrada se esta ocorrer durante o processo de introdução manual),
- tipo de entrada (início ou final, condição da entrada),
- país e região onde ocorre a entrada,
- valor odométrico do veículo.

088 A memória deve poder guardar durante pelo menos 365 dias os dados relativos ao início e/ou ao final dos períodos de trabalho diário (partindo-se do princípio de que um condutor introduz dois registos por dia).

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

12.6. *Dados odométricos*

090 O aparelho de controlo deve registar na sua memória de dados o valor odométrico do veículo e a correspondente data, à meia-noite de cada dia de calendário.

091 A memória deve poder guardar durante pelo menos 365 dias de calendário os valores odométricos registados à meia-noite.

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

12.7. *Dados relativos à velocidade*

093 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.

12.8. *Dados relativos a incidentes*

Na acepção deste parágrafo, os tempos são registados com uma resolução de 1 segundo.

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

Incidente	Regras de memorização	Dados a registar por cada incidente
Conflito de cartões	— os 10 incidentes mais recentes	— data e hora do início do incidente — data e hora do final do incidente — tipo, número e Estado-Membro emissor 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 e Estado-Membro emissor de qualquer cartão inserido no início e/ou no final do incidente — número de incidentes similares nesse dia
Inserção de cartão durante a condução	— o último incidente de cada um dos últimos 10 dias de ocorrência	— data e hora do incidente — tipo, número e Estado-Membro emissor do cartão — número de incidentes similares nesse dia
Última sessão de cartão encerrada incorrectamente	— os 10 incidentes mais recentes	— data e hora de inserção do cartão — tipo, número e Estado-Membro emissor do cartão — dados da última sessão, conforme leitura do cartão: — data e hora de inserção do cartão — VRN e Estado-Membro de matrícula
Excesso de velocidade ⁽¹⁾	— o incidente mais grave (i.e., o caso de velocidade média mais elevada) de cada um dos últimos 10 dias de ocorrência — os 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 e Estado-Membro emissor do cartão do condutor (se pertinente) — número de incidentes similares nesse dia

Incidente	Regras de memorização	Dados a registar por cada incidente
Interrupção da alimentação energética ⁽²⁾	<ul style="list-style-type: none"> — o incidente mais longo de cada um dos últimos 10 dias de ocorrência — os 5 incidentes mais longos dos últimos 365 dias 	<ul style="list-style-type: none"> — data e hora do início do incidente — data e hora do final do incidente — tipo, número e Estado-Membro emissor de qualquer cartão inserido no início e/ou no final do incidente — número de incidentes similares nesse dia
Erro nos dados de movimento	<ul style="list-style-type: none"> — o incidente mais longo de cada um dos últimos 10 dias de ocorrência — os 5 incidentes mais longos dos últimos 365 dias 	<ul style="list-style-type: none"> — data e hora do início do incidente — data e hora do final do incidente — tipo, número e Estado-Membro emissor de qualquer cartão inserido no início e/ou no final do incidente — número de incidentes similares nesse dia
Tentativa de violação da segurança	<ul style="list-style-type: none"> — os 10 incidentes mais recentes por tipo de incidente 	<ul style="list-style-type: none"> — data e hora do início do incidente — data e hora do final do incidente (se pertinente) — tipo, número e Estado-Membro emissor de qualquer cartão inserido no início e/ou no final do incidente — tipo de incidente

095

(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.

12.9. *Dados relativos a falhas*

Na aceção deste parágrafo, os tempos são registados com uma resolução de 1 segundo.

096

Relativamente a cada falha detectada, 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
Falha do cartão	<ul style="list-style-type: none"> — as 10 falhas mais recentes de cartão de condutor 	<ul style="list-style-type: none"> — data e hora do início da falha — data e hora do final da falha — tipo, número e Estado-Membro emissor do cartão
Falhas do aparelho de controlo	<ul style="list-style-type: none"> — as 10 falhas mais recentes por tipo de falha — a primeira falha ocorrida desde a última calibração 	<ul style="list-style-type: none"> — data e hora do início da falha — data e hora do final da falha — tipo de falha — tipo, número e Estado-Membro emissor de qualquer cartão inserido no início e/ou no final da falha

12.10. Dados relativos à calibração

- 097 O aparelho de controlo deve registar e memorizar na sua memória dados com interesse para:
- parâmetros conhecidos de calibração no momento da activação,
 - a primeira calibração após a activação,
 - a primeira calibração no veículo em questão (identificado pelo NIV),
 - as 5 calibrações mais recentes (se ocorrerem várias no mesmo dia de calendário, é memorizada unicamente a última desse dia).
- 098 Para cada uma das seguintes calibrações, são registados os seguintes dados:
- objectivo da calibração (activação, primeira instalação, instalação, inspecção periódica),
 - nome e endereço do centro de ensaio,
 - número, Estado-Membro emissor e prazo de validade do cartão de centro de ensaio,
 - identificação do veículo,
 - parâmetros actualizados ou confirmados: dimensão w, k, l, medida do pneumático, ponto de regulação do dispositivo de limitação da velocidade, odómetro (antigo e novo valores), data e hora (antigo e novo valores).
- 099 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).

12.11. Dados relativos ao ajustamento do tempo

- 100 O aparelho de controlo deve registar e memorizar na sua memória dados com interesse para:
- o mais recente ajustamento do tempo,
 - os 5 mais extensos ajustamentos do tempo, desde a última calibração,
- entendendo-se que os ajustamentos são efectuados em modo de calibração, fora do âmbito de uma calibração regular (definição f).
- 101 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 do centro de ensaio,
 - número, Estado-Membro emissor e prazo de validade do cartão de centro de ensaio.

12.12. Dados relativos à actividade de controlo

- 102 O aparelho de controlo deve registar e memorizar na sua memória os seguintes dados relativos às 20 mais recentes actividades de controlo:
- data e hora do controlo,
 - número e Estado-Membro emissor do cartão de controlo,
 - tipo do controlo (visualização, impressão, descarregamento da VU e/ou descarregamento do cartão).
- 103 Em caso de descarregamento, são igualmente registadas as datas dos dias descarregados mais remoto e mais recente.

12.13 Dados relativos aos bloqueamentos da empresa

- 104 O aparelho de controlo deve registar e memorizar na sua memória os seguintes dados relativos aos 20 mais recentes bloqueamentos da empresa:
- data e hora de início do bloqueamento (lock-in),
 - data e hora de cessação do bloqueamento (lock-out),

- número e Estado-Membro emissor do cartão da empresa,
- nome e endereço da empresa.

12.14. *Dados relativos à actividade de descarregamento*

105 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 e Estado-Membro emissor do cartão de empresa ou de centro de ensaio,
- nome da empresa ou do centro de ensaio.

12.15. *Dados relativos às condições especiais*

105a O aparelho de controlo deve registar e memorizar na sua memória os seguintes dados relativos a condições especiais:

- data e hora de introdução da condição especial,
- tipo de condição especial.

105b A memória deve poder guardar os dados relativos a condições especiais durante pelo menos 365 dias (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.

13. *Leitura de cartões tacográficos*

106 O aparelho de controlo deve poder ler nos cartões tacográficos, 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 actividade seleccionada nesse momento,
- verificar se a última sessão do cartão foi correctamente 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.

107 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.

14. *Registo e memorização de dados nos cartões tacográficos*

108 O aparelho de controlo deve lançar no cartão de condutor ou de centro de ensaio, imediatamente após a sua inserção, os "dados da sessão do cartão".

109 O aparelho de controlo deve actualizar os dados memorizados em cartões válidos de condutor, de centro de ensaio 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 na secção IV.

109a O aparelho de controlo deve actualizar os dados relativos à actividade do condutor e à localização (secções 4.5.2.5 e 4.5.2.6), memorizados em cartões válidos de condutor e/ou de centro de ensaio, com os dados relativos à actividade e à localização que o titular introduz manualmente

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

111 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.

112 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".

15. Visualização (displaying)

113 Na visualização de mensagens deve haver pelo menos 20 caracteres.

114 As dimensões mínimas de um carácter devem ser de 5 mm de altura por 3,5 mm de largura.

114a A visualização deve aceitar os caracteres Latin 1 e Greek definidos pela norma ISO 8859, partes 1 e 7 (ver apêndice 1, capítulo 4). A visualização pode utilizar símbolos simplificados (p.ex., ausência de acento gráfico, maiúsculas em lugar de minúsculas, etc.).

115 Na visualização deve ser utilizada iluminação adequada, não ofuscante.

116 As indicações devem ser visíveis de fora do aparelho de controlo.

117 O aparelho de controlo deve poder exibir para visualização:

— dados relativos a funcionamento deficiente,

— dados relativos a aviso (alerta),

— dados relativos ao acesso ao menu,

— outros dados pretendidos por um utilizador.

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

118 O dispositivo de visualização (visor) do aparelho de controlo deve utilizar os pictogramas ou combinações de pictogramas indicados no apêndice 3. Podem ser utilizados pictogramas ou combinações adicionais, desde que claramente distinguíveis dos primeiros.

119 O visor deve estar sempre ligado (posição ON) com o veículo em movimento.

120 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.

15.1. Visualização por defeito (default display)

121 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,

— actividade em curso do condutor e actividade em curso do ajudante,

— informação relativa ao condutor:

— se a sua actividade em curso for DRIVING: seu actual tempo de condução contínua e seu actual tempo acumulado de pausas,

— se a sua actividade em curso não for DRIVING: duração dessa actividade (desde que foi seleccionada) e seu actual tempo acumulado de pausas,

— informação relativa ao ajudante:

— duração da sua actividade em curso (desde que foi seleccionada).

122 A exibição dos dados relativos ao condutor e ao ajudante deve ser clara, directa 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.

123 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.

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

124a A abertura de uma condição "OUT OF SCOPE" deve ser assinalada na visualização por defeito, com recurso aos pictogramas pertinentes (é aceitável que a actividade em curso do condutor não seja visualizada ao mesmo tempo).

15.2. *Visualização de aviso ou de alerta (warning display)*

125 O aparelho de controlo deve exibir informações de aviso ou de alerta, primordialmente com recurso aos pictogramas constantes do apêndice 3, complementados, se necessário, por informação adicional numericamente codificada. Pode também ser acrescentada uma descrição literal da mensagem, no idioma de preferência do condutor.

15.3. *Acesso ao menu*

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

15.4. *Outras visualizações*

127 Deve ser possível visualizar selectivamente, conforme se pretenda:

- data e hora UTC,
- modo de funcionamento (caso não indicado por defeito),
- 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,
- conteúdo de qualquer destas seis mensagens, no mesmo formato da mensagem impressa.

128 A visualização do conteúdo das mensagens deve ser sequencial, linha a linha. Se a largura do visor for inferior a 24 caracteres, o utilizador deve poder obter a informação completa por um meio adequado (linhas múltiplas, desenrolamento ou scrolling, etc.). As linhas reservadas a informação manuscrita podem ser omitidas na visualização.

16. *Impressão (printing)*

129 O aparelho de controlo deve poder imprimir informação contida na sua memória de dados e/ou nos cartões tacrográficos:

- actividades de condutor, da impressão diária dos cartões,
- actividades 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.

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 seis impressões *supra*.

130 As funções "actividades 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 centro de ensaio. Antes de iniciar a impressão, o aparelho de controlo actualiza os dados memorizados no cartão em causa.

- 131 Para concretizar a impressão de “actividades de condutor, da impressão diária dos cartões” e de “incidentes e falhas, da impressão dos cartões”, o aparelho de controlo deve:
- seleccionar automaticamente o cartão de condutor ou de centro de ensaio, 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.
- 132 A impressora deve poder imprimir 24 caracteres por linha.
- 133 As dimensões mínimas de um carácter devem ser de 2,1 mm de altura por 1,5 mm de largura.
- 133a A impressora deve aceitar os caracteres Latin 1 e Greek definidos pela norma ISO 8859, partes 1 e 7 (ver apêndice 1, capítulo 4).
- 134 As impressoras devem ser projectadas de modo a que as impressões tenham um grau de definição susceptível de evitar ambiguidades de leitura.
- 135 A impressão deve conservar as dimensões e os registos em condições normais de humidade (10-90 %) e de temperatura.
- 136 O papel utilizado pelo aparelho de controlo deve exibir a correspondente marca de homologação e a indicação do tipo de aparelho no qual pode ser utilizado. As impressões devem manter-se claramente legíveis e identificáveis em condições normais de memorização, no atinente a intensidade luminosa, humidade e temperatura, durante pelo menos um ano.
- 137 A estes documentos deve ser igualmente possível acrescentar notas manuscritas, como a assinatura do condutor.
- 138 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 efectuada a recarga do papel, retomar a impressão desde o início ou prosseguir-la, fazendo, nesta última hipótese, uma referência inequívoca à parte anteriormente impressa.
- 17. Avisos ou alertas (warnings)**
- 139 O aparelho de controlo deve prevenir o condutor quando detectar algum incidente e/ou alguma falha.
- 140 A sinalização de um incidente de interrupção da alimentação energética poderá ser adiada até a alimentação ser restabelecida.
- 141 O aparelho de controlo deve avisar o condutor 15 minutos antes e no momento em que se ultrapassam 4h 30min de tempo de condução contínua.
- 142 Os sinais de aviso ou alerta devem ser visuais. Complementarmente, podem ser também emitidos sinais sonoros.
- 143 Os avisos visuais devem ser claramente reconhecíveis pelo utilizador, situar-se no seu campo de visão e ser claramente legíveis tanto de dia como à noite.
- 144 Os avisos visuais podem ser incorporados no aparelho de controlo ou ter uma localização à distância (localização remota).
- 145 No último caso, o sinal deve comportar um símbolo “T” e ser de cor âmbar ou laranja.
- 146 Os avisos devem ter a duração mínima de 30 segundos, a menos que o condutor acuse a sua emissão premindo uma tecla do aparelho de controlo. Este primeiro reconhecimento não deve eliminar a visualização da causa do alerta (ver n.º 147).
- 147 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 comando específico.
- 148 Podem ser emitidos avisos adicionais, desde que não provoquem a confusão do condutor em relação a avisos previamente definidos.

18. Descarregamento de dados para meios externos

- 149 Caso se pretenda, deve poder descarregar dados da sua memória ou de um cartão de condutor para meios externos de memorização, através do conector de calibração/d Descarregamento. Antes de iniciar o descarregamento, o aparelho de controlo actualiza os dados memorizados no cartão em causa.
- 150 Complementarmente, e como função opcional, o aparelho de controlo deve, em qualquer modo de funcionamento, poder descarregar dados por intermédio de outro conector, para uma empresa autenticada através deste canal. Nesse caso, aplicar-se-ão ao descarregamento direitos de acesso aos dados em modo de empresa.
- 151 O descarregamento não deve alterar ou apagar dados memorizados.

A interface eléctrica do conector de calibração/d Descarregamento é especificada no apêndice 6.

Os protocolos relativos ao descarregamento são especificados no apêndice 7.

19. Transmissão ou saída (output) de dados para dispositivos externos adicionais

- 152 Se não possuir funções de visualização da velocidade e/ou dos elementos odométricos, o aparelho de controlo deve permitir sinais de saída para a visualização da velocidade do veículo (velocímetro) e/ou da distância total percorrida por ele (odómetro).
- 153 Para permitir o seu processamento por outras unidades electrónicas instaladas no veículo, a unidade-veículo deve igualmente poder transmitir os seguintes dados, utilizando uma competente ligação dedicada em série, independente de uma ligação opcional CAN a autocarro (ISO 11898 Road Vehicles — Interchange of digital information — Controller Area Network-CAN for high speed communication):
- data e hora UTC actuais,
 - velocidade do veículo,
 - distância total percorrida pelo veículo (odómetro),
 - actividade do condutor e do ajudante seleccionada no momento,
 - informação quanto a um cartão tacográfico estar no momento inserido na ranhura do condutor e na ranhura do ajudante e (se for caso disso) dados identificativos dos cartões (número e Estado-Membro emissor).

Adicionalmente a esta lista, podem ser transmitidos outros dados.

Estando ligada a ignição do veículo (ignition ON), estes dados devem ser transmitidos permanentemente. Com a ignição desligada (ignition OFF), pelo menos uma mudança na actividade do condutor ou do ajudante e/ou uma inserção ou retirada de um cartão tacográfico deve gerar a saída (transmissão) dos correspondentes dados. Na eventualidade de a saída de dados ter sido suspensa enquanto a ignição se mantém desligada, os mesmos devem ser disponibilizados logo que a ignição volte a ser ligada.

20. Calibração

- 154 A função de calibração deve permitir:
- emparelhar automaticamente o sensor de movimentos com a unidade-veículo,
 - adaptar digitalmente a constante k do aparelho de controlo ao coeficiente w característico do veículo (os veículos com duas ou mais razões de eixo devem ser equipados com dispositivos de comutação que reajustem automaticamente essas razões à razão segundo a qual o aparelho foi adaptado ao veículo),
 - ajustar (sem limitação) o tempo actual,
 - ajustar o valor odométrico actual,
 - actualizar os dados de identificação do sensor de movimentos, memorizados na memória,
 - actualizar ou confirmar outros parâmetros conhecidos pelo aparelho de controlo (identificação do veículo, w , l , medida do pneumático, ponto de regulação do eventual dispositivo de limitação da velocidade).

- 155 O emparelhamento do sensor de movimentos com a unidade-veículo deve consistir, pelo menos, em:
- actualizar 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.

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

21. Ajustamento do tempo

- 157 A função de ajustamento do tempo deve permitir acertar o tempo actual por saltos máximos de 1 minuto, a intervalos mínimos de 7 dias.
- 158 A função de ajustamento do tempo deve permitir acertar o tempo actual sem limitação, em modo de calibração.

22. Características de desempenho

- 159 A unidade-veículo deve ser plenamente funcional no intervalo de temperatura de -20°C a $+70^{\circ}\text{C}$, e o sensor de movimentos no intervalo de -40°C a $+135^{\circ}\text{C}$. O conteúdo da memória de dados deve ser preservado até à temperatura de -40°C .
- 160 O aparelho de controlo deve ser plenamente funcional no intervalo de humidade de 10 % a 90 %.
- 161 O aparelho de controlo deve ser protegido contra sobretensão eléctrica, inversão da polaridade da sua alimentação energética e curtos-circuitos.
- 162 O aparelho de controlo deve cumprir o disposto na Directiva 95/54/CE da Comissão, de 31 de Outubro de 1995 ⁽¹⁾, que adapta ao progresso técnico a Directiva 72/245/CEE do Conselho, relativa à compatibilidade electromagnética, e deve ser protegido contra descargas electrostáticas e contra transitórios.

23. Materiais

- 163 Todas as peças constituintes do aparelho de controlo devem ser em material com estabilidade e resistência mecânica suficientes e com características electromagnéticas estáveis.
- 164 Em condições normais de utilização, todas as peças internas do aparelho de controlo devem ser protegidas contra humidade e poeiras.
- 165 A unidade-veículo deve cumprir o grau de protecção IP 40, e o sensor de movimentos deve cumprir o grau de protecção IP 64 (cf. norma IEC 529).
- 166 O aparelho de controlo deve cumprir as especificações técnicas aplicáveis em matéria de ergonomia.
- 167 O aparelho de controlo deve ser protegido contra danos acidentais.

24. Marcações

- 168 Se o aparelho de controlo exibir o valor odométrico 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",

⁽¹⁾ JO L 266 de 8.11.1995, p. 1.

— 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”.

169 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.

170 Se não houver espaço suficiente para a exposição de todos os elementos *supra*, a placa descritiva deve indicar pelo menos o nome ou logotipo do fabricante e o número da peça.

IV. REQUISITOS DE CONSTRUÇÃO E DE FUNCIONAMENTO DOS CARTÕES TACOGRÁFICOS

1. Dados visíveis

O averso do cartão terá o seguinte conteúdo:

171 os termos “CARTÃO DE CONDUTOR”, “CARTÃO DE CONTROLO”, “CARTÃO DE CENTRO DE ENSAIO” ou “CARTÃO DE EMPRESA”, consoante o tipo de cartão, impressos em maiúsculas na(s) língua(s) oficial(is) do Estado-Membro emissor do cartão,

172 os mesmos termos nas restantes línguas oficiais da União Europeia, impressos no verso do cartão:

ES	TARJETA DEL CONDUCTOR	TARJETA DE CONTROL	TARJETA DEL CENTRO DE ENSAYO	TARJETA DE LA EMPRESA
DK	FØRERKORT	KONTROLKORT	VÆRKSTEDSKORT	VIRKSOMHEDSKORT
DE	FAHRERKARTE	KONTROLLKARTE	WERKSTATTKARTE	UNTERNEHMENSKARTE
EL	KAPTA ΟΔΗΓΟΥ	KAPTA ΕΛΕΓΧΟΥ	KAPTA ΚΕΝΤΡΟΥ ΔΟΚΙΜΩΝ	KAPTA ΕΠΙΧΕΙΡΗΣΗΣ
EN	DRIVER CARD	CONTROL CARD	WORKSHOP CARD	COMPANY CARD
FR	CARTE DE CONDUCTEUR	CARTE DE CONTROLEUR	CARTE D'ATELIER	CARTE D'ENTREPRISE
GA	CÁRTA TIOMÁNAÍ	CÁRTA STIÚRTHA	CÁRTA CEARDLAINNE	CÁRTA COMHLACHTA
IT	CARTA DEL CONDUCENTE	CARTA DI CONTROLLO	CARTA DEL CENTRO DI PROVA	CARTA DELL'AZIENDA
NL	BESTUURDERS KAART	CONTROLEKAART	CONTROLESTATION KAART	BEDRIJFSKAART
PT	CARTÃO DE CONDUTOR	CARTÃO DE CONTROLO	CARTÃO DO CENTRO DE ENSAIO	CARTÃO DE EMPRESA
FIN	KULJETTAJA KORTILLA	VALVONTA KORTILLA	TESTAUSASEMA KORTILLA	YRITYSKORTILLA
SV	FÖRARKORT	KONTROLLKORT	VERKSTADSKORT	FÖRETAGSKORT

173 o nome do Estado-Membro emissor do cartão (opcional),

174 o código distintivo do Estado-Membro emissor do cartão, impresso em negativo e com um círculo de doze estrelas amarelas à volta, dentro de um rectângulo azul, sendo os seguintes os códigos distintivos dos Estados-Membros:

B	Bélgica
DK	Dinamarca
D	Alemanha
GR	Grécia
E	Espanha
F	França
IRL	Irlanda
I	Itália
L	Luxemburgo
NL	Países Baixos
A	Áustria
P	Portugal
FIN	Finlândia
S	Suécia
UK	Reino Unido

175 elementos específicos do cartão, com a seguinte numeração:

	Cartão de condutor	Cartão de controlo	Cartão de empresa ou de centro de ensaio
1.	apelido do condutor	nome do organismo de controlo	nome da empresa ou do centro de ensaio
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		
(b)	data do final da validade do cartão (se aplicável)		
(c)	nome da autoridade emissora (pode ser impresso no verso)		
(d)	número diferente do que figura em 5, para efeitos administrativos (opcional)		
5.(a)	número da carta de condução (à data da emissão do cartão de condutor)	—	—
5.(b)	número do cartão		
6.	fotografia do condutor	fotografia do controlador (opcional)	—
7.	assinatura do condutor	assinatura do titular (opcional)	
8.	lugar de residência habitual ou endereço postal do titular (opcional)	endereço postal do organismo de controlo	endereço postal da empresa ou do centro de ensaio

176 datas, com o formato “dd/mm/aaaa” ou “dd.mm.aaaa” (dia, mês, ano).

O verso do cartão terá o seguinte conteúdo:

177 explicação dos elementos numerados que constam do anverso,

178 com carácter 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.

COMMUNITY MODEL TACHOGRAPH CARDS

FRONT	REVERSE
<div style="text-align: center;">  </div> <p>DRIVER CARD</p> <p>1. _____ 2. _____ 3. _____ 4a. _____ 4c. _____ (4d.) _____ 5a. _____ 5b. _____ 7. _____ (8.) _____</p> <p style="text-align: center;">MEMBER STATE</p> <p>TARJETA DEL CONDUCTOR FØRERKORT FAHRREKARTE KAPTA O ΔΗΤΟΥ 4b. DRIVER CARD CARTE DE CONDUCTEUR CÁRTA TIOMÁNAÍ CARTA DEL CONDUCENTE BESTUURDERSKAART CARTÃO DE CONDUTOR KULJETTAJAKORTILLA FÖRARKORT</p>	<p>1. Surname 2. First name(s) 3. Birth date 4a. Date of start of validity of card 4b. Administrative expiry date of card 4c. Issuing authority (4d.) No for national administrative purposes 5a. Driving license number 5b. Card number 6. Photograph 7. Signature (8.) Address</p> <p style="text-align: center;"><i>Please return to:</i></p> <p style="text-align: center;">NAME OF AUTHORITY AND ADDRESS</p>
<div style="text-align: center;">  </div> <p>CONTROL CARD</p> <p>1. _____ (2.) _____ (3.) _____ 4a. _____ 4c. _____ (4d.) _____ 5b. _____ (7.) _____ 8. _____</p> <p style="text-align: center;">MEMBER STATE</p> <p>TARJETA DE CONTROL KONTROLKORT KONTROLLKARTE 4b.) KAPTA ΕΛΕΓΧΟΥ CONTROL CARD CARTE DE CONTROLEUR CÁRTA STIÚRTHA CARTA DI CONTROLLO CONTROLEKAART CARTÃO DE CONTROLO VALVONTAKORTILLA KONTROLLKORT</p>	<p>1. Control Body (2.) Surname (3.) First name(s) 4a. Date of start of validity of card (4b.) Administrative expiry date of card 4c. Issuing authority (4d.) No for national administrative purposes 5b. Card number (6.) Photograph (7.) Signature 8. Address</p> <p style="text-align: center;"><i>Please return to:</i></p> <p style="text-align: center;">NAME OF AUTHORITY AND ADDRESS</p>
<div style="text-align: center;">  </div> <p>WORKSHOP CARD</p> <p>1. _____ (2.) _____ (3.) _____ 4a. _____ 4c. _____ (4d.) _____ 5b. _____ (7.) _____ 8. _____</p> <p style="text-align: center;">MEMBER STATE</p> <p>TARJETA DEL CENTRO DE ENSAIO VÆRKSTEDSKORT WERKSTATTKARTE KAPTA 4b. ΚΕΝΤΡΟΥ ΔΟΚΙΜΩΝ WORKSHOP CARD CARTE D'ATELIER CÁRTA CEARDLAINNE CARTA DEL CENTRO DI PROVA CONTROLESTATIONKAART CARTÃO DO CENTRO DE ENSAIO TESTAUSASEMAKORTILLA VERKSTADSKORT</p>	<p>1. Workshop Name (2.) Surname (3.) First name(s) 4a. Date of start of validity of card 4b. Administrative expiry date of card 4c. Issuing authority (4d.) No for national administrative purposes 5b. Card number (7.) Signature 8. Address</p> <p style="text-align: center;"><i>Please return to:</i></p> <p style="text-align: center;">NAME OF AUTHORITY AND ADDRESS</p>
<div style="text-align: center;">  </div> <p>COMPANY CARD</p> <p>1. _____ (2.) _____ (3.) _____ 4a. _____ 4c. _____ (4d.) _____ 5b. _____ (7.) _____ 8. _____</p> <p style="text-align: center;">MEMBER STATE</p> <p>TARJETA DE LA EMPRESA VIRKSOMHEDSKORT UNTERNEHMENSKARTE KAPTA ΕΠΙΧΕΙΡΗΣΕΩΣ 4b. COMPANY CARD CARTE D'ENTREPRISE CÁRTA COMHLACHTA CARTA DELL'AZIENDA BEDRIJFSKAART CARTÃO DE EMPRESA YRITYSKORTILLA FÖRETAGSKORT</p>	<p>1. Company Name (2.) Surname (3.) First name(s) 4a. Date of start of validity of card 4b. Administrative expiry date of card 4c. Issuing authority (4d.) No for national administrative purposes 5b. Card number (7.) Signature 8. Address</p> <p style="text-align: center;"><i>Please return to:</i></p> <p style="text-align: center;">NAME OF AUTHORITY AND ADDRESS</p>

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

- cartão de condutor: branco
- cartão de controlo: azul
- cartão de centro de ensaio: vermelho
- cartão de empresa: amarelo.

180 Os cartões tacográficos devem ter as seguintes características de protecção contra falsificações:

- fundo de segurança em guiloché fino e impressão irisada,
- na zona da fotografia, sobreposição do fundo de segurança e da fotografia,
- pelo menos uma linha de microimpressão bicromática.

- 181 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.

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, excluindo qualquer possibilidade de falsificação dos dados memorizados nos cartões, prevenindo contrafações e detectando quaisquer tentativas nesse sentido.

- 182 Com vista a conseguir a segurança do sistema, os cartões tacográficos devem cumprir os requisitos definidos nos objectivos gerais de segurança (apêndice 10).

- 183 Os cartões tacográficos devem ser legíveis por outros aparelhos, como computadores pessoais.

3. Normas

- 184 Os cartões tacográficos devem obedecer às seguintes normas:

- ISO/IEC 7810 Identification cards — Physical characteristics
- ISO/IEC 7816 Identification cards — Integrated circuits with contacts:
 - Part 1: Physical characteristics,
 - Part 2: Dimensions and location of the contacts,
 - Part 3: Electronic signals and transmission protocols,
 - Part 4: Inter-industry commands for interchange,
 - Part 8: Security related inter-industry commands,
- ISO/IEC 10373 Identification cards — Test methods.

4. Especificações ambientais e eléctricas

- 185 Os cartões tacográficos devem poder funcionar correctamente nas condições climáticas normalmente ocorrentes no território da União Europeia e pelo menos no intervalo térmico de -25°C a $+70^{\circ}\text{C}$, com picos ocasionais até $+85^{\circ}\text{C}$, 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.

- 186 Os cartões tacográficos devem poder funcionar correctamente no intervalo de humidade entre 10 % e 90 %.

- 187 Os cartões tacográficos devem poder funcionar correctamente durante um período de cinco anos, desde que utilizados em conformidade com as especificações ambientais e eléctricas.

- 188 No âmbito do seu funcionamento, os cartões tacográficos devem cumprir o disposto na Directiva 95/54/CE da Comissão, de 31 de Outubro de 1995, relativa à compatibilidade electromagnética ⁽¹⁾, e devem ser protegidos contra descargas electrostáticas.

5. Memorização de dados

Para efeitos da presente secção,

- as medidas de tempo são registadas com uma resolução de 1 minuto, salvo indicação diversa,
- os valores odométricos são registados com uma resolução de 1 km,
- as velocidades são registadas com uma resolução de 1 km/h.

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

⁽¹⁾ JO L 266 de 8.11.1995, p. 1.

189 Nesta secção, é especificada 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 efectiva de memorização desses ficheiros.

A memorização dos dados relativos a outras aplicações, para as quais o cartão tenha eventualmente capacidade, deve cumprir o disposto na Directiva 95/46/CE. (1)

5.1. **Dados de identificação e de segurança do cartão**

5.1.1. *Identificação da aplicação*

190 Os cartões tacográficos devem poder memorizar os seguintes dados de identificação da aplicação:

- identificação da aplicação tacográfica,
- identificação do tipo de cartão tacográfico.

5.1.2. *Identificação da pastilha (chip)*

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

- número de série do CI,
- referências de fabrico do CI.

5.1.3. *Identificação do cartão*

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

- número de série do cartão (incluindo referências de fabrico),
- número de homologação do tipo de cartão,
- identificação personalizada do cartão (ID),
- identificação do fabricante do cartão,
- identificador do CI.

5.1.4. *Elementos de segurança*

193 Os cartões tacográficos devem poder memorizar os seguintes elementos de segurança:

- chave pública europeia,
- certificado do Estado-Membro,
- certificado do cartão,
- chave privada do cartão.

5.2. **Cartão de condutor**

5.2.1. *Identificação do cartão*

194 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.

5.2.2. *Identificação do titular*

195 O cartão de condutor deve poder memorizar os seguintes dados de identificação do respectivo titular:

- apelido,
- nome próprio,

(1) JO L 281, de 23.11.1995, p. 31.

— data de nascimento,

— idioma preferencial.

5.2.3. Elementos relativos à carta de condução

196 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).

5.2.4. Dados relativos à utilização de veículos

197 Relativamente a cada dia de calendário 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 odométrico 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),

— valor odométrico do veículo no momento,

— VRN e Estado-Membro de matrícula do veículo.

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

5.2.5. Dados relativos à actividade de condutor

199 Relativamente a cada dia de calendário em que o cartão seja utilizado ou relativamente ao qual o condutor introduza actividades 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 de calendário),

— distância total percorrida pelo condutor nesse dia,

— situação do condutor às 00h00,

— a cada mudança da actividade 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)

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

— tempo (hora) da mudança.

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

201 Os dados referidos nos n.ºs 197 e 199 devem ser memorizados de modo a permitir a recuperação de actividades segundo a sua ordem de ocorrência, mesmo na eventualidade de sobreposição de tempos.

5.2.6. Locais de início e/ou final dos períodos de trabalho diário

202 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 odométrico do veículo.

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

5.2.7. *Dados relativos a incidentes*

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

204 O cartão de condutor deve poder memorizar os dados relativos aos seguintes incidentes detectados 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 incorrectamente (se este cartão for o protagonista do incidente),
- interrupção da alimentação energética,
- erro nos dados de movimento,
- tentativa de violação da segurança.

205 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 incorrectamente”:

- a data e a hora de início do incidente devem corresponder à data e à hora de inserção do cartão na sessão encerrada incorrectamente,
- 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 detectado (sessão em curso),
- os dados relativos ao veículo devem corresponder ao veículo no qual a sessão não foi encerrada correctamente.

206 O cartão de condutor deve poder memorizar os dados relativos aos 6 incidentes mais recentes de cada um dos seis tipos indicados no n.º 204 (ou seja, os dados relativos a 36 incidentes).

5.2.8. *Dados relativos a falhas*

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

- 207 O cartão de condutor deve poder memorizar os dados relativos às seguintes falhas detectadas 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.
- 208 O cartão de condutor deve poder memorizar os seguintes dados relativos àquelas falhas:
- código da 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.
- 209 O cartão de condutor deve poder memorizar os dados relativos às 12 falhas mais recentes de cada um dos dois tipos indicados no n.º 207 (ou seja, os dados relativos a 24 falhas).

5.2.9. *Dados relativos à actividade de controlo*

- 210 O cartão de condutor deve poder memorizar os seguintes dados relativos a actividades de controlo:
- data e hora do controlo,
 - número e Estado-Membro emissor do cartão de controlo,
 - tipo do 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.

- 211 O cartão de condutor deve poder guardar 1 registo deste tipo.

5.2.10. *Dados relativos à sessão de cartão*

- 212 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.

5.2.11. *Dados relativos às condições especiais*

- 212a 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,
 - tipo de condição especial.
- 212b O cartão de condutor deve poder guardar 56 registos deste tipo.

5.3. *Cartão de centro de ensaio*

5.3.1. *Elementos de segurança*

- 213 O cartão de centro de ensaio deve poder memorizar um número de identificação pessoal (código PIN).
- 214 O cartão de centro de ensaio deve poder memorizar as chaves criptográficas necessárias ao emparelhamento dos sensores de movimentos com as unidades-veículo.

5.3.2. Identificação do cartão

215 O cartão de centro de ensaio 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.

5.3.3. Identificação do titular

216 O cartão de centro de ensaio deve poder memorizar os seguintes dados de identificação do respectivo titular:

- nome do centro de ensaio,
- endereço do centro de ensaio,
- apelido do titular,
- nome próprio do titular,
- idioma preferencial.

5.3.4. Dados relativos à utilização de veículos

217 O cartão de centro de ensaio deve poder memorizar os dados relativos à utilização de veículos de modo idêntico a um cartão de condutor.

218 O cartão de centro de ensaio deve poder memorizar pelo menos 4 registos deste tipo.

5.3.5. Dados relativos à actividade de condutor

219 O cartão de centro de ensaio deve poder memorizar os dados relativos à actividade de condutor de modo idêntico a um cartão de condutor.

220 O cartão de centro de ensaio deve poder guardar os dados relativos à actividade de condutor durante pelo menos 1 dia de actividade média do condutor.

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

221 O cartão de centro de ensaio 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.

222 O cartão de centro de ensaio deve poder guardar pelo menos 3 pares de registos deste tipo.

5.3.7. Dados relativos a incidentes e a falhas

223 O cartão de centro de ensaio deve poder memorizar os dados relativos a incidentes e a falhas de modo idêntico a um cartão de condutor.

224 O cartão de centro de ensaio deve poder memorizar os dados relativos aos 3 incidentes mais recentes de cada um dos seis tipos indicados no n.º 204 (ou seja, os dados relativos a 18 incidentes) e os dados relativos às 6 falhas mais recentes de cada um dos dois tipos indicados no n.º 207 (ou seja, os dados relativos a 12 falhas).

5.3.8. Dados relativos à actividade de controlo

225 O cartão de centro de ensaio deve poder memorizar os dados relativos à actividade de controlo de modo idêntico a um cartão de condutor.

5.3.9. Dados relativos à calibração e ao ajustamento do tempo

226 O cartão de centro de ensaio 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.

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

- finalidade da calibração (primeira instalação, instalação, inspecção periódica),
- identificação do veículo,
- parâmetros actualizados ou confirmados (dimensões w, k, l, w, k, l, medida do pneumático, ponto de regulação do eventual dispositivo de limitação da velocidade, valor odométrico actual e anterior, data e hora actual e anterior),
- identificação do aparelho de controlo (número de peça da VU, número de série da VU, número de série do sensor de movimentos).

228 O cartão de centro de ensaio deve poder memorizar pelo menos 88 registos deste tipo.

229 O cartão de centro de ensaio deve ser equipado com um contador que indique o número total de calibrações executadas com o cartão.

230 O cartão de centro de ensaio deve ser equipado com um contador que indique o número de calibrações executadas desde o seu último descarregamento.

5.3.10. *Dados relativos às condições especiais*

230a O cartão de centro de ensaio deve poder memorizar os dados relativos às condições especiais de modo idêntico a um cartão de condutor. O cartão de centro de ensaio deve poder memorizar 2 registos deste tipo.

5.4. **Cartão de controlo**

5.4.1. *Identificação do cartão*

231 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.

5.4.2. *Identificação do titular*

232 O cartão de controlo deve poder memorizar os seguintes dados de identificação do respectivo titular:

- nome do organismo de controlo,
- endereço do organismo de controlo,
- apelido do titular,
- nome próprio do titular,
- idioma preferencial.

5.4.3. *Dados relativos à actividade de controlo*

233 O cartão de controlo deve poder memorizar os seguintes dados relativos a actividades de controlo:

- data e hora do controlo,
- tipo do controlo (visualização, impressão, descarregamento da VU e/ou descarregamento do cartão),
- 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.

234 O cartão de controlo deve poder guardar pelo menos 230 registos deste tipo.

5.5. **Cartão de empresa**

5.5.1. *Identificação do cartão*

235 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.

5.5.2. *Identificação do titular*

236 O cartão de empresa deve poder memorizar os seguintes dados de identificação do respectivo titular:

- nome da empresa,
- endereço da empresa.

5.5.3. Dados relativos à actividade da empresa

- 237 O cartão de empresa deve poder memorizar os seguintes dados relativos à actividade da empresa:
- data e hora da actividade,
 - tipo de actividade: 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).
- 238 O cartão de empresa deve poder guardar pelo menos 230 registos deste tipo.

V. INSTALAÇÃO DO APARELHO DE CONTROLO

1. Instalação

- 239 Os aparelhos de controlo novos devem ser entregues não-activados aos instaladores ou fabricantes dos veículos, com todos os parâmetros de instalação, constantes da secção III.20, 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”.
- 240 Antes da activação, o aparelho de controlo deve dar acesso à função de calibração, mesmo que não esteja em modo de calibração.
- 241 Antes da activação, o aparelho de controlo não deve registar nem memorizar dados referidos nas secções 3.12.3 a 3.12.9 e nas secções 3.12.12 a 3.12.14, inclusive.
- 242 Durante a instalação, o fabricante do veículo deve pré-ajustar todos os parâmetros conhecidos.
- 243 O instalador ou fabricante do veículo deve activar o aparelho instalado antes de o veículo abandonar o local da instalação.
- 244 A activação do aparelho de controlo deve ser automaticamente accionada pela primeira inserção de um cartão de centro de controlo em qualquer das suas interfaces.
- 245 As eventuais operações específicas de emparelhamento entre o sensor de movimentos e a unidade-veículo devem processar-se automaticamente ante ou durante a activação.
- 246 Uma vez activado, o aparelho de controlo deve cumprir plenamente as funções e os direitos de acesso aos dados.
- 247 As funções de registo e de memorização do aparelho de controlo devem ficar plenamente operacionais após a activação.
- 248 À instalação deve seguir-se uma calibração. A primeira calibração incluirá a introdução do VRN e terá lugar no prazo de duas semanas após a última das seguintes operações: instalação ou atribuição do VRN.
- 248a 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.

2. Placa de instalação

- 249 Verificada a instalação do aparelho de controlo, deve ser afixada uma placa de instalação claramente legível e facilmente acessível, em cima, dentro ou ao lado do aparelho de controlo. No final de qualquer inspecção efectuada por um agente instalador ou centro/oficina homologado, a placa anterior deve ser substituída por uma nova placa.
- 250 Na placa devem figurar pelo menos os seguintes elementos:
- nome, endereço ou designação comercial do agente instalador ou centro/oficina homologado,
 - coeficiente característico do veículo, sob a forma “w = ... imp/km”,
 - constante do aparelho de controlo, sob a forma “k = ... imp/km”,
 - perímetro efectivo dos pneus das rodas, sob a forma “l = ... mm”,
 - medida do pneumático,
 - data de determinação do coeficiente característico do veículo e de medição do perímetro efectivo dos pneus das rodas,
 - número de identificação do veículo (NIV).

3. Selagem

- 251 Devem ser seladas as seguintes peças:
- quaisquer ligações que, uma vez desfeitas, possam causar alterações indetectáveis ou perda indetectável de dados,
 - placa de instalação, excepto se for fixa de tal modo que não possa ser removida sem se destruírem as suas marcações.
- 252 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 correctamente e ser de novo selado por um agente instalador ou centro/oficina homologado (em conformidade com a secção 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.
- 253 Cada vez que os selos forem removidos, deve ser redigida e disponibilizada à autoridade competente uma declaração de motivos.

VI. VERIFICAÇÕES, INSPECÇÕES E REPARAÇÕES

Os requisitos aplicáveis à remoção dos selos, nos termos do artigo 12.º, n.º 5, do Regulamento (CEE) n.º 3821/85 do Conselho, com a última redacção que lhe foi dada pelo Regulamento (CE) n.º 2135/98, figuram na secção V.3, do presente anexo.

1. Homologação de agentes e de centros/oficinas de instalação

Os Estados-Membros homologarão, sujeitarão a controlo regular e certificarão os organismos responsáveis pelas seguintes operações:

- instalação,
- verificação,
- inspecção,
- reparação.

No âmbito do artigo 12.º, n.º 1, do presente regulamento, os cartões de centro de ensaio serão emitidos unicamente em nome de instaladores e/ou oficinas homologados para efeitos de activação e/ou calibração dos aparelhos de controlo, em conformidade com o presente anexo e, salvo devida justificação:

- não elegíveis para atribuição de cartão de empresa,
- cujas restantes actividades profissionais não representem um compromisso potencial para a segurança geral do sistema, na acepção do apêndice 10.

2. Verificação de instrumentos novos ou reparados

- 254 Cada dispositivo individual, novo ou reparado, deve ser verificado a respeito do seu funcionamento correcto e da precisão dos seus registos e leituras, dentro dos limites estabelecidos nas secções 3.2.1 e 3.2.2, por meio de selagem nos termos da secção V.3 e de calibração.

3. Inspeção da instalação

- 255 Na fixação a um veículo, o conjunto da instalação (incluindo o aparelho de controlo) deve cumprir o disposto em matéria de tolerâncias máximas (secções 3.2.1 e 3.2.2).

4. Inspeções periódicas

- 256 Após qualquer reparação dos aparelhos, após qualquer alteração do coeficiente característico do veículo ou do perímetro efectivo dos pneus das rodas, quando a hora UTC do aparelho de controlo apresentar desfasamentos superiores a 20 minutos, quando o VRN for alterado e pelo menos uma vez no prazo de dois anos (24 meses) após a última inspecção, devem ser efectuadas inspeções periódicas aos aparelhos instalados nos veículos.

- 257 Estas inspeções devem incluir as seguintes verificações:
- funcionamento correcto do aparelho de controlo, incluindo a função de memorização de dados nos cartões tacográficos,
 - cumprimento do disposto nas secções 3.2.1 e 3.2.2 em matéria de tolerâncias máximas para a instalação,

- colocação da marca de homologação de tipo,
- colocação da placa de instalação,
- estado dos selos no aparelho de controlo e nas outras peças da instalação,
- medida do pneumático e perímetro efectivo dos pneumáticos das rodas.

258 Estas inspecções devem incluir uma calibração.

5. Medição de erros

259 A medição de erros na instalação e durante a utilização deve ser efectuada segundo as condições que se seguem e que serão consideradas condições normais de teste ou ensaio:

- veículo sem carga e em ordem normal de marcha,
- pressão dos pneus conforme às instruções do fabricante,
- desgaste dos pneus conforme aos limites autorizados pela legislação nacional,
- movimento do veículo:
 - movimento de avanço, por acção do seu próprio motor, em linha recta, em terreno plano e à velocidade de 50 ± 5 km/h, sendo de 1 000 m a distância mínima de medição,
- sob condição de terem precisão comparável, métodos alternativos, como um banco de ensaios adequado.

6. Reparações

260 Os centros de ensaio devem poder descarregar dados do aparelho de controlo para a empresa de transportes pertinente.

261 O centro/oficina homologado deve emitir em nome da empresa de transportes um certificado relativo à impossibilidade de descarregamento de dados quando um mau funcionamento do aparelho de controlo inviabilizar o descarregamento de dados previamente registados, mesmo após reparação efectuada por esse centro/oficina. O centro/oficina guardará, durante o período mínimo de um ano, uma cópia de cada certificado emitido.

VII. EMISSÃO DE CARTÕES

Os processos de emissão de cartões estabelecidos pelos Estados-Membros devem cumprir as seguintes condições:

- 262 O número de um cartão tacográfico relativo à sua primeira emissão em nome de um requerente deve ter um índice de série (eventualmente), um índice de substituição e um índice de renovação ajustado a "0".
- 263 Os números dos cartões tacográficos não pessoais emitidos em nome de um só organismo de controlo, de um só centro de ensaio ou de uma só empresa de transportes devem ter os mesmos 13 primeiros algarismos, mas diferentes índices de série.
- 264 Um cartão tacográfico emitido em substituição de outro existente deve ter o mesmo número do cartão substituído, com excepção do índice de substituição, que é acrescido de "1" (segundo a ordem 0, ..., 9, A, ..., Z).
- 265 Um cartão tacográfico emitido em substituição de outro existente deve ter o mesmo prazo de validade do substituído.
- 266 Um cartão tacográfico emitido para renovação de outro existente deve ter o mesmo número do cartão renovado, com excepção do índice de substituição, que é ajustado a "0", e do índice de renovação, que é acrescido de "1" (segundo a ordem 0, ..., 9, A, ..., Z).
- 267 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.
- 268 O "apelido do portador" em cartões de controlo ou de centro de ensaio (cartões não pessoais) deve ser preenchido com a designação do organismo de controlo ou do centro de ensaio.

VIII. HOMOLOGAÇÃO DE TIPO DOS APARELHOS DE CONTROLO E DOS CARTÕES TACOGRAFÍCOS

1. Generalidades

Na acepção da presente secção, por “aparelho de controlo” entende-se “o aparelho de controlo e os seus componentes”. Não é necessária homologação de tipo para os cabos que ligam o sensor de movimentos à VU. O papel utilizado no aparelho de controlo é considerado um componente do mesmo.

- 269 O aparelho de controlo deve ser apresentado à homologação acompanhado de quaisquer dispositivos integrados adicionais.
- 270 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 ser declarados por certificados correspondentes.
- 271 As autoridades responsáveis pela homologação de tipo nos Estados-Membros não podem emitir certificados de homologação de tipo em conformidade com o disposto no artigo 5.º do presente regulamento se não lhes forem disponibilizados:
- um certificado de segurança,
 - um certificado de funcionalidade,
 - um certificado de interoperabilidade,

para o aparelho de controlo ou o cartão tacográfico que são objecto do pedido de homologação de tipo.

- 272 Qualquer modificação no suporte lógico (software), no equipamento informático (hardware) 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 confirmará ao fabricante a extensão da homologação ou pedirá uma actualização ou confirmação dos certificados de segurança, de funcionalidade e/ou de interoperabilidade.
- 273 Os procedimentos tendentes à reclassificação (beneficiação) *in-situ* do suporte lógico aplicado ao aparelho de controlo devem ser homologados pela autoridade que concedeu a homologação de tipo deste último. A beneficiação do suporte lógico não deve alterar nem apagar dados memorizados no aparelho de controlo e relativos às actividades dos condutores. A beneficiação do suporte lógico só pode ser efectuada sob a responsabilidade do fabricante do aparelho.

2. Certificado de segurança

- 274 O certificado de segurança é entregue em conformidade com o disposto no apêndice 10 do presente anexo.

3. Certificado de funcionalidade

- 275 Os candidatos à homologação de tipo devem fornecer às autoridades nacionais competentes todo o material e documentação que estas queiram.
- 276 Ao fabricante só poderá ser concedido um certificado de funcionalidade depois de efectuados com êxito pelo menos todos os ensaios de funcionalidade especificados no apêndice 9.
- 277 A autoridade responsável pela homologação de tipo emite o certificado de funcionalidade, do qual, para além do nome do beneficiário e da identificação do modelo, constará uma lista dos ensaios executados e dos respectivos resultados.

4. Certificado de interoperabilidade

- 278 Os ensaios de interoperabilidade são executados por um laboratório, sob a autoridade e a responsabilidade da Comissão Europeia.
- 279 O laboratório regista, segundo a ordem cronológica de chegada, os pedidos de ensaio de interoperabilidade apresentados pelos fabricantes.
- 280 Os pedidos de ensaio só serão 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,
 - certificado de segurança correspondente,
 - certificado de funcionalidade correspondente.

A data de registo do pedido é comunicada ao fabricante.

- 281 O laboratório não poderá efectuar ensaios de interoperabilidade para aparelhos de controlo e cartões tacográficos relativamente aos quais não tenham sido emitidos certificados de segurança e certificados de funcionalidade.
- 282 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 mesmo.

283 Os ensaios de interoperabilidade serão executados, em conformidade com o disposto no n.º 5 do apêndice 9 do presente anexo, respectivamente 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.

284 O certificado de interoperabilidade só será passado pelo laboratório ao fabricante depois de executados com êxito todos os ensaios de interoperabilidade requeridos.

285 Se os ensaios de interoperabilidade não tiverem êxito relativamente a um ou mais aparelhos de controlo ou cartões tacográficos, conforme dispõe o n.º 283, o certificado de interoperabilidade não será emitido até o fabricante requerente efectuar as modificações necessárias e obter resultados positivos nos ensaios. O laboratório identificará a causa do problema com a ajuda dos fabricantes afectos à falha de interoperabilidade e procurará 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.

286 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.

287 Os elementos susceptíveis de originar falhas de interoperabilidade não podem ser utilizados para a obtenção de vantagens ou posições dominantes.

5. Certificado de homologação de tipo

288 A autoridade nacional competente pode emitir o certificado de homologação de tipo logo que disponha dos três certificados requeridos.

289 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.

290 O laboratório competente para os ensaios de interoperabilidade deve gerir um sítio público na internet do qual constará uma lista actualizada 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.

6. Recurso extraordinário: primeiros certificados de interoperabilidade

291 Durante o período de quatro meses após um conjunto de aparelho de controlo e cartões tacográficos (cartão de condutor, cartão de controlo, cartão de centro de ensaio e cartão de empresa) ter sido certificado pela primeira vez como interoperável, será considerado provisório qualquer certificado de interoperabilidade (incluindo esse primeiro) emitido em resposta a pedidos registados ao longo do referido período.

292 Se, no final do referido período, todos os produtos em causa forem mutuamente interoperáveis, tornar-se-ão efectivos os correspondentes certificados de interoperabilidade.

293 Se, ao longo do referido período, forem detectadas falhas de interoperabilidade, o laboratório responsável pelos ensaios de interoperabilidade identificará as causas dos problemas com a ajuda dos fabricantes envolvidos e convidá-los-á a efectuarem as necessárias modificações.

294 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, determinará as causas dessas falhas e estabelecerá as modificações a introduzir por cada um dos fabricantes envolvidos. A procura de soluções técnicas prolongar-se-á 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, decidirá qual ou quais os aparelhos de controlo e cartões tacográficos que devem receber certificado definitivo de interoperabilidade, com especificação dos motivos.

295 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 n.º 294, ficarão em suspenso até se encontrarem resolvidos os problemas iniciais de interoperabilidade. Os pedidos serão então processados segundo a ordem cronológica do registo.

*Apêndice 1***DICIONÁRIO DE DADOS****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 abstracta um" ou ASN.1), o que permite que dados simples e estruturados sejam definidos sem uma 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/CEI 8824-1, o que tem as seguintes implicações:

- sempre que possível, a significação do tipo de dado está implícita nos nomes seleccionados;
- 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 caracteres 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 susceptível 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. Os identificadores de gamas de valores são definidos na secção 3.

1.2. Referências

No presente apêndice, são utilizadas as seguintes referências:

- | | |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ISO 639 | Code for the representation of names of languages. First Edition: 1988. |
| EN 726-3 | Identification cards systems — Telecommunications integrated circuit(s) cards and terminals — Part 3: Application independent card requirements. December 1994. |
| ISO 3779 | Road vehicles — Vehicle identification number (VIN) — Content and structure. Edition 3: 1983. |
| ISO/CEI 7816-5 | Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 5: Numbering system and registration procedure for application identifiers. First edition: 1994 + Amendment 1: 1996. |
| ISO/CEI 8824-1 | Information technology — Abstract Syntax Notation 1 (ASN.1): Specification of basic notation. Edition 2: 1998. |
| ISO/CEI 8825-2 | Information technology — ASN.1 encoding rules: Specification of Packed Encoding Rules (PER). Edition 2: 1998. |
| ISO/CEI 8859-1 | Information technology — 8 bit single-byte coded graphic character sets — Part 1: Latin alphabet Nº 1. First edition: 1998. |
| ISO/CEI 8859-7 | Information technology — 8 bit single-byte coded graphic character sets — Part 7: Latin/Greek alphabet. First edition: 1987. |
| ISO 16844-3 | Road vehicles — Tachograph systems — Motion Sensor Interface. WD 3-20/05/99. |

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 dado com bytes 'FF'.

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 (mudanças) na actividade e/ou alterações na situação da condução e/ou alterações na situação do cartão, quer para o condutor principal quer para o ajudante. Este tipo de dado está relacionado com os requisitos 084, 109a, 199 e 219.

ActivityChangeInfo ::= OCTET STRING (SIZE(2))

Comprimento atribuído — Alinhamento de octetos: 'scpaatttttttttttt' B (16 bits)

Para registos na memória de dados:

's' B	Ranhura:
	'0' B: DRIVER,
	'1' B: 2. CO-DRIVER,
'c' B	Situação da condução:
	'0' B: SINGLE,
	'1' B: CREW,
'p' B	Situação do cartão de condutor (ou de centro de ensaio) na ranhura pertinente:
	'0' B: INSERTED, está inserido um cartão,
	'1' B: NOT INSERTED, não está inserido nenhum cartão (ou foi retirado um),
'aa' B	Actividade:
	'00' B: BREAK/REST,
	'01' B: AVAILABILITY,
	'10' B: WORK,
	'11' B: DRIVING,
'tttttttttttt' B	Momento da mudança: quantidade de minutos desde as 00h00 no dia em questão.

Para registos no cartão de condutor (ou de centro de ensaio):

's' B	Ranhura (não pertinente quando 'p' = 1, excepto nota <i>infra</i>):	
	'0' B: DRIVER,	
	'1' B: 2. CO-DRIVER,	
'c' B	Situação da condução (caso 'p' = 0) ou cf. situação da actividade (caso 'p' = 1):	
	'0' B: SINGLE,	'0' B: UNKNOWN
	'1' B: CREW,	'1' B: KNOWN (= entrada manual)
'p' B	Situação do cartão:	
	'0' B: INSERTED, o cartão está inserido num aparelho de controlo,	
	'1' B: NOT INSERTED, o cartão não está inserido (ou foi retirado),	

'aa'B Actividade (não pertinente quando 'p' = 1 e 'c' = 0, excepto nota *infra*):

'00'B: BREAK/REST,

'01'B: AVAILABILITY,

'10'B: WORK,

'11'B: DRIVING,

'ttttttttttt'B Momento da mudança: quantidade de minutos desde as 00h00 no dia em questão.

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 0,
- 'aa' deve codificar a actividade em curso, seleccionada no momento.

Em resultado de uma entrada manual, os bits 'c' e 'aa' da palavra (memorizada num cartão) podem ser posteriormente reescritos por cima, reflectindo a entrada.

2.2. Address

Um endereço.

```
Address ::= SEQUENCE {
    codePage          INTEGER (0..255),
    address           OCTET STRING (SIZE(35))
}
```

codePage especifica a parte da norma ISO/CEI 8859 utilizada para codificar o endereço,

address é um endereço codificado em conformidade com a norma ISO/CEI 8859-codePage.

2.3. BCDString

BCDString aplica-se na representação de Binary Code Decimal (“código binário decimal” ou BCD). Este tipo de dado é utilizado para representar um algarismo decimal num semi-octeto (4 bits). BCDString baseia-se em “CharacterString-Type” da norma ISO/CEI 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 semi-octeto mais significativo do primeiro octeto. Para produzir um múltiplo de octetos, devem ser inseridos os necessários semi-octetos de zeros à direita, a partir da posição de semi-octeto mais à esquerda no primeiro octeto.

Algarismos autorizados: 0, 1, ... 9.

2.4. 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.

```
CalibrationPurpose ::= OCTET STRING (SIZE(1))
```

Comprimento atribuído:

- '00'H valor reservado,
- '01'H activação: registo de parâmetros de calibração conhecidos, no momento da activação da VU,

'02'H primeira instalação: primeira calibração da VU depois de activada,

'03'H instalação: primeira calibração da VU no veículo actual,

'04'H inspecção periódica.

2.5. CardActivityDailyRecord

Informação memorizada num cartão e relativa às actividades de condutor num determinado dia de calendário. Este tipo de dado está relacionado com os requisitos 199 e 219.

```
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 na secção 3). 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.

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 actividade por minuto). Este conjunto inclui sempre a ActivityChangeInfo que codifica a situação do condutor às 00h00.

2.6. CardActivityLengthRange

Número de bytes num cartão de condutor ou de centro de ensaio, disponíveis para memorizar registos da actividade de condutor.

```
CardActivityLengthRange ::= INTEGER(0..216-1)
```

Comprimento atribuído: ver secção 3.

2.7. CardApprovalNumber

Número de homologação do tipo de cartão.

```
CardApprovalNumber ::= IA5String(SIZE(8))
```

Comprimento atribuído: não especificado.

2.8. CardCertificate

Certificado da chave pública de um cartão.

```
CardCertificate ::= Certificate
```

2.9. CardChipIdentification

Informação memorizada num cartão e relativa à identificação do circuito integrado (CI) desse cartão (requisito 191).

```
CardChipIdentification ::= SEQUENCE {
    icSerialNumber                OCTET STRING (SIZE(4)),
    icManufacturingReferences     OCTET STRING (SIZE(4))
}
```


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.

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 relativos à actividade de condutor (estrutura dos dados: CardActivityDailyRecord) por cada dia de calendário em que o cartão tenha sido utilizado.

Comprimento atribuído: esta cadeia de octetos é ciclicamente preenchida com registos de CardActivityDailyRecord. Na primeira utilização, a memorização é iniciada 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 uma descontinuidade dentro de um elemento de dado. Antes de se colocarem novos dados de actividade na cadeia (aumentando o actual activityDailyRecord ou colocando um novo activityDailyRecord) em substituição dos dados de actividade mais antigos, o activityPointerOldestDayRecord tem de ser actualizado, em reflexo da nova localização do mais antigo registo diário completo, e a activityPreviousRecordLength deste (novo) registo diário completo mais antigo deve ser fixada em 0.

2.14. CardDrivingLicenceInformation

Informação memorizada num cartão de condutor e relativa aos dados da carta de condução do titular do cartão (requisito 196).

```
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.

2.15. CardEventData

Informação memorizada num cartão de condutor ou de centro de ensaio e relativa aos incidentes associados ao titular do cartão (requisitos 204 e 223).

```
CardEventData ::= SEQUENCE SIZE(6) OF {
    cardEventRecords                SET SIZE(NoOfEventsPerType) OF
                                     CardEventRecord
}
```

CardEventData é uma sequência de registos cardEventRecords (com excepção 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).

2.16. CardEventRecord

Informação memorizada num cartão de condutor ou de centro de ensaio e relativa a um incidente associado ao titular do cartão (requisitos 205 e 223).

```
CardEventRecord ::= SEQUENCE {
    eventType                        EventFaultType,
    eventBeginTime                   TimeReal,
    eventEndTime                     TimeReal,
    eventVehicleRegistration         VehicleRegistrationIdentification
}
```

eventType é o tipo do incidente.

eventBeginTime é a data e a hora do início do incidente.

eventEndTime é a data e a hora do final do incidente.

eventVehicleRegistration é o VRN (número de matrícula) e o Estado-Membro de registo do veículo no qual ocorreu o incidente.

2.17. CardFaultData

Informação memorizada num cartão de condutor ou de centro de ensaio e relativa às falhas associadas ao titular do cartão (requisitos 207 e 223).

```
CardFaultData ::= SEQUENCE SIZE(2) OF {
    cardFaultRecords                               SET SIZE(NoOfFaultsPerType) OF
                                                    CardFaultRecord
}
```

CardFaultData é uma 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 é um conjunto de registos de falhas de determinada categoria (falhas do aparelho de controlo ou do cartão).

2.18. CardFaultRecord

Informação memorizada num cartão de condutor ou de centro de ensaio e relativa a uma falha associada ao titular do cartão (requisitos 208 e 223).

```
CardFaultRecord ::= SEQUENCE {
    faultType                                     EventFaultType,
    faultBeginTime                               TimeReal,
    faultEndTime                                 TimeReal,
    faultVehicleRegistration                     VehicleRegistrationIdentification
}
```

faultType é o tipo da falha.

faultBeginTime é a data e a hora do início da falha.

faultEndTime é a data e a hora do final da falha.

faultVehicleRegistration é o VRN (número de matrícula) e o Estado-Membro de registo do veículo no qual ocorreu a falha.

2.19. CardIccIdentification

Informação memorizada num cartão e relativa à identificação do circuito integrado (CI) (requisito 192).

```
CardIccIdentification ::= SEQUENCE {
    clockStop                                     OCTET STRING (SIZE(1)),
    cardExtendedSerialNumber                     ExtendedSerialNumber,
    cardApprovalNumber                           CardApprovalNumber
    cardPersonaliserID                           OCTET STRING (SIZE(1)),
    embedderIcAssemblerId                       OCTET STRING (SIZE(5)),
    icIdentifier                                  OCTET STRING (SIZE(2))
}
```

clockStop é o modo Clockstop (relógio parado), cf. definição na norma EN 726-3.

cardExtendedSerialNumber é o número de série do cartão de CI e a sua referência de fabrico, cf. definição na norma EN 726-3 e especificação através do tipo de dado ExtendedSerialNumber.

cardApprovalNumber é o número de homologação de tipo do cartão.

cardPersonaliserID é a ID personalizadora do cartão, cf. definição na norma EN 726-3.

embedderIcAssemblerId é o identificador do fabricante ou montador do CI, cf. definição na norma EN 726-3.

icIdentifier é o identificador do CI no cartão e do seu fabricante, cf. definição na norma EN 726-3.

2.20. CardIdentification

Informação memorizada num cartão e relativa à sua identificação (requisitos 194, 215, 231 e 235).

```
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 actual titular.

cardValidityBegin é a data de início da validade do cartão.

cardExpiryDate é a data-limite da validade do cartão.

2.21. CardNumber

Um número de cartão, em conformidade com a definição g do presente anexo I(B).

```
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 um centro de ensaio 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 um centro de ensaio, de um organismo de controlo ou de uma empresa.

2.22. CardPlaceDailyWorkPeriod

Informação memorizada num cartão de condutor ou de centro de ensaio e relativa aos locais onde se iniciam e/ou terminam os períodos de trabalho diário (requisitos 202 e 221).

```
CardPlaceDailyWorkPeriod ::= SEQUENCE {
    placePointerNewestRecord      INTEGER(0..NoOfCardPlaceRecords-1),
    placeRecords                  SET SIZE(NoOfCardPlaceRecords) OF PlaceRecord
}
```

placePointerNewestRecord é o índice do último registo actualizado do local.

Comprimento atribuído: número correspondente ao numerador do registo do local, começando por '0' à primeira ocorrência de registos de local na estrutura.

placeRecords é o conjunto dos registos que contêm informação acerca dos locais introduzidos.

2.23. CardPrivateKey

A chave privada de um cartão.

```
CardPrivateKey ::= RSAKeyPrivateExponent
```

2.24. CardPublicKey

A chave pública de um cartão.

```
CardPublicKey ::= PublicKey
```

2.25. CardRenewalIndex

O índice de renovação de um cartão [definição i do presente anexo I(B)].

```
CardRenewalIndex ::= IA5String(SIZE(1))
```

Comprimento atribuído: (ver secção VII do presente anexo).

'0' Primeira emissão.

Ordem de acréscimo: '0, ..., 9, A, ..., Z'

2.26. CardReplacementIndex

O índice de substituição de um cartão [definição j do presente anexo I(B)].

```
CardReplacementIndex ::= IA5String(SIZE(1))
```

Comprimento atribuído: (ver secção VII do presente anexo).

'0' Cartão original.

Ordem de acréscimo: '0, ..., 9, A, ..., Z'

2.27. CardSlotNumber

Código que distingue as duas ranhuras de uma unidade-veículo (ranhura do condutor principal e ranhura do ajudante).

```
CardSlotNumber ::= INTEGER {
    driverSlot          (0),
    co-driverSlot      (1)
}
```

Comprimento atribuído: sem mais especificações.

2.28. CardSlotsStatus

Código que indica o tipo dos cartões inseridos nas duas ranhuras da unidade-veículo.

```
CardSlotsStatus ::= OCTET STRING (SIZE(1))
```

Comprimento atribuído — Alinhamento de octetos: 'ccccddd'B

'cccc'B Identificação do tipo de cartão inserido na ranhura do ajudante,
 'ddd'B Identificação do tipo de cartão inserido na ranhura do condutor principal,
 com os seguintes códigos de identificação:

'0000'B nenhum cartão inserido,
 '0001'B inserido um cartão de condutor,
 '0010'B inserido um cartão de centro de ensaio,
 '0011'B inserido um cartão de controlo,
 '0100'B inserido um cartão de empresa.

2.29. CardStructureVersion

Código que indica a versão da estrutura aplicada num cartão tacográfico.

CardStructureVersion ::= OCTET STRING (SIZE(2))

Comprimento atribuído: 'aabb'H:

'aa'H Índice para alterações da estrutura,
 'bb'H Índice para alterações relativas à utilização dos elementos de dados definidos para a estrutura dada pelo byte elevado.

2.30. CardVehicleRecord

Informação memorizada num cartão de condutor ou de centro de ensaio e relativa a um período de utilização de um veículo durante um dia de calendário (requisitos 197 e 217).

```
CardVehicleRecord ::= SEQUENCE {
    vehicleOdometerBegin           OdometerShort,
    vehicleOdometerEnd            OdometerShort,
    vehicleFirstUse               TimeReal,
    vehicleLastUse                TimeReal,
    vehicleRegistration           VehicleRegistrationIdentification,
    vuDataBlockCounter            VuDataBlockCounter
}
```

vehicleOdometerBegin é o valor odométrico do veículo no início do período da sua utilização.

vehicleOdometerEnd é o valor odométrico 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 registo do veículo.

vuDataBlockCounter é o valor exibido pelo vuDataBlockCounter (contador do bloco de dados da VU) aquando da última extracção do período de utilização do veículo.

2.31. CardVehiclesUsed

Informação memorizada num cartão de condutor ou de centro de ensaio e relativa aos veículos utilizados pelo titular do cartão (requisitos 197 e 217).

```
CardVehiclesUsed ::= SEQUENCE {
    vehiclePointerNewestRecord    INTEGER(0..NoOfCardVehicleRecords-1),
    cardVehicleRecords           SET SIZE(NoOfCardVehicleRecords) OF
                                CardVehicleRecord
}
```

vehiclePointerNewestRecord é o índice do último registo actualizado do veículo.

Comprimento atribuído: número correspondente ao numerador do registo do veículo, começando por '0' à primeira ocorrência de registos do veículo na estrutura.

cardVehicleRecords é o conjunto dos registos que contém informação acerca dos veículos utilizados.

2.32. Certificate

Certificado de uma chave pública emitida por uma autoridade certificadora.

Certificate ::= OCTET STRING (SIZE(194))

Comprimento atribuído: assinatura digital com recuperação parcial de um CertificateContent (conteúdo de certificado) em conformidade com os Mecanismos comuns de segurança (apêndice 11): assinatura (128 bytes) || remanescente da chave pública (58 bytes) || referência da autoridade certificadora (8 bytes).

2.33. CertificateContent

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 correspondente certificado.

Comprimento atribuído: '01h' para esta versão.

CertificationAuthorityReference identifica a autoridade certificadora 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.

2.34. CertificateHolderAuthorisation

Identificação dos direitos do titular de um certificado.

```
CertificateHolderAuthorisation ::= SEQUENCE {
    tachographApplicationID        OCTET STRING(SIZE(6))
    equipmentType                  EquipmentType
}
```

tachographApplicationID é o identificador da aplicação tacográfica.

Comprimento atribuído: 'FFh' '54h' '41h' '43h' '48h' '4Fh'. Este AID é um identificador de aplicação não-registada de proprietário, em conformidade com a norma ISO/CEI 7816-5.

equipmentType é a identificação do tipo de equipamento ao qual se refere o certificado.

Comprimento atribuído: em conformidade com o tipo de dado EquipmentType. 0 se se tratar do certificado de um Estado-Membro.

2.35. CertificateRequestID

Identificação, única, de um pedido de certificado. Pode também ser utilizada como identificador da chave pública de uma unidade-veículo se o número de série da VU à qual a chave se destina não for conhecido no momento da geração do certificado.

```
CertificateRequestID ::= SEQUENCE {
    requestSerialNumber      INTEGER(0..232-1)
    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.

Comprimento atribuído: codificação BCD do mês (dois algarismos) e do ano (os dois últimos algarismos).

crIdentifier é um identificador que estabelece a distinção entre um pedido de certificado e um número de série alargado.

Comprimento atribuído: 'FFh'.

manufacturerCode é o código numérico do fabricante que pede o certificado.

2.36. CertificationAuthorityKID

Identificador da chave pública de uma autoridade certificadora nacional ou da autoridade certificadora europeia.

```
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 certificadora nacional.

keySerialNumber é um número de série que distingue as diferentes chaves da autoridade certificadora caso sejam alteradas.

additionalInfo additionalInfo é um campo de dois bytes para codificações adicionais (específico da autoridade certificadora).

caIdentifier caIdentifier é um identificador que estabelece a distinção entre o identificador da chave de uma autoridade certificadora e outros identificadores de chave.

Comprimento atribuído: '01h'.

2.37. CompanyActivityData

Informação memorizada num cartão de empresa e relativa às actividades executadas com o cartão (requisito 237).

```
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 (“registo da actividade da empresa”) actualizado.

Comprimento atribuído: número correspondente ao numerador do registo da actividade da empresa, começando por '0' à primeira ocorrência de registos da actividade da empresa na estrutura.

companyActivityRecords é o conjunto de todos os registos de actividade da empresa.

companyActivityRecord é a sequência de informação relativa à actividade da empresa.

companyActivityType é o tipo em que se integra a actividade da empresa.

companyActivityTime é a data e a hora da actividade da empresa.

cardNumberInformation é o número e o Estado-Membro emissor do cartão eventualmente descarregado.

vehicleRegistrationInformation é o VRN (número de matrícula) e o Estado-Membro de registo do veículo descarregado, bloqueado ou desbloqueado.

downloadPeriodBegin e **downloadPeriodEnd** é o período eventualmente descarregado da VU.

2.38. CompanyActivityType

Código que indica uma actividade executada por uma empresa, utilizando o respectivo cartão.

```

CompanyActivityType ::= INTEGER {
  card downloading          (1),
  VU downloading           (2),
  VU lock-in                (3),
  VU lock-out               (4)
}

```

2.39. CompanyCardApplicationIdentification

Informação memorizada num cartão de empresa e relativa à identificação da aplicação do cartão (requisito 190).

```

CompanyCardApplicationIdentification ::= SEQUENCE {
  typeOfTachographCardId   EquipmentType,
  cardStructureVersion      CardStructureVersion,
  noOfCompanyActivityRecords NoOfCompanyActivityRecords
}

```

typeOfTachographCardId especifica o tipo de cartão aplicado.

cardStructureVersion especifica a versão da estrutura que é aplicada no cartão.

noOfCompanyActivityRecords é o número de registos de actividade da empresa que o cartão pode memorizar.

2.40. CompanyCardHolderIdentification

Informação memorizada num cartão de empresa e relativa à identificação do seu titular (requisito 236).

```

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.

2.41. ControlCardApplicationIdentification

Informação memorizada num cartão de controlador e relativa à identificação da aplicação do cartão (requisito 190).

```
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 actividade de controlo que o cartão pode memorizar.

2.42. ControlCardControlActivityData

Informação memorizada num cartão de controlador e relativa à actividade de controlo executada com o cartão (requisito 233).

```
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 actualizado da actividade de controlo.

Comprimento atribuído: Número correspondente ao numerador do registo da actividade de controlo, começando por '0' à primeira ocorrência de registos da actividade de controlo na estrutura.

controlActivityRecords é o conjunto de todos os registos de actividade de controlo.

controlActivityRecord é a sequência de informação relativa a um controlo.

controlType é o tipo em que se integra o 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 (número de matrícula) e o Estado-Membro de registo do veículo no qual o controlo foi efectuado.

controlDownloadPeriodBegin e **controlDownloadPeriodEnd** é o período eventualmente descarregado.

2.43. ControlCardHolderIdentification

Informação memorizada num cartão de controlador e relativa à identificação do titular do cartão (requisito 232).

```
ControlCardHolderIdentification ::= SEQUENCE {
    controlBodyName          Name,
    controlBodyAddress       Address,
    cardHolderName           HolderName,
    cardHolderPreferredLanguage Language
}
```

controlBodyName é o nome (a designação) 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.

cardHolderPreferredLanguage é o idioma preferencial do titular do cartão.

2.44. ControlType

Código que indica as actividades executadas durante um controlo. Este tipo de dado tem a ver com os requisitos 102, 210 e 225.

```
ControlType ::= OCTET STRING (SIZE(1))
```

Comprimento atribuído — Alinhamento de octetos: 'c'p'd'xxxx'B (8 bits)

'c'B descarregamento do cartão:
 '0'B: cartão não descarregado durante esta actividade de controlo,
 '1'B: cartão descarregado durante esta actividade de controlo

'v'B descarregamento da VU:
 '0'B: VU não descarregada durante esta actividade de controlo,
 '1'B: VU descarregada durante esta actividade de controlo

'p'B impressão ("printing"):
 '0'B: não efectuada impressão durante esta actividade de controlo,
 '1'B: efectuada impressão durante esta actividade de controlo

'd'B visualização ("display"):
 '0'B: não utilizada visualização durante esta actividade de controlo,
 '1'B: utilizada visualização durante esta actividade de controlo

'xxxx'B Não utilizado.

2.45. CurrentDateTime

Data e hora actuais do aparelho de controlo.

```
CurrentDateTime ::= TimeReal
```

Comprimento atribuído: sem mais especificações.

2.46. DailyPresenceCounter

Contador, memorizado num cartão de condutor ou de centro de ensaio, que vai sofrendo acréscimos unitários por cada dia de calendário em que o cartão tenha estado inserido numa VU. Este tipo de dado tem a ver com os requisitos 199 e 219.

```
DailyPresenceCounter ::= BCDString(SIZE(2))
```

Comprimento atribuído: Número consecutivo com o valor máximo de 9 999, recomeçando por 0. No momento da primeira emissão do cartão, o número é fixado em 0.

2.47. Datef

Data expressa num formato numérico que pode ser impresso de imediato.

```
Datef ::= SEQUENCE {
    year      BCDString(SIZE(2)),
    ano       BCDString(SIZE(1)),
    mês       BCDString(SIZE(1))
}
```

Comprimento atribuído:

aaaa Ano

mm Mês

dd Dia

'00000000'H não denota explicitamente qualquer data.

2.48. Distance

Uma distância percorrida (resulta do cálculo da diferença entre dois valores odométricos do veículo, em quilómetros).

```
Distance ::= INTEGER(0..216-1)
```

Comprimento atribuído: Valor em km no intervalo operacional de 0 a 9 999 km.

2.49. DriverCardApplicationIdentification

Informação memorizada num cartão de condutor e relativa à identificação da aplicação do cartão (requisito 190).

```
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 que é aplicada no cartão.

noOfEventsPerType é o número de incidentes, por tipo de incidente, que o cartão pode registar.

noOfFaultsPerType é o número de falhas, por tipo de falha, que o cartão pode registar.

activityStructureLength indica o número de bytes disponíveis para memorizar registos de actividade.

noOfCardVehicleRecords é o número de registos de veículos que o cartão pode conter.

noOfCardPlaceRecords é o número de registos de locais que o cartão pode registar.

2.50. DriverCardHolderIdentification

Informação memorizada num cartão de condutor e relativa à identificação do titular do cartão (requisito 195).

```
DriverCardHolderIdentification ::= SEQUENCE {
    cardHolderName                     HolderName,
    cardHolderBirthDate                Datef,
    cardHolderPreferredLanguage        Language
}
```

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.

2.51. 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.

```
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)
}
```

Comprimento atribuído: em conformidade com a norma ISO/IEC8824-1.

2.52. EquipmentType

Código que distingue diferentes tipos de equipamento para a aplicação tacográfica.

```
EquipmentType ::= INTEGER(0..255)
-- 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)
```

Comprimento atribuído: em conformidade com a norma ISO/IEC8824-1.

O valor 0 é reservado para designar um Estado-Membro ou a Europa no campo de certificados CHA.

2.53. EuropeanPublicKey

A chave pública europeia.

```
EuropeanPublicKey ::= PublicKey
```

2.54. EventFaultType

Código que qualifica um incidente ou uma falha.

```
EventFaultType ::= OCTET STRING (SIZE(1))
```

Comprimento atribuído:

'0x'H	Incidentes gerais,
'00'H	Sem mais pormenores,
'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 incorrectamente,
'07'H	Excesso de velocidade,

'08'H	Interrupção da alimentação energética,
'09'H	Erro nos dados de movimento,
'0A'H .. '0F'H	RFU ("ready for use", i.e., em situação operacional)
'1x'H	Incidentes de tentativa de violação da segurança relativos à VU,
'10'H	Sem mais pormenores,
'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 (i.e., do hardware),
'19'H .. '1F'H	RFU
'2x'H	Incidentes de tentativa de violação da segurança relativos ao sensor,
'20'H	Sem mais pormenores,
'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 hardware,
'26'H .. '2F'H	RFU,
'3x'H	Falhas do aparelho de controlo,
'30'H	Sem mais pormenores,
'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 .. '3F'H	RFU,
'4x'H	Falhas do cartão,
'40'H	Sem mais pormenores,
'41'H .. '4F'H	RFU,
'50'H .. '7F'H	RFU,
'80'H .. 'FF'H	Específico do fabricante.

2.55. EventFaultRecordPurpose

Código que explica por que foram registados um incidente ou uma falha.

EventFaultRecordPurpose ::= OCTET STRING (SIZE(1))

Comprimento 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	incidente ou falha activos ou em curso
'08'H .. '7F'H	RFU
'80'H .. 'FF'H	específico do fabricante.

2.56. ExtendedSerialNumber

Identificação, única, de um equipamento. Pode também ser utilizado como identificador da chave pública do equipamento.

```
ExtendedSerialNumber ::= SEQUENCE {
    serialNumber          INTEGER(0..232-1)
    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 do equipamento e para o mês *infra*.

monthYear é a identificação do mês e do ano de fabrico (ou de atribuição do número de série).

Comprimento atribuído: codificação BCD de Month (mês, com dois algarismos) e de Year (ano, com os dois últimos algarismos).

type é um identificador do tipo do equipamento.

Comprimento atribuído: específico do fabricante, com valor reservado 'FFh'.

manufacturerCode é o código numérico do fabricante do equipamento.

2.57. 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.

2.58. HighResOdometer

Valor odométrico do veículo. Cúmulo das distâncias percorridas pelo veículo durante o seu funcionamento.

```
HighResOdometer ::= INTEGER(0..232-1)
```

Comprimento atribuído: Binário sem sinal. Valor em l/200 km no intervalo operacional de 0 a 21 055 406 km.

2.59. HighResTripDistance

Distância percorrida durante um dia ou parte de um dia.

```
HighResTripDistance ::= INTEGER(0..232-1)
```

Comprimento atribuído: Binário sem sinal. Valor em l/200 km no intervalo operacional de 0 a 21 055 406 km.

2.60. 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.

Comprimento atribuído: Se o cartão não for pessoal, holderSurname (“apelido do titular”) contém a mesma informação que companyName (“nome ou designação da empresa”), workshopName (“nome ou designação do centro de ensaio”) ou controlBodyName (“nome ou designação do organismo de controlo”).

holderFirstNames é o nome próprio, eventualmente composto e com iniciais, do titular.

2.61. K-ConstantOfRecordingEquipment

Constante do aparelho de controlo [definição m do presente anexo I(B)].

K-ConstantOfRecordingEquipment ::= INTEGER(0..2¹⁶-1)

Comprimento atribuído: Impulsos por quilómetro no intervalo operacional de 0 a 64 255 imp/km.

2.62. KeyIdentifier

Identificador, único, de uma chave pública por ele referenciada e seleccionada. Identifica também o titular da chave.

```
KeyIdentifier ::= CHOICE {
    extendedSerialNumber          ExtendedSerialNumber,
    certificateRequestID           CertificateRequestID,
    certificationAuthorityKID      CertificationAuthorityKID
}
```

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.

2.63. L-TyreCircumference

Perímetro efectivo dos pneumáticos das rodas [definição u do presente anexo I(B)].

L-TyreCircumference ::= INTEGER(0..2¹⁶-1)

Comprimento atribuído: Binário sem sinal. Valor em 1/8 mm no intervalo operacional de 0 a 8 031 mm.

2.64. Language

Código identificativo de um idioma.

Language ::= IA5String(SIZE(2))

Comprimento atribuído: Código constituído por duas letras minúsculas, em conformidade com a norma ISO 639.

2.65. LastCardDownload

Data e hora, memorizados num cartão de condutor e relativos ao último descarregamento do cartão (para outras finalidades que não o controlo). Este dado é actualizável por uma VU ou por qualquer leitor de cartões.

LastCardDownload ::= TimeReal

Comprimento atribuído: sem mais especificações.

2.66. ManualInputFlag

Código que identifica se o titular introduziu manualmente actividades de condutor no momento da inserção do cartão (requisito 081).

```
ManualInputFlag ::= INTEGER {
    noEntry                (0)
    manualEntries          (1)
}
```

Comprimento atribuído: sem mais especificações.

2.67. ManufacturerCode

Código identificativo de um fabricante.

```
ManufacturerCode ::= INTEGER(0..255)
```

Comprimento atribuído:

'00'H	Sem informação disponível
'01'H	Valor reservado
'02'H .. '0F'H	Reservado para utilização futura
'10'H	ACTIA
'11'H .. '17'H	Reservado a fabricantes cujo nome comece por 'A'
'18'H .. '1F'H	Reservado a fabricantes cujo nome comece por 'B'
'20'H .. '27'H	Reservado a fabricantes cujo nome comece por 'C'
'28'H .. '2F'H	Reservado a fabricantes cujo nome comece por 'D'
'30'H .. '37'H	Reservado a fabricantes cujo nome comece por 'E'
'38'H .. '3F'H	Reservado a fabricantes cujo nome comece por 'F'
'40'H	Giesecke & Devrient GmbH
'41'H	GEM plus
'42'H .. '47'H	Reservado a fabricantes cujo nome comece por 'G'
'48'H .. '4F'H	Reservado a fabricantes cujo nome comece por 'H'
'50'H .. '57'H	Reservado a fabricantes cujo nome comece por 'I'
'58'H .. '5F'H	Reservado a fabricantes cujo nome comece por 'J'
'60'H .. '67'H	Reservado a fabricantes cujo nome comece por 'K'
'68'H .. '6F'H	Reservado a fabricantes cujo nome comece por 'L'
'70'H .. '77'H	Reservado a fabricantes cujo nome comece por 'M'
'78'H .. '7F'H	Reservado a fabricantes cujo nome comece por 'N'
'80'H	OSCARD
'81'H .. '87'H	Reservado a fabricantes cujo nome comece por 'O'
'88'H .. '8F'H	Reservado a fabricantes cujo nome comece por 'P'
'90'H .. '97'H	Reservado a fabricantes cujo nome comece por 'Q'
'98'H .. '9F'H	Reservado a fabricantes cujo nome comece por 'R'
'A0'H	SETEC
'A1'H	SIEMENS VDO
'A2'H	STONERIDGE
'A3'H .. 'A7'H	Reservado a fabricantes cujo nome comece por 'S'
'AA'H	TACHOCONTROL
'AB'H .. 'AF'H	Reservado a fabricantes cujo nome comece por 'T'
'B0'H .. 'B7'H	Reservado a fabricantes cujo nome comece por 'U'
'B8'H .. 'BF'H	Reservado a fabricantes cujo nome comece por 'V'
'C0'H .. 'C7'H	Reservado a fabricantes cujo nome comece por 'W'
'C8'H .. 'CF'H	Reservado a fabricantes cujo nome comece por 'X'
'D0'H .. 'D7'H	Reservado a fabricantes cujo nome comece por 'Y'
'D8'H .. 'DF'H	Reservado a fabricantes cujo nome comece por 'Z'

2.68. MemberStateCertificate

Certificado da chave pública de um Estado-Membro, emitido pela autoridade certificadora europeia.

```
MemberStateCertificate ::= Certificate
```

2.69. MemberStatePublicKey

Chave pública de um Estado-Membro.

MemberStatePublicKey ::= PublicKey

2.70. Name

Um nome.

```
Name ::= SEQUENCE {
    codePage                INTEGER (0..255),
    name                    OCTET STRING (SIZE(35))
}
```

codePage especifica a parte da norma ISO/CEI 8859 utilizada para codificar o nome.

name é um nome codificado em conformidade com a norma ISO/CEI 8859-codePage.

2.71. NationAlpha

Referência alfabética a um país, em conformidade com a codificação convencional dos países utilizada em autocolantes nos pára-choques dos veículos e/ou no documento de seguro harmonizado internacionalmente (carta verde).

NationAlpha ::= IA5String(SIZE(3))

Comprimento atribuído:

' '	Sem informação disponível,
'A'	Áustria,
'AL'	Albânia,
'AND'	Andorra,
'ARM'	Arménia,
'AZ'	Azerbaijão,
'B'	Bélgica,
'BG'	Bulgária,
'BIH'	Bósnia-Herzegovina,
'BY'	Belarus (Bielorrússia),
'CH'	Suíça,
'CY'	Chipre,
'CZ'	República Checa,
'D'	Alemanha,
'DK'	Dinamarca,
'E'	Espanha,
'EST'	Estónia,
'F'	França,
'FIN'	Finlândia,
'FL'	Liechtenstein (Listenstaine),
'FR'	Ilhas Feroé,
'UK'	Reino Unido, Alderney, Guernsey, Jersey, Ilha de Man, Gibraltar,
'GE'	Geórgia,
'GR'	Grécia,
'H'	Hungria,
'HR'	Croácia,
'I'	Itália,
'IRL'	Irlanda,
'IS'	Islândia,
'KZ'	Cazaquistão,
'L'	Luxemburgo,
'LT'	Lituânia,
'LV'	Letónia,
'M'	Malta,
'MC'	Mónaco,

'MD '	República da Moldova (Moldávia),
'MK '	Macedónia,
'N '	Noruega,
'NL '	Países Baixos,
'P '	Portugal,
'PL '	Polónia,
'RO '	Roménia,
'RSM'	San Marino,
'RUS'	Federação Russa,
'S '	Suécia,
'SK '	Eslováquia,
'SLO'	Eslovénia,
'TM '	Turquemenistão,
'TR '	Turquia,
'UA '	Ucrânia,
'V '	Cidade do Vaticano,
'YU '	Jugoslávia,
'UNK'	Desconhecido,
'EC '	Comunidade Europeia,
'EUR'	Resto da Europa,
'WLD'	Resto do mundo.

2.72. NationNumeric

Referência numérica a um país.

NationNumeric ::= INTEGER(0..255)

Comprimento atribuído:

-- Sem informação disponível	(00)H,
-- Áustria	(01)H,
-- Albânia	(02)H,
-- Andorra	(03)H,
-- Arménia	(04)H,
-- Azerbaijão	(05)H,
-- Bélgica	(06)H,
-- Bulgária	(07)H,
-- Bósnia-Herzegovina	(08)H,
-- Belarus	(09)H,
-- Suíça	(0A)H,
-- Chipre	(0B)H,
-- República Checa	(0C)H,
-- Alemanha	(0D)H,
-- Dinamarca	(0E)H,
-- Espanha	(0F)H,
-- Estónia	(10)H,
-- França	(11)H,
-- Finlândia	(12)H,
-- Liechtenstein	(13)H,
-- Ilhas Feroé	(14)H,
-- Reino Unido	(15)H,
-- Geórgia	(16)H,
-- Grécia	(17)H,
-- Hungria	(18)H,
-- Croácia	(19)H,
-- Itália	(1A)H,
-- Irlanda	(1B)H,
-- Islândia	(1C)H,
-- Cazaquistão	(1D)H,
-- Luxemburgo	(1E)H,
-- Lituânia	(1F)H,
-- Letónia	(20)H,

-- Malta	(21)H,
-- Mónaco	(22)H,
-- República da Moldova	(23)H,
-- Macedónia	(24)H,
-- Noruega	(25)H,
-- Países Baixos	(26)H,
-- Portugal	(27)H,
-- Polónia	(28)H,
-- Roménia	(29)H,
-- San Marino	(2A)H,
-- Federação Russa	(2B)H,
-- Suécia	(2C)H,
-- Eslováquia	(2D)H,
-- Eslovénia	(2E)H,
-- Turquemenistão	(2F)H,
-- Turquia	(30)H,
-- Ucrânia	(31)H,
-- Cidade do Vaticano	(32)H,
-- Jugoslávia	(33)H,
-- RFU	(34..FC)H,
-- Comunidade Europeia	(FD)H,
-- Resto da Europa	(FE)H,
-- Resto do mundo	(FF)H

2.73. NoOfCalibrationRecords

Número de registos de calibração que um cartão de centro de ensaio pode memorizar.

NoOfCalibrationRecords ::= INTEGER(0..255)

Comprimento atribuído: ver secção 3.

2.74. NoOfCalibrationsSinceDownload

Contador que indica o número de calibrações efectuadas com um cartão de centro de ensaio desde o seu último descarregamento (requisito 230).

NoOfCalibrationsSinceDownload ::= INTEGER(0..2¹⁶-1),

Comprimento atribuído: sem mais especificações.

2.75. NoOfCardPlaceRecords

Número de registos de local que um cartão de condutor ou de centro de ensaio pode memorizar.

NoOfCardPlaceRecords ::= INTEGER(0..255)

Comprimento atribuído: ver secção 3.

2.76. NoOfCardVehicleRecords

Número de registos de utilização de veículos que um cartão de condutor ou de centro de ensaio pode memorizar.

NoOfCardVehicleRecords ::= INTEGER(0..2¹⁶-1)

Comprimento atribuído: ver secção 3.

2.77. NoOfCompanyActivityRecords

Número de registos de actividade de empresa que um cartão de empresa pode memorizar.

NoOfCompanyActivityRecords ::= INTEGER(0..2¹⁶-1)

Comprimento atribuído: ver secção 3.

2.78. NoOfControlActivityRecords

Número de registos de actividade de controlo que um cartão de controlador pode memorizar.

NoOfControlActivityRecords ::= INTEGER(0..2¹⁶-1)

Comprimento atribuído: ver secção 3.

2.79. NoOfEventsPerType

Número de incidentes, por tipo de incidente, que um cartão pode memorizar.

NoOfEventsPerType ::= INTEGER(0..255)

Comprimento atribuído: ver secção 3.

2.80. NoOfFaultsPerType

Número de falhas, por tipo de falha, que um cartão pode memorizar.

NoOfFaultsPerType ::= INTEGER(0..255)

Comprimento atribuído: ver secção 3.

2.81. OdometerValueMidnight

Valor odométrico do veículo à meia-noite de um dia determinado (requisito 090).

OdometerValueMidnight ::= OdometerShort

Comprimento atribuído: sem mais especificações.

2.82. OdometerShort

Valor odométrico do veículo sob forma sincopada (abreviada).

OdometerShort ::= INTEGER(0..2²⁴-1)

Comprimento atribuído: Binário sem sinal. Valor em km no intervalo operacional de 0 a 9 999 999 km.

2.83. OverspeedNumber

Número de incidentes de velocidade excessiva desde o último controlo de excesso de velocidade.

OverspeedNumber ::= INTEGER(0..255)

Comprimento atribuído: 0 significa que, desde o último controlo de excesso de velocidade, não ocorreu nenhum incidente de velocidade excessiva, 1 significa que ocorreu um incidente, ... 255 significa que ocorreram 255 ou mais incidentes.

2.84. PlaceRecord

Informação relativa a um local onde se inicia ou termina um período de trabalho diário (requisitos 087, 202 e 221).

```
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 odométrico no momento da introdução do local.

2.85. PreviousVehicleInfo

Informação relativa ao veículo previamente utilizado por um condutor no momento em que insere o seu cartão numa unidade-veículo (requisito 081).

```
PreviousVehicleInfo ::= SEQUENCE {
    vehicleRegistrationIdentification      VehicleRegistrationIdentification,
    cardWithdrawalTime                    TimeReal
}
```

vehicleRegistrationIdentification é o VRN (número de matrícula) e o Estado-Membro de registo do veículo.

cardWithdrawalTime é a data e a hora de retirada do cartão.

2.86. PublicKey

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.

2.87. RegionAlpha

Referência alfabética a uma região, dentro de um país especificado.

```
RegionAlpha ::= IA5STRING(SIZE(3))
```

Comprimento atribuído:

' ' Sem informação disponível,

Espanha:

'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

2.88. RegionNumeric

Referência numérica a uma região, dentro de um país especificado.

```
RegionNumeric ::= OCTET STRING (SIZE(1))
```

Comprimento atribuído:

'00'H Sem informação disponível,

Espanha:

'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

2.89. RSAKeyModulus

Módulo de um par de chaves RSA.

RSAKeyModulus ::= OCTET STRING (SIZE(128))

Comprimento atribuído: Não especificado.

2.90. RSAKeyPrivateExponent

Expoente privado de um par de chaves RSA.

RSAKeyPrivateExponent ::= OCTET STRING (SIZE(128))

Comprimento atribuído: Não especificado.

2.91. RSAKeyPublicExponent

Expoente público de um par de chaves RSA.

RSAKeyPublicExponent ::= OCTET STRING (SIZE(8))

Comprimento atribuído: Não especificado.

2.92. SensorApprovalNumber

Número de homologação de tipo do sensor.

SensorApprovalNumber ::= IA5String(SIZE(8))

Comprimento atribuído: Não especificado.

2.93. SensorIdentification

Informação memorizada num sensor de movimentos e relativa à identificação do mesmo (requisito 077).

```
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.

sensorOSIdentifier é o identificador do sistema operacional do sensor de movimentos.

2.94. **SensorInstallation**

Informação memorizada num sensor de movimentos e relativa à instalação do mesmo (requisito 099).

```
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 actual emparelhamento do sensor de movimentos com a VU.

currentVuApprovalNumber é o número de homologação da unidade-veículo actualmente emparelhada com o sensor de movimentos.

currentVUSerialNumber é o número de série da unidade-veículo actualmente emparelhada com o sensor de movimentos.

2.95. **SensorInstallationSecData**

Informação memorizada num cartão de centro de ensaio e relativa aos dados de segurança necessários para emparelhar sensores de movimentos a unidades-veículo (requisito 214).

```
SensorInstallationSecData ::= TDesSessionKey
```

Comprimento atribuído: em conformidade com a norma ISO 16844-3.

2.96. **SensorOSIdentifier**

Identificador do sistema operacional do sensor de movimentos.

```
SensorOSIdentifier ::= IA5String(SIZE(2))
```

Comprimento atribuído: específico do fabricante.

2.97. **SensorPaired**

Informação memorizada numa unidade-veículo e relativa à instalação do sensor de movimentos emparelhado com ela (requisito 079).

```
SensorPaired ::= SEQUENCE {
    sensorSerialNumber          SensorSerialNumber,
    sensorApprovalNumber        SensorApprovalNumber,
    sensorPairingDateFirst      SensorPairingDate
}
```

sensorSerialNumber é o número de série do sensor de movimentos actualmente emparelhado com a unidade-veículo.

sensorApprovalNumber é o número de homologação do sensor de movimentos actualmente emparelhado com a unidade-veículo.

sensorPairingDateFirst é a data em que o sensor de movimentos actualmente emparelhado com a unidade-veículo foi emparelhado pela primeira vez com uma VU.

2.98. **SensorPairingDate**

Data do emparelhamento do sensor de movimentos com uma VU.

SensorPairingDate ::= TimeReal

Comprimento atribuído: Não especificado.

2.99. **SensorSerialNumber**

Número de série do sensor de movimentos.

SensorSerialNumber ::= ExtendedSerialNumber

2.100. **SensorSCIdentifier**

Identificador do componente de segurança do sensor de movimentos.

SensorSCIdentifier ::= IA5String(SIZE(8))

Comprimento atribuído: específico do fabricante do componente.

2.101. **Signature**

Uma assinatura digital.

Signature ::= OCTET STRING (SIZE(128))

Comprimento atribuído: em conformidade com o apêndice 11 (Mecanismos comuns de segurança).

2.102. **SimilarEventsNumber**

Número de incidentes similares num dia determinado (requisito 094).

SimilarEventsNumber ::= INTEGER(0..255)

Comprimento atribuído: 0 não é utilizado, 1 significa que, no dia em questão, somente um incidente deste tipo foi memorizado, 2 significa que ocorreram dois incidentes do tipo (memorizado somente um), ... 255 significa que ocorreram 255 ou mais incidentes.

2.103. **SpecificConditionType**

Informação memorizada num cartão de condutor ou de centro de ensaio ou numa unidade-veículo e relativa a uma condição especial (requisitos 105a, 212a e 230a).

SpecificConditionType ::= INTEGER(0..255)

Comprimento 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

2.104. **SpecificConditionRecord**

Informação memorizada num cartão de condutor ou de centro de ensaio ou numa unidade-veículo e relativa a uma condição especial (requisitos 105a, 212a e 230a).

```
SpecificConditionRecord ::= SEQUENCE {
    entryTime                TimeReal,
    specificConditionType    SpecificConditionType
}
```

entryTime é a data e a hora da entrada.

specificConditionType é o código que identifica a condição especial.

2.105. Speed

Velocidade do veículo (km/h).

```
Speed ::= INTEGER(0..255)
```

Comprimento atribuído: quilómetros por hora no intervalo operacional de 0 a 220 km/h.

2.106. SpeedAuthorised

Velocidade máxima autorizada para o veículo [definição bb do presente anexo I(B)].

```
SpeedAuthorised ::= Speed
```

2.107. SpeedAverage

Velocidade média num intervalo de duração previamente definido (km/h).

```
SpeedAverage ::= Speed
```

2.108. SpeedMax

Velocidade máxima num intervalo de duração previamente definido.

```
SpeedMax ::= Speed
```

2.109. TDesSessionKey

Uma chave tripla de sessão DES.

```
TDesSessionKey ::= SEQUENCE {
    tDesKeyA                OCTET STRING (SIZE(8))
    tDesKeyB                OCTET STRING (SIZE(8))
}
```

Comprimento atribuído: sem mais especificações.

2.110. 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)
```

Comprimento 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.

2.111. TyreSize

Designação das dimensões dos pneus.

```
TyreSize ::= IA5String(SIZE(15))
```

Comprimento atribuído: em conformidade com a Directiva 92/23/CEE, de 31.3.1992 (JO L 129 de 14.5.1992, p. 95).

2.112. VehicleIdentificationNumber

Número de identificação do veículo (NIV), referente ao veículo como um todo. Normalmente, número de série do chassis.

VehicleIdentificationNumber ::= IA5String(SIZE(17))

Comprimento atribuído: conforme definição na norma ISO 3779.

2.113. 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 registado.

vehicleRegistrationNumber é o número de matrícula do veículo (VRN).

2.114. VehicleRegistrationNumber

Número de matrícula do veículo (VRN), atribuído pela autoridade responsável pela concessão da licença.

```
VehicleRegistrationNumber ::= SEQUENCE {
    codePage                        INTEGER (0..255),
    vehicleRegNumber                OCTET STRING (SIZE(13))
}
```

codePage especifica a parte da norma ISO/CEI 8859 utilizada para codificar o vehicleRegNumber.

vehicleRegNumber é um VRN codificado em conformidade com ISO/CEI 8859-codePage.

Comprimento atribuído: Específico do país.

2.115. VuActivityDailyData

Informação memorizada numa VU e relativa a mudanças na actividade e/ou na situação da condução e/ou na situação do cartão num determinado dia de calendário (requisito 084) e/ou na situação das ranhuras às 00h00 desse dia.

```
VuActivityDailyData ::= SEQUENCE {
    noOfActivityChanges            INTEGER SIZE(0..1440),
    activityChangeInfos            SET SIZE(noOfActivityChanges) OF
    ActivityChangeInfo
}
```

noOfActivityChanges é o número de palavras ActivityChangeInfo no conjunto activityChangeInfos.

activityChangeInfos é o 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.

2.116. VuApprovalNumber

Número de homologação de tipo da unidade-veículo.

VuApprovalNumber ::= IA5String(SIZE(8))

Comprimento atribuído: Não especificado.

2.117. VuCalibrationData

Informação memorizada numa VU e relativa às calibrações do aparelho de controlo (requisito 098).

```
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.

2.118. VuCalibrationRecord

Informação memorizada numa VU e relativa a uma calibração do aparelho de controlo (requisito 098).

```
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 objectivo (motivo, finalidade) da calibração.

workshopName, **workshopAddress**, são o nome e o endereço do centro de ensaio.

workshopCardNumber identifica o cartão de centro de ensaio utilizado durante a calibração.

workshopCardExpiryDate é a data-limite de validade do cartão.

vehicleIdentificationNumber é o NIV.

vehicleRegistrationIdentification contém o VRN e o Estado-Membro de registo.

wVehicleCharacteristicConstant é o coeficiente característico do veículo.

kConstantOfRecordingEquipment é a constante do aparelho de controlo.

lTyreCircumference é o perímetro efectivo dos pneus das rodas.

tyreSize é a designação das dimensões dos pneus montados no veículo.

authorisedSpeed é a velocidade autorizada para o veículo.

oldOdometerValue, **newOdometerValue** são os valores antigo e novo do odómetro.

oldTimeValue, **newTimeValue**, são os valores antigo e novo da data e da hora.

nextCalibrationDate é a data da próxima calibração do tipo especificado em CalibrationPurpose, a efectuar pela autoridade responsável pela inspecção.

2.119. VuCardIWData

Informação memorizada numa VU e relativa aos ciclos de inserção e retirada de cartões de condutor ou de centro de ensaio nessa VU (requisito 081).

```
VuCardIWData ::= SEQUENCE {
    noOfIWRecords              INTEGER(0..216-1),
    vuCardIWRecords            SET SIZE(noOfIWRecords) OF
                                VuCardIWRecord
}
```

noOfIWRecords é o número de registos no conjunto **vuCardIWRecords**.

vuCardIWRecords é um conjunto de registos relativos aos ciclos de inserção e retirada de cartões.

2.120. **VuCardIWRecord**

Informação memorizada numa VU e relativa a um ciclo de inserção e retirada de um cartão de condutor ou de centro de ensaio nessa VU (requisito 081).

```
VuCardIWRecord ::= SEQUENCE {
    cardHolderName           HolderName,
    fullCardNumber           FullCardNumber,
    cardExpiryDate          TimeReal,
    cardInsertionTime        TimeReal,
    vehicleOdometerValueAtInsertion OdometerShort,
    cardSlotNumber           CardSlotNumber,
    cardWithdrawalTime       TimeReal,
    vehicleOdometerValueAtWithdrawal OdometerShort,
    previousVehicleInfo      PreviousVehicleInfo
    manualInputFlag          ManualInputFlag
}
```

cardHolderName é o apelido e o nome próprio do titular do cartão de condutor ou de centro de ensaio, memorizados no mesmo.

fullCardNumber é o tipo, o Estado-Membro emissor e o número do cartão, nele memorizados.

cardExpiryDate é o prazo de validade do cartão, nele memorizado.

cardInsertionTime é a data e a hora a que o cartão foi inserido.

vehicleOdometerValueAtInsertion é o valor odométrico do veículo no momento da inserção do cartão.

cardSlotNumber é a ranhura na qual o cartão foi inserido.

cardWithdrawalTime é a data e a hora a que o cartão foi retirado.

vehicleOdometerValueAtWithdrawal é o valor odométrico do veículo no momento da retirada do cartão.

previousVehicleInfo contém informação, memorizada no cartão, acerca do anterior veículo utilizado pelo condutor.

manualInputFlag é uma bandeira que identifica se o titular do cartão introduziu manualmente actividades de condutor no momento da inserção do cartão.

2.121. **VuCertificate**

Certificado da chave pública de uma VU.

```
VuCertificate ::= Certificate
```

2.122. **VuCompanyLocksData**

Informação memorizada numa VU e relativa aos bloqueios de uma empresa (requisito 104).

```
VuCompanyLocksData ::= SEQUENCE {
    noOfLocks                INTEGER(0..20),
    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.

2.123. VuCompanyLocksRecord

Informação memorizada numa VU e relativa a um bloqueio de uma empresa (requisito 104).

```
VuCompanyLocksRecord ::= SEQUENCE {
    lockInTime           TimeReal,
    lockOutTime          TimeReal,
    companyName          Name,
    companyAddress       Address,
    companyCardNumber    FullCardNumber
}
```

lockInTime, lockOutTime, são a data e a hora de iniciação (lock-in) e de cessação (lock-out) do bloqueio.

companyName, companyAddress, são o nome e o endereço da empresa relacionada com a iniciação do bloqueio (lock-in).

companyCardNumber identifica o cartão utilizado na iniciação do bloqueio (lock-in).

2.124. VuControlActivityData

Informação memorizada numa VU e relativa aos controlos executados por meio da mesma (requisito 102).

```
VuControlActivityData ::= SEQUENCE {
    noOfControls          INTEGER(0..20),
    vuControlActivityRecords SET SIZE(noOfControls) OF
                          VuControlActivityRecord
}
```

noOfControls é o número de controlos que constam de vuControlActivityRecords.

vuControlActivityRecords é o conjunto de registos da actividade de controlo.

2.125. VuControlActivityRecord

Informação memorizada numa VU e relativa a um controlo executado por meio da mesma (requisito 102).

```
VuControlActivityRecord ::= SEQUENCE {
    controlType           ControlType,
    controlTime           TimeReal,
    controlCardNumber     FullCardNumber,
    downloadPeriodBeginTime TimeReal,
    downloadPeriodEndTime TimeReal
}
```

controlType é o tipo do controlo.

controlTime é a data e a hora do controlo.

ControlCardNumber identifica o cartão de controlador utilizado para o controlo.

downloadPeriodBeginTime é a hora de início do período de eventual descarregamento.

downloadPeriodEndTime é a hora de finalização do período de eventual descarregamento.

2.126. VuDataBlockCounter

Contador memorizado num cartão e que identifica sequencialmente os ciclos de inserção e retirada do mesmo em unidades-veículo.

```
VuDataBlockCounter ::= BCDString(SIZE(2))
```

Comprimento atribuído: Número consecutivo, com o valor máximo de 9 999 e recomeçando em 0.

2.127. VuDetailedSpeedBlock

Informação memorizada numa VU e relativa à velocidade detalhada do veículo num minuto durante o qual o mesmo esteve em movimento (requisito 093).

```
VuDetailedSpeedBlock ::= SEQUENCE {
    speedBlockBeginDate      TimeReal,
    speedsPerSecond          SEQUENCE SIZE(60) OF Speed
}
```

speedBlockBeginDate é a data e a hora do primeiro valor da velocidade no bloco.

speedsPerSecond é a sequência cronológica de velocidades medidas em cada segundo durante o minuto que começa em speedBlockBeginDate (inclusive).

2.128. VuDetailedSpeedData

Informação memorizada numa VU e relativa à velocidade detalhada do veículo.

```
VuDetailedSpeedData ::= SEQUENCE
    noOfSpeedBlocks          INTEGER(0..216-1),
    vuDetailedSpeedBlocks    SET SIZE(noOfSpeedBlocks) OF
                             VuDetailedSpeedBlock
}
```

noOfSpeedBlocks é o número de blocos de velocidade no conjunto vuDetailedSpeedBlocks.

vuDetailedSpeedBlocks é o conjunto de blocos de velocidade detalhada.

2.129. VuDownloadablePeriod

Datas mais antiga e mais recente relativamente às quais uma VU detém dados referentes às actividades dos condutores (requisitos 081, 084 ou 087).

```
VuDownloadablePeriod ::= SEQUENCE {
    minDownloadableTime      TimeReal
    maxDownloadableTime      TimeReal
}
```

minDownloadableTime é a mais antiga data e hora de inserção do cartão, de mudança de actividade ou de entrada de um local, memorizada na VU.

maxDownloadableTime é a mais recente data e hora de retirada do cartão, de mudança de actividade ou de entrada de um local, memorizada na VU.

2.130. VuDownloadActivityData

Informação memorizada numa VU e relativa ao seu último descarregamento (requisito 105).

```
VuDownloadActivityData ::= SEQUENCE {
    downloadingTime          TimeReal,
    fullCardNumber           FullCardNumber,
    companyOrWorkshopName    Name
}
```

downloadingTime é a data e a hora do descarregamento.

fullCardNumber identifica o cartão utilizado para autorizar o descarregamento.

companyOrWorkshopName é o nome da empresa ou do centro de ensaio.

2.131. VuEventData

Informação memorizada numa VU e relativa aos incidentes (requisito 094, com excepção do incidente "excesso de velocidade").

```
VuEventData ::= SEQUENCE {
    noOfVuEvents             INTEGER(0..255),
    vuEventRecords           SET SIZE(noOfVuEvents) OF
                             VuEventRecord
}
```

noOfVuEvents é o número de incidentes que constam do conjunto vuEventRecords.

vuEventRecords é um conjunto de registos de incidentes.

2.132. VuEventRecord

Informação memorizada numa VU e relativa a um incidente (requisito 094, com excepção do incidente “excesso de velocidade”).

```
VuEventRecord ::= SEQUENCE {
    eventType                EventFaultType,
    eventRecordPurpose       EventFaultRecordPurpose,
    eventBeginTime           TimeReal,
    eventEndTime             TimeReal,
    cardNumberDriverSlotBegin FullCardNumber,
    cardNumberCodriverSlotBegin FullCardNumber,
    cardNumberDriverSlotEnd FullCardNumber,
    cardNumberCodriverSlotEnd FullCardNumber,
    similarEventsNumber      SimilarEventsNumber
}
```

eventType é o tipo de incidente.

eventRecordPurpose é o objectivo (motivo, finalidade) pelo qual este incidente foi registado.

eventBeginTime é a data e a hora de início do incidente.

eventEndTime é a data e a hora de cessação do incidente.

cardNumberDriverSlotBegin identifica o cartão que se encontrava inserido na ranhura do condutor principal no momento em que se iniciou o incidente.

cardNumberCodriverSlotBegin identifica o cartão que se encontrava inserido na ranhura do ajudante no momento em que se iniciou o incidente.

cardNumberDriverSlotEnd identifica o cartão que se encontrava inserido na ranhura do condutor principal 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 é o número de incidentes similares no dia em questão.

Esta sequência pode ser utilizada para quaisquer incidentes, com excepção dos incidentes de excesso de velocidade.

2.133. VuFaultData

Informação memorizada numa VU e relativa às falhas (requisito 096).

```
VuFaultData ::= SEQUENCE {
    noOfVuFaults            INTEGER(0..255),
    vuFaultRecords          SET SIZE(noOfVuFaults) OF VuFaultRecord
}
```

noOfVuFaults é o número de falhas que constam do conjunto vuFaultRecords.

vuFaultRecords é um conjunto de registos de falhas.

2.134. VuFaultRecord

Informação memorizada numa VU e relativa a uma falha (requisito 096).

```
VuFaultRecord ::= SEQUENCE {
    faultType                EventFaultType,
    faultRecordPurpose       EventFaultRecordPurpose,
    faultBeginTime           TimeReal,
    faultEndTime             TimeReal,
    cardNumberDriverSlotBegin FullCardNumber,
    cardNumberCodriverSlotBegin FullCardNumber,
    cardNumberDriverSlotEnd FullCardNumber,
    cardNumberCodriverSlotEnd FullCardNumber
}
```

faultType é o tipo de falha no aparelho de controlo.

faultRecordPurpose é o objectivo (motivo, finalidade) pelo qual esta falha foi registada.

faultBeginTime é a data e a hora de início da falha.

faultEndTime é a data e a hora de cessação da falha.

cardNumberDriverSlotBegin identifica o cartão que se encontrava inserido na ranhura do condutor principal no momento em que se iniciou a falha.

cardNumberCodriverSlotBegin identifica o cartão que se encontrava inserido na ranhura do ajudante no momento em que se iniciou a falha.

cardNumberDriverSlotEnd identifica o cartão que se encontrava inserido na ranhura do condutor principal no momento em que terminou a falha.

cardNumberCodriverSlotEnd identifica o cartão que se encontrava inserido na ranhura do ajudante no momento em que terminou a falha.

2.135. **VuIdentification**

Informação memorizada numa VU e relativa à sua identificação (requisito 075).

```
VuIdentification ::= SEQUENCE {
    vuManufacturerName          VuManufacturerName,
    vuManufacturerAddress      VuManufacturerAddress,
    vuPartNumber               VuPartNumber,
    vuSerialNumber             VuSerialNumber,
    vuSoftwareIdentification   VuSoftwareIdentification,
    vuManufacturingDate       VuManufacturingDate,
    vuApprovalNumber           VuApprovalNumber
}
```

vuManufacturerName é o nome do fabricante da VU.

vuManufacturerAddress é o endereço do fabricante da VU.

vuPartNumber é o número de peça da VU.

vuSerialNumber é o número de série da VU.

vuSoftwareIdentification identifica o suporte lógico implantado na VU.

vuManufacturingDate é a data de fabrico da VU.

vuApprovalNumber é o número de homologação de tipo da VU.

2.136. **VuManufacturerAddress**

Endereço do fabricante da VU.

```
VuManufacturerAddress ::= Address
```

Comprimento atribuído: Não especificado.

2.137. **VuManufacturerName**

Nome do fabricante da VU.

```
VuManufacturerName ::= Name
```

Comprimento atribuído: Não especificado.

2.138. **VuManufacturingDate**

Data de fabrico da VU.

```
VuManufacturingDate ::= TimeReal
```

Comprimento atribuído: Não especificado.

2.139. VuOverSpeedingControlData

Informação memorizada numa VU e relativa a incidentes de excesso de velocidade desde o último controlo desse excesso (requisito 095).

```
VuOverSpeedingControlData ::= SEQUENCE {
    lastOverspeedControlTime      TimeReal,
    firstOverspeedSince           TimeReal,
    numberOfOverspeedSince       OverspeedNumber
}
```

lastOverspeedControlTime é a data e a hora do último controlo do excesso de velocidade.

firstOverspeedSince é a data e a hora do primeiro excesso de velocidade desde aquele controlo.

numberOfOverspeedSince é o número de incidentes de excesso de velocidade desde o último controlo do excesso de velocidade.

2.140. VuOverSpeedingEventData

Informação memorizada numa VU e relativa a incidentes de excesso de velocidade (requisito 094).

```
VuOverSpeedingEventData ::= SEQUENCE {
    noOfVuOverSpeedingEvents      INTEGER(0..255),
    vuOverSpeedingEventRecords    SET SIZE(noOfVuOverSpeedingEvents) OF
                                   VuOverSpeedingEventRecord
}
```

noOfVuOverSpeedingEvents é o número de incidentes que constam do conjunto **vuOverSpeedingEventRecords**.

vuOverSpeedingEventRecords é um conjunto de registos de incidentes de excesso de velocidade.

2.141. VuOverSpeedingEventRecord

Informação memorizada numa VU e relativa a incidentes de excesso de velocidade (requisito 094).

```
VuOverSpeedingEventRecord ::= SEQUENCE {
    eventType                     EventFaultType,
    eventRecordPurpose           EventFaultRecordPurpose,
    eventBeginTime               TimeReal,
    eventEndTime                 TimeReal,
    maxSpeedValue                SpeedMax,
    averageSpeedValue            SpeedAverage,
    cardNumberDriverSlotBegin    FullCardNumber,
    similarEventsNumber          SimilarEventsNumber
}
```

eventType é o tipo de incidente.

eventRecordPurpose é o objectivo (motivo, finalidade) pelo qual este incidente foi registado.

eventBeginTime é a data e a hora de início do incidente.

eventEndTime é a data e a hora de cessação do incidente.

maxSpeedValue é a velocidade máxima medida durante o incidente.

averageSpeedValue é a média aritmética da velocidade medida durante o incidente.

cardNumberDriverSlotBegin identifica o cartão que se encontrava inserido na ranhura do condutor principal no momento em que se iniciou o incidente.

similarEventsNumber é o número de incidentes similares no dia em questão.

2.142. VuPartNumber

Número de peça da VU.

```
VuPartNumber ::= IA5String(SIZE(16))
```

Comprimento atribuído: Específico do fabricante da VU.

2.143. VuPlaceDailyWorkPeriodData

Informação memorizada numa VU e relativa aos locais onde os condutores iniciam ou terminam um período de trabalho diário (requisito 087).

```
VuPlaceDailyWorkPeriodData ::= SEQUENCE {  
    noOfPlaceRecords          INTEGER(0..255),  
    vuPlaceDailyWorkPeriodRecords SET SIZE(noOfPlaceRecords) OF  
                                VuPlaceDailyWorkPeriodRecord  
}
```

noOfPlaceRecords é o número de registos que constam do conjunto `vuPlaceDailyWorkPeriodRecords`.

vuPlaceDailyWorkPeriodRecords é um conjunto de registos relativos à localização.

2.144. VuPlaceDailyWorkPeriodRecord

Informação memorizada numa VU e relativa a um local onde um condutor inicia ou termina um período de trabalho diário (requisito 087).

```
VuPlaceDailyWorkPeriodRecord ::= SEQUENCE {  
    fullCardNumber            FullCardNumber,  
    placeRecord               PlaceRecord  
}
```

fullCardNumber é o tipo, o Estado-Membro emissor e o número do cartão do condutor.

placeRecord contém a informação relativa ao local.

2.145. VuPrivateKey

A chave privada de uma VU.

```
VuPrivateKey ::= RSAKeyPrivateExponent
```

2.146. VuPublicKey

A chave pública de uma VU.

```
VuPublicKey ::= PublicKey
```

2.147. VuSerialNumber

O número de série da VU (requisito 075).

```
VuSerialNumber ::= ExtendedSerialNumber
```

2.148. VuSoftInstallationDate

Data de instalação da versão de suporte lógico na VU.

```
VuSoftInstallationDate ::= TimeReal
```

Comprimento atribuído: Não especificado.

2.149. VuSoftwareIdentification

Informação memorizada numa VU e relativa ao suporte lógico nela instalado.

```
VuSoftwareIdentification ::= SEQUENCE {  
    vuSoftwareVersion          VuSoftwareVersion,  
    vuSoftInstallationDate     VuSoftInstallationDate  
}
```

vuSoftwareVersion é o número da versão de suporte lógico da VU.

vuSoftInstallationDate é a data de instalação da versão de suporte lógico.

2.150. VuSoftwareVersion

Número da versão de suporte lógico da VU.

```
VuSoftwareVersion ::= IA5String(SIZE(4))
```

Comprimento atribuído: Não especificado.

2.151. VuSpecificConditionData

Informação memorizada numa VU e relativa às condições especiais.

```
VuSpecificConditionData ::= SEQUENCE {
  noOfSpecificConditionRecords      INTEGER(0..216-1)
  specificConditionRecords          SET SIZE
                                     (noOfSpecificConditionRecords) OF
                                     SpecificConditionRecord
}
```

noOfSpecificConditionRecords é o número de registos que constam do conjunto **specificConditionRecords**.

specificConditionRecords é um conjunto de registos relativos às condições especiais.

2.152. VuTimeAdjustmentData

Informação memorizada numa VU e relativa aos ajustamentos do tempo executados fora do âmbito de uma calibração regular (requisito 101).

```
VuTimeAdjustmentData ::= SEQUENCE {
  noOfVuTimeAdjRecords             INTEGER(0..6),
  vuTimeAdjustmentRecords          SET SIZE(noOfVuTimeAdjRecords) OF
                                     VuTimeAdjustmentRecord
}
```

noOfVuTimeAdjRecords é o número de registos em **vuTimeAdjustmentRecords**.

vuTimeAdjustmentRecords é um conjunto de registos de ajustamento do tempo.

2.153. VuTimeAdjustmentRecord

Informação memorizada numa VU e relativa a um ajustamento do tempo executado fora do âmbito de uma calibração regular (requisito 101).

```
VuTimeAdjustmentRecord ::= SEQUENCE {
  oldTimeValue                     TimeReal,
  newTimeValue                     TimeReal,
  workshopName                     Name,
  workshopAddress                   Address,
  workshopCardNumber               FullCardNumber
}
```

oldTimeValue, **newTimeValue**, são os valores antigo e novo da data e da hora.

workshopName, **workshopAddress**, são o nome e o endereço do centro de ensaio.

workshopCardNumber identifica o cartão de centro de ensaio utilizado para efectuar o ajustamento do tempo.

2.154. W-VehicleCharacteristicConstant

Coefficiente característico do veículo [definição k do presente anexo I(B)].

```
W-VehicleCharacteristicConstant ::= INTEGER(0..216-1)
```

Comprimento atribuído: Impulsos por quilómetro no intervalo operacional de 0 a 64 255 imp/km.

2.155. WorkshopCardApplicationIdentification

Informação memorizada num cartão de centro de ensaio e relativa à identificação da aplicação desse cartão (requisito 190).

```
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 é o número de incidentes, por tipo de incidente, que o cartão pode registar.

noOfFaultsPerType é o número de falhas, por tipo de falha, que o cartão pode registar.

activityStructureLength indica o número de bytes disponíveis para memorizar registos de actividade.

noOfCardVehicleRecords é o número de registos de veículo que o cartão pode conter.

noOfCardPlaceRecords é o número de locais que o cartão pode registar.

noOfCalibrationRecords é o número de registos de calibração que o cartão pode memorizar.

2.156. WorkshopCardCalibrationData

Informação memorizada num cartão de centro de ensaio e relativa à actividade desse centro executada com o cartão (requisitos 227 e 229).

```
WorkshopCardCalibrationData ::= SEQUENCE {
    calibrationTotalNumber            INTEGER(0..216-1),
    calibrationPointerNewestRecord    INTEGER(0..NoOfCalibrationRecords-1),
    calibrationRecords                SET SIZE(NoOfCalibrationRecords) OF
                                        WorkshopCardCalibrationRecord
}
```

calibrationTotalNumber é o número total de calibrações efectuadas com o cartão.

calibrationPointerNewestRecord é o índice do último registo actualizado de calibração.

Comprimento atribuído: Comprimento atribuído: Número correspondente ao numerador do registo de calibração, começando por '0' à primeira ocorrência de registos de calibração na estrutura.

calibrationRecords é o conjunto de registos que contém informação relativa a calibração e/ou a ajustamento do tempo.

2.157. WorkshopCardCalibrationRecord

Informação memorizada num cartão de centro de ensaio e relativa a uma calibração executada com esse cartão (requisito 227).

```
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 é o objectivo da calibração.

vehicleIdentificationNumber é o NIV.

vehicleRegistration contém o VRN e o Estado-Membro de registo.

wVehicleCharacteristicConstant é o coeficiente característico do veículo.

kConstantOfRecordingEquipment é a constante do aparelho de controlo.

ITyreCircumference é o perímetro efectivo dos pneus das rodas.

tyreSize é a designação das dimensões dos pneus montados no veículo.

authorisedSpeed é a velocidade máxima autorizada para o veículo.

oldOdometerValue, **newOdometerValue**, são os valores antigo e novo do odómetro.

oldTimeValue, **newTimeValue**, são os valores antigo e novo da data e da hora.

nextCalibrationDate é a data da próxima calibração do tipo especificado em CalibrationPurpose, a efectuar pela autoridade responsável pela inspecção.

vuPartNumber, **vuSerialNumber** and **sensorSerialNumber**, são os elementos de dados relativos à identificação do aparelho de controlo.

2.158. WorkshopCardHolderIdentification

Informação memorizada num cartão de centro de ensaio e relativa à identificação do seu titular (requisito 216).

```
WorkshopCardHolderIdentification ::= SEQUENCE {
    workshopName                Name,
    workshopAddress              Address,
    cardHolderName                HolderName,
    cardHolderPreferredLanguage  Language
}
```

workshopName é o nome do centro de ensaio do titular do cartão.

workshopAddress é o endereço do centro de ensaio 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.

2.159. WorkshopCardPIN

Número de identificação pessoal do cartão de centro de ensaio (requisito 213).

```
WorkshopCardPIN ::= IA5String(SIZE(8))
```

Comprimeto atribuído: o PIN conhecido pelo titular do cartão, preenchido à direita com bytes 'FF' até um máximo de 8 bytes.

3. DEFINIÇÕES DOS VALORES E DOS INTERVALOS DE DIMENSÃO

Definição dos valores variáveis utilizados nas definições da secção 2 deste apêndice.

TimeRealRange ::= $2^{32}-1$

3.1. Definições relativas ao cartão de condutor:

Nome do valor variável	Mín	Máx
CardActivityLengthRange	5 544 bytes (28 dias, 93 mudanças de actividade por dia)	13 776 bytes (28 dias, 240 mudanças de actividade por dia)
NoOfCardPlaceRecords	84	112
NoOfCardVehicleRecords	84	200
NoOfEventsPerType	6	12
NoOfFaultsPerType	12	24

3.2. Definições relativas ao cartão de centro de ensaio:

Nome do valor variável	Mín	Máx
CardActivityLengthRange	198 bytes (1 dia, 93 mudanças de actividade)	492 bytes (1 dia, 240 mudanças de actividade)
NoOfCardPlaceRecords	6	8
NoOfCardVehicleRecords	4	8
NoOfEventsPerType	3	3
NoOfFaultsPerType	6	6
NoOfCalibrationRecords	88	255

3.3. Definições relativas ao cartão de controlador:

Nome do valor variável	Mín	Máx
NoOfControlActivityRecords	230	520

3.4. Definições relativas ao cartão de empresa:

Nome do valor variável	Mín	Máx
NoOfCompanyActivityRecords	230	520

4. CONJUNTOS DE CARACTERES

IA5Strings utiliza os caracteres ASCII definidos na norma ISO/CEI 8824-1. Por uma questão de legibilidade e de mais fácil referência, indica-se abaixo a atribuição de valor (comprimento atribuído). Na eventualidade de discrepância, a norma ISO/CEI 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 caracteres (Address, Name, VehicleRegistrationNumber) utilizam, adicionalmente, os caracteres definidos pelos códigos 192 a 255 da norma ISO/CEI 8859-1 (conjunto de caracteres Latin 1) ou da norma ISO/CEI 8859-7 (conjunto de caracteres Greek).

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/CEI 8825-2, variante alinhada.

Apêndice 2

ESPECIFICAÇÕES APLICÁVEIS AOS CARTÕES TACOGRÁFICOS

1. INTRODUÇÃO

1.1. Abreviaturas

Para efeitos do presente apêndice, aplicam-se as seguintes abreviaturas:

AC	Condições de acesso
AID	Identificador de uma aplicação
ALW	Sempre
APDU	Unidade de dados do protocolo de uma aplicação (estrutura de um comando)
ATR	Resposta à reinicialização
AUT	Autenticado
C6, C7	Contactos n.ºs 6 e 7 do cartão, cf. norma ISO/CEI 7816-2
cc	Ciclos do relógio
CHV	Informação sobre a verificação do titular do cartão
CLA	Byte de classe de um comando APDU
DF	Ficheiro dedicado. Um DF pode conter outros ficheiros (EF ou DF)
EF	Ficheiro elementar
ENC	Criptado ou codificado: acesso possível unicamente por dados de codificação
etu	Unidade elementar de tempo
IC	Circuito integrado
ICC	Cartão de 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 (input data) de um comando APDU
Le	Comprimento dos dados esperados (dados de saída ou output data para um comando)
MF	Ficheiro principal (DF raiz)
P1-P2	Bytes de parâmetro
NAD	Endereço de nó utilizado no protocolo T=1
NEV	Nunca
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 ou restabelecimento (do cartão)
SM	Envio seguro de mensagens
SW1-SW2	Bytes de estatuto ou de situação
TS	Carácter inicial de ATR
VPP	Tensão eléctrica (voltagem) de programação
XXh	Valor XX em notação hexadecimal
	Símbolo de concatenação 03 04=0304

1.2. Referências

No presente apêndice utilizam-se as seguintes referências:

EN 726-3	Identification cards systems — Telecommunications integrated circuit(s) cards and terminals — Part 3: Application independent card requirements. December 1994.
ISO/CEI 7816-2	Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 2: Dimensions and location of the contacts. First edition: 1999.
ISO/CEI 7816-3	Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 3: Electronic signals and transmission protocol. Edition 2: 1997.
ISO/CEI 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/CEI 7816-6	Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 6: Interindustry data elements. First Edition: 1996 + Cor 1: 1998.
ISO/CEI 7816-8	Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 8: Security related interindustry commands. First Edition: 1999.
ISO/CEI 9797	Information technology — Security techniques — Data integrity mechanism using a cryptographic check function employing a block cipher algorithm. Edition 2: 1994.

2. CARACTERÍSTICAS ELÉTRICAS E FÍSICAS

TCS_200 Salvo especificação diversa, os sinais electrónicos devem cumprir o prescrito na norma ISO/CEI 7816-3.

TCS_201 A localização e as dimensões dos contactos do cartão devem cumprir o prescrito na norma ISO/CEI 7816-2.

2.1. Tensão de alimentação e consumo eléctrico

TCS_202 O cartão deve funcionar em conformidade com os limites de consumo especificados na norma ISO/CEI 7816-3.

TCS_203 O cartão deve funcionar com $V_{cc} = 3\text{ V } (+/- 0,3\text{ V})$ ou com $V_{cc} = 5\text{ V } (+/- 0,5\text{ V})$.

A selecção da tensão deve cumprir o prescrito na norma ISO/CEI 7816-3.

2.2. Tensão eléctrica de programação (V_{pp})

TCS_204 O cartão não deve necessitar de uma tensão de programação no pin C6. Prevê-se que o pin 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_205 O cartão deve funcionar com uma gama de frequência de 1 a 5 MHz. No âmbito de uma sessão de cartão, a frequência do relógio pode variar $\pm 2\%$. A frequência do relógio é gerada pela unidade-veículo e não propriamente pelo cartão. O ciclo de funcionamento (duty cycle) pode variar entre 40% e 60%.

TCS_206 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 Clockstop ("paragem do relógio") (para mais informações, consultar norma EN 726-3):

Baixo	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 baixo
0	0	0	Clockstop não permitido
0	1	0	Clockstop permitido somente em nível elevado
1	0	0	Clockstop permitido somente em nível baixo

Os bits 4 a 8 não são utilizados.

2.4. Contacto I/O

TCS_207 O contacto I/O C7 é utilizado para receber dados do IFD e transmitir-lhos. Durante o funcionamento unicamente, estarão em modo de transmissão ou o cartão ou o IFD. Se ambas as unidades estiverem em modo de transmissão, não sobrevirá qualquer dano ao cartão. Salvo se estiver a transmitir, o cartão deve introduzir o modo de recepção.

2.5. Estados do cartão

TCS_208 Enquanto lhe for aplicada a tensão de alimentação, o cartão trabalha em dois estados:

- estado de operação ou de funcionamento durante a execução de comandos ou acções de interface com a unidade digital,
- estado de repouso em todo o tempo restante, devendo então reter todos os dados.

3. EQUIPAMENTO INFORMÁTICO (HARDWARE) E COMUNICAÇÃO

3.1. Introdução

Esta secção refere as condições mínimas de funcionalidade requeridas pelos cartões tacográficos e pelas VU, para funcionamento e interoperabilidade correctos.

Os cartões tacográficos cumprem o mais rigorosamente possível as normas ISO/CEI aplicáveis (com destaque para as ISO/CEI 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_300 O protocolo de transmissão deve cumprir a norma ISO/CEI 7816-3. Em particular, a VU deve reconhecer extensões de tempo de espera enviadas pelo cartão.

3.2.1. Protocolos

TCS_301 O cartão deve proporcionar quer o protocolo T=0 quer o protocolo T=1.

- TCS_302 T=0 é o protocolo por defeito, pelo que é necessário um comando PTS para o passar a T=1.
- TCS_303 Em ambos os protocolos haverá dispositivos de apoio a direct convention: a “convenção directa” é, pois, obrigatória para o cartão.
- TCS_304 O byte de information field size card (cartão da dimensão do campo de informação) deve ser apresentado na ATR em carácter TA3. Este valor será, pelo menos, 'F0h' (= 240 bytes).

Aos protocolos aplicam-se as seguintes restrições:

- TCS_305 T=0
- O dispositivo de interface deve suportar uma resposta em I/O depois da elevação do sinal em RST a partir de 400 cc.
 - O dispositivo de interface deve poder ler caracteres separados de 12 etu.
 - O dispositivo de interface deve ler um carácter errado e a sua repetição quando separados de 13 etu. Se for detectado um carácter errado, o sinal Error em I/O pode ocorrer entre 1 etu e 2 etu. O dispositivo deve suportar 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 tempo suplementar de guarda deve estar presente para caracteres enviados pelo dispositivo de interface, embora os caracteres enviados pelo cartão possam estar ainda separados de 12 etu. O mesmo se verifica relativamente ao carácter ACK enviado pelo cartão depois de um carácter P3 emitido pelo dispositivo de interface.
 - O dispositivo de interface deve ter em conta um carácter 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 susceptível de exceder 255 bytes.
- TCS_306 T=1
- Byte NAD: não utilizado (NAD deve ser colocado no valor '00').
 - ABORT no bloco-S: não utilizado.
 - Erro de estado do VPP no bloco-S: 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 IFS do bloco-S a seguir à ATR, e o cartão devolve o IFS do bloco-S. O valor recomendado para o IFSD é de 254 bytes.
 - O cartão não pede reajustamento da IFS.

3.2.2. ATR

- TCS_307 O dispositivo verifica os bytes da ATR, em conformidade com a norma ISO/CEI 7816-3. Não é feita qualquer verificação aos caracteres históricos da ATR.

Exemplo de biprotocolo ATR de base, em conformidade com ISO/CEI 7816-3

Carácter	Valor	Observações
TS	'3Bh'	Indica convenção directa
T0	'85h'	TD1 presente; presentes 5 bytes históricos
TD1	'80h'	TD2 presente; T=0 a utilizar
TD2	'11h'	TA3 presente; T=1 a utilizar
TA3	'XXh' (pelo menos 'F0h')	Cartão da dimensão do campo de informação (IFSC)
TH1 a TH5	'XXh'	Caracteres históricos
TCK	'XXh'	Verificar carácter (exclusivo OR)

TCS_308 Depois da resposta à reinicialização (ATR), o ficheiro principal (MF) é implicitamente seleccionado, tornando-se o directório em curso.

3.2.3. PTS

TCS_309 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_310 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/CEI 7816-3, a PTS pode ser utilizada para passar a báudios mais elevados do que o de defeito, eventualmente proposto pelo cartão na ATR [byte TA(1)].

Báudios mais elevados são opcionais para o cartão.

TCS_311 Se somente o báudio de defeito for suportado (ou se o báudio seleccionado não for suportado), o cartão responderá correctamente à PTS, em conformidade com ISO/CEI 7816-3, omitindo o byte PPS1.

Exemplos de PTS de base para selecção de protocolo:

Carácter	Valor	Observações
PPSS	'FFh'	Iniciar carácter.
PPS0	'00h' ou '01h'	PPS1 a PPS3 não presentes; '00h' para seleccionar T0, '01h' para seleccionar T1.
PK	'XXh'	Verificar carácter: 'XXh' = 'FFh' se PPS0 = '00h', 'XXh' = 'FEh' se PPS0 = '01h'.

3.3. Condições de acesso (AC)

As condições de acesso (AC) para os comandos UPDATE BINARY e READ BINARY são definidas relativamente a cada ficheiro elementar.

TCS_312 As AC do ficheiro em curso devem ser cumpridas antes do acesso ao ficheiro por intermédio destes comandos.

Definição das condições de acesso existentes:

- ALW: a acção é sempre possível e pode ser executada sem qualquer restrição.
- NEV: a acção nunca é possível.
- AUT: os direitos correspondentes a uma autenticação externa bem sucedida devem ser abertos (o que é feito pelo comando EXTERNAL AUTHENTICATE).
- PRO SM: o comando deve ser transmitido com uma soma criptográfica de teste, utilizando o envio seguro de mensagens (ver apêndice 11).
- AUT e PRO SM (em combinação).

Relativamente aos comandos de processamento (UPDATE BINARY e READ BINARY), podem ser fixadas no cartão as seguintes condições de acesso:

	UPDATE BINARY	READ BINARY
ALW	Sim	Sim
NEV	Sim	Sim
AUT	Sim	Sim
PRO SM	Sim	Não
AUT e PRO SM	Sim	Não

A condição de acesso PRO SM não é disponível para o comando READ BINARY, o que significa que a presença de uma soma criptográfica de teste para um comando READ nunca é obrigatória. Contudo, utilizando o valor 'OC' para a classe, é possível utilizar o comando READ BINARY com envio seguro de mensagens, conforme se refere no ponto 3.6.2.

3.4. Criptagem de dados

Se for necessário proteger a confidencialidade de dados a ler num ficheiro, este último é marcado como "Encrypted" (criptado). A criptagem é efectuada por meio do envio seguro de mensagens (ver apêndice 11).

3.5. Descrição de comandos e códigos de erro

Os comandos e a organização dos ficheiros são deduzidos da norma ISO/CEI 7816-4, à qual devem, ademais, obedecer.

TCS_313 A presente secção incide nos seguintes pares comando-resposta de APDU:

Comando	INS
SELECT FILE	A4
READ BINARY	B0
UPDATE BINARY	D6
GET CHALLENGE	84
VERIFY	20
GET RESPONSE	C0
PERFORM SECURITY OPERATION: VERIFY CERTIFICATE COMPUTE DIGITAL SIGNATURE VERIFY DIGITAL SIGNATURE HASH	2A
INTERNAL AUTHENTICATE	88
EXTERNAL AUTHENTICATE	82
MANAGE SECURITY ENVIRONMENT: SETTING A KEY	22
PERFORM HASH OF FILE	2A

TCS_314 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	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 certificate errado (durante a sua verificação) ou criptograma errado (durante autenticação externa) ou assinatura errada (durante a sua verificação)
67	00	Comprimento errado (Lc ou Le errados)
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	Faltam os objectos esperados do envio seguro de mensagens
69	88	Objectos incorrectos no envio seguro de mensagens
6A	82	Ficheiro não encontrado
6A	86	Parâmetros P1-P2 errados
6A	88	Dados referenciados não encontrados
6B	00	Parâmetros errados (desvio fora do EF)

SW1	SW2	Significado
6C	XX	Comprimento errado; SW2 indica comp. exacto; não devolvido campo de dados
6D	00	Código de instrução não suportado ou inválido
6E	00	Classe não suportada
6F	00	Outros erros de verificação

3.6. Descrição dos comandos

O presente capítulo incide nos comandos obrigatórios para os cartões tacográficos.

O apêndice 11 (Mecanismos comuns de segurança) 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 respectivos valor, comprimento e descrição.

TCS_315 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 3.6.6) com P3=Le.

TCS_316 Sendo pedidos ambos os bytes de comprimento e Le=0 (envio seguro de mensagens):

- ao utilizar o protocolo T=1, o cartão responde a Le=0 enviando todos os dados de saída (output data) disponíveis;
- ao utilizar o protocolo T=0, o IFD envia o primeiro comando com P3=Lc + dados, o cartão responde (a este implícito Le=0) 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.

3.6.1. Select File

Este comando cumpre a norma ISO/CEI 7816-4, mas tem uma utilização restrita, a comparar com o comando definido na norma.

O comando SELECT FILE é utilizado para:

- seleccionar uma aplicação DF (tem de ser utilizada selecção por nome)
- seleccionar um ficheiro elementar correspondente ao ID do ficheiro apresentado.

3.6.1.1. Selecção por nome (AID)

Este comando permite seleccionar um DF de aplicação no cartão.

TCS_317 Este comando pode ser executado a partir de qualquer ponto na estrutura do ficheiro (depois da ATR ou em qualquer momento).

TCS_318 A selecção de uma aplicação reinicializa (restabelece) o ambiente de segurança vigente. Executada a selecção da aplicação, mais nenhuma chave pública em curso é seleccionada, e a anterior chave de sessão deixa de estar disponível para envio seguro de mensagens. A condição de acesso AUT perde-se igualmente.

TCS_319 Mensagem de comando

Byte	Comprimento	Valor	Descrição
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'04h'	Selecção 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

Não é necessária resposta ao comando SELECT FILE (Le ausente em T=1, ou não é pedida resposta em T=0).

TCS_320 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 FILE, o estado devolvido é '6900'.
- Se a aplicação seleccionada for considerada corrompida (o erro de integridade é detectado nos atributos do ficheiro), o estado de processamento devolvido é '6400' ou '6581'.

3.6.1.2. *Seleção de um ficheiro elementar utilizando o seu identificador*

TCS_321 Mensagem de comando

Byte	Comprimento	Valor	Descrição
CLA	1	'00h'	
INS	1	'A4h'	
P1	1	'02h'	Seleção de um EF sob o DF em curso
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 FILE (Le ausente em T=1, ou não é pedida resposta em T=0).

TCS_322 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 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 FILE, o estado devolvido é '6900'.
- Se o ficheiro seleccionado for considerada corrompido (o erro de integridade é detectado nos atributos do ficheiro), o estado de processamento devolvido é '6400' ou '6581'.

3.6.2. **Read Binary**

Este comando cumpre a norma ISO/CEI 7816-4, mas tem uma utilização restrita, a comparar 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.

TCS_323 O comando só pode ser executado se o estatuto de segurança satisfizer os atributos de segurança definidos para o EF relativamente à função READ.

3.6.2.1. *Comando sem envio seguro de mensagens*

Este comando permite ao IFD ler dados do EF seleccionado de momento, sem envio seguro de mensagens.

TCS_324 A leitura de dados de um ficheiro marcado como "criptado" não deve ser possível por intermédio deste comando.

TCS_325 Mensagem de comando

Byte	Comprimento	Valor	Descrição
CLA	1	'00h'	Não pedido envio seguro de mensagens
INS	1	'B0h'	
P1	1	'XXh'	Desvio em bytes desde início do ficheiro: byte mais significativo
P2	1	'XXh'	Desvio em bytes desde 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 colocado em 0.

TCS_326 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 seleccionado nenhum EF, o estado de processamento devolvido é '6986'.
- Se o controlo de acesso do ficheiro seleccionado não for satisfeito, o comando é interrompido com '6982'.
- Se o desvio não for compatível com a dimensão do EF (desvio > dimensão EF), o estado de processamento devolvido é '6B00'.
- Se a dimensão dos dados a ler não for compatível com a dimensão do EF (desvio + Le > dimensão EF), o estado de processamento devolvido é '6700' ou '6Cxx', onde 'xx' indica o comprimento exacto.
- Se for detectado um erro de integridade nos atributos do ficheiro, o cartão considera o ficheiro corrompido e irrecoverável e o estado de processamento devolvido é '6400' ou '6581'.
- Se for detectado um erro de integridade nos dados memorizados, o cartão devolve os dados pedidos e o estado de processamento devolvido é '6281'.

3.6.2.2. *Comando com envio seguro de mensagens*

Este comando permite ao IFD ler dados do EF seleccionado de momento, com envio seguro de mensagens, a fim de verificar a integridade dos dados recebidos e proteger a sua confidencialidade caso o EF esteja marcado como "criptado".

TCS_327 Mensagem de comando

Byte	Comprimento	Valor	Descrição
CLA	1	'0Ch'	Pedido envio seguro de mensagens
INS	1	'B0h'	INS
P1	1	'XXh'	P1 (desvio em bytes desde início do ficheiro): byte mais significativo
P2	1	'XXh'	P2 (desvio em bytes desde início do ficheiro): byte menos significativo
Lc	1	'09h'	Comprimento dos dados de entrada para envio seguro de mensagens
#6	1	'97h'	T _{LE} : marcador (tag) para a especificação do comprimento esperado
#7	1	'01h'	L _{LE} : comprimento do comprimento esperado
#8	1	'NNh'	Especificaç. do comprim. esperado (Le original): número de bytes a ler

Byte	Comprimento	Valor	Descrição
#9	1	'8Eh'	T _{CC} : etiqueta ou marcador (tag) para soma criptográfica de teste
#10	1	'04h'	L _{CC} : comprimento da soma criptográfica de teste infra
#11-#14	4	'XX..XXh'	Soma criptográfica de teste (4 bytes mais significativos)
Le	1	'00h'	Cf. norma ISO/CEI 7816-4

TCS_328 Mensagem de resposta se o EF não estiver marcado como “criptado” e o formato de entrada do envio seguro de mensagens estiver correcto:

Byte	Comprimento	Valor	Descrição
#1	1	'81h'	T _{PV} : etiqueta/marcador (tag) para dados de valor simples
#2	L	'NNh' ou '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
#(2+L+NN)	1	'8Eh'	T _{CC} : marcador para soma criptográfica de teste
#(3+L+NN)	1	'04h'	L _{CC} : comprimento da soma criptográfica de teste infra
#(4+L+NN)-#(7+L+NN)	4	'XX..XXh'	Soma criptográfica de teste (4 bytes mais significativos)
SW	2	'XXXXh'	Palavras de estatuto (SW1, SW2)

TCS_329 Mensagem de resposta se o EF estiver marcado como “criptado” e o formato de entrada do envio seguro de mensagens estiver correcto:

Byte	Comprimento	Valor	Descrição
#1	1	'87h'	T _{PI CG} : marcador (tag) para dados criptados (criptograma)
#2	L	'MMh' ou '81 MMh'	L _{PI CG} : comprimento dos dados criptados devolvidos (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 criptados: indicador de enchimento e criptograma
#(2+L+MM)	1	'8Eh'	T _{CC} : etiqueta ou marcador para soma criptográfica de teste
#(3+L+MM)	1	'04h'	L _{CC} : comprimento da soma criptográfica de teste infra
#(4+L+MM)-#(7+L+MM)	4	'XX..XXh'	Soma criptográfica de teste (4 bytes mais significativos)
SW	2	'XXXXh'	Palavras de estatuto (SW1, SW2)

Os dados criptados devolvidos contêm um primeiro byte que indica o modo de preenchimento utilizado. Para a aplicação tacográfica, o indicador de preenchimento toma sempre o valor '01h', indicando que o modo de preenchimento utilizado é o especificado na norma ISO/CEI 7816-4 (um byte com o valor '80h', seguido de alguns bytes nulos: ISO/CEI 9797, método I).

Os estados de processamento “regular”, descritos relativamente ao comando READ BINARY sem envio seguro de mensagens (ver ponto 3.6.2.1), 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 ser envolvida nenhuma estrutura de envio seguro de mensagens:

TCS_330 Mensagem de resposta se o formato de entrada do envio seguro de mensagens estiver incorrecto:

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).

— Se no formato de envio seguro de mensagens faltarem alguns objectos de dado esperados (cf. especificação supra), o estado de processamento '6987' é devolvido: este erro ocorre se faltar um marcador ou etiqueta (tag) esperado ou se o corpo do comando não for construído adequadamente.

— Se alguns objectos de dado estiverem incorrectos, o estado de processamento devolvido é '6988': este erro ocorre se todos os marcadores (tags) requeridos 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'.

3.6.3. Update Binary

Este comando cumpre a norma ISO/CEI 7816-4, mas tem uma utilização restrita, a comparar com o comando definido na norma.

A mensagem de comando UPDATE BINARY inicia a actualização ou update (erase + write) dos bits já presentes num binário EF com os bits dados no comando APDU.

TCS_331 O comando só pode ser executado se o estatuto de segurança satisfizer os atributos de segurança definidos para o EF para a função UPDATE (se o controlo do acesso à função UPDATE incluir PRO SM, deve ser acrescentado ao comando um envio seguro de mensagens).

3.6.3.1. Comando sem envio seguro de mensagens

Este comando permite ao IFD escrever dados no EF seleccionado de momento, sem o cartão verificar a integridade dos dados recebidos. Este modo simples só é autorizado se o ficheiro correspondente não estiver marcado como "criptado".

TCS_332 Mensagem de comando

Byte	Comprimento	Valor	Descrição
CLA	1	'00h'	Não pedido envio seguro de mensagens
INS	1	'D6h'	
P1	1	'XXh'	Desvio em bytes desde início do ficheiro: byte mais significativo
P2	1	'XXh'	Desvio em bytes desde início do ficheiro: byte menos significativo
Lc	1	'NNh'	Comprim. Lc dos dados a actualizar: número de bytes a escrever
#6-#(5+NN)	NN	'XX..XXh'	Dados a escrever

Nota: o bit 8 de P1 deve ser colocado em 0.

TCS_333 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 seleccionado nenhum EF, o estado de processamento devolvido é '6986'.

— Se o controlo de acesso do ficheiro seleccionado não for satisfeito, o comando é interrompido com '6982'.

— Se o desvio não for compatível com a dimensão do EF (desvio > dimensão EF), o estado de processamento devolvido é '6B00'.

— Se a dimensão dos dados a escrever não for compatível com a dimensão do EF (desvio + Le > dimensão EF), o estado de processamento devolvido é '6700'.

— Se for detectado 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'.

3.6.3.2. Comando com envio seguro de mensagens

Este comando permite ao IFD escrever dados no EF seleccionado de momento, com o cartão a verificar a integridade dos dados recebidos. Como não é exigida confidencialidade, os dados não são criptados.

TCS_334 Mensagem de comando

Byte	Comprimento	Valor	Descrição
CLA	1	'0Ch'	Pedido envio seguro de mensagens
INS	1	'D6h'	INS
P1	1	'XXh'	Desvio em bytes desde início do ficheiro: byte mais significativo
P2	1	'XXh'	Desvio em bytes desde início do ficheiro: byte menos significativo
Lc	1	'XXh'	Comprimento do campo de dados securizado
#6	1	'81h'	T _{PV} : etiqueta (tag) para dados de valor simples
#7	L	'NNh' ou '81NNh'	L _{PV} : comprimento dos dados transmitidos L é 2 bytes se L _{PV} > 127 bytes
#(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	'04h'	L _{CC} : comprimento da soma criptográfica de teste infra
#(9+L+NN)-#(12+L+NN)	4	'XX..XXh'	Soma criptográf. de teste (4 bytes mais significativos)
Le	1	'00h'	Cf. norma ISO/CEI 7816-4

TCS_335 Mensagem de resposta se o formato de entrada do envio seguro de mensagens estiver correcto:

Byte	Comprimento	Valor	Descrição
#1	1	'99h'	T _{SW} : etiqueta (tag) para palavras de estatuto (a proteger por CC)
#2	1	'02h'	L _{SW} : comprimento das palavras de estatuto devolvidas
#3-#4	2	'XXXXh'	Palavras de estatuto (SW1, SW2)
#5	1	'8Eh'	T _{CC} : etiqueta ou marcador para soma criptográfica de teste
#6	1	'04h'	L _{CC} : comprimento da soma criptográfica de teste infra
#7-#10	4	'XX..XXh'	Soma criptográfica de teste (4 bytes mais significativos)
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 3.6.3.1), 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 ser envolvida nenhuma estrutura de envio seguro de mensagens:

TCS_336 Mensagem de resposta se houver erro no envio seguro de mensagens:

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.
- Se no formato de envio seguro de mensagens faltarem alguns objectos de dado esperados (cf. especificação supra), o estado de processamento '6987' é devolvido: este erro ocorre se faltar um marcador ou etiqueta (tag) esperado ou se o corpo do comando não for construído adequadamente.
- Se alguns objectos de dado estiverem incorrectos, o estado de processamento devolvido é '6988': este erro ocorre se todos os marcadores requeridos 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'.

3.6.4. *Get Challenge*

Este comando cumpre a norma ISO/CEI 7816-4, mas tem uma utilização restrita, a comparar com o comando definido na norma.

O comando GET CHALLENGE pede ao cartão que emita um desafio (challenge), a fim de o utilizar num procedimento de segurança no âmbito do qual são enviados ao cartão um criptograma ou alguns dados cifrados.

TCS_337 O desafio emitido pelo cartão só é válido para o comando seguinte enviado ao cartão e que utiliza desafio.

TCS_338 Mensagem de comando

Byte	Comprimento	Valor	Descrição
CLA	1	'00h'	CLA
INS	1	'84h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2
Le	1	'08h'	Le (comprimento do desafio esperado)

TCS_339 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 e P2 forem incorrectos, o estado de processamento é '6A86'.

3.6.5. *Verify*

Este comando cumpre a norma ISO/CEI 7816-4, mas tem uma utilização restrita, a comparar com o comando definido na norma.

O comando VERIFY inicia a comparação, no cartão, entre os dados CHV (PIN) enviados do comando e a CHV de referência memorizada no cartão.

Nota: o PIN introduzido pelo utilizador deve ser preenchido à direita pelo IFD com bytes 'FFh', até um comprimento de 8 bytes.

TCS_340 Se o comando for bem sucedido, os direitos correspondentes à apresentação da CHV são abertos e reinicializa-se o contador de tentativas remanescentes da CHV.

TCS_341 Uma comparação mal sucedida é registada no cartão, a fim de limitar a quantidade de novas tentativas de utilização da CHV de referência.

TCS_342 Mensagem de comando

Byte	Comprimento	Valor	Descrição
CLA	1	'00h'	CLA
INS	1	'20h'	INS
P1	1	'00h'	P1
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_343 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 $X = 'F'$, o contador de tentativas da CHV é maior do que 'F').
- Se a CHV de referência for considerada corrompida, o estado de processamento devolvido é '6400' ou '6581'.

3.6.6. **Get Response**

Este comando cumpre a norma ISO/CEI 7816-4.

Este comando (somente necessário e disponível 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_344 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

TCS_345 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 exacto 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 suportado (protocolo T=1), o cartão devolve '6D00'.

3.6.7. **PSO: Verify Certificate**

Este comando cumpre a norma ISO/CEI 7816-8, mas tem uma utilização restrita, a comparar 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.

TCS_346 Quando um comando VERIFY CERTIFICATE é bem sucedido, a chave pública é memorizada para futura utilização no ambiente de segurança. Esta chave deve ser explicitamente estabelecida para utilização em comandos relativos à segurança (INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE ou VERIFY CERTIFICATE) pelo comando MSE (ver ponto 3.6.10), recorrendo ao seu identificador de chave.

TCS_347 Em qualquer caso, o comando VERIFY CERTIFICATE utiliza a chave pública previamente seleccionada pelo comando MSE para abrir o certificado. Esta chave pública deve ser a de um Estado-Membro ou da Europa.

TCS_348 Mensagem de comando

Byte	Comprimento	Valor	Descrição
CLA	1	'00h'	CLA
INS	1	'2Ah'	Perform Security Operation (executar operação de segurança)
P1	1	'00h'	P1
P2	1	'AEh'	P2: dados codificados não BER-TLV (concatenação de elementos de dado)
Lc	1	'CEh'	Lc: Comprimento do certificado, 194 bytes
#6-#199	194	'XX..XXh'	Certificado: concatenação de elementos de dado (ver apêndice 11)

TCS_349 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 é descrito no apêndice 11.
- Se nenhuma chave pública estiver presente no ambiente de segurança, é devolvido '6A88'.
- Se a chave pública seleccionada (utilizada para desmontar o certificado) for considerada corrompida, o estado de processamento devolvido é '6400' ou '6581'.
- Se a chave pública seleccionada (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'.

3.6.8. Internal Authenticate

Este comando cumpre a norma ISO/CEI 7816-4.

É por intermédio do comando INTERNAL AUTHENTICATE que o IFD pode autenticar o cartão.

O processo de autenticação é descrito no apêndice 11. Inclui as seguintes declarações:

TCS_350 O comando INTERNAL AUTHENTICATE utiliza a chave privada do cartão (implicitamente seleccionada) para assinar dados de autenticação, incluindo K1 (primeiro elemento para acordo de chave de sessão) e RND1, e utiliza a chave pública seleccionada no momento (através do último comando MSE) para criptar a assinatura e formar o testemunho de autenticação (mais pormenores no apêndice 11).

TCS_351 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_352 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, é devolvido '6A88'.
- Se nenhuma chave privada estiver presente no ambiente de segurança, é devolvido '6A88'.
- Se VU.CHR não corresponder ao identificador de chave pública em curso, o estado de processamento devolvido é '6A88'.
- Se a chave privada seleccionada for considerada corrompida, o estado de processamento devolvido é '6400' ou '6581'.

TCS_353 Se o comando INTERNAL_AUTHENTICATE for bem sucedido, a chave de sessão em curso, se existir, é apagada e deixa de estar disponível. Para dispor de uma nova chave de sessão, tem de ser executado com êxito o comando EXTERNAL_AUTHENTICATE.

3.6.9. External Authenticate

Este comando cumpre a norma ISO/CEI 7816-4.

É por intermédio do comando EXTERNAL_AUTHENTICATE que o cartão pode autenticar o IFD.

O processo de autenticação é descrito no apêndice 11. Inclui as seguintes declarações:

- TCS_354 O comando EXTERNAL_AUTHENTICATE deve ser imediatamente precedido por um comando GET_CHALLENGE. O cartão emite um desafio (challenge) para o exterior (RND3).
- TCS_355 A verificação do criptograma utiliza o RND3 (desafio emitido pelo cartão), a chave privada do cartão (implicitamente seleccionada) e a chave pública previamente seleccionada pelo comando MSE.
- TCS_356 O cartão verifica o criptograma e, se este estiver correcto, abre-se a condição de acesso AUT.
- TCS_357 O criptograma de entrada transporta o segundo elemento para acordo de chave de sessão K2.

TCS_358 Mensagem de comando

Byte	Comprimento	Valor	Descrição
CLA	1	'00h'	CLA
INS	1	'82h'	INS
P1	1	'00h'	P1
P2	1	'00h'	P2 (a chave pública a utilizar é implicitamente conhecida e foi previamente estabelecida pelo comando MSE)
Lc	1	'80h'	Lc (comprimento dos dados enviados ao cartão)
#6-#133	128	'XX..XXh'	Criptograma (ver apêndice 11)

TCS_359 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 nenhuma chave pública estiver presente no ambiente de segurança, é devolvido '6A88'.
- 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' (ver apêndice 11).
- 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 o comando não for imediatamente precedido por um comando GET CHALLENGE, o estado de processamento devolvido é '6985'.
- Se a chave privada seleccionada for considerada corrompida, o estado de processamento devolvido é '6400' ou '6581'.

TCS_360 Se o comando EXTERNAL AUTHENTICATE for bem sucedido, e se a primeira parte da chave de sessão estiver disponível a partir de um comando INTERNAL AUTHENTICATE recentemente executado com êxito, a chave de sessão é estabelecida para futuros comandos que utilizem o envio seguro de mensagens.

TCS_361 Se a primeira parte da chave de sessão não estiver disponível a partir de um anterior comando INTERNAL AUTHENTICATE, a segunda parte da chave de sessão, enviada pelo IFD, não é memorizada no cartão. Este mecanismo assegura que o processo de autenticação mútua seja efectuado segundo a ordem especificada no apêndice 11.

3.6.10. *Manage Security Environment*

Este comando é utilizado para estabelecer uma chave pública com fins de autenticação.

Este comando cumpre a norma ISO/CEI 7816-8. A comparar com a norma, a sua utilização é restrita.

TCS_362 A chave referenciada no campo de dados MSE é válida para todos os ficheiros do DF tacográfico.

TCS_363 A chave referenciada no campo de dados MSE mantém-se como chave pública em curso até ao comando MSE correcto que se seguir.

TCS_364 Se a chave referenciada não estiver (já) presente no cartão, o ambiente de segurança mantém-se inalterado.

TCS_365 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'	Etiqueta (tag) para referenciar uma chave pública em casos assimétricos
#7	1	'08h'	Comprimento da referência da chave (identificador da chave)
#8-#15	08h	'XX..XXh'	Identificador de chave, conforme especifica o apêndice 11

TCS_366 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 chave referenciada não estiver presente no cartão, o estado de processamento devolvido é '6A88'.
- Se no formato de envio seguro de mensagens faltarem alguns objectos de dado esperados, o estado de processamento '6987' é devolvido, o que pode ocorrer se faltar o marcador (tag) '83h'.
- Se alguns objectos de dado estiverem incorrectos, o estado de processamento devolvido é '6988', o que pode ocorrer se o comprimento do identificador de chave não for '08h'.
- Se a chave seleccionada for considerada corrompida, o estado de processamento devolvido é '6400' ou '6581'.

3.6.11. **PSO: Hash**

Este comando é utilizado para transferir para o cartão o resultado de um cálculo de controlo (hash calculation) sobre alguns dados. Serve para a verificação de assinaturas digitais. O valor (hash value) é memorizado em EEPROM para o comando subsequente verificar a assinatura digital.

Este comando cumpre a norma ISO/CEI 7816-8. A comparar com a norma, a sua utilização é restrita.

TCS_367 Mensagem de comando

Byte	Comprimento	Valor	Descrição
CLA	1	'00h'	CLA
INS	1	'2Ah'	Perform Security Operation (executar operação de segurança)
P1	1	'90h'	Devolver código de hash (hash code)
P2	1	'A0h'	Etiqueta: o campo de dados contém DOs com interesse para o hashing
Lc	1	'16h'	Comprimento Lc de campo de dados subsequente
#6	1	'90h'	Etiqueta ou marcador (tag) para o código de hash
#7	1	'14h'	Comprimento do código de hash
#8-#27	20	'XX..XXh'	Código de hash (hash code)

TCS_368 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 objectos de dado esperados (cf. especificação supra), o estado de processamento '6987' é devolvido, o que pode ocorrer se faltar uma das etiquetas (tags) '90h'.
- Se alguns objectos de dado estiverem incorrectos, o estado de processamento devolvido é '6988': este erro ocorre se a etiqueta requerida estiver presente mas com comprimento diferente de '14h'.

3.6.12. **Perform Hash of File**

Este comando não segue a norma ISO/CEI 7816-8. Por conseguinte, o seu byte CLA indica que existe uma utilização própria (proprietary use) do PERFORM SECURITY OPERATION/HASH.

TCS_369 O comando PERFORM HASH OF FILE utiliza-se para controlar em relação a dados não significativos a área do EF transparente seleccionado no momento.

TCS_370 O resultado da operação hash é memorizado no cartão, podendo então ser utilizado para obter uma assinatura digital do ficheiro, por intermédio do comando PSO: COMPUTE DIGITAL SIGNATURE. Este resultado mantém-se disponível para o comando COMPUTE DIGITAL SIGNATURE até ao seguinte comando PERFORM HASH OF FILE que for bem sucedido.

TCS_371 Mensagem de comando

Byte	Comprimento	Valor	Descrição
CLA	1	'80h'	CLA
INS	1	'2Ah'	Perform Security Operation (executar operação de segurança)
P1	1	'90h'	Etiqueta ou marcador: hash
P2	1	'00h'	P2: controlar os dados do ficheiro transparente seleccionado

TCS_372 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 nenhuma aplicação for seleccionada, é devolvido o estado de processamento '6985'.
- Se o EF seleccionado 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 seleccionado não for transparente, o estado de processamento devolvido é '6986'.

3.6.13. PSO: Compute Digital Signature

Este comando é utilizado para calcular a assinatura digital de um código hash previamente calculado (ver PERFORM HASH OF FILE, ponto 3.6.12).

Este comando cumpre a norma ISO/CEI 7816-8. A comparar com a norma, a sua utilização é restrita.

TCS_373 A chave privada do cartão é utilizada para calcular a assinatura digital e é implicitamente conhecida pelo cartão.

TCS_374 O cartão executa uma assinatura digital por um método de preenchimento que segue PKCS1 (ver apêndice 11).

TCS_375 Mensagem de comando

Byte	Comprimento	Valor	Descrição
CLA	1	'00h'	CLA
INS	1	'2Ah'	Perform Security Operation (executar operação de segurança)
P1	1	'9Eh'	Assinatura digital a devolver
P2	1	'9Ah'	Etiqueta (tag): 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 do ficheiro)
Le	1	'80h'	Comprimento da assinatura esperada

TCS_376 Mensagem de resposta

Byte	Comprimento	Valor	Descrição
#1-#128	128	'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 seleccionada for considerada corrompida, o estado de processamento devolvido é '6400' ou '6581'.

3.6.14. PSO: Verify Digital Signature

Este comando é utilizado para verificar a assinatura digital, fornecida sob a forma de input (entrada), em conformidade com PKCS1 de uma mensagem, cujo hash é conhecido pelo cartão. O algoritmo da assinatura é implicitamente conhecido pelo cartão.

Este comando cumpre a norma ISO/CEI 7816-8. A comparar com a norma, a sua utilização é restrita.

TCS_377 O comando VERIFY DIGITAL SIGNATURE utiliza sempre a chave pública seleccionada pelo anterior comando MANAGE SECURITY ENVIRONMENT e o anterior código hash introduzido por um comando PSO: HASH.

TCS_378 Mensagem de comando

Byte	Comprimento	Valor	Descrição
CLA	1	'00h'	CLA
INS	1	'2Ah'	Perform Security Operation (executar operação de segurança)
P1	1	'00h'	
P2	1	'A8h'	Etiqueta: campo de dados contém DOs com interesse para verificação
Lc	1	'83h'	Comprimento Lc do campo de dados subsequente
#28	1	'9Eh'	Marcador (tag) para assinatura digital
#29-#30	2	'8180h'	Comprimento da assinatura digital (128 bytes, codificação conforme ISO/CEI 7816-6)
#31-#158	128	'XX..XXh'	Conteúdo da assinatura digital

TCS_379 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'. Processo de verificação descrito no apêndice 11.
- Se nenhuma chave pública for seleccionada, o estado de processamento devolvido é '6A88'.
- Se faltarem alguns objectos de dado esperados (cf. especificação supra), o estado de processamento '6987' é devolvido, o que pode ocorrer se faltar um dos marcadores (tags) requeridos.
- Se não estiver disponível nenhum código hash para processar o comando (em resultado de um anterior comando PSO: HASH), o estado de processamento devolvido é '6985'.
- Se alguns objectos de dado estiverem incorrectos, o estado de processamento devolvido é '6988', o que pode ocorrer se for incorrecto o comprimento de um dos objectos de dado requeridos.
- Se a chave pública seleccionada for considerada corrompida, o estado de processamento devolvido é '6400' ou '6581'.

4. ESTRUTURA DOS CARTÕES TACOGRÁFICOS

Esta secção especifica as estruturas de ficheiro dos cartões tacográficos para memorização de dados acessíveis.

Não especifica estruturas internas dependentes do fabricante do cartão, como, por exemplo, marcadores de ficheiro ou marcadores-cabeçalho (file headers), nem a memorização ou o manuseamento de elementos de dado necessários unicamente para utilização interna, como `EuropeanPublicKey`, `CardPrivateKey`, `TDesSessionKey` ou `WorkshopCardPin`.

A capacidade útil de memorização dos cartões tacográficos deve ser, no mínimo, de 11 kbytes, podendo, no entanto, exceder este valor, caso em que a estrutura do cartão se mantém, mas aumenta o número de registos de alguns elementos da estrutura. Esta secção especifica os valores mínimos e máximos destes números de registos.

4.1. Estrutura do cartão de condutor

TCS_400 Uma vez personalizado, o cartão de condutor deve ter permanentemente as seguintes estrutura de ficheiro e condições de acesso:

Ficheiro	ID do ficheiro	Condições de acesso		
		Ler	Actualizar	Criptado
MF	3F00			
EF ICC	0002	ALW	NEV	Não
EF IC	0005	ALW	NEV	Não
DF Tachograph	0500			
EF Application_Identification	0501	ALW	NEV	Não
EF Card_Certificate	C100	ALW	NEV	Não
EF CA_Certificate	C108	ALW	NEV	Não
EF Identification	0520	ALW	NEV	Não
EF Card_Download	050E	ALW	ALW	Não
EF Driving_Licence_Info	0521	ALW	NEV	Não
EF Events_Data	0502	ALW	PRO SM / AUT	Não
EF Faults_Data	0503	ALW	PRO SM / AUT	Não
EF Driver_Activity_Data	0504	ALW	PRO SM / AUT	Não
EF Vehicles_Used	0505	ALW	PRO SM / AUT	Não
EF Places	0506	ALW	PRO SM / AUT	Não
EF Current_Usage	0507	ALW	PRO SM / AUT	Não
EF Control_Activity_Data	0508	ALW	PRO SM / AUT	Não
EF Specific_Conditions	0522	ALW	PRO SM / AUT	Não

TCS_401 Todas as estruturas de EF devem ser transparentes.

TCS_402 A leitura com envio seguro de mensagens deve ser possível para todos os ficheiros no âmbito de tacógrafos com DF.

TCS_403 O cartão de condutor deve ter a seguinte estrutura de dados:

Ficheiro/Elemento de dados	N.º de registos	Dimensão (bytes)		Valores por defeito
		Mín	Máx	
MF		11411	24959	
EF ICC		25	25	
CardIccIdentification		25	25	
clockStop	1	1	1	{00}
cardExtendedSerialNumber	8	8	8	{00..00}
cardApprovalNumber	8	8	8	{20..20}
cardPersonaliserID	1	1	1	{00}
embedderIcAssemblerId	5	5	5	{00..00}
icIdentifier	2	2	2	{00 00}
EF IC		8	8	
CardChipIdentification		8	8	
icSerialNumber	4	4	4	{00..00}
icManufacturingReferences	4	4	4	{00..00}
DF Tachograph		11378	24926	
EF Application_Identification		10	10	
DriverCardApplicationIdentification		10	10	
typeOfTachographCardId	1	1	1	{00}
cardStructureVersion	2	2	2	{00 00}
noOfEventsPerType	1	1	1	{00}
noOfFaultsPerType	1	1	1	{00}
activityStructureLength	2	2	2	{00 00}
noOfCardVehicleRecords	2	2	2	{00 00}
noOfCardPlaceRecords	1	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	1	{00}
cardNumber	16	16	16	{20..20}
cardIssuingAuthorityName	36	36	36	{20..20}
cardIssueDate	4	4	4	{00..00}
cardValidityBegin	4	4	4	{00..00}
cardExpiryDate	4	4	4	{00..00}
DriverCardHolderIdentification		78	78	
cardHolderName		72	72	
holderSurname	36	36	36	{00, 20..20}
holderFirstNames	36	36	36	{00, 20..20}
cardHolderBirthDate	4	4	4	{00..00}
cardHolderPreferredLanguage	2	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	
└ eventTypes		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	
└ faultTypes		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		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	
└ controlTypes		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}

TCS_404 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:

		Mín	Máx
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 mudan- ças de actividade)	13 776 Bytes (28 dias * 240 mu- danças de actividade)

4.2. Estrutura do cartão de centro de ensaio

TCS_405 Uma vez personalizado, o cartão de centro de ensaio deve ter permanentemente as seguintes estrutura de ficheiro e condições de acesso:

Ficheiro	ID do ficheiro	Condições de acesso		
		Ler	Actualizar	Criptado
MF	3F00			
EF ICC	0002	ALW	NEV	Não
EF IC	0005	ALW	NEV	Não
DF Tachograph	0500			
EF Application_Identification	0501	ALW	NEV	Não
EF Card_Certificate	C100	ALW	NEV	Não
EF CA_Certificate	C108	ALW	NEV	Não
EF Identification	0520	ALW	NEV	Não
EF Card_Download	0509	ALW	ALW	Não
EF Calibration	050A	ALW	PRO SM / AUT	Não
EF Sensor_Installation_Data	050B	ALW	NEV	Sim
EF Events_Data	0502	ALW	PRO SM / AUT	Não
EF Faults_Data	0503	ALW	PRO SM / AUT	Não
EF Driver_Activity_Data	0504	ALW	PRO SM / AUT	Não
EF Vehicles_Used	0505	ALW	PRO SM / AUT	Não
EF Places	0506	ALW	PRO SM / AUT	Não
EF Current_Usage	0507	ALW	PRO SM / AUT	Não
EF Control_Activity_Data	0508	ALW	PRO SM / AUT	Não
EF Specific_Conditions	0522	ALW	PRO SM / AUT	Não

TCS_406 Todas as estruturas de EF devem ser transparentes.

TCS_407 A leitura com envio seguro de mensagens deve ser possível para todos os ficheiros no âmbito de tacógrafos com DF.

TCS_408 O cartão de centro de ensaio deve ter a seguinte estrutura de dados:

Ficheiro/Elemento de dados	N.º de regis- tos	Dimensão (bytes)		Valores por de- feito
		Mín	Máx	
MF		11088	29061	
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}
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}
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	
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	10	10	
SpecificConditionRecord	2	5	
entryTime	4	4	{00..00}
SpecificConditionType	1	1	{00}

TCS_409 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 centro de ensaio deve utilizar:

		Mín	Máx
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 actividade)	492 bytes (1 dia * 240 mudan- ças de actividade)

4.3. Estrutura do cartão de controlador

TCS_410 Uma vez personalizado, o cartão de controlo (ou de controlador) deve ter permanentemente as seguintes estrutura de ficheiro e condições de acesso:

Ficheiro	ID do ficheiro	Condições de acesso		
		Ler	Actualizar	Criptado
MF	3F00			
EF ICC	0002	ALW	NEV	Não
EF IC	0005	ALW	NEV	Não
DF Tachograph	0500			
EF Application_Identification	0501	ALW	NEV	Não
EF Card_Certificate	C100	ALW	NEV	Não
EF CA_Certificate	C108	ALW	NEV	Não
EF Identification	0520	AUT	NEV	Não
EF Controller_Activity_Data	050C	ALW	PRO SM / AUT	Não

TCS_411 Todas as estruturas de EF devem ser transparentes.

TCS_412 A leitura com envio seguro de mensagens deve ser possível para todos os ficheiros no âmbito de tacógrafos com DF.

TCS_413 O cartão de controlo deve ter a seguinte estrutura de dados:

Ficheiro/Elemento de dados	N.º de regis- tos	Dimensão (bytes)		Valores por de- feito
		Mín	Máx	
MF		11219	24559	
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}
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_414 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:

		Mín	Máx
n ₇	NoOfControlActivityRecords	230	520

4.4. Estrutura do cartão de empresa

TCS_415 Uma vez personalizado, o cartão de empresa deve ter permanentemente as seguintes estrutura de ficheiro e condições de acesso:

Ficheiro	ID do ficheiro	Condições de acesso		
		Ler	Actualizar	Criptado
MF	3F00			
EF ICC	0002	ALW	NEV	Não
EF IC	0005	ALW	NEV	Não
DF Tachograph	0500			
EF Application_Identification	0501	ALW	NEV	Não
EF Card_Certificate	C100	ALW	NEV	Não
EF CA_Certificate	C108	ALW	NEV	Não
EF Identification	0520	AUT	NEV	Não
EF Company_Activity_Data	050D	ALW	PRO SM / AUT	Não

TCS_416 Todas as estruturas de EF devem ser transparentes.

TCS_417 A leitura com envio seguro de mensagens deve ser possível para todos os ficheiros no âmbito de tacógrafos com DF.

TCS_418 O cartão de empresa deve ter a seguinte estrutura de dados:

Ficheiro/Elemento de dados	N.º de registos	Dimensão (bytes)		Valores por defeito
		Mín	Máx	
MF		11147	24487	
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}
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}

cardNumberInformation			
cardType	1	1	{00}
cardIssuingMemberState	1	1	{00}
cardNumber	16	16	{20..20}
downloadPeriodBegin	4	4	{00..00}
downloadPeriodEnd	4	4	{00..00}

TCS_419 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:

		Min	Máx
n ₈	NoOfCompanyActivityRecords	230	520

Apêndice 3

PICTOGRAMAS

PIC_001 O aparelho de controlo pode utilizar os seguintes pictogramas e combinações de pictogramas:

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	Inspecção/calibração	Modo de calibração
	Fabricante		

	Actividades	Duração
	Disponível	Período de disponibilidade em curso
	Condução	Tempo de condução contínua
	Repouso	Período de repouso em curso
	Trabalho	Período de trabalho em curso
	Pausa	Tempo acumulado de pausas
	Actividade desconhecida	

	Equipamento	Funções
	Ranhura do condutor	
	Ranhura do ajudante	
	Cartão	
	Relógio	
	Visor	Visualização
	Memorização externa	Descarregamento
	Alimentação energética	
	Impressora	Impressão
	Sensor	
	Dimensão de pneumático	
	Veículo/unidade-veículo	

	Condições específicas
	Fora de âmbito
	Travessia batelão/comboio

	Diversos
	Acontecimentos
	Falhas
	Início do período de trabalho diário
	Final do período de trabalho diário
	Local
	Introdução manual das actividades do condutor
	Segurança
	Velocidade
	Tempo
	Total/síntese

Qualificadores

24h	Diário
I	Semanal
II	Quinzenal
+	De ou para

2. COMBINAÇÕES DE PICTOGRAMAS**Diversos**

	Local de controlo
	Local de início do período de trabalho diário
	Local de final do período de trabalho diário
	Das horas
	Às horas
	Do veículo
	Início de fora de âmbito
	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
	Tempo de condução por uma semana
	Tempo de condução por duas semanas

Impressão

24h	Impressão diária das actividades do condutor a partir do cartão
24h	Impressão diária das actividades do condutor a partir da VU
	Acontecimentos e falhas a partir de impressões do cartão
	Acontecimentos e falhas a partir de impressões da VU
	Impressão de dados técnicos
	Impressão de excesso de velocidade

Acontecimentos

	Inserção de cartão não válido
	Conflito de cartões
	Sobreposição de tempos
	Condução sem cartão adequado
	Inserção de cartão durante condução
	Última sessão de cartão encerrada incorrectamente
	Excesso de velocidade
	Interrupção da alimentação energética
	Erro nos dados de movimento
	Violação da segurança
	Ajustamento do tempo (pela oficina)
	Controlo do excesso de velocidade

Falhas

×■1	Falha do cartão (ranhura do condutor)
×■2	Falha do cartão (ranhura do ajudante)
×□	Falha do visor
×⚡	Falha do descarregamento
×⚙	Falha da impressora
×⚙	Falha do sensor
×⚙	Falha interna da VU

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 caracteres de impressão ou identificadores de registo.

2 Tipo de impressão

Identificador de bloco
 Combinação de pictogramas de impressão (ver apêndice 3)
 Fixação do dispositivo de limitação da velocidade (apenas impressão de velocidade excessiva)

```

-----T-----
Picto xxx km/h
  
```

3 Identificação do titular do cartão

Identificador de bloco. P = pictograma de pessoa
 Apelido do titular
 Nome próprio do titular (eventual)
 Identificação do cartão
 Prazo de validade do cartão (eventual)
 Se se tratar de um cartão não pessoal, ao qual não se aplique apelido do titular, o nome impresso será o da empresa, do centro de ensaio ou do organismo de controlo.

```

-----P-----
P Apelido _____
  Nome_Próprio _____
  Identificação_do_cartão ____
  dd/mm/aaaa
  
```

4 Identificação do veículo

Identificador de bloco
 VIN
 Estado-Membro de matrícula e VRN

```

-----A-----
A VIN _____
  Nac/VRN _____
  
```

5 Identificação da VU

Identificador de bloco
 Nome do fabricante da VU
 Número de peça da VU

```

-----B-----
B Fabricante_da_VU _____
  Número_de_peça_da_VU ____
  
```

6 Última calibração do aparelho de controlo

Identificador de bloco
 Nome do centro de ensaio
 Identificação do cartão do centro de ensaio
 Data da calibração

```

-----T-----
T Apelido _____
  Identificação_do_cartão ____
  T dd/mm/aaaa
  
```

7 Último controlo (por um agente controlador)

Identificador de bloco
 Identificação do cartão do controlador
 Data, hora e tipo do controlo
 Tipo de controlo: até quatro pictogramas. O tipo de controlo pode ser (uma combinação) de:
 B: Descarregamento do cartão, T: Descarregamento da VU,
 T: Impressão, B: Visualização

```

-----B-----
  Identificação_do_cartão ____
  B dd/mm/aaaa hh:mm pppp
  
```

8 Actividades de condutor memorizadas num cartão por ordem de ocorrência

Identificador de bloco
 Data do pedido (dia de calendário que é alvo da impressão)
 + Contador de presença diária do cartão

```

-----B-----
  dd/mm/aaaa xxx
  
```

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 e de final, duração

8.1c Actividade introduzida manualmente

Pictograma da actividade, hora de início e de final (inclusive), duração, períodos de repouso de pelo menos uma hora assinalados por uma estrela.

```

-----
? hh:mm hh:mm hh:mm
A hh:mm hh:mm hh:mm *
  
```

<p>8.2 <i>Inserção do cartão na ranhura S</i> Identificador de registo; S = Pictograma de ranhura Estado-Membro de matrícula e VRN do veículo Valor odométrico do veículo à inserção do cartão</p>	<pre> -----S----- A Nac/VRN _____ x xxx xxx km </pre>
<p>8.3 <i>Actividade (enquanto o cartão esteve inserido)</i> Pictograma da actividade, hora de início e de final (inclusive), duração, situação da condução (pictograma de tripulação se for CREW, em branco se for SINGLE), períodos de repouso de pelo menos uma hora assinalados por uma estrela.</p>	<pre> A hh:mm hh:mm hh:mm ☐☐ * </pre>
<p>8.3a <i>Condição especial.</i> Hora de introdução, pictograma da condição especial (ou combinação de pictogramas).</p>	<pre> hh:mm ----- pppp ----- </pre>
<p>8.4 <i>Retirada do cartão</i> Valor odométrico do veículo e distância percorrida desde a última inserção com valor odométrico conhecido</p>	<pre> x xxx xxx km; x xxx km </pre>
<p>9 Actividades de condutor memorizadas numa VU por ranhura e em ordem cronológica Identificador de bloco Data do pedido (dia de calendário alvo da impressão) Valor odométrico do veículo às 00:00 e às 24:00</p>	<pre> -----☐----- dd/mm/aaaa x xxx xxx - x xxx xxx km </pre>
<p>10 Actividades tratadas na ranhura S Identificador de bloco</p>	<pre> ----- S ----- </pre>
<p>10.1 <i>Período em que não esteve nenhum cartão inserido na ranhura S</i> Identificador de registo Nenhum cartão inserido Valor odométrico do veículo no início do período</p>	<pre> ----- ☐☐ --- x xxx xxx km </pre>
<p>10.2 <i>Inserção de cartão</i> Identificador de registo da inserção do cartão Apelido do condutor Nome próprio do condutor Identificação do cartão de condutor Prazo de validade do cartão de condutor EM de matrícula e VRN do veículo anterior Data e hora de retirada do cartão do veículo anterior Linha em branco Valor odométrico do veículo à inserção do cartão, bandeira a indicar se houve introdução manual de actividades de condutor (M se sim, em branco se não).</p>	<pre> ----- ☐ Apelido _____ Nome próprio _____ Identificação_do_cartão ___ dd/mm/aaaa A + Nac/VRN _____ dd/mm/aaaa hh:mm x xxx xxx km M </pre>
<p>10.3 <i>Actividade</i> Pictograma da actividade, hora de início e de final (inclusive), duração, situação da condução (pictograma de tripulação se for CREW, em branco se for SINGLE), períodos de repouso de pelo menos uma hora assinalados por uma estrela.</p>	<pre> A hh:mm hh:mm hh:mm ☐☐ * </pre>

- 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 odométrico do veículo à 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
- 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 0 0 - - -
- 11.2 **Síntese da VU para os períodos sem cartão na ranhura do ajudante**
Identificador de bloco
- 2 0 0 - - -
- 11.3 **Síntese da VU por cada condutor (principal ou ajudante)**
Identificador de registo
Apelido do condutor
Nome próprio do condutor
Identificação do cartão de condutor
- Apelido _____
 Nome_próprio _____
 Identificação_do_cartão ____
- 11.4 *Introdução do lugar de início e/ou final de um período de trabalho diário*
pi = pictograma do lugar, hora, país, região,
Valor odométrico
- pihh:mm Paí Reg
x xxx xxx km
- 11.5 *Totais de actividade (de um cartão)*
Duração total da condução, distância percorrida
Duração total do trabalho e da disponibilidade
Duração total dos períodos de repouso e desconhecidos
Duração total das actividades da tripulação
- hhhmm x xxx km
 ✖ hhhmm hhhmm
 H hhhmm ? hhhmm
 hhhmm
- 11.6 *Totais de actividade (períodos sem ranhura de cartão de condutor principal)*
Duração total da condução, distância percorrida
Duração total do trabalho e da disponibilidade
Duração total dos períodos de repouso
- hhhmm x xxx km
 ✖ hhhmm hhhmm
 H hhhmm
- 11.7 *Totais de actividade (períodos sem ranhura de cartão de ajudante)*
Duração total do trabalho e da disponibilidade
Duração total dos períodos de repouso
- ✖ hhhmm hhhmm
 H hhhmm

11.8 Totais de actividade (por condutor, incluídas ambas as ranhuras)

Duração total da condução, distância percorrida
 Duração total do trabalho e da disponibilidade
 Duração total dos períodos de repouso
 Duração total das actividades de tripulação
 Se se pretender uma impressão deste tipo para a data actual, a síntese diária é calculada com base nos dados disponíveis no momento da impressão.

```

    ☐ hhhmm x xxx km
    ✖ hhhmm ☐ hhhmm
    H hhhmm
    ☐☐ hhhmm
    
```

12 Incidentes e/ou falhas memorizados num cartão

12.1 Identificador de bloco para os últimos 5 "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, objectivo do registo, data e hora de início
 Código adicional do incidente/falha (eventual), duração
 Estado-Membro de matrícula e VRN do veículo no qual se produziu o incidente ou a falha

```

    -----
    Pic          dd/mm/aaaa hh:mm
    | xxx                      hhhmm
    ☐ Nac/VRN _____
    
```

13 Incidentes e/ou falhas memorizados ou em curso numa VU

13.1 Identificador de bloco para os últimos 5 "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, objectivo do registo, data e hora de início
 Código adicional do incidente/falha (eventual), quantidade de incidentes similares no mesmo dia, duração
 Identificação dos cartões inseridos no início ou final do incidente ou falha (até 4 linhas sem repetir duas vezes os mesmos números de cartão)

```

    -----
    Pic (p)      dd/mm/aaaa hh:mm
    | xxx        (xxx)      hhhmm

    Identificação_do_cartão ____
    Identificação_do_cartão ____
    Identificação_do_cartão ____
    Identificação_do_cartão ____

    ☐ ---
    
```

Caso em que não esteja nenhum cartão inserido
 O objectivo do registo (p) é um código numérico que explica por que foi registado o incidente ou a falha, codificado segundo o elemento de dado EventFaultRecord-Purpose.

14 Identificação da VU

Identificador de bloco
 Nome do fabricante da VU
 Endereço do fabricante da VU
 Número de peça da VU
 Número de homologação da VU
 Número de série da VU
 Ano de fabrico da VU
 Versão do software da VU e sua data de instalação

```

-----B-----
B Nome _____
  Endereço _____
  Número_de_peça _____
  Homol _____
  N.º_de_série ____
  aaaa
  V  xx.xx.xx  dd/mm/aaaa
  
```

15 Identificação do sensor

Identificador de bloco
 Número de série do sensor
 Número de homologação do sensor
 Data da primeira instalação do sensor

```

-----L-----
L N.º_de_série _____
  Homol _____
  dd/mm/aaaa
  
```

16 Dados da calibração

Identificador de bloco

```

-----T-----
  
```

16.1 Registo da calibração

Identificador de registo
 Centro de ensaio que efectuou a calibração
 Endereço do centro de ensaio
 Identificação do cartão do centro de ensaio
 Prazo de validade do cartão do centro de ensaio
 Linha em branco
 Data da calibração + objectivo da calibração
 VIN
 Estado-Membro de matrícula e VRN
 Coeficiente característico do veículo
 Constante do aparelho de controlo
 Perímetro efectivo dos pneumáticos das rodas
 Dimensão dos pneumáticos montados
 Instalação do dispositivo de limitação da velocidade
 Valores odométricos antigo e novo
 O objectivo da calibração (p) é um código numérico que explica por que foram registados estes parâmetros de calibração, codificados segundo o elemento de dado CalibrationPurpose.

```

-----
T Nome_do_centro _____
  Endereço_do_centro _____
  Identificação_do_cartão ____
  dd/mm/aaaa

T dd/mm/aaaa (p)
A VIN _____
  Nac/VRN _____

w xx xxx Imp/km
k xx xxx Imp/km
l xx xxx mm
e DimensãoPneus _____
> xxx km/h
x xxx xxx - x xxx xxx km
  
```

17 Ajustamento do tempo

Identificador de bloco

```

-----C-----
  
```

17.1 Registo do ajustamento do tempo

Identificador do registo
 Data e hora antigas
 Data e hora novas
 Centro de ensaio que efectuou o ajustamento do tempo
 Endereço do centro de ensaio
 Identificação do cartão do centro de ensaio
 Prazo de validade do cartão do centro de ensaio

```

-----
! C dd/mm/aaaa hh:mm
C dd/mm/aaaa hh:mm
T Nome_do_centro _____
  Endereço_do_centro _____
  Identificação_do_cartão _
  dd/mm/aaaa
  
```

18 Incidente e falha mais recentes registados na VU

Identificador de bloco
 Data e hora do incidente mais recente
 Data e hora da falha mais recente

```
----- ! x A -----
! dd/mm/aaaa hh:mm
x dd/mm/aaaa hh:mm
```

19 Informação sobre controlo de excesso de velocidade

Identificador de bloco
 Data e hora do último OVER SPEEDING CONTROL
 Data e hora do primeiro excesso de velocidade e quantidade de tais incidentes desde então

```
----- >> -----
> dd/mm/aaaa hh:mm
>> dd/mm/aaaa hh:mm (nnn)
```

20 Registo do excesso de velocidade

20.1 Identificador do bloco “primeiro excesso de velocidade desde a última calibração”

```
----- >>↑ -----
```

20.2 Identificador do bloco “os 5 mais graves nos últimos 365 dias”

```
----- >>(365) -----
```

20.3 Identificador do bloco “o mais grave de cada um dos últimos 10 dias de ocorrência”

```
----- >>(10) -----
```

20.4 Identificador do registo
 Data, hora e duração
 Velocidades máxima e média, quantidade de incidentes similares no mesmo dia
 Apelido do condutor
 Nome próprio do condutor
 Identificação do cartão do condutor

```
-----
>> dd/mm/aaaa hh:mm hh:mm
xxx km/h xxx km/h (xxx)
@ Apelido _____
Nome próprio _____
Identificação_do_cartão ____
```

20.5 Não existindo registo de excesso de velocidade num bloco

```
>> - - -
```

21 Informação manuscrita

Identificador de bloco
 21.1 Lugar do controlo
 21.2 Assinatura do controlador
 21.3 Das horas
 21.4 Às horas
 21.5 Assinatura do condutor
 “Informação manuscrita”: por cima de um atributo manuscrito, inserir linhas em branco em quantidade suficiente para poder escrever a informação necessária ou proceder à assinatura.

```
-----
@+ .....
@ .....
@+ .....
+@ .....
@ .....
-----
```

3. ESPECIFICAÇÕES APLICÁVEIS À IMPRESSÃO

Nesta secção aplicam-se as seguintes convenções de notação:

N	Número de bloco ou de registo de impressão
N	Número de bloco ou de registo de impressão repetido as vezes necessárias
X/Y	Blocos ou registos de impressão X e/ou Y conforme necessário, e repetidos as vezes necessárias.

3.1. Actividades de condutor, da impressão diária dos cartões

PRT_007 As actividades 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)
4	Identificação do veículo (veículo do qual a impressão é tomada)
5	Identificação da VU (VU da qual a impressão é tomada)
6	Última calibração desta VU
7	Último controlo a que o condutor foi sujeito
8	Delimitador das actividades de condutor
8.1a / 8.1b / 8.1c / 8.2 / / 8.3 / 8.3a / 8.4	Actividades do condutor por ordem de ocorrência
11	Delimitador da síntese diária
11.4	Lugares introduzidos, por ordem cronológica
11.5	Totais de actividade
12.1	Incidentes ou falhas, com base no delimitador do cartão
12.4	Registos de incidente/falha (últimos 5 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)
21.1	Lugar do controlo
21.2	Assinatura do controlador
21.5	Assinatura do condutor

3.2. Actividades de condutor, da impressão diária da VU

PRT_008 As actividades 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 (para todos os cartões inseridos na VU)
4	Identificação do veículo (veículo do qual a impressão é tomada)
5	Identificação da VU (VU da qual a impressão é tomada)
6	Última calibração desta VU
7	Último controlo neste aparelho de controlo
9	Delimitador das actividades de condutor
10	Delimitador da ranhura do condutor principal (ranhura 1)
10.1 / 10.2 / 10.3 / 10.3a / / 10.4	Actividades por ordem cronológica (ranhura do condutor principal)
10	Delimitador da ranhura do ajudante (ranhura 2)
10.1 / 10.2 / 10.3 / 10.3a / / 10.4	Actividades por ordem cronológica (ranhura do ajudante)
11	Delimitador da síntese diária
11.1	Síntese dos períodos sem cartão na ranhura do condutor principal
11.4	Lugares introduzidos, por ordem cronológica
11.6	Totais de actividade

11.2	Síntese dos períodos sem cartão na ranhura do ajudante
11.4	Lugares introduzidos, por ordem cronológica
11.7	Totais de actividade
11.3	Síntese das actividades de um condutor, incluídas ambas as ranhuras
11.4	Lugares introduzidos por este condutor, por ordem cronológica
11.7	Totais de actividade para este condutor
13.1	Delimitador de incidentes/falhas
13.4	Registos de incidente/falha (últimos 5 incidentes ou falhas memorizados ou em curso na VU)
21.1	Lugar do controlo
21.2	Assinatura do controlador
21.3	Das horas (espaço para um condutor sem cartão indicar os períodos pertinentes)
21.4	Às horas
21.5	Assinatura do condutor

3.3. Incidentes e falhas, da impressão do cartão

PRT_009 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)
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)
21.1	Lugar do controlo
21.2	Assinatura do controlador
21.5	Assinatura do condutor

3.4. Incidentes e falhas, da impressão da VU

PRT_010 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)
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 no cartão)
13.3	Delimitador de falhas
13.4	Registos de falhas (todas as falhas memorizadas no cartão)
21.1	Lugar do controlo
21.2	Assinatura do controlador
21.5	Assinatura do condutor

3.5. Impressão de dados técnicos

PRT_011 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)
4	Identificação do veículo (veículo do qual a impressão é tomada)
14	Identificação da VU
15	Identificação do sensor
16	Delimitador dos dados de calibração
16.1	Registos de calibração (todos os registos disponíveis por ordem cronológica)
17	Delimitador do ajustamento do tempo
17.1	Registos de ajustamento do tempo (todos os registos disponíveis de ajustamento do tempo e de registo de dados da calibração)
18	Incidente e falha mais recentes registados na VU

3.6. Impressão do excesso de velocidade

PRT_012 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)
4	Identificação do veículo (veículo do qual a impressão é tomada)
19	Informação relativa ao controlo do excesso de velocidade
20.1	Identificador de dados do excesso de velocidade
20.4 / 20.5	Primeiro excesso de velocidade desde a última calibração
20.2	Identificador dos dados de excesso de velocidade
20.4 / 20.5	Os 5 incidentes mais graves de excesso de velocidade dos últimos 365 dias
20.3	Identificador dos dados de excesso de velocidade
20.4 / 20.5	O mais grave excesso de velocidade de cada um dos últimos 10 dias
21.1	Lugar do controlo
21.2	Assinatura do controlador
21.5	Assinatura do condutor

Apêndice 5

VISUALIZAÇÃO

No presente apêndice, aplicam-se as seguintes convenções à notação de formato:

- caracteres **a negro (bold)** indicam texto normal a imprimir (a impressão vem em caracteres normais),
 - caracteres normais indicam variáveis (pictogramas ou dados) a substituir pelos seus valores na impressão,
- 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 (ou modo de operação).

DIS_001 O aparelho de controlo deve exibir (dar a visualizar) os dados, mediante os seguintes formatos:

Dados	Formato
Visualização por defeito	
Hora local	hh:mm
Modo de funcionamento	O
Informação relativa ao condutor princ	1 Dh <h>h hh<h>h </h></h>
Informação relativa ao ajudante	2 Dh <h>h </h>
Condição "fora de âmbito" aberta	OUT
Visualização de aviso ou de alerta	
Excesso de condução contínua	1 ⓪ hh <h>h hh<h>h </h></h>
Incidente ou falha	EF
Outras visualizações	
Data UTC	UTC ⓪ dd/mm/aaaa ou UTC ⓪ dd.mm.aaaa
Hora	hh:mm
Tempo de condução contínua e pausas acumuladas do condutor princ	1 ⓪ hh <h>h hh<h>h </h></h>
Tempo de condução contínua e pausas acumuladas do ajudante	2 ⓪ hh <h>h hh<h>h </h></h>
Tempo acumulado de condução contínua do condutor principal nas semanas anterior e em curso	1 ⓪ hh <h>h </h>
Tempo acumulado de condução contínua do ajudante nas semanas anterior e em curso	2 ⓪ hh <h>h </h>

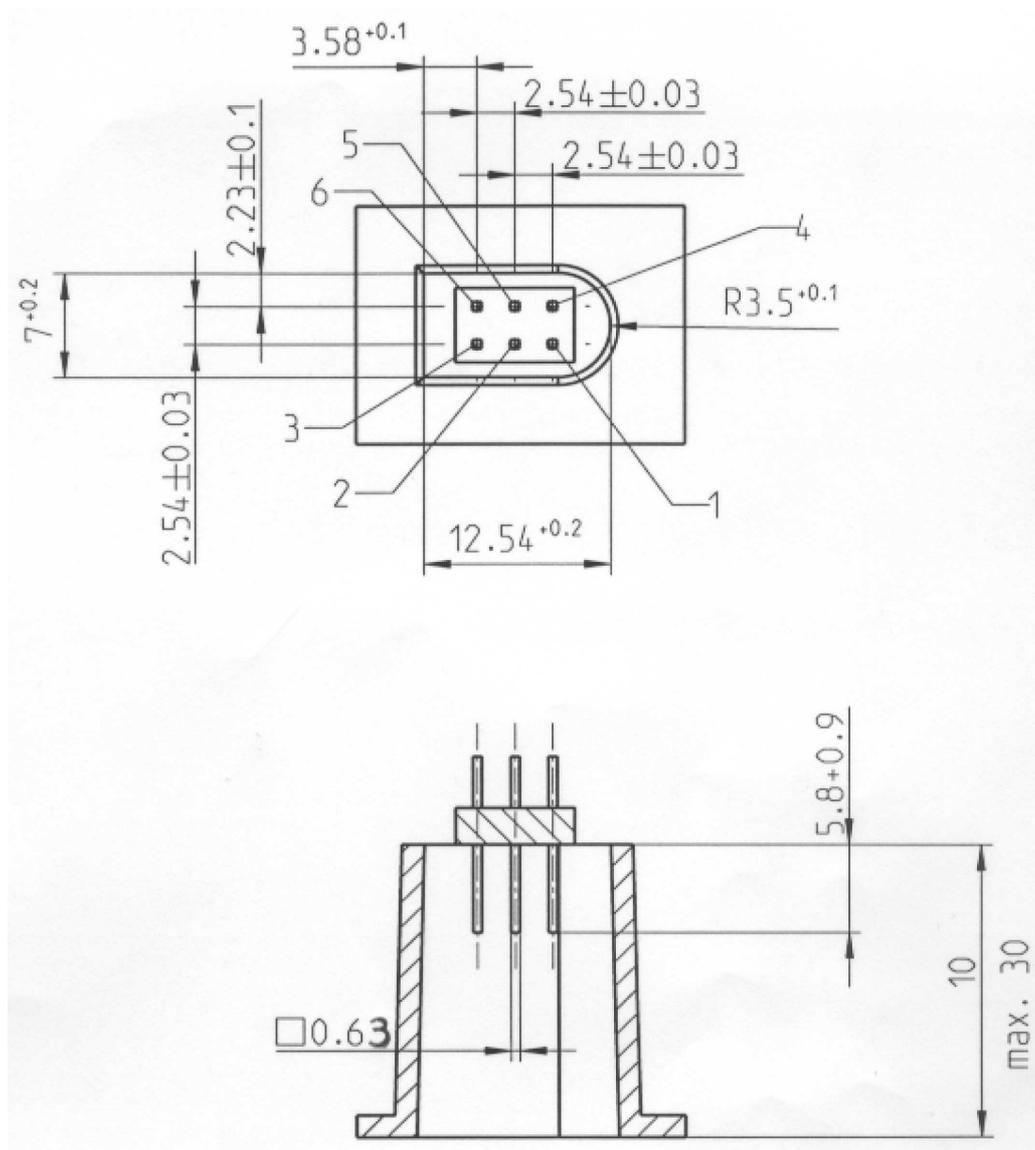
Apêndice 6

INTERFACES EXTERNAS

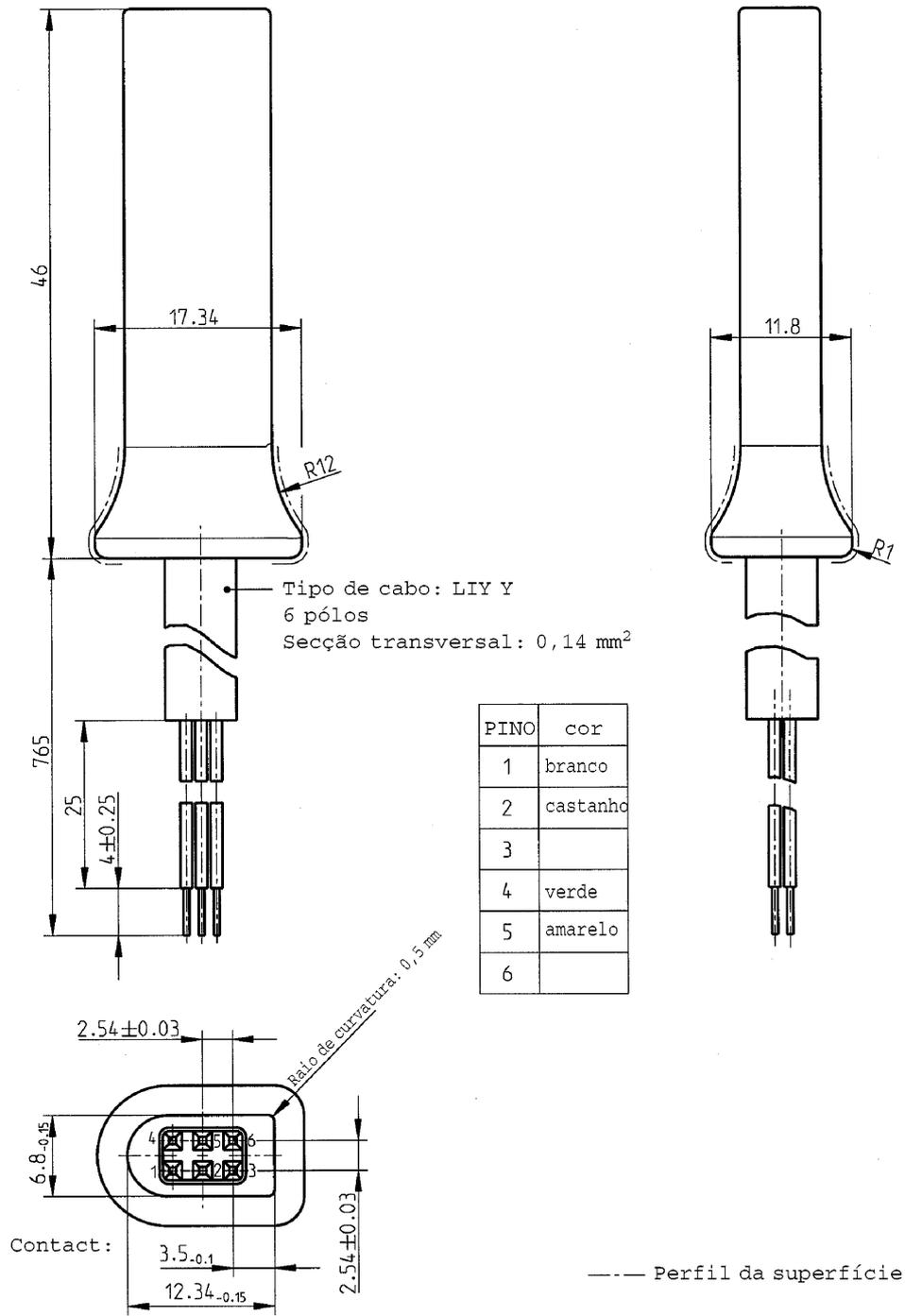
1. EQUIPAMENTO INFORMÁTICO (HARDWARE)

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 aparelho de controlo, e deve corresponder ao seguinte esquema (dimensões em milímetros):



O diagrama seguinte indica uma ficha de ligação (mating plug) típica de 6 pinos:



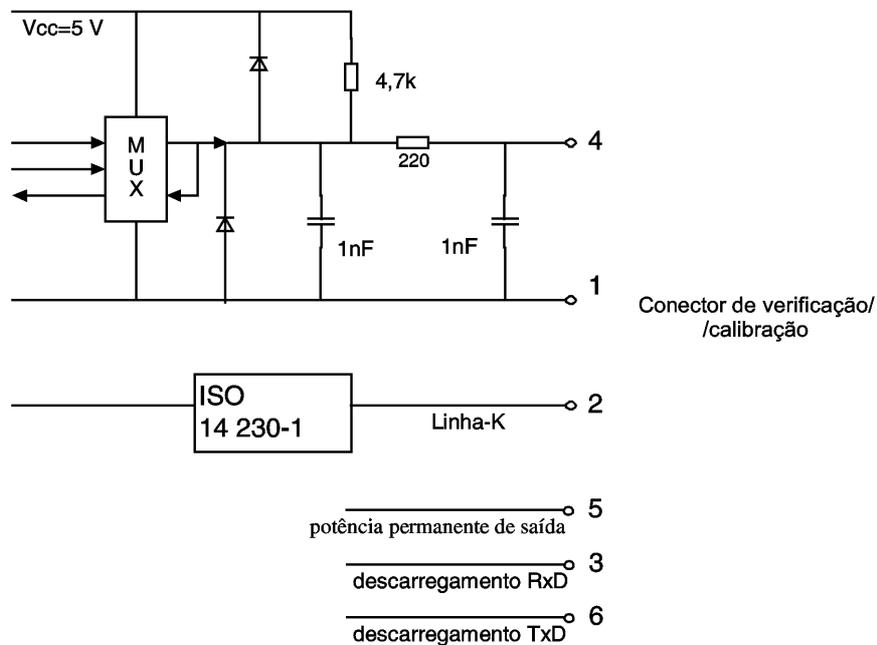
1.2. Distribuição dos contactos

INT_002 Os contactos serão definidos em conformidade com a seguinte tabela:

Pino	Descrição	Nota
1	Pólo negativo da bateria	Conectado (ligado) ao pólo negativo da bateria do veículo
2	Comunicação de dados	Linha-K (ISO 14230-1)
3	Descarregamento RxD	Entrada (input) de dados no aparelho de controlo
4	Sinal de input/output	Calibração
5	Valor permanente da 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 protecção Saída (output): 40 mA
6	Descarregamento TxD	Saída (output) de dados do aparelho de controlo

1.3. Diagrama de blocos

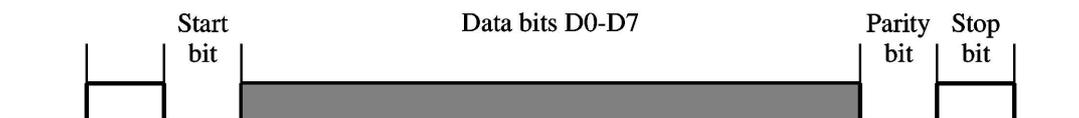
INT_003 O diagrama de blocos deve obedecer ao seguinte esquema:



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 par e 1 bit de paragem.



Organização dos bytes de dados

Start bit (bit de início): um bit com nível lógico 0;

Data bits (bits de dados): transmitidos com LSB first;

Parity bit (bit de paridade): paridade par;

Stop bit (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.

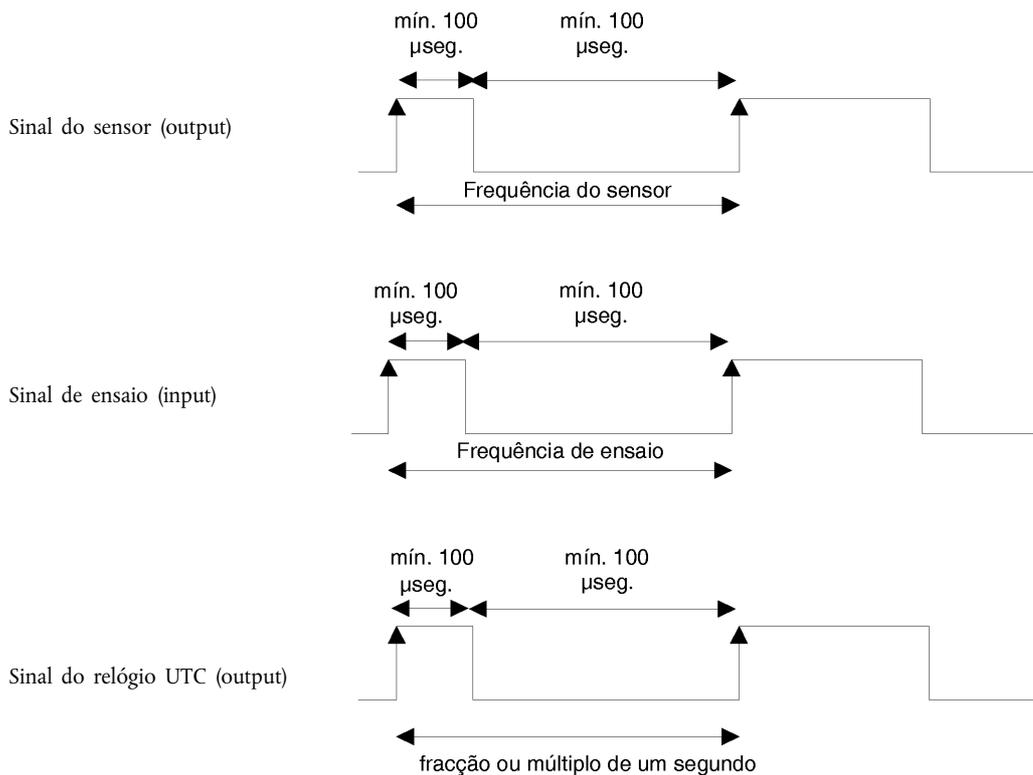
3. INTERFACE DE CALIBRAÇÃO

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 (ISO 14230-1 Veículos Rodoviários — Sistemas de Diagnóstico — Protocolo de Palavras-Chave 2000 — 1.ª parte: Nível Físico, 1.ª edição: 1999).

INT_008 O sinal de input/output (entrada/saída) deve cumprir a seguinte especificação eléctrica:

Parâmetro	Mínimo	Típico	Máximo	Nota
U _{baixo} (input)			1,0 V	I = 750 µA
U _{alto} (input)	4 V			I = 200 µA
Frequência			4 kHz	
U _{baixo} (output)			1,0 V	I = 1 mA
U _{alto} (output)	4 V			I = 1 mA

INT_009 O sinal de input/output (entrada/saída) deve cumprir os seguintes diagramas cronológicos:



Apêndice 7

PROTOCOLOS APLICÁVEIS AO DESCARREGAMENTO DE DADOS**1. INTRODUÇÃO**

O presente apêndice especifica os procedimentos a adoptar na execução dos diversos tipos de descarregamento de dados para meios externos de memorização ou armazenamento (ESM), juntamente com os protocolos que devem ser concretizados para assegurar a transferência correcta dos dados e a compatibilidade total do formato dos dados descarregados, para que um controlador, antes de os analisar, possa inspecioná-los e controlar as suas autenticidade e integridade.

1.1. Âmbito

Pode haver descarregamento de dados para um ESM:

- a partir de uma unidade-veículo, por meio de um equipamento dedicado inteligente (IDE) ligado a essa VU;
- a partir de um cartão tacográfico, por meio de um IDE equipado com um dispositivo de interface para o cartão (IFD);
- a partir de um cartão tacográfico, via uma unidade-veículo, por meio de um IDE ligado a essa VU.

Para tornar possível verificar a autenticidade e a integridade dos dados descarregados memorizados num ESM, os dados são descarregados com uma assinatura apensa em conformidade com o apêndice 11 (Mecanismos comuns de segurança). A identificação do equipamento-fonte (VU ou cartão) e os seus 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.

1.2. Acrónimos e notações

No presente apêndice, utilizam-se os seguintes acrónimos:

AID	Identificador de uma 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 de 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	Seleccção de parâmetro de protocolo
PSO	Perform Security Operation (executar operação de segurança)
SID	SID Identificador de serviço
SRC	Byte-fonte
TGT	Byte-alvo
TLV	Valor do comprimento de um marcador ou etiqueta (tag)
TREP	Parâmetro de resposta de transferência
TRTP	Parâmetro de pedido de transferência
VU	Unidade-veículo

2. DESCARREGAMENTO DE DADOS DE UMA VU

2.1. Procedimento relativo ao descarregamento

Para descarregar dados de uma VU, o utilizador deve executar as seguintes operações:

- inserir o seu cartão tacográfico numa ranhura da VU ⁽¹⁾;
- ligar o IDE ao conector de descarregamento da VU;
- estabelecer a ligação entre o IDE e a VU;
- seleccionar no IDE os dados a descarregar e enviar o pedido à VU;
- fechar (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 Keyword protocol 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 actual projecto da norma ISO 14229-1 (Road vehicles — Diagnostic systems — Part 1: Diagnostic services, version 6 of 22 February 2001).

2.2.1. Estrutura da mensagem

DDP_002 Todas as mensagens intercambiadas entre o IDE e a VU são formatadas com uma estrutura que consiste 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	DATA	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 (número de bits) 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.

⁽¹⁾ O cartão inserido desencadeia os devidos direitos de acesso à função de descarregamento e aos dados.

DDP_003 No caso de os dados a transmitir pela mensagem serem mais longos do que os espaços disponíveis na parte campo de dados, a mensagem é enviada em diversas sub-mensagens, cada uma das quais contém um cabeçalho, os mesmos SID e TREP e um contador de sub-mensagem de 2 bytes indicando o número da sub-mensagem no contexto da mensagem total. Para efeitos de verificar erros e abortar, o IDE acusa cada uma das sub-mensagens. O IDE pode aceitar a sub-mensagem, pedir a sua retransmissão, pedir o recomeço à VU ou abortar a transmissão.

DDP_004 Se a última sub-mensagem contiver exactamente 255 bytes no campo de dados, deve ser apenas uma sub-mensagem final com um campo de dados vazio (exceptuando SID, TREP e o contador dessa sub-mensagem), 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	Sub-mensagem 1	CS
4 bytes	255 bytes					

Cabeçalho	SID	TREP	00	02	Sub-mensagem 2	CS
4 bytes	255 bytes					

...

Cabeçalho	SID	TREP	xx	yy	Sub-mensagem n	CS
4 bytes	Menos de 255 bytes					

ou sob a seguinte forma:

Cabeçalho	SID	TREP	00	01	Sub-mensagem 1	CS
4 bytes	255 bytes					

Cabeçalho	SID	TREP	00	02	Sub-mensagem 2	CS
4 bytes	255 bytes					

...

Cabeçalho	SID	TREP	xx	yy	Sub-mensagem n	CS
4 bytes	255 bytes					

Cabeçalho	SID	TREP	xx	yy+1	CS
4 bytes	4 bytes				

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:

IDE ->	<- VU	Máx 4 bytes Cabeçalho				Máx 255 bytes Dados			1 byte Soma de teste
		FMT	TGT	SRC	LEN	SID	DS_ /TRTP	DATA	
Start Communication Request		81	EE	F0		81			E0
Positive Response Start Communication		80	F0	EE	03	C1		8F,EA	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									
Panorâmica		80	EE	F0	02	36	01		97
Actividades		80	EE	F0	06	36	02	Data	CS
Incidentes e falhas		80	EE	F0	02	36	03		99
Velocidade detalhada		80	EE	F0	02	36	04		9A
Dados técnicos		80	EE	F0	02	36	05		9B
Descarregamento do cartão		80	EE	F0	02	36	06		9C
Positive Response Transfer Data		80	F0	EE	Len	76	TREP	Dados	CS
Request Transfer Exit		80	EE	F0	01	37			96
Positive Response Request Transfer Exit		80	F0	EE	01	77			D6
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		Dados	CS
Negative Responses									
Rejeição geral		80	F0	EE	03	7F	Sid Req	10	CS
Serviço não suportado		80	F0	EE	03	7F	Sid Req	11	CS
Sub-função não suportada		80	F0	EE	03	7F	Sid Req	12	CS
Comprimento de mensagem incorrecto		80	F0	EE	03	7F	Sid Req	13	CS
Condições incorrectas ou erro de sequência do pedido		80	F0	EE	03	7F	Sid Req	22	CS
Pedido fora do alcance		80	F0	EE	03	7F	Sid Req	31	CS
Carregamento não aceite		80	F0	EE	03	7F	Sid Req	50	CS
Resposta pendente		80	F0	EE	03	7F	Sid Req	78	CS
Dados não disponíveis		80	F0	EE	03	7F	Sid Req	FA	CS

Notas:

- Sid Req = o SID do correspondente pedido; Lid Req = o LID do correspondente pedido.
- 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 sub-mensagens potenciais de 2 bytes não figuram neste quadro.

2.2.2.1. *Start Communication Request (SID 81)*

DDP_005 Esta mensagem (pedido de começo da comunicação) é emitida pelo IDE para estabelecer o elo de comunicação com a VU. As comunicações iniciais são sempre executadas a 9 600 báudios (até o ritmo dos báudios ser alterado por meio dos serviços competentes de controlo de elo).

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 '8F' e 'EA', o que indica que a unidade suporta 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 Esta mensagem é emitida pelo IDE para pedir uma nova sessão de diagnóstico com a VU. A sub-função "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 Esta mensagem é enviada pela VU em resposta positiva ao pedido de sessão de diagnóstico (Diagnostic Session Request).

2.2.2.5. *Link Control Service (SID 87)*

DDP_052 Este serviço de controlo de elo é utilizado pelo IDE para iniciar uma modificação no ritmo dos báudios, o que ocorre em duas fases. Na primeira fase, o IDE propõe a modificação do ritmo dos báudios, indicando o novo ritmo. Ao receber uma mensagem positiva da VU, o IDE envia-lhe a confirmação da modificação no ritmo dos báudios (segunda fase) e adopta o novo ritmo. Depois de receber a confirmação, a VU passa, por sua vez, para o novo ritmo dos báudios.

2.2.2.6. *Link Control Positive Response (SID C7)*

DDP_053 Esta mensagem é emitida pela VU em resposta positiva ao pedido de serviço de controlo de elo (Link Control Service), o qual tinha constituído a primeira fase. Note-se que não é dada resposta ao pedido de confirmação, que constituiu a segunda fase.

2.2.2.7. *Request Upload (SID 35)*

DDP_009 O IDE emite esta mensagem 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 em 0, o formato é descriptado 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.

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),
- Actividades de uma 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 pode ser verificada a assinatura digital).

No segundo caso (TRTP 02), a mensagem Transfer Data Request inclui a indicação do dia de calendário 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 ao pedido de transferência de dados (Transfer Data Request). Contém os dados pedidos, com um TREP (Transfer Response Parameter ou parâmetro de resposta de transferência) correspondente ao TRTP do pedido.

DDP_055 No primeiro caso (TRTP 01), a VU envia dados para ajudar o operador do IDE a escolher os que pretende descarregar mais tarde. É a seguinte a informação contida nesta mensagem:

- certificados de segurança,
- identificação do veículo,
- data e hora actuais 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.

2.2.2.11. Request Transfer Exit (SID 37)

DDP_013 Esta mensagem (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 recepção de cada parte de uma mensagem que seja transmitida sob a forma de diversas sub-mensagens. O campo de dados contém o SID recebido da VU e um código de 2 bytes, a saber:

- MsgC + 1 acusa a recepção correcta da sub-mensagem n.º MsgC.
Pedido do IDE à VU para que envie a sub-mensagem seguinte.
- MsgC indica um problema na recepção da sub-mensagem n.º MsgC.
Pedido do IDE à VU para que envie novamente a sub-mensagem.
- 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 sub-mensagem de uma mensagem (byte LEN < 255) pode ser acusada por intermédio de qualquer um destes códigos, ou não ser acusada.

É a seguinte a resposta da VU que consiste em diversas sub-mensagens:

- Positive Response Transfer Data (SID 76).

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 acção não pode ser executada por uma razão não contemplada adiante.
- 11 serviço não suportado
O SID do pedido não é entendido.
- 12 sub-função não suportada
O DS_ ou o TRTP do pedido não são entendidos ou não há mais sub-mensagens a transmitir.
- 13 comprimento de mensagem incorrecto
O comprimento da mensagem recebida está errado.
- 22 condições incorrectas ou erro de sequência do pedido
O serviço requerido não está activo ou a sequência das mensagens de pedido não está correcta.
- 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 acção pedida não pode ser completada a tempo e a VU não está preparada para aceitar outro pedido.
- FA dados não disponíveis
O objecto 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

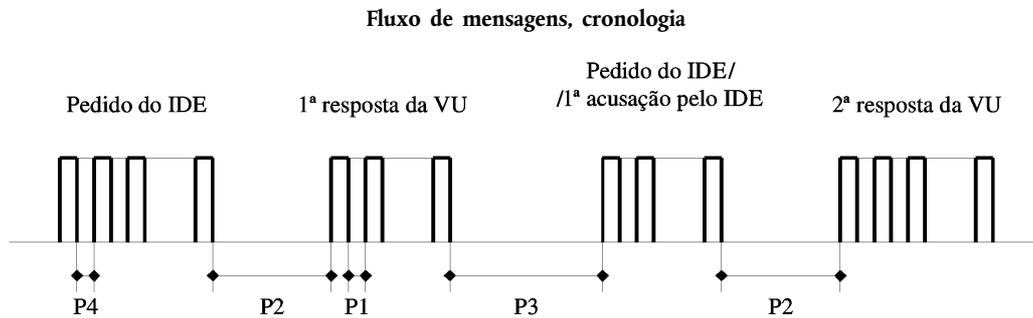
É o seguinte o fluxo típico de mensagens durante um procedimento normal de descarregamento de dados:

IDE		VU
Start Communication Request	⇨ ⇩	Positive Response
Start Diagnostic Service Request	⇨ ⇩	Positive Response
Request Upload	⇨ ⇩	Positive Response
Transfer Data Request Overview	⇨ ⇩	Positive Response
Transfer Data Request #2	⇨	Positive Response #1 Positive Response #2 Positive Response #m Positive Response (Data Field < 255 Bytes)
Acknowledge Sub Message #1	⇩	
Acknowledge Sub Message #2	⇨	
Acknowledge Sub Message #m	⇩	
Acknowledge Sub Message (optional)	⇨	
	⇩	
...		
Transfer Data Request #n	⇨ ⇩	Positive Response
Request Transfer Exit	⇨ ⇩	Positive Response
Stop Communication Request	⇨ ⇩	Positive Response

2.2.4. Sucessão cronológica

DDP_019 Durante o funcionamento normal, destacam-se os parâmetros de tempo indicados no esquema seguinte:

Figura 1



Sendo:

P1 = intervalo inter-bytes 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 inter-bytes para o pedido do IDE.

P5 = valor alargado de P3 para descarregamento de cartões.

Os valores autorizados para os parâmetros de tempo são indicados na tabela seguinte (conjunto de parâmetros de tempo alargado do KWP, utilizado em caso de endereçamento físico para maior rapidez de comunicação):

Parâmetro de tempo	Limite inferior (ms)	Limite superior (ms)
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 correctamente 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 detectado o erro e a mensagem que lhe tiver dado origem.

Nas figuras 2 e 3 são indicados os procedimentos de tratamento de erros, respectivamente para a VU e para o IDE.

2.2.5.1. Fase de Start Communication

DDP_020 Se o IDE detectar um erro durante a fase Start Communication ("iniciar comunicação"), quer pela cronologia quer pela sucessão de bits, aguarda durante um período P3mín antes de emitir novamente o pedido.

DDP_021 Se a VU detectar 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 Communication

Podem ser definidas duas áreas distintas de tratamento de erros:

1. A VU detecta um erro de transmissão do IDE

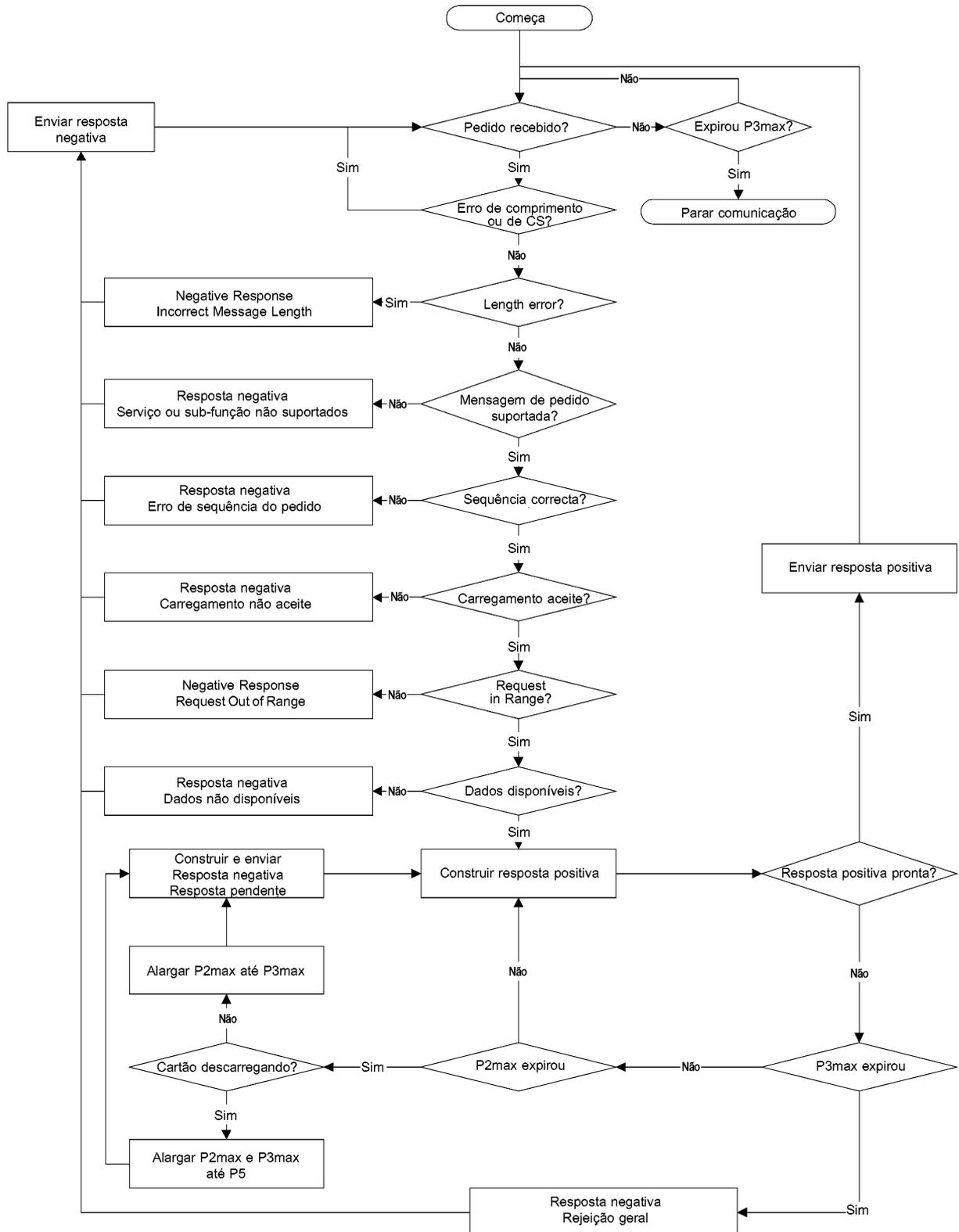
DDP_022 Por cada mensagem recebida, a VU detecta erros de cronologia, erros de formato dos bytes (por exemplo, violações nos bits de início e de fim) e erros de enquadramento (frame errors, como um número errado de bytes recebidos, um byte errado de soma de teste).

DDP_023 Se a VU detectar um dos erros *supra*, não envia qualquer resposta e ignora a mensagem recebida.

DDP_024 A VU pode detectar outros erros no formato ou no conteúdo da mensagem recebida (por exemplo, mensagem não suportada) 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.

Figura 2

Tratamento de erros por parte da VU

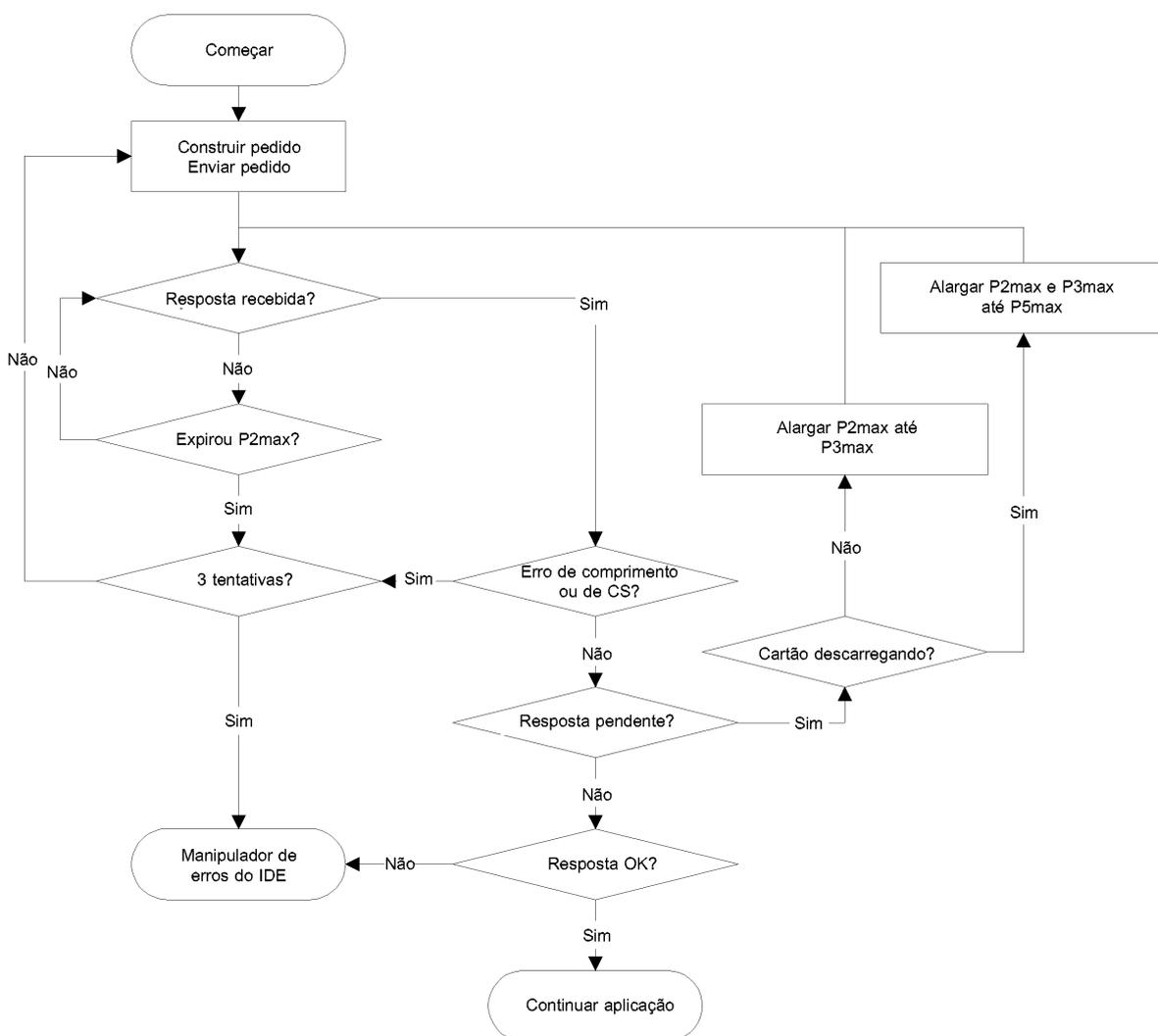


2. O IDE detecta um erro de transmissão da VU

- DDP_025 Por cada mensagem recebida, o IDE detecta erros de cronologia, erros de formato dos bytes (por exemplo, violações nos bits de início e de fim) e erros de enquadramento (frame errors, como um número errado de bytes recebidos, um byte errado de soma de teste).
- DDP_026 O IDE detecta erros de sequência, como, por exemplo, incrementos incorrectos no contador de sub-mensagens, em mensagens recebidas sucessivamente.
- DDP_027 Se o IDE detectar 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 detecção de erro, a acusação de uma sub-mensagem será considerada como um pedido à VU.
- 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 detectado o erro.

Figura 3

Tratamento de erros por parte do IDE



2.2.6. Conteúdo da mensagem de resposta

Esta secção especifica o conteúdo (ou teor) dos campos de dados das várias mensagens de resposta positiva.

Os elementos de dado são definidos no apêndice 1 (DICIONÁRIO DE DADOS).

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 sub-mensagens:

Elemento de dado	Comprimento (bytes)	Comentário
MemberStateCertificate VUCertificate	194 194	Certificados de segurança da VU
VehicleIdentificationNumber VehicleRegistrationIdentification vehicleRegistrationNation vehicleRegistrationNumber	17 1 14	Identificação do veículo
CurrentDateTime	4	Data e hora actuais da VU
VuDownloadablePeriod minDownloadableTime maxDownloadableTime	4 4	Período descarregável
CardSlotsStatus	1	Tipo de cartões inseridos na VU
VuDownloadActivityData downloadingTime fullCardNumber companyOrWorkshopName	4 18 36	Descarregamento prévio da VU
VuCompanyLocksData noOfLocks ... Vu Company Locks Record lockInTime lockOutTime companyName companyAddress companyCardNumber	1 (98) 4 4 36 36 18	Todos os bloqueios de empresa memorizados. Se a secção estiver vazia, só é enviado noOfLocks = 0
VuControlActivityData noOfControls ... Vu Control Activity Record controlType controlTime controlCardNumber downloadPeriodBeginTime downloadPeriodEndTime	1 (31) 1 4 18 4 4	Todos os registos de controlo memorizados na VU. Se a secção estiver vazia, só é enviado noOfControls = 0
Signature	128	Assinatura RSA de todos os dados (excepto certificados), desde VehicleIdentificationNumber até ao último byte do último VuControlActivityRecord

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 sub-mensagens:

Elemento de dado	Comprimento (bytes)	Comentário
TimeReal	4	Dia do descarregamento
OdometerValueMidnight	3	Valor odométrico no final do dia do descarregamento
VuCardIWData		Dados dos ciclos de inserção e retirada de cartões.
NoOfVuCardIWRecords	2	
...	(129)	— Se esta secção não contiver dados disponíveis, só é enviado noOfVuCardIWRecords = 0
VuCardIWRecord		— Quando um registo VuCardIWRecord se coloca em 00:00 (inserção do cartão no dia anterior) ou em 24:00 (retirada do cartão no dia seguinte), aparece por inteiro nos dois dias em causa
cardHolderName	36	
holderSurname	36	
holderFirstNames	36	
fullCardNumber	18	
cardExpiryDate	4	
cardInsertionTime	4	
vehicleOdometerValueAtInsertion	3	
cardSlotNumber	1	
cardWithdrawalTime	4	
vehicleOdometerValueAtWithdrawal	3	
previousVehicleInfo		
vehicleRegistrationIdentification	1	
vehicleRegistrationNation	14	
vehicleRegistrationNumber	14	
cardWithdrawalTime	4	
manualInputFlag	1	
...		
VuActivityDailyData		Situação das ranhuras às 00h00 e mudanças de actividade registadas relativamente ao dia do descarregamento.
noOfActivityChanges	2	
...		
ActivityChangeInfo	2	
...		
VuPlaceDailyWorkPeriodData		Dados relativos à localização registados relativamente ao dia do descarregamento. Se a secção estiver vazia, só é enviado noOfPlaceRecords = 0.
noOfPlaceRecords	1	
...	(28)	
VuPlaceDailyWorkPeriodRecord		
fullCardNumber	18	
placeRecord		
entryTime	4	
entryTypeDailyWorkPeriod	1	
dailyWorkPeriodCountry	1	
dailyWorkPeriodRegion	1	
vehicleOdometerValue	3	
...		
VuSpecificConditionData		Dados relativos às condições especiais registados relativamente ao dia do descarregamento. Se a secção estiver vazia, só é enviado noOfSpecificConditionRecords = 0.
noOfSpecificConditionRecords	2	
...	(5)	
SpecificConditionRecord		
EntryTime	4	
specificConditionType	1	
...		
Signature	128	Assinatura RSA de todos os dados, desde TimeReal até ao último byte do último registo de condição especial.

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 sub-mensagens:

Elemento de dado		Comprimento (bytes)	Comentário
VuFaultData			
NoOfVuFaults		1	Todas as falhas memorizadas ou em curso na VU. Se a secção estiver vazia, só é enviado noOfVuFaults = 0
...		(82)	
VuFaultRecord	FaultType	1	
	FaultRecordPurpose	1	
	FaultBeginTime	4	
	FaultEndTime	4	
	CardNumberDriverSlotBegin	18	
	CardNumberCodriverSlotBegin	18	
VuFaultRecord	CardNumberDriverSlotEnd	18	
	CardNumberCodriverSlotEnd	18	
...			
VuEventData			
NoOfVuEvents		1	Todos os incidentes (excepto excesso de velocidade) memorizados ou em curso na VU. Se a secção estiver vazia, só é enviado noOfVuEvents = 0
...		(83)	
VuEventRecord	EventType	1	
	EventRecordPurpose	1	
	EventBeginTime	4	
	EventEndTime	4	
	CardNumberDriverSlotBegin	18	
	CardNumberCodriverSlotBegin	18	
	CardNumberDriverSlotEnd	18	
	CardNumberCodriverSlotEnd	18	
	SimilarEventsNumber	1	
...			
VuOverSpeedingControlData			
LastOverspeedControlTime		4	Dados relativos ao último controlo de excesso de velocidade (valor por defeito se não houver dados)
FirstOverspeedSince		4	
NumberOfOverspeedSince		1	
VuOverSpeedingEventData			
NoOfVuOverSpeedingEvents		1	Todos os incidentes de excesso de velocidade memorizados na VU. Se a secção estiver vazia, só é enviado noOfVuOverSpeedingEvents = 0.
...		(31)	
VuOverSpeedingEventRecord	EventType	1	
	EventRecordPurpose	1	
	EventBeginTime	4	
	EventEndTime	4	
	MaxSpeedValue	1	
	AverageSpeedValue	1	
	CardNumberDriverSlotBegin	18	
	SimilarEventsNumber	1	
	...		
VuTimeAdjustmentData			
NoOfVuTimeAdjRecords		1	Todos os incidentes de ajustamento do tempo memorizados na VU (fora do âmbito de uma calibração plena). Se a secção estiver vazia, só é enviado noOfVuTimeAdjRecords = 0.
...		(98)	
VuTimeAdjustmentRecord	OldTimeValue	4	
	NewTimeValue	4	
	WorkshopName	36	
	WorkshopAddress	36	
	WorkshopCardNumber	18	
...			
Signature		128	Assinatura RSA de todos os dados, desde noOfVuFaults até ao último byte do último registo de ajustamento do tempo

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 sub-mensagens:

Elemento de dado	Comprimento (bytes)	Comentário
VuDetailedSpeedData		
NoOfSpeedBlocks	2	Todos os dados de velocidade detalhada memorizados na VU (um bloco de velocidade por cada minuto durante o qual o veículo tenha estado em movimento) 60 valores de velocidade por minuto (um por segundo)
...		
VuDetailedSpeedBlock	4	
SpeedBlockBeginDate speedsPerSecond	60	
...		
Signature	128	Assinatura RSA de todos os dados, desde noOfSpeedBlocks até ao último byte do último bloco de velocidade

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 uma divisão e uma contagem adequadas das sub-mensagens:

Elemento de dado	Comprimento (bytes)	Comentário
VuIdentification		
vuManufacturerName	36	Todos os registos de calibração memorizados na VU
vuManufacturerAddress	36	
vuPartNumber	16	
vuSerialNumber	8	
vuSoftwareIdentification		
vuSoftwareVersion	4	
vuSoftInstallationDate	4	
vuManufacturingDate	4	
vuApprovalNumber	8	
SensorPaired		
sensorSerialNumber	8	
sensorApprovalNumber	8	
sensorPairingDateFirst	4	
VuCalibrationData		
noOfVuCalibrationRecords	1	
...	(164)	
VuCalibrationRecord		
calibrationPurpose	1	
workshopName	36	
workshopAddress	36	
workshopCardNumber	18	
workshopCardExpiryDate	4	
vehicleIdentificationNumber	17	
vehicleRegistrationIdentification		
vehicleRegistrationNation	1	
vehicleRegistrationNumber	14	
wVehicleCharacteristicConstant	2	
kConstantOfRecordingEquipment	2	
lTyreCircumference	2	
tyreSize	15	
authorisedSpeed	1	
oldOdometerValue	3	
newOdometerValue	3	
oldTimeValue	4	
newTimeValue	4	
nextCalibrationDate	4	
...		
Signature	128	Assinatura RSA de todos os dados, desde vuManufacturerName até ao último byte do último registo VuCalibrationRecord

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 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 sub-mensagens, sub-mensagens vazias e somas de teste, mas incluem o SID e o TREP (da primeira sub-mensagem apenas, se houver várias sub-mensagens).

3. PROTOCOLO APLICÁVEL AO DESCARREGAMENTO DE DADOS DE CARTÕES TACOGRAFÍCOS

3.1. Âmbito

A presente secção incide no descarregamento directo dos dados de um cartão tacográfico para um IDE. Como este último não faz parte do ambiente securizado, não é efectuada 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 (o restabelecimento) do ICC por um IFD até à desactivação do ICC (retirada do cartão ou reinicialização seguinte).

Ficheiro de dados assinado: Um ficheiro do ICC. O ficheiro é transferido em texto corrido para o IFD. No ICC, é dividido (hashed) 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 etapas:

— Descarregamento da informação comum do cartão para os EF ICC e IC. Esta informação é opcional e não é securizada com uma assinatura digital.

— Descarregamento dos EF Card_Certificate e CA_Certificate. Esta informação não é securizada com uma assinatura digital.

É obrigatório descarregar estes ficheiros por cada sessão de descarregamento.

— Descarregamento dos outros EF de dados de aplicação (dentro do DF Tachograph), com excepção do EF Card_Download. Esta informação é securizada com uma 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,

— Control_Activity_Data,

— Specific_Conditions.

— No descarregamento de um cartão de condutor, actualizar a data de LastCardDownload no EF Card_Download.

— No descarregamento de um cartão de centro de ensaio, reinicializar o contador de calibração no EF Card_Download.

3.3.1. Sequência de inicialização

DDP_036 O IDE inicia a sequência do seguinte modo:

Cartão	Direcção	IDE/IFD	Significado/Observações
	←	Reinicialização do hardware	
ATR	⇒		

É opcional utilizar PPS para passar a um ritmo mais elevado de báudios, desde que o ICC o suporte.

3.3.2. Sequência para ficheiros de dados não assinados

DDP_037 É a seguinte a sequência de descarregamento dos EF ICC, IC, Card_Certificate e CA_Certificate:

Cartão	Direcção	IDE/IFD	Significado/Observações
	←	Select File	Seleção por identificadores de ficheiro
OK	⇒		
	←	Read Binary	Se o ficheiro contiver mais dados do que o tamanho do tampão do leitor ou do cartão, o comando tem de ser repetido até todo o ficheiro ter sido lido.
Dados do ficheiro OK	⇒	Memorizar dados no ESM	Em conformidade com 3.4 (Formato de memorização dos dados).

Nota: Antes de seleccionar o EF Card_Certificate, deve ser seleccionada a aplicação tacográfica (selecção por AID).

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 respectivas 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 seleccionado, 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 suportar, o comando tem de ser repetido até todo o ficheiro ter sido lido.
Dados do ficheiro OK	⇒	Memorizar no ESM dados recebidos	Em conformidade com 3.4 (Formato de memorização dos dados).
	←	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	Em conformidade com 3.4 (Formato de memorização dos dados).

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 centro de ensaio:

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	→		

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 são memorizados transparentes, ou seja, na sua transferência 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.

3.4.2. Formato dos ficheiros

DDP_041 O formato dos ficheiros é uma concatenação de diversos objectos de TLV.

DDP_042 O marcador ou etiqueta (tag) 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, não é memorizado nada que com ele se relacione (marcador ou comprimento zero).

DDP_046 Uma assinatura é memorizada como o objecto TLV imediatamente a seguir ao objecto 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 EF Vehicles_Used
05 05 01	00 80	Assinatura do EF Vehicles_Used

4. DESCARREGAMENTO DE UM CARTÃO TACOGRÁFICO VIA UMA UNIDADE-VEÍCULO

- DDP_047 A VU deve permitir descarregar para um IDE a ela conectado o conteúdo de um cartão de condutor inserido.
- DDP_048 O IDE envia à VU uma mensagem "Transfer Data Request Card Download", para iniciar este modo (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".
- DDP_050 O IDE saca os dados da mensagem "Positive Response Transfer Data" (seleccionando todos os cabeçalhos, SID, TREP, contadores de sub-mensagens e somas de teste) e memoriza-os num ficheiro físico, em conformidade com a secção 2.3.
- DDP_051 Conforme o caso, a VU actualiza então o ficheiro `Control_Activity_Data` ou o ficheiro `Card_Download` do cartão de condutor.
-

Apêndice 8

PROTOCOLO APLICÁVEL À CALIBRAÇÃO

1. INTRODUÇÃO

O presente apêndice incide no modo como os dados são intercambiados entre uma unidade-veículo (VU) e um tester (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 (input/output) 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 selecção da sessão de diagnóstico é referida na secção 5 ("Serviços de gestão").

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 (requisitos 097 e 098), a unidade-veículo deve, ademais, encontrar-se no modo de funcionamento CALIBRATION.

A transferência de dados através da linha-K é referida na secção 6 ("Serviços de transmissão de dados"). Os formatos dos dados transferidos são descritos na secção 8 ("Formatos dos registos de dados").

CPR_002 A "ECUAdjustmentSession" permite seleccionar 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 referido na secção 7 ("Controlo de impulsos de teste — Unidade funcional de controlo de input/output ou 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 correctamente a qualquer endereço. O endereço físico da VU é 0xEE.

2. TERMOS, DEFINIÇÕES E REFERÊNCIAS

Os protocolos, mensagens e códigos de erro baseiam-se principalmente no actual projecto 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, respectivamente, ao dispositivo de teste e à VU.

O termo ECU significa "unidade de controlo electrónico" (Electronic Control Unit) e refere-se à VU (unidade-veículo).

Referências:

ISO 14230-2: Road Vehicles — Diagnostic Systems — Keyword Protocol 2000 — Part 2: Data Link Layer. First edition: 1999. Vehicles — Diagnostic Systems.

3. PANORÂMICA DOS SERVIÇOS

3.1. **Serviços disponíveis**

A tabela que se segue fornece uma panorâmica dos serviços disponíveis no aparelho de controlo e que são definidos no presente documento.

CPR_004 A tabela indica os serviços disponíveis numa sessão de diagnóstico activada (enabled).

— 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.

Quadro 1

Tabela de síntese de valores dos identificadores de serviços

Nome do serviço de diagnóstico	Secção n.º	Sid Valor de pedido	Sessões de diagnóstico		
			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 (application layer). Os serviços disponíveis são discriminados na seguinte tabela:

Quadro 2

Serviços de comunicação

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

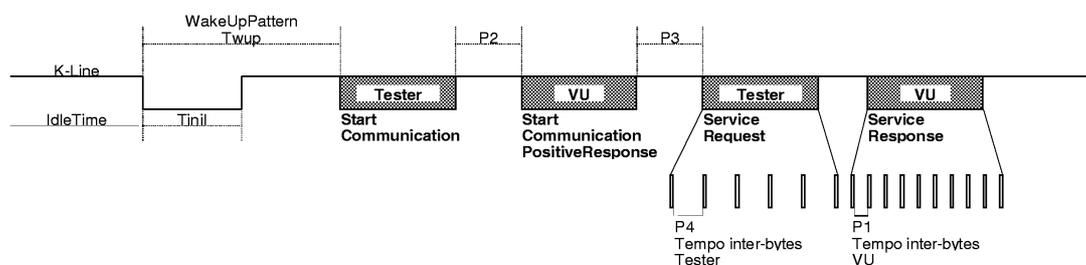
CPR_005 O serviço StartCommunication é utilizado para desencadear uma comunicação. Para a execução de qualquer serviço, a comunicação tem de ser iniciada e os seus parâmetros têm de ser adequados ao modo pretendido.

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.

CPR_007 A VU executa então as acções necessárias para desencadear o elo de comunicação e envia uma primitiva de resposta StartCommunication com os parâmetros Positive Response (resposta positiva) seleccionados.

- CPR_008 Se uma VU que tiver já 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 é reinicializada.
- 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 inicialização da VU para serviços é efectuada mediante um método de “inicialização rápida”:
- Há um tempo morto (*bus-idle time*) antes de qualquer actividade.
 - O dispositivo de teste envia então um modelo (*pattern*) de inicialização.
 - Toda a informação necessária ao estabelecimento da comunicação está contida na resposta da VU.
- CPR_012 Após a conclusão da inicialização:
- Os parâmetros de comunicação são todos 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, desactivada (*disabled*).
- CPR_014 O ritmo dos dados na linha-K será de 10 400 báudios.
- CPR_016 A inicialização rápida é despoletada com o dispositivo de teste (*tester*) a transmitir um “modelo de despertar” (*Wake up pattern* ou Wup) sobre a linha-K. O modelo começa a seguir ao tempo morto (*idle time*) na linha-K (*K-line*), 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.



- CPR_017 Os valores cronológicos para a inicialização rápida e comunicações em geral são indicados na tabela seguinte. Há diferentes possibilidades para o tempo morto (*idle time*):
- Primeira transmissão a seguir a *power on* (comutação), Tidle = 300 ms.
 - Após a conclusão de um serviço StopCommunication, Tidle = P3 min.
 - Depois de parar a comunicação no momento-limite P3 max, Tidle = 0.

Quadro 3

Valores cronológicos na inicialização rápida

Parâmetro	Valor mín	Valor máx
Tinil	25 ± 1 ms	24 ms
Twup	50 ± 1 ms	49 ms

Quadro 4

Valores cronológicos de comunicação

Parâmetro cronológico	Descrição do parâmetro	Limite inferior (ms)	
		mín.	máx.
P1	Tempo inter-bytes 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 inter-bytes para pedido do dispositivo de teste	5	20

CPR_018 O formato da mensagem de inicialização rápida é indicado na tabela seguinte:

Quadro 5

Mensagem de pedido de início de comunicação (StartCommunication Request)

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
#4	StartCommunication Request Service Id	81	SCR
#5	Soma de teste	00-FF	CS

Quadro 6

Mensagem de resposta positiva ao pedido de início de comunicação (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 de início de comunicação (StartCommunication Request). Se não houver mensagem de resposta positiva a transmitir, a VU não é inicializada, mantém-se no seu funcionamento normal e nada é transmitido.

4.2. Serviço StopCommunication**4.2.1. Descrição de mensagens**

O propósito deste serviço de camada (ou 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 acções 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 (resposta positiva) seleccionados, 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) seleccionados.

CPR_023 Se a VU detectar o tempo-limite P3 max, é posto termo à comunicação, sem emissão de qualquer primitiva de resposta.

4.2.2. Formato de mensagens

CPR_024 Os formatos das mensagens para as primitivas StopCommunication figuram nas tabelas seguintes:

Quadro 7

Mensagem de pedido de fim de comunicação (StopCommunication 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	01	LEN
#5	StopCommunication Request Service Id	82	SPR
#6	Soma de teste	00-FF	CS

Quadro 8

Mensagem de resposta positiva ao pedido de fim de comunicação (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 de resposta negativa ao pedido de fim de comunicação (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
#5	negative Response Service Id	7F	NR
#6	StopCommunication Request Service Identification	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 de mensagens

O serviço TesterPresent é utilizado pelo *tester* (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 activa a sessão de diagnóstico/comunicação recolocando no seu estado de defeito o cronómetro (*timer*) P3 cada vez que é recebido um pedido relativo ao serviço.

4.3.2. Formato de mensagens

CPR_079 Os formatos das mensagens para as primitivas TesterPresent figuram nas tabelas seguintes:

Quadro 10

Mensagem de pedido de presença do dispositivo de teste (TesterPresent 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	02	LEN
#5	TesterPresent Request Service Id	3E	TP
#6	Sub-função = responseRequired = [yes no]	01 02	RESPREQ_Y RESPREQ_NO
#7	Soma de teste	00-FF	CS

CPR_080 Se o parâmetro responseRequired tomar o valor “no”, não é enviada qualquer resposta pelo servidor; se o parâmetro responseRequired tomar o valor “yes”, o servidor responde com a seguinte mensagem de resposta positiva:

Quadro 11

Mensagem de resposta positiva ao pedido de presença do tester (TesterPresent Request)

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 suportar os seguintes códigos de resposta negativa:

Quadro 12

Mensagem de resposta negativa ao pedido de presença do tester ou dispositivo de teste

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	TesterPresent Request Service Identification	3E	TP
#7	responseCode = [SubFunctionNotSupported-InvalidFormat incorrectMessageLength]	12	RC_SFNS_IF
		13	RC_IML
#8	Soma de teste	00-FF	CS

5. SERVIÇOS DE GESTÃO

Os serviços disponíveis figuram na seguinte tabela:

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 de mensagens

CPR_025 O serviço StartDiagnosticSession é utilizado para activar diversas sessões de diagnóstico no servidor. Uma sessão de diagnóstico activa um conjunto específico de serviços, em conformidade com o quadro 17. Uma sessão pode activar 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 exactamente uma sessão de diagnóstico activa na VU.
- Uma vez ligada, a VU iniciará sempre a sessão de diagnóstico por defeito (StandardDiagnosticSession). Se não for iniciada outra sessão de diagnóstico, a StandardDiagnosticSession prosseguirá enquanto a VU estiver ligada.
- Se uma sessão de diagnóstico em curso tiver sido pedida pelo tester ou 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 a StartDiagnosticSession antes de a nova sessão ser activada nela. Se não puder iniciar a nova sessão de diagnóstico pedida, a VU enviará uma resposta negativa a StartDiagnosticSession e a sessão em curso prosseguirá.

CPR_026 Uma sessão de diagnóstico só é iniciada se tiver sido estabelecida comunicação entre o cliente e a VU.

CPR_027 Os parâmetros cronológicos definidos no quadro 4 devem ficar activos 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 activa.

5.1.2. **Formato de mensagens**

CPR_028 Os formatos das mensagens para as primitivas StartDiagnosticSession figuram nas tabelas seguintes:

Quadro 14

Mensagem de pedido de início de sessão de diagnóstico (StartDiagnosticSession 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	02	LEN
#5	StartDiagnosticSession Request Service Id	10	STDS
#6	diagnosticSession = [um valor do quadro 17]	xx	DS_ . .
#7	Soma de teste	00-FF	CS

Quadro 15

Mensagem de resposta positiva ao pedido de início de sessão de diagnóstico (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 byte 6 quadro 14]	xx	DS_ . .
#7	Soma de teste	00-FF	CS

Quadro 16

Mensagem de resposta negativa ao pedido de início de sessão de diagnóstico (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
#4	Byte adicional de comprimento	03	LEN
#5	Negative Response Service Id	7F	NR
#6	StartDiagnosticSession Request Service Id	10	STDS
#7	ResponseCode = [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 n.º 6 da mensagem de pedido não é suportado (não consta do quadro 17)

^(b) Erro no comprimento da mensagem

^(c) Não cumpridos os critérios no pedido de início de sessão de diagnóstico (StartDiagnosticSession)

5.1.3. Definição de parâmetros

CPR_029 O parâmetro diagnosticSession (DS_) é utilizado pelo serviço StartDiagnosticSession para seleccionar o comportamento específico do(s) servidor(es). No presente documento são especificadas as seguintes sessões de diagnóstico:

Quadro 17

Definição de valores de sessão de diagnóstico (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 activa uma vez concluída com êxito a inicialização entre o cliente (dispositivo de teste) e o servidor (VU). Pode ser sobreposta (overwritten) por outras sessões de diagnóstico especificadas nesta secção.	SD
85	ECUProgrammingSession Esta sessão de diagnóstico possibilita todos os serviços especificados no quadro 1, coluna 6, "ECUPS". Estes serviços suportam a programação da memória de um servidor (VU). Esta sessão de diagnóstico pode ser sobreposta (overwritten) por outras sessões de diagnóstico especificadas nesta secção.	ECUPS
87	ECUAdjustmentSession Esta sessão de diagnóstico possibilita todos os serviços especificados no quadro 1, coluna 5, "ECUAS". Estes serviços suportam o controlo do input/output de um servidor (VU). Esta sessão de diagnóstico pode ser sobreposta (overwritten) por outras sessões de diagnóstico especificadas nesta secção.	ECUAS

5.2. Serviço SecurityAccess

Não é possível escrever dados de calibração nem aceder à linha de *input/output* de calibração se a VU não estiver em modo CALIBRATION. Além da inserção de um cartão válido de centro de ensaio na VU, é necessário introduzir o PIN devido na VU, para ser garantido o acesso ao modo CALIBRATION.

O serviço SecurityAccess fornece um meio para introduzir o PIN e indicar ao dispositivo de teste se a VU está ou não em modo CALIBRATION.

São aceitáveis métodos alternativos para introduzir o PIN.

5.2.1. Descrição de mensagens

O serviço SecurityAccess ("acesso à segurança") 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 CALIBRATION, 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 centro de ensaio, 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 centro de ensaio inserido não é válido, quer porque não foi inserido nenhum cartão de centro de ensaio, 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 conditions-NotCorrectOrRequestSequenceError.
- 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 efectue o processo de autenticação do cartão, a VU utiliza o código de resposta negativa requestCorrectlyReceived-ResponsePending para ampliar o tempo destinado à resposta (o qual, em todo o caso, não excederá 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 CALIBRATION.

CPR_039 Nos casos que se seguem, a VU responde a este pedido por uma Negative Response, com os seguintes códigos de resposta:

- subFunctionNotSupported: formato não válido para o parâmetro da sub-função (accessType)
- conditionsNotCorrectOrRequestSequenceError: VU não pronta 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 correcto mas falhou autenticação mútua com o cartão de centro de ensaio

5.2.2. Formato de mensagens — SecurityAccess — requestSeed

CPR_040 Os formatos das mensagens para as primitivas "requestSeed" do SecurityAccess figuram nas tabelas seguintes:

Quadro 18

Mensagem de pedido de acesso à segurança (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	SecurityAccess Request Service Id	27	SA
#6	accessType — requestSeed	7D	AT_RSD
#7	Soma de teste	00-FF	CS

Quadro 19

Mensagem de resposta positiva ao pedido de acesso à segurança (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 High	00-FF	SEEDH
#8	Seed Low	00-FF	SEEDL
#9	Soma de teste	00-FF	CS

Quadro 20

Mensagem de resposta negativa ao pedido de acesso à segurança (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	SecurityAccess Request Service Id	27	SA
#7	responseCode = [conditionsNotCorrectOrRequestSequenceError incorrectMessageLength]	22 13	RC_CNC RC_IML
#8	Soma de teste	00-FF	CS

5.2.3. Formato de mensagens — SecurityAccess — sendKey

CPR_041 Os formatos das mensagens para as primitivas “sendKey” do SecurityAccess figuram nas tabelas seguintes:

Quadro 21

Mensagem de pedido de acesso à segurança (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	SecurityAccess Request Service Id	27	SA
#6	accessType — sendKey	7E	AT_SK
de #7 a #m+6	Chave #1 (alta) ... 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 de resposta positiva ao pedido de acesso à segurança (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

Quadro 23

Mensagem de resposta negativa ao pedido de acesso à segurança (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	SecurityAccess Request Service Id	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 na seguinte tabela:

Quadro 24

Serviços de transmissão de dados

Nome do serviço	Descrição
ReadDataByIdentifier	O cliente pede a transmissão do valor actual de um registo com acesso por recordDataIdentifier (identificador de dados de registo)
WriteDataByIdentifier	O cliente pede para escrever um registo com acesso por recordDataIdentifier

6.1. Serviço ReadDataByIdentifier**6.1.1. Descrição de mensagens**

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. É da responsabilidade do fabricante da VU as condições do servidor serem cumpridas aquando da execução deste serviço.

6.1.2. Formato de mensagens

CPR_051 Os formatos das mensagens para as primitivas ReadDataByIdentifier figuram nas tabelas seguintes:

Quadro 25

Mensagem de pedido de leitura de dados por identificador (ReadDataByIdentifier 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	03	LEN
#5	ReadDataByIdentifier Request Service Id	22	RDBI
#6 e #7	recordDataIdentifier = [um valor do quadro 28]	xxxx	RDI_ . .
#8	Soma de teste	00-FF	CS

Quadro 26

Mensagem de resposta positiva ao pedido de leitura de dados por identificador (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 a #7	recordDataIdentifier = [mesmo valor que bytes 6 e 7 do quadro 25]	xxxx	RDI_...
de #8 a #m+7	dataRecord[] = [data#1 : data#m]	xx : xx	DREC_DATA1 : DREC_DATAm
#m+8	Soma de teste	00-FF	CS

Quadro 27

Mensagem de resposta negativa ao pedido de leitura de dados por identificador (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	readDataByIdentifier Request Service Id	22	RDBI
#7	ResponseCode = [requestOutOfRange incorrectMessageLength conditionsNotCorrect]	31 13 22	RC_ROOR RC_IML 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 dado) especifica o elemento do apêndice 1 no qual se baseia o recordDataIdentifier (é por vezes necessária transcodificação).
- A 3.ª coluna (Descrição) especifica o nome do recordDataIdentifier.
- A 4.ª coluna (Mnemónica) especifica a mnemónica deste recordDataIdentifier.

Quadro 28

Valores de definição do “recordDataIdentifier” (identificador de dados de registo)

Hex	Elemento de dado	Nome do recordDataIdentifier (v. 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 a 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 (registos de dados) 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 de mensagens

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 aquando da execução deste serviço. Para actualizar os parâmetros constantes do quadro 28, a VU deve estar em modo CALIBRATION.

6.2.2. Formato de mensagens

CPR_057 Os formatos das mensagens para as primitivas WriteDataByIdentifier figuram nas tabelas seguintes:

Quadro 29

Mensagem de pedido de escrita de dados por identificador (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	03	LEN
#5	WriteDataByIdentifier Request Service Id	2E	WDBI
#6 e #7	recordDataIdentifier = [um valor do quadro 28]	xxxx	RDI_...
de #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 de resposta positiva ao pedido de escrita de dados por identificador (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 e #7	recordDataIdentifier = [mesmo valor que bytes 6 e 7 quadro 29]	xxxx	RDI_...
#m+8	Soma de teste	00-FF	CS

Quadro 31

Mensagem de resposta negativa ao pedido de escrita de dados por identificador (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	WriteDataByIdentifier Request Service Id	2E	WBDI
#7	ResponseCode = [requestOutOfRange incorrectMessageLength conditionsNotCorrect]	31 13 22	RC_ROOR RC_IML 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 INPUT/OUTPUT

Os serviços disponíveis figuram na seguinte tabela:

Quadro 32

Unidade funcional de controlo de entrada/saída (input/output)

Nome do serviço	Descrição
InputOutputControlByIdentifier	O cliente pede o controlo de um input/output específico do servidor

7.1. Serviço InputOutputControlByIdentifier**7.1.1. Descrição de mensagens**

Através do conector frontal, existe uma ligação que permite controlar ou acompanhar os impulsos de teste por meio de um dispositivo de teste adequado.

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 seleccionar a função de entrada (*input*) ou de saída (*output*) pretendida para a linha. Estados que a linha pode apresentar:

- desactivada
- 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
- 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.

CPR_059 Para configurar o estado da linha, a unidade-veículo deve ter dado entrada a uma sessão de ajustamento e estar em modo CALIBRATION. Saindo da sessão de ajustamento ou do modo CALIBRATION, a VU deve assegurar que a linha de sinal I/O regressa ao estado *disabled* (desactivada, o estado 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 *input*, então a linha de sinal I/O deve ser apontada para *output* ou recolocada em estado *disabled*.

CPR_061 É a seguinte a sequência:

- estabelecer comunicações pelo serviço StartCommunication
- introduzir uma sessão de ajustamento pelo serviço StartDiagnosticSession e ficar em modo de funcionamento CALIBRATION (a ordem destas duas operações é arbitrária)
- mudar o estado da saída pelo serviço InputOutputControlByIdentifier.

7.1.2. Formato de mensagens

CPR_062 Os formatos das mensagens para as primitivas InputOutputControlByIdentifier figuram nas tabelas seguintes:

Quadro 33

Mensagem de pedido de controlo de entrada e saída por identificador (InputOutputControlByIdentifier 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	xx	LEN
#5	InputOutputControlByIdentifier Request Sid	30	IOCBI
#6 e #7	InputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 ou #8 e #9	ControlOptionRecord = [inputOutputControlParameter — um valor do quadro 36 controlState — um valor do quadro 37 (ver nota <i>infra</i>)	xx	CO_... IOCP_... 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 de resposta positiva ao pedido de controlo de entrada e saída por identificador (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	04	LEN
#5	inputOutputControlByIdentifier Positive Response SId	6F	IOCBIPR
#6 e #7	inputOutputIdentifier = [CalibrationInputOutput]	F960	IOI_CIO
#8 ou #8 e #9	controlStatusRecord = [inputOutputControlParameter (mesmo valor que byte 8 quadro 33) controlState (mesmo valor que byte 9 quadro 33) (se for caso)]	xx xx	CSR_ IOCP_... CS_...
#9 ou #10	Soma de teste	00-FF	CS

Quadro 35

Mensagem de resposta negativa ao pedido de controlo de entrada e saída por identificador (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 conditionsNotCorrect requestOutOfRange deviceControlLimitsExceeded]	13 22 31 7A	RC_IML RC_CNC RC_ROOR RC_DCLE
#8	Soma de teste	00-FF	CS

7.1.3. Definição de parâmetros

CPR_064 O parâmetro InputOutputControlParameter (IOCP_) é definido na tabela seguinte:

Quadro 36

Definição de valores do inputOutputControlParameter (parâmetro de controlo de entrada/saída)

Hex	Descrição	Mnemónica
00	ReturnControlToECU Este valor indica ao servidor (VU) que o dispositivo de teste (<i>tester</i>) 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 de defeito a linha de calibração de sinal I/O	RTD
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 na tabela seguinte, está presente somente quando o inputOutputControlParameter (parâmetro de controlo de entrada/saída) é colocado em ShortTermAdjustment (ajustamento de curta duração):

Quadro 37

Definição de valores de controlState (controlo do estado)

Modo	Valor hex	Descrição
Desactivação	00	Linha I/O desactivada (estado por defeito)
Activação	01	Activar a linha I/O como speedSignalInput
Activação	02	Activar a linha I/O como realTimeSpeedSignalOutputSensor
Activação	03	Activar a linha I/O como RTCOutput

8. FORMATOS DOS REGISTOS DE DADOS

A presente secção incide sobre:

- 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 correspondentes serviços, descritos na secção 6.

CPR_067 Todos os parâmetros identificados devem ser suportados 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 actual 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 aparelho de controlo.

CPR_071 Os valores da gama "not available" (indisponível) servem para a unidade-veículo transmitir uma mensagem contendo um parâmetro não disponível ou não suportado 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 receptor.

CPR_072 Se a falha de um componente impedir a transmissão de dados válidos relativos a um parâmetro, deve ser utilizado 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 deve utilizar-se 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 byte (valor hex)	ASCII
Sinal válido	de 00 a FA	de 0000 a FAFF	de 00000000 a FFFFFFFF	de 1 a 254
Indicador específico do parâmetro	FB	de FB00 a FBFF	de FB000000 a FBFFFFFF	nenhum
Gama reservada para futuros bits de indicador	de FC a FD	de FC00 a FDFF	de FC000000 a FDFFFFFF	nenhum
Indicador de erro	FE	de FE00 a FEFF	de FE000000 a FEFFFFFF	0
Indisponível ou não pedido	FF	de FF00 a FFFF	de FF000000 a FFFFFFFF	FF

CPR_073 No caso dos parâmetros codificados em ASCII, o carácter "*" é reservado como delimitador.

8.2. Formatos dos dataRecords

Os quadros que se seguem (39 a 42) referem 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 (bytes)	Resolução	Gama de funcionamento
TimeDate	8	V. quadro 40	
HighResolutionTotalVehicleDistance	4	ganho 5 m/bit, deslocamento 0 m	0 a + 21 055 406 km
Kfactor	2	ganho 0,001 imp./m/bit, deslocamento 0	0 a 64,255 imp./m
LfactorTyreCircumference	2	ganho 0,125 10 ⁻³ m/bit, deslocamento 0	0 a 8 031 m
WvehicleCharacteristicFactor	2	ganho 0,001 imp./m/bit, deslocamento 0	0 a 64,255 imp./m
TyreSize	15	ASCII	ASCII
NextCalibrationDate	3	V. quadro 41	
SpeedAuthorised	2	ganho 1/256 km/h/bit, deslocamento 0	0 a 250 996 km/h
RegisteringMemberState	3	ASCII	ASCII
VehicleRegistrationNumber	14	V. 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 F00B do recordDataIdentifier)

Byte	Definição do parâmetro	Resolução	Gama de funcionamento
1	Segundos	ganho 0,25 s/bit, deslocamento 0 s	0 a 59,75 s
2	Minutos	ganho 1 min/bit, deslocamento 0 min	0 a 59 min
3	Horas	ganho 1 h/bit, deslocamento 0 h	0 a 23 h
4	Mês	ganho 1 mês/bit, deslocamento 0 meses	1 a 12 meses
5	Dia	ganho 0,25 dias/bit, deslocamento 0 dias (v. Nota quadro 41)	0,25 a 31,75 dias
6	Ano	ganho 1 ano/bit, deslocamento +1985 anos (v. Nota quadro 41)	1985 a 2235 anos
7	Deslocamento local em minutos	ganho 1 min/bit, deslocamento - 125 min	- 59 a 59 min
8	Deslocamento local em horas	ganho 1 h/bit, deslocamento - 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 F022 do recordDataIdentifier)

Byte	Definição do parâmetro	Resolução	Gama de funcionamento
1	Mês	ganho 1 mês/bit, deslocamento 0 meses	1 a 12 meses
2	Dia	ganho 0,25 dia/bit, deslocamento 0 dias (v. Nota <i>infra</i>)	0,25 a 31,75 dias
3	Ano	ganho 1 ano/bit, deslocamento +1985 anos (v. Nota <i>infra</i>)	1985 a 2235 anos

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; e assim sucessivamente.
2. Este parâmetro não influi no parâmetro "Horas" nem o altera.

Nota relativa à utilização do parâmetro "Ano":

O valor 0 identifica o ano de 1985; o valor 1 identifica o ano de 1986; e assim sucessivamente.

CPR_078 O quadro 42 indica os formatos dos diversos bytes do parâmetro VehicleRegistrationNumber:

Quadro 42

Formatos detalhados do parâmetro VehicleRegistrationNumber (valor F07E do recordDataIdentifier)

Byte	Definição do parâmetro	Resolução	Gama de funcionamento
1	Code Page (cf. definição Apêndice 1)	ASCII	01 a 0A
2 a 14	VehicleRegistrationNumber VRN (cf. definição Apêndice 1)	ASCII	ASCII

Apêndice 9

HOMOLOGAÇÃO DE TIPO — RELAÇÃO DOS ENSAIOS MÍNIMOS REQUERIDOS**1. INTRODUÇÃO****1.1. Homologação de tipo**

A homologação CEE de tipo para um aparelho de controlo (ou componente) ou para um cartão tacográfico tem por base:

- uma certificação de segurança, efectuada por uma autoridade ITSEC, tendo por referência uma meta de segurança que cumpra inteiramente o disposto no apêndice 10 do presente anexo,
- uma certificação de funcionalidade, efectuada por uma autoridade do Estado-Membro, certificando 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, efectuada pelo organismo competente, certificando que o aparelho de controlo (ou cartão tacográfico) é totalmente interoperável com os modelos necessários de cartão tacográfico (ou de aparelho de controlo) (ver secção VIII do presente anexo).

O presente apêndice especifica os ensaios que devem, no mínimo, ser efectuados pela autoridade nacional no âmbito dos ensaios de funcionalidade, bem como os ensaios que devem, no mínimo, ser efectuados pelo organismo competente no âmbito dos ensaios de interoperabilidade. Não são fornecidos mais elementos sobre os procedimentos de execução nem sobre o tipo de ensaios.

Os aspectos relativos à certificação de segurança não são abordados no presente apêndice. Se, durante o processo de certificação e de avaliação da segurança, forem executados alguns dos ensaios requeridos para efeitos da homologação de tipo, não é necessário proceder novamente a eles. Em tal eventualidade, somente os resultados destes ensaios de segurança poderão ser inspeccionados. 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.

O presente apêndice considera a homologação de tipo do sensor de movimentos separadamente da da unidade-veículo, como componentes do aparelho de controlo. Não é exigida a interoperabilidade entre cada modelo de sensor de movimentos e cada modelo de unidade-veículo, pelo que a homologação de tipo de um sensor de movimentos só pode ser concedida conjuntamente com a homologação de tipo de uma unidade-veículo, e vice-versa.

1.2. Referências

No presente apêndice, são utilizadas as seguintes referências:

- | | |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IEC 68-2-1 | Ensaio ambiental — 2ª parte: Ensaio — Ensaio A: Frio. 1990 + 2ª emenda: 1994. |
| IEC 68-2-2 | Ensaio ambiental — 2ª parte: Ensaio — Ensaio B: Calor seco. 1974 + 2ª emenda: 1994. |
| IEC 68-2-6 | Procedimento de base para o ensaio ambiental — Métodos de ensaio — Ensaio Fc e orientação: Vibração (sinusoidal). 6ª edição: 1985. |
| IEC 68-2-14 | Procedimento de base para o ensaio ambiental — Métodos de ensaio — Ensaio N: Mudança de temperatura 1ª modificação: 1996 |
| IEC 68-2-27 | Procedimento de base para o ensaio ambiental — Métodos de ensaio — Ensaio Ea e orientação: Choque. 3ª edição: 1987. |
| IEC 68-2-30 | Procedimento de base para o ensaio ambiental — Métodos de ensaio — Ensaio Db e orientação: Calor húmido, cíclico (ciclo horário 12 + 12 -). 1ª modificação: 1985. |
| IEC 68-2-35 | Procedimento de base para o ensaio ambiental — Métodos de ensaio — Ensaio Fda: Banda larga de vibração aleatória - Reprodutibilidade elevada. 1ª modificação: 1983. |
| IEC 529 | Graus de protecção proporcionados por recintos (código IP). 2ª edição: 1989. |
| IEC 61000-4-2 | Compatibilidade electromagnética (EMC) — Técnicas de ensaio e de medição — Ensaio de imunidade à descarga electrostática: 1995/1ª emenda: 1998 |
| ISO 7637-1 | Veículos rodoviários — Perturbação eléctrica na condução e no acoplamento — 1ª parte: Automóveis de turismo e veículos comerciais ligeiros com 12 V de tensão nominal de alimentação — Condução do transitório eléctrico ao longo das linhas de alimentação apenas. 2ª edição: 1990. |

- ISO 7637-2 Veículos rodoviários — Perturbação eléctrica na condução e no acoplamento — 2ª parte: Veículos comerciais com 24 V de tensão nominal de alimentação — Condução do transitório eléctrico ao longo das linhas de alimentação apenas. 1ª edição: 1990.
- ISO 7637-3 Veículos rodoviários — Perturbação eléctrica na condução e no acoplamento — 3ª parte: Veículos com 12 V ou 24 V de tensão de alimentação — Transmissão do transitório eléctrico por acoplamento capacitivo e indutivo via outras linhas que não as de alimentação. 1ª edição: 1995 + 1ª cor: 1995.
- ISO/IEC 7816-1 Cartões de identificação — Cartões de circuito(s) integrado(s) com contactos — 1ª parte: Características físicas. 1ª edição: 1998.
- ISO/IEC 7816-2 Tecnologia de informação — Cartões de identificação — Cartões de circuito(s) integrado(s) com contactos — 2ª parte: Dimensões e localização dos contactos. 1ª edição: 1999.
- ISO/IEC 7816-3 Tecnologia de informação — Cartões de identificação — Cartões de circuito(s) integrado(s) com contactos — 3ª parte: Sinais electrónicos e protocolo de transmissão. 2ª edição: 1997.
- ISO/IEC 10373 Cartões de identificação — Métodos de ensaio. 1ª edição: 1993.

2. ENSAIOS DE FUNCIONALIDADE DA UNIDADE-VEÍCULO

N.º	Ensaio	Descrição	Requisitos correlatos
1.	Exame administrativo		
1.1.	Documentação	Justeza da documentação	
1.2.	Resultados do ensaio do fabricante	Resultados do ensaio efectuado pelo fabricante durante a integração. Demonstrações em papel	070, 071, 073
2.	Inspeção visual		
2.1.	Conformidade à documentação		
2.2.	Identificação / marcações		168, 169
2.3.	Materiais		163 a 167
2.4.	Selagem		251
2.5.	Interfaces externas		
3.	Ensaio de funcionalidade		
3.1.	Funções disponíveis		002, 004, 244
3.2.	Modos de funcionamento		006*, 007*, 008*, 009*, 106, 107
3.3.	Direitos de acesso a funções e a dados		010*, 011*, 240, 246, 247
3.4.	Controlo da inserção e da retirada de cartões		013, 014, 015*, 016*, 106
3.5.	Medição da velocidade e da distância		017 a 026
3.6.	Medição do tempo (ensaio efectuado a 20 °C)		027 a 032

N.º	Ensaio	Descrição	Requisitos correlatos
3.7.		Controlo das actividades do condutor	033 a 043, 106
3.8.		Controlo da situação de condução	044, 045, 106
3.9.		Entradas efectuadas manualmente	046 a 050b
3.10.		Gestão dos bloqueamentos da empresa	051 a 055
3.11.		Vigilância das actividades de controlo	056, 057
3.12.		Detecção de incidentes e/ou falhas	059 a 069, 106
3.13.		Dados de identificação do aparelho	075*, 076*, 079
3.14.		Dados relativos à inserção e à retirada de cartões de condutor	081* a 083*
3.15.		Dados relativos à actividade de condutor	084* a 086*
3.16.		Dados relativos à localização	087* a 089*
3.17.		Dados odométricos	090* a 092*
3.18.		Dados pormenorizados relativos à velocidade	093*
3.19.		Dados relativos a incidentes	094*, 095
3.20.		Dados relativos a falhas	096*
3.21.		Dados relativos à calibração	097*, 098*
3.22.		Dados relativos ao ajustamento do tempo	100*, 101*
3.23.		Dados relativos à actividade de controlo	102*, 103*
3.24.		Dados relativos aos bloqueamentos da empresa	104*
3.25.		Dados relativos à actividade de descarregamento	105*
3.26.		Dados relativos às condições especiais	105a*, 105b*
3.27.		Registo e memorização de dados nos cartões tacográficos	108, 109*, 109a*, 110*, 111, 112
3.28.		Visualização	072, 106, 113 a 128, PIC_001, DIS_001
3.29.		Impressão	072, 106, 129 a 138, PIC_001, PRT_001 a PRT_012
3.30.		Avisos ou alertas	106, 139 a 148, PIC_001
3.31.		Descarregamento de dados para meios externos	072, 106, 149 a 151
3.32.		Saída (output) de dados para dispositivos externos adicionais	152, 153
3.33.		Calibração	154*, 155*, 156*, 245
3.34.		Ajustamento do tempo	157*, 158*
3.35.		Não-interferência de funções adicionais	003, 269

N.º	Ensaio	Descrição	Requisitos correlatos
4.	Ensaio ambientais		
4.1.	Temperatura	<p>Verificar funcionalidade através de:</p> <ul style="list-style-type: none"> — IEC 68-2-1, ensaio Ad, com a duração de 72 horas à temperatura mais baixa (- 20 °C), 1 hora em funcionamento, 1 hora fora de funcionamento, — IEC 68-2-2, ensaio Bd, com a duração de 72 horas à temperatura mais alta (+ 70 °C), 1 hora em funcionamento, 1 hora fora de funcionamento. <p>Ciclos de temperatura: verificar se a unidade-veículo suporta variações rápidas da temperatura ambiente, através de IEC 68-2-14 ensaio Na, 20 ciclos, cada um com a temperatura a variar do valor mais baixo (- 20 °C) ao mais alto (+ 70 °C) e estabilização de 2 horas tanto à temperatura mais baixa como à mais alta.</p> <p>Pode ser efectuado 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.</p>	159
4.2.	Humidade	<p>Verificar se a unidade-veículo suporta variações cíclicas de humidade (ensaio térmico) através de IEC 68-2-30, 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</p>	160
4.3.	Vibração	<p>1. Vibrações sinusoidais:</p> <p>Verificar se a unidade-veículo suporta vibrações sinusoidais com as seguintes características:</p> <p>deslocamento constante entre 5 e 11 Hz: pico de 10 mm</p> <p>aceleração constante entre 11 e 300 Hz: 5 g.</p> <p>Este requisito é verificado através de IEC 68-2-6, ensaio Fc, com a duração mínima de 3 x 12 horas (12 horas por eixo)</p> <p>2. Vibrações aleatórias:</p> <p>Verificar se a unidade-veículo suporta vibrações aleatórias com as seguintes características:</p> <p>frequência 5-150 Hz, nível $0,02g^2/Hz$</p> <p>Este requisito é verificado através de IEC 68-2-35, ensaio Ffda, com a duração mínima de 3 x 12 horas (12 horas por eixo), 1 hora em funcionamento, 1 hora fora de funcionamento</p> <p>Os dois ensaios <i>supra</i> são executados sobre duas amostras distintas do tipo de equipamento em teste</p>	163
4.4.	Protecção contra água e corpos estranhos	<p>Verificar se o índice de protecção da unidade-veículo, nos termos de IEC 529, é pelo menos IP 40, com a unidade montada em condições de funcionamento num veículo</p>	164, 165
4.5.	Protecção contra sobre-tensão	<p>Verificar se a unidade-veículo suporta as seguintes tensões de alimentação:</p> <p>Versões de 24 V: 34 V a + 40 °C por 1 hora</p> <p>Versões de 12 V: 17 V a + 40 °C por 1 hora</p>	161
4.6.	Protecção contra polaridade inversa	<p>Verificar se a unidade-veículo suporta uma inversão na alimentação eléctrica</p>	161
4.7.	Protecção contra curto-circuito	<p>Verificar se os sinais de entrada-saída estão protegidos contra curtos-circuitos na alimentação eléctrica e na terra</p>	161

N.º	Ensaio	Descrição	Requisitos correlatos
5.	Ensaio de CEM		
5.1.	Emissões por radiação e susceptibilidade	Verificar conformidade à Directiva	162
5.2.	Descarga electrostática	Verificar conformidade a IEC 61000-4-2, ± 2 kV (nível I)	162
5.3.	Susceptibilidade do transitório conduzido em relação à alimentação eléctrica	<p>Versões de 24 V: conformidade a ISO 7637-2:</p> <p>impulso 1a: $V_s = -100$ V, $R_i = 10$ ohms</p> <p>impulso 2: $V_s = +100$ V, $R_i = 10$ ohms</p> <p>impulso 3a: $V_s = -100$ V, $R_i = 50$ ohms</p> <p>impulso 3b: $V_s = +100$ V, $R_i = 50$ ohms</p> <p>impulso 4: $V_s = -16$ V $V_a = -12$ V, $t_6 = 100$ ms</p> <p>impulso 5: $V_s = +120$ V, $R_i = 2,2$ ohms, $t_d = 250$ ms</p> <p>Versões de 12 V: conformidade a ISO 7637-1:</p> <p>impulso 1: $V_s = -100$ V, $R_i = 10$ ohms</p> <p>impulso 2: $V_s = +100$ V, $R_i = 10$ ohms</p> <p>impulso 3a: $V_s = -100$ V, $R_i = 50$ ohms</p> <p>impulso 3b: $V_s = +100$ V, $R_i = 50$ ohms</p> <p>impulso 4: $V_s = -6$ V, $V_a = -5$ V, $t_6 = 15$ ms</p> <p>impulso 5: $V_s = +65$ V, $R_i = 3$ ohms, $t_d = 100$ ms</p> <p>O ensaio do impulso 5 só será efectuado em unidades-veículo destinadas a ser instaladas em veículos sem protecção externa comum contra descarga</p>	162

3. ENSAIOS DE FUNCIONALIDADE DO SENSOR DE MOVIMENTOS

N.º	Ensaio	Descrição	Requisitos correlatos
1.	Exame administrativo		
1.1.	Documentação	Justeza da documentação	
2.	Inspecção visual		
2.1.	Conformidade à documentação		
2.2.	Identificação/marcações		169, 170
2.3.	Materiais		163 a 167
2.4.	Selagem		251
3.	Ensaio de funcionalidade		
3.1.	Dados de identificação do sensor de movimentos		077*
3.2.	Emparelhamento do sensor de movimentos com a unidade-veículo		099*, 155
3.3.	Detecção de movimentos Precisão da medição de movimentos		022 bis 026

N.º	Ensaio	Descrição	Requisitos correlatos
4.	Ensaio ambientais		
4.1.	Temperatura de funcionamento	Verificar funcionalidade (cf. definição no ensaio 3.3) na amplitude térmica [— 40 °C; + 135 °C], através de: — IEC 68-2-1 ensaio Ad, com a duração de 96 horas à temperatura mais baixa T_{min} — IEC 68-2-2 ensaio Bd, com a duração de 96 horas à temperatura mais alta T_{max}	159
4.2.	Ciclos térmicos	Verificar funcionalidade (cf. definição no ensaio 3.3) através de IEC 68-2-14 ensaio Na, 20 ciclos, cada um com a temperatura a variar do valor mais baixo (- 40 °C) ao mais alto (+ 135 °C) e estabilização de 2 horas tanto à temperatura mais baixa como à mais alta Pode ser efectuado um conjunto reduzido de ensaios (entre os definidos no ensaio 3.3) à temperatura mais baixa, à temperatura mais alta e durante os ciclos de temperatura	159
4.3.	Ciclos de humidade	Verificar funcionalidade (cf. definição no ensaio 3.3) através de IEC 68-2-30, 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	160
4.4.	Vibração	Verificar funcionalidade (cf. definição no ensaio 3.3) através de IEC 68-2-6, ensaio Fc, com a duração de 100 ciclos de frequência: deslocamento constante entre 10 e 57 Hz: pico de 1,5 mm aceleração constante entre 57 e 500 Hz: 20 g	163
4.5.	Choque mecânico	Verificar funcionalidade (cf. definição no ensaio 3.3) através de IEC 68-2-27, ensaio Ea, três choques em ambas as direcções dos três eixos ortogonais	163
4.6.	Protecção contra água e corpos estranhos	Verificar se o índice de protecção do sensor de movimentos, nos termos de IEC 529, é pelo menos IP 64, com o sensor montado em condições de funcionamento num veículo	165
4.7.	Protecção contra polaridade inversa	Verificar se o sensor de movimentos suporta uma inversão na alimentação eléctrica	161
4.8.	Protecção contra curto-circuito	Verificar se os sinais de entrada-saída estão protegidos contra curtos-circuitos na alimentação eléctrica e na terra	161
5.	Ensaio de CEM		
5.1.	Emissões por radiação e susceptibilidade	Verificar conformidade à Directiva 95/54/CEE	162
5.2.	Descarga electrostática	Verificar conformidade a IEC 61000-4-2, ± 2 kV (nível I)	162
5.3.	Susceptibilidade do transitório conduzido em relação às linhas de dados	Verificar conformidade a ISO7637-3 (nível III)	162

4. ENSAIOS DE FUNCIONALIDADE DOS CARTÕES TACOGRÁFICOS

N.º	Ensaio	Descrição	Requisitos correlatos
1.	Exame administrativo		
1.1.	Documentação	Justeza da documentação	
2.	Inspecção visual		
2.1.		Verificar se todos os elementos de protecção e dados visíveis estão conformes e correctamente impressos no cartão	171 a 181
3.	Ensaio físicos		
3.1.	Verificar dimensão do cartão e localização dos contactos		184 ISO/IEC 7816-1 ISO/IEC 7816-2
4.	Ensaio de protocolo		
4.1.	ATR	Verificar a conformidade da ATR	ISO/IEC 7816-3 TCS 304, 307, 308
4.2.	T=0	Verificar a conformidade do protocolo T=0	ISO/IEC 7816-3 TCS 302, 303, 305
4.3.	PTS	Verificar a conformidade do comando PTS, passando de T=0 a T=1	ISO/IEC 7816-3 TCS 309 a 311
4.4.	T=1	Verificar a conformidade do protocolo T=1	ISO/IEC 7816-3 TCS 303, / 306
5.	Estrutura do cartão		
5.1.		Verificar a conformidade da estrutura de ficheiro do cartão, controlando a presença dos ficheiros obrigatórios no cartão e as suas condições de acesso	TCS 312 TCS 400*, 401, 402, 403*, 404, 405*, 406, 407, 408*, 409, 410*, 411, 412, 413*, 414, 415*, 416, 417, 418*, 419
6.	Ensaio de funcionalidade		
6.1.	Processamento normal	Verificar pelo menos uma vez cada uma das utilizações autorizadas de cada comando (ex: ensaiar o comando UPDATE BINARY com CLA='00', com 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 313 a TCS 379
6.2.	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 (excepto os erros de integridade '6400' controlados durante a certificação de segurança)	
7.	Ensaio ambientais		
7.1.		Verificar se o funcionamento dos cartões respeita as condições-limite definidas segundo ISO/IEC 10373	185 a 188 ISO/IEC 7816-1

5. ENSAIOS DE INTEROPERABILIDADE

N.º	Ensaio	Descrição
1.	Autenticação mútua	Verificar se funciona normalmente a autenticação mútua entre a unidade-veículo e o cartão tacográfico
2.	Ensaio de leitura/escrita	Encenar uma actividade típica na unidade-veículo. O cenário deve ser adaptado ao tipo de cartão em ensaio e envolver escritas em tantas funções quantas as possíveis no cartão Por meio de um descarregamento do cartão, verificar se todos os correspondentes registos foram executados correctamente Por meio de uma impressão diária do cartão, verificar se todos os correspondentes registos podem ser lidos correctamente

Apêndice 10

OBJECTIVOS GENÉRICOS DE SEGURANÇA

O presente apêndice especifica o teor mínimo exigível para os objectivos de segurança relativos ao sensor de movimentos, à unidade-veículo e ao cartão tacográfico.

Para atingirem os objectivos de segurança relativamente aos quais podem pedir a certificação de segurança, os fabricantes devem aperfeiçoar e completar os documentos na medida do necessário, sem alterarem ou eliminarem eventuais ameaças, objectivos, meios de procedimento ou especificações de funções de concretização da segurança.

OBJECTIVO GENÉRICO DE SEGURANÇA DO SENSOR DE MOVIMENTOS**1. Introdução**

O presente documento contém uma descrição do sensor de movimentos, das ameaças contra as quais ele deve poder actuar e dos objectivos de segurança que ele deve cumprir. Especifica igualmente as funções exigíveis de concretização da segurança, bem como a energia mínima dos mecanismos de segurança e o necessário nível de garantia no desenvolvimento e na avaliação do sensor.

Os requisitos referidos neste documento são os que constam do anexo I B. Por motivos de clareza na leitura, registam-se algumas duplicações entre os requisitos do anexo I B e os requisitos dos objectivos de segurança. Em caso de ambiguidade entre um requisito dos objectivos de segurança e o requisito do anexo I B referido por esse requisito dos objectivos de segurança, prevalece o requisito do anexo I B.

Os requisitos do anexo I B não referidos por objectivos de segurança não são objecto de funções de concretização da segurança.

Às ameaças, aos objectivos, aos meios processuais e às especificações de funções de concretização da segurança foram assignadas etiquetas únicas, para efeitos de rastreabilidade dos documentos de desenvolvimento e avaliação.

2. Abreviaturas, definições e referências**2.1. Abreviaturas**

ROM Read only memory (memória exclusivamente de leitura; memória morta)

SEF Security enforcing function (função de concretização da segurança)

TBD To be defined (a definir)

TOE Target of evaluation (alvo de avaliação)

VU Vehicle unit (unidade-veículo; unidade montada num veículo)

2.2. Definições

Tacógrafo digital Aparelho de controlo

Entidade Dispositivo ligado ao sensor de movimentos

Dados de movimento Dados intercambiados com a VU, representativos da velocidade do veículo e da distância por ele percorrida

Partes fisicamente separadas Componentes físicos do sensor de movimentos que se distribuem pelo veículo, em oposição aos componentes físicos reunidos no sensor

Dados de segurança	Os dados específicos necessários para apoiar as funções de concretização da segurança (por exemplo, chaves criptadas)
Sistema	Equipamento, pessoas ou organizações que de algum modo tenham a ver com o aparelho de controlo
Utilizador	Pessoa que utiliza o sensor de movimentos
Dados de utilização	Quaisquer dados, com excepção dos dados de movimento ou de segurança, registados ou memorizados pelo sensor de movimentos

2.3. Referências

ITSEC ITSEC Information Technology Security Evaluation Criteria ("Critérios de Avaliação da Segurança nas Tecnologias da Informação"), 1991

3. Características do produto

3.1. Descrição e método de utilização do sensor de movimentos

O sensor de movimentos destina-se a ser instalado em veículos de transporte rodoviário. A sua finalidade é proporcionar uma VU (unidade-veículo, ou seja, tacógrafo montado no veículo) com dados securizados representativos da velocidade de circulação do veículo e da distância por ele percorrida.

O sensor de movimentos está ligado por interface mecânica a uma parte do veículo cuja deslocação possa ser representativa da velocidade deste ou da distância que ele percorre. Pode localizar-se na caixa de velocidades ou em qualquer outra parte do veículo.

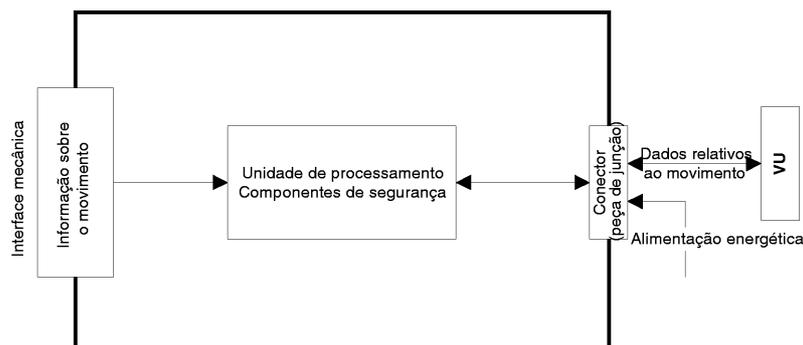
Em modo de funcionamento, o sensor de movimentos está ligado a uma VU.

Pode ser igualmente ligado a equipamento específico para objectivos de gestão (TBD pelo fabricante).

O típico sensor de movimentos é ilustrado pelo esquema seguinte:

Figura 1

Sensor de movimentos típico

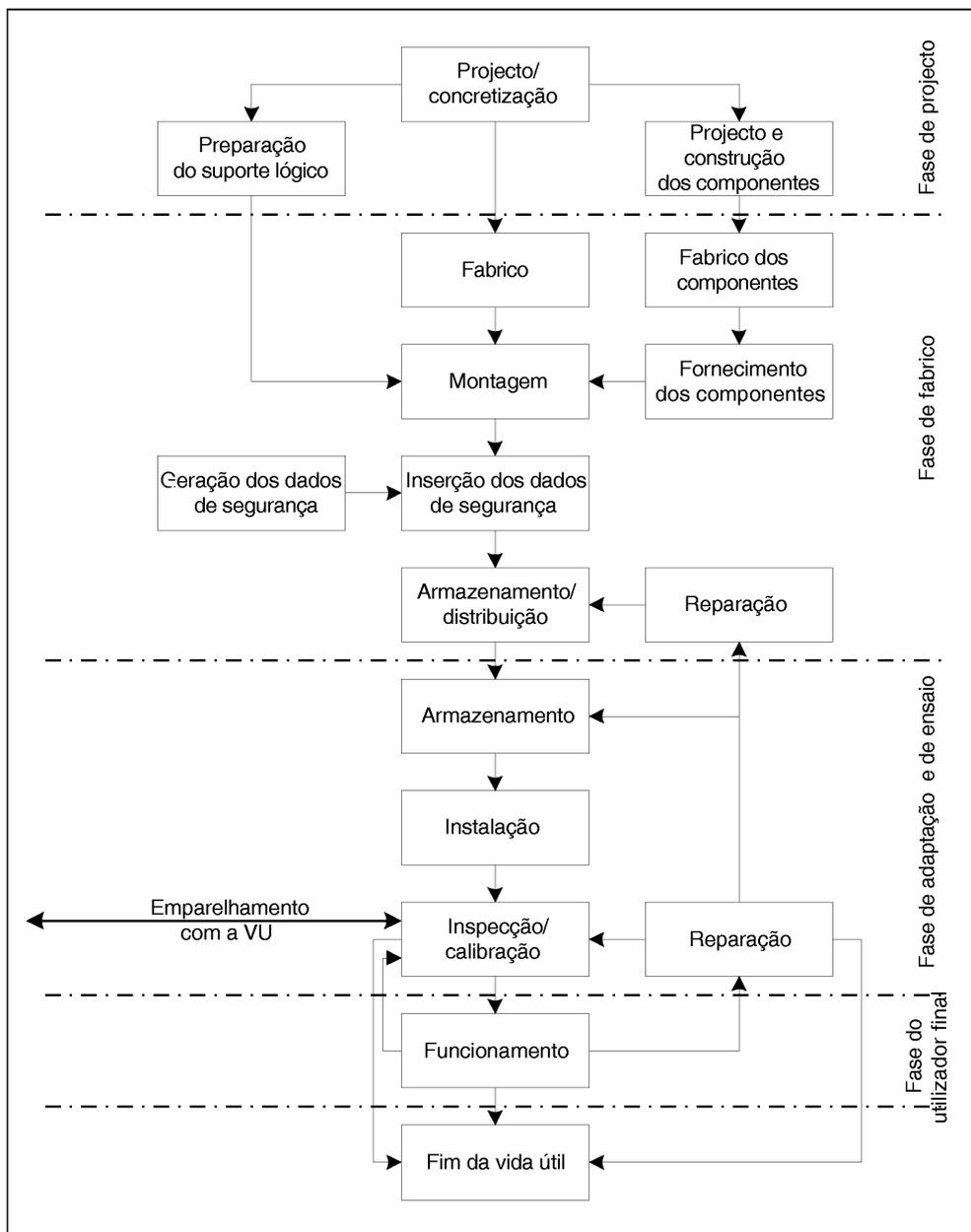


3.2. Ciclo de vida de um sensor de movimentos

O típico ciclo de vida do sensor de movimentos é ilustrado pelo esquema seguinte:

Figura 2

Ciclo de vida típico de um sensor de movimentos



3.3. Ameaças

Nesta secção, referem-se as ameaças susceptíveis de se apresentarem ao sensor de movimentos.

3.3.1. Ameaças às políticas de controlo do acesso

T.Access

Possibilidade de o utilizador tentar acesso a funções que lhe são defesas

3.3.2. Ameaças relacionadas com a concepção

T.Faults	Falhas no equipamento informático, no suporte informático (suporte lógico) ou nos procedimentos de comunicação podem colocar o sensor de movimentos em condições imprevistas, comprometendo a sua segurança
T.Tests	O recurso a modos de ensaio não validados ou a estratégias pode comprometer a segurança do sensor de movimentos
T.Design	Possibilidade de o utilizador tentar obter conhecimento ilícito de elementos conceptuais, através quer do material do fabricante (por furto, suborno, etc.) quer de desmontagem do sensor

3.3.3. Ameaças relacionadas com o funcionamento

T.Environment	Possibilidade de o utilizador comprometer a segurança do sensor de movimentos através de ataques ambientais (térmicos, electromagnéticos, ópticos, químicos, mecânicos, etc.)
T.Hardware	Possibilidade de o utilizador tentar modificar o equipamento informático do sensor de movimentos
T.Mechanical_Origin	Possibilidade de o utilizador tentar manipular a instalação do sensor de movimentos (por exemplo, desaparafusando-o da caixa de velocidades)
T.Motion_Data	Possibilidade de o utilizador tentar modificar os dados relativos ao movimento do veículo (adição, alteração, eliminação ou apagamento, reprodução do sinal)
T.Power_Supply	Possibilidade de o utilizador tentar anular os objectivos de segurança do sensor de movimentos mediante a modificação (por corte, redução ou acréscimo) da sua alimentação energética
T.Security_Data	Possibilidade de o utilizador tentar obter conhecimento ilícito dos dados de segurança durante a geração, o transporte ou a memorização deles no equipamento
T.Software	Possibilidade de o utilizador tentar modificar o suporte lógico instalado no sensor de movimentos
T.Stored_Data	Possibilidade de o utilizador tentar modificar os dados memorizados (dados de segurança ou dados de utilização)

3.4. Objectivos de segurança

É o seguinte o principal objectivo de segurança do sistema tacográfico digital:

O.Main	Os dados a verificar pelas autoridades responsáveis pelo controlo devem estar disponíveis e reflectir plenamente e com rigor as actividades dos condutores e dos veículos sujeitos a controlo, no atinente a condução, trabalho, disponibilidade, períodos de repouso e velocidade do veículo
--------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Portanto, o objectivo de segurança do sensor de movimentos que contribui para o objectivo de segurança genérico, é o seguinte:

O.Sensor_Main	Os dados transmitidos pelo sensor de movimentos devem ser disponibilizados à VU para que esta determine plenamente e com rigor o movimento do veículo, em termos de velocidade e de distância percorrida
---------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

3.5. Objectivos de segurança próprios das tecnologias da informação

São os seguintes os objectivos de segurança do sensor de movimentos, próprios das IT, que contribuem para o objectivo de segurança genérico:

O.Access	O sensor de movimentos deve controlar o acesso que as entidades conectadas têm a funções e dados
O.Audit	O sensor de movimentos deve inspeccionar tentativas de ataque à sua segurança e detectar a correspondente relação com entidades associadas
O.Authentication	O sensor de movimentos deve autenticar as entidades conectadas

O.Processing	O sensor de movimentos deve garantir o rigor do processo de entrada de dados relativos ao movimento
O.Reliability	O sensor de movimentos deve proporcionar um serviço fiável
O.Secured_Data_Exchange	O sensor de movimentos deve garantir segurança no intercâmbio de dados com a VU

3.6. Meios físicos, humanos e processuais

Nesta secção, referem-se os requisitos físicos, humanos e processuais que contribuem para a segurança do sensor de movimentos.

3.6.1. Concepção do equipamento

M.Development	No decurso do processo de criação, os criadores de sensores de movimentos devem assegurar a atribuição de responsabilidades numa perspectiva de manutenção da segurança IT
M.Manufacturing	No decurso do processo de fabrico, os fabricantes de sensores de movimentos devem assegurar a atribuição de responsabilidades numa perspectiva de manutenção da segurança IT, bem como a protecção dos sensores contra ataques físicos susceptíveis de comprometer a segurança IT

3.6.2. Entrega do equipamento

M.Delivery	Os fabricantes de sensores de movimentos, os fabricantes e adaptadores de veículos e os centros de ensaio devem assegurar o manuseamento dos sensores de modo a não comprometer a segurança IT
------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

3.6.3. Geração e entrega dos dados de segurança

M.Sec_Data_Generation	Os algoritmos de geração dos dados de segurança devem ser acessíveis exclusivamente a pessoal autorizado
M.Sec_Data_Transport	Os dados de segurança devem ser gerados, transportados e inseridos no sensor de movimentos de um modo que preserve as suas confidencialidade e integridade

3.6.4. Instalação, calibração e inspecção do aparelho de controlo

M.Approved_Workshops	A instalação, a calibração e a reparação do aparelho de controlo devem ser efectuadas por agentes adaptadores ou centros de ensaio providos da devida autorização
M.Mechanical_Interface	Devem ser fornecidos meios (por exemplo, selagem) para detectar interferências físicas com a interface mecânica
M.Regular_Inspections	O aparelho de controlo deve ser sujeito a inspecção e calibração periódicas

3.6.5. Controlo da aplicação da legislação

M.Controls	Devem ser efectuados, com regularidade e aleatoriamente, controlos que incluam auditorias relativas à aplicação da legislação
------------	-------------------------------------------------------------------------------------------------------------------------------

3.6.6. Actualização do suporte lógico

M.Software_Upgrade	Antes de executadas nos sensores de movimentos, as revisões do suporte lógico devem ser sujeitas a uma certificação de segurança
--------------------	----------------------------------------------------------------------------------------------------------------------------------

4. Funções de concretização da segurança

4.1. Identificação e autenticação

UIA_101	O sensor de movimentos deve poder estabelecer, em qualquer interacção, a identidade de uma entidade à qual esteja conectado (isto é, ligado).
---------	-----------------------------------------------------------------------------------------------------------------------------------------------

UIA_102 A identidade de uma entidade conectada deve consistir em:

- grupo da entidade:
 - VU
 - dispositivo de gestão
 - outros
- ID da entidade (somente VU).

UIA_103 O ID de uma VU conectada deve consistir no número de homologação e no número de série dessa VU.

UIA_104 O sensor de movimentos deve poder autenticar qualquer VU ou dispositivo de gestão a que esteja ligado:

- ao ser efectuada a ligação da entidade
- ao ser restabelecida a alimentação energética.

UIA_105 O sensor de movimentos deve poder reautenticar periodicamente a VU a que esteja ligado.

UIA_106 O sensor de movimentos deve detectar e impedir a utilização de dados de autenticação que tenham sido copiados e reproduzidos.

UIA_107 Logo que sejam detectadas (TBD pelo fabricante, mas não mais de 20) tentativas consecutivas de autenticação infrutífera, a SEF deve:

- gerar um registo de auditoria do incidente,
- avisar (alertar) a entidade,
- continuar a exportar dados de movimento em modo não securizado.

4.2. **Controlo do acesso**

Os controlos do acesso asseguram que a informação seja lida do TOE, criada no TOE ou modificada para o TOE apenas por agente devidamente autorizado.

4.2.1. *Política de controlo do acesso*

ACC_101 O sensor de movimentos deve controlar os direitos de acesso a funções e dados.

4.2.2. *Direitos de acesso a dados*

ACC_102 O sensor de movimentos deve garantir que os dados da sua identificação possam ser escritos somente uma vez (requisito 078).

ACC_103 O sensor de movimentos deve aceitar e/ou memorizar dados de utilização provenientes somente de entidades autenticadas.

ACC_104 O sensor de movimentos deve facultar os devidos direitos de acesso (leitura e escrita) a dados de segurança.

4.2.3. *Estrutura de ficheiro e condições de acesso*

ACC_105 A estrutura dos ficheiros de dados de aplicação e as condições de acesso devem ser criadas durante o processo de fabrico, bloqueando-se em seguida a possibilidade de quaisquer modificações ou apagamento subsequentes.

4.3. **Responsabilização**

ACT_101 O sensor de movimentos deve guardar na sua memória os dados da sua identificação (requisito 077).

ACT_102 O sensor de movimentos deve guardar na sua memória os dados da instalação (requisito 099).

ACT_103 O sensor de movimentos deve poder transmitir (output) dados de responsabilização (accountability data) a entidades autenticadas, a pedido destas.

4.4. Auditoria

AUD_101 O sensor de movimentos deve gerar registos de auditoria de incidentes que ponham em causa a sua segurança.

AUD_102 Incidentes susceptíveis de afectar a segurança do sensor de movimentos:

- tentativas de violação da segurança:
 - falha da autenticação
 - erro de integridade de dados memorizados
 - erro de transferência interna de dados
 - abertura não autorizada da caixa
 - sabotagem do equipamento informático (ou seja, do hardware)
- falha do sensor.

AUD_103 Os registos de auditoria devem incluir os seguintes dados:

- data e hora do incidente,
- tipo de incidente,
- identidade da entidade conectada.

Se os dados requeridos não estiverem disponíveis, deve ser dada por defeito uma indicação adequada (TBD pelo fabricante).

AUD_104 No momento da geração dos registos de auditoria, o sensor de movimentos deve enviá-los para a VU, podendo também armazená-los na sua memória (isto é, memorizá-los).

AUD_105 Caso memorize registos de auditoria, o sensor de movimentos deve assegurar que 20 deles se mantenham indemnes ao esgotamento da capacidade de memorização, e deve igualmente poder transmitir (output) registos de auditoria memorizados a entidades autenticadas, a pedido destas.

4.5. Precisão

4.5.1. Política de controlo do fluxo de informação

ACR_101 O sensor de movimentos deve assegurar que os dados de movimento só possam ser processados e derivados a partir de entradas (input) mecânicas no sensor.

4.5.2. Transferências internas de dados

O disposto nesta secção aplica-se somente se o sensor de movimentos for composto por peças fisicamente separadas.

ACR_102 Se forem transferidos entre peças do sensor de movimentos fisicamente separadas, os dados devem ser protegidos contra o risco de modificação.

ACR_103 Se se detectar algum erro durante uma transferência interna de dados, a transmissão deve ser repetida e a SEF gerará um registo de auditoria do incidente.

4.5.3. Integridade dos dados memorizados

ACR_104 O sensor de movimentos deve verificar a ocorrência de erros de integridade nos dados de utilização armazenados na sua memória.

ACR_105 Se detectar algum erro de integridade nos dados de utilização memorizados, a SEF deve gerar um registo de auditoria.

4.6. Fiabilidade do serviço

4.6.1. Ensaios

RLB_101 Os comandos, acções e pontos de teste específicos dos requisitos de ensaio na fase de fabrico devem ser todos desactivados ou removidos antes de terminar essa fase, não devendo ser possível restaurá-los para posterior reutilização.

RLB_102 O sensor de movimentos deve executar auto-ensaios de funcionamento correcto quer durante o arranque quer durante o funcionamento normal. Os auto-ensaios do sensor de movimentos incluirão uma verificação da integridade dos dados de segurança e uma verificação da integridade do código executável memorizado (se não estiver na ROM).

RLB_103 Se for detectada alguma falha interna no decurso dos auto-ensaios, a SEF deve gerar um registo de auditoria (falha do sensor).

4.6.2. Suporte lógico

RLB_104 Não deve haver possibilidade de analisar ou esmiuçar (debug) o suporte lógico (software) do sensor de movimentos no campo.

RLB_105 As entradas (inputs) de fontes externas não devem ser aceites como código executável.

4.6.3. Protecção física

RLB_106 Se tiver sido projectado de modo a poder ser aberto, o sensor de movimentos deve detectar qualquer abertura da caixa, mesmo sem alimentação energética externa durante um mínimo de 6 meses. Neste caso, a SEF gerará um registo de auditoria do incidente (é aceitável que o registo de auditoria seja gerado e memorizado após o restabelecimento da alimentação energética).

Se por concepção não puder ser aberto, o sensor de movimentos deve ser projectado de modo a poderem ser facilmente detectadas (por inspecção visual, por exemplo) tentativas de fraude física.

RLB_107 O sensor de movimentos deve detectar sabotagens (TBD pelo fabricante) do hardware ou equipamento informático.

RLB_108 No caso *supra*, a SEF deve gerar um registo de auditoria e o sensor de movimentos deve: (TBD pelo fabricante).

4.6.4. Interrupções da alimentação energética

RLB_109 O sensor de movimentos deve preservar um estado de segurança durante cortes ou variações da alimentação energética.

4.6.5. Condições de restabelecimento (reset)

RLB_110 Na eventualidade de interrupção na alimentação energética ou de paragem prematura de uma transacção, ou ainda em quaisquer situações de restabelecimento (reset conditions), o sensor de movimentos deve ser restaurado ou restabelecido (reset) sem choque.

4.6.6. Disponibilidade dos dados

RLB_111 O sensor de movimentos deve assegurar o acesso, sempre que requerido, aos recursos, e que os recursos não sejam requeridos nem retidos desnecessariamente.

4.6.7. Aplicações múltiplas

RLB_112 Se o sensor de movimentos proporcionar aplicações para além da aplicação tacográfica, todas elas devem ser física e/ou logicamente separadas umas das outras. Estas aplicações não devem partilhar dados de segurança. Em cada momento, estará activada uma só função.

4.7. Intercâmbio de dados

DEX_101 O sensor de movimentos deve exportar dados de movimento para a VU com atributos de segurança associados, de modo a que a VU possa verificar as suas integridade e autenticidade.

4.8. Apoio criptográfico

O disposto nesta secção aplica-se somente quando necessário, dependendo dos mecanismos de segurança utilizados e das soluções do fabricante.

CSP_101 As operações criptográficas executadas pelo sensor de movimentos devem obedecer a um algoritmo especificado e a uma dimensão especificada de chave criptográfica.

CSP_102 A eventual geração de chaves criptográficas pelo sensor de movimentos deve obedecer a algoritmos especificados de geração e a dimensões especificadas das chaves.

CSP_103 A eventual distribuição de chaves criptográficas pelo sensor de movimentos deve obedecer a métodos especificados de distribuição das chaves.

CSP_104 O eventual acesso a chaves criptográficas pelo sensor de movimentos deve obedecer a métodos especificados de acesso às chaves.

CSP_105 A eventual destruição de chaves criptográficas pelo sensor de movimentos deve obedecer a métodos especificados de destruição das chaves.

5. Definição de mecanismos de segurança

Os mecanismos que enformam as funções de execução da segurança dos sensores de movimentos são definidos pelos fabricantes destes.

6. Energia mínima dos mecanismos de segurança

A energia mínima dos mecanismos de segurança do sensor de movimentos é High ("elevada"), conforme definição da norma ITSEC.

7. Nível de garantia

O nível objectivado de garantia para o sensor de movimentos é o nível ITSEC E3, conforme definição da norma ITSEC.

8. Síntese lógica

As matrizes que se seguem contêm uma síntese lógica das SEF, indicando:

- as SEF ou os meios e as correspondentes ameaças a que se contrapõem
- as SEF e os correspondentes objectivos de segurança IT por elas cumpridos.

	Ameaças											Objectivos IT						
	T.Access	T.Faults	T.Tests	T.Design	T.Environment	T.Hardware	T.Mechanical_Origin	T.Motion_Data	T.Power_Supply	T.Security_Data	T.Software	T.Stored_Data	O.Access	O.Audit	O.Authentication	O.Processing	O.Reliability	O.Secured_Data_Exchange
Meios físicos, humanos ou processuais																		
Desenvolvimento		x	x	x														
Fabrico			x	x														
Entrega						x					x	x						
Geração de dados de segurança									x									
Transporte de dados de segurança									x									
Centros de ensaio homologados							x											
Interface mecânica							x											
Inspeção regular						x	x		x	x								
Controlos de aplicação da lei					x	x	x		x	x	x							
Actualizações do software										x								
Funções de concretização da segurança																		
Identificação e autenticação																		
UIA_101 Identificação de entidades	x							x				x	x					x
UIA_102 Identidade de entidades	x											x	x					
UIA_103 Identidade da VU													x					
UIA_104 Autenticação de entidades	x						x					x	x					x
UIA_105 Re-autenticação	x						x					x	x					x
UIA_106 Autenticação infalsificável	x						x					x	x					
UIA_107 Falha da autenticação							x						x				x	
Controlo do acesso																		
ACC_101 Política de controlo do acesso	x								x		x	x						
ACC_102 ID do sensor de movimento											x	x						

OBJECTIVO GENÉRICO DE SEGURANÇA DA UNIDADE-VEÍCULO

1. Introdução

O presente documento contém uma descrição da unidade-veículo, das ameaças contra as quais ela deve poder actuar e dos objectivos de segurança que ela deve cumprir. Especifica igualmente a energia mínima dos mecanismos de segurança e o necessário nível de garantia no desenvolvimento e na avaliação da unidade.

Os requisitos referidos neste documento são os que constam do anexo I B. Por motivos de clareza na leitura, registam-se algumas duplicações entre os requisitos do anexo I B e os requisitos dos objectivos de segurança. Em caso de ambiguidade entre um requisito dos objectivos de segurança e o requisito do anexo I B referido por esse requisito dos objectivos de segurança, prevalece o requisito do anexo I B.

Os requisitos do anexo I B não referidos por objectivos de segurança não são objecto de funções de concretização da segurança.

Às ameaças, aos objectivos, aos meios processuais e às especificações de funções de concretização da segurança foram assignadas etiquetas únicas, para efeitos de rastreabilidade dos documentos de desenvolvimento e avaliação.

2. Abreviaturas, definições e referências**2.1. Abreviaturas**

PIN Personal identification number (número de identificação pessoal)

ROM Read only memory (memória exclusivamente de leitura; memória morta)

SEF (Security enforcing function (função de concretização da segurança)

TBD To be defined (a definir)

TOE Target of evaluation (objectivo de avaliação)

VU Vehicle unit (unidade-veículo; unidade montada num veículo)

2.2. Definições

Tacógrafo digital Aparelho de controlo

Dados de movimento Dados intercambiados com o sensor de movimentos, representativos da velocidade do veículo e da distância por ele percorrida

Partes fisicamente separadas Componentes físicos da VU que se distribuem pelo veículo, em oposição aos componentes físicos reunidos na caixa da VU

Dados de segurança Os dados específicos necessários para apoiar as funções de concretização da segurança (por exemplo, chaves criptadas)

Sistema Equipamento, pessoas ou organizações que de algum modo tenham a ver com o aparelho de controlo

Utilizador Pessoa que utiliza o equipamento. Entre os utilizadores normais da VU, contam-se condutores, controladores, centros de ensaio e empresas.

Dados de utilização Quaisquer dados, com excepção dos dados de segurança, registados ou memorizados pela VU, nos termos da secção III.12

2.3. Referências

ITSEC ITSEC Information Technology Security Evaluation Criteria ("Critérios de Avaliação da Segurança nas Tecnologias da Informação"), 1991

3. Características do produto**3.1. Descrição e método de utilização da unidade-veículo**

A VU destina-se a ser instalada em veículos de transporte rodoviário. A sua finalidade é registar, memorizar, visualizar (isto é, exibir, display), imprimir e transmitir (output) dados relativos às actividades dos condutores.

A VU está ligada a um sensor de movimentos com o qual intercambia dados relativos à deslocação do veículo.

Os utilizadores identificam-se perante a VU por intermédio de cartões tacográficos.

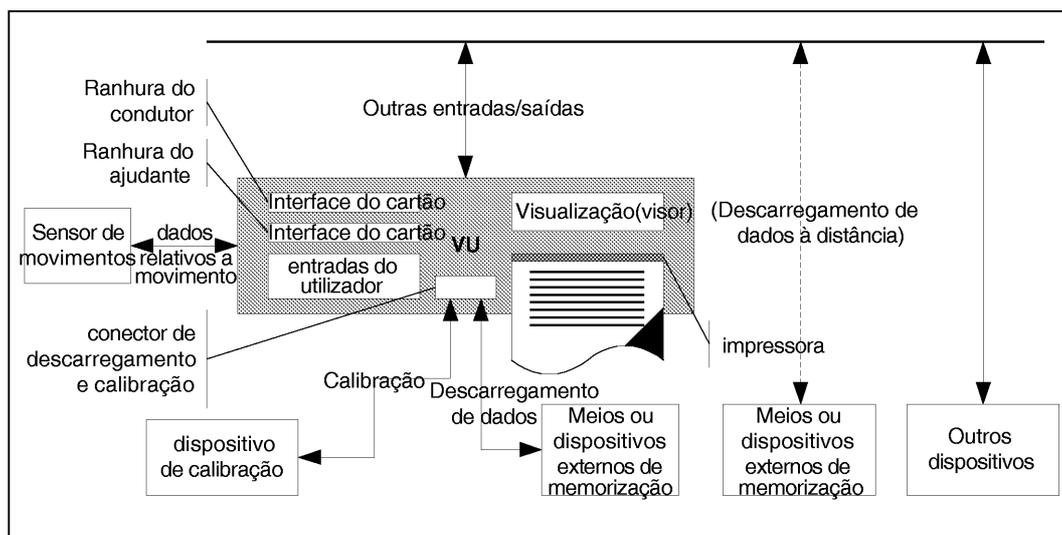
A VU regista e armazena na sua memória (ou seja, memoriza) os dados relativos às actividades dos utilizadores, registando-os também nos cartões tacográficos.

A VU transmite (output) dados para um visor (display), uma impressora e outros dispositivos externos.

O ambiente (cenário) operacional da VU instalada num veículo é ilustrado pelo esquema seguinte:

Figura 1

Ambiente ou cenário operacional da VU



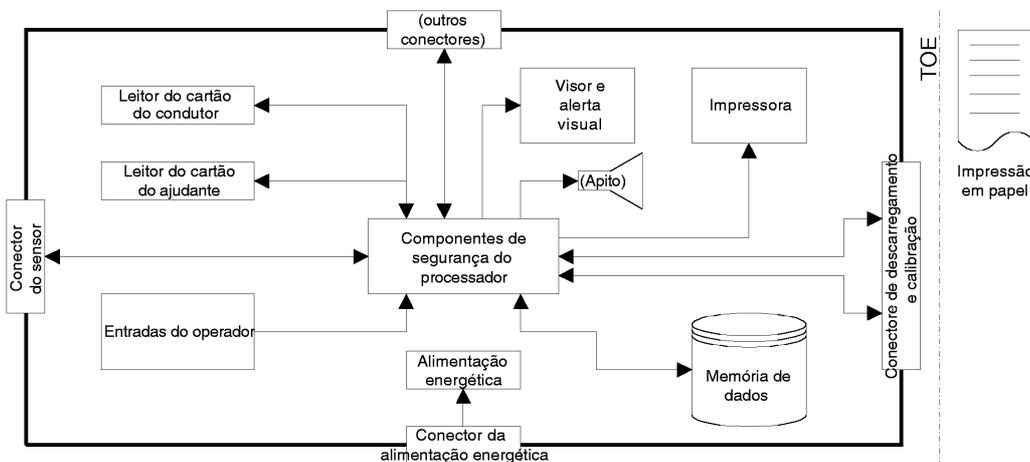
As características gerais, funções e modos de funcionamento (ou de operação) da VU constam do anexo I B, secção II.

Os requisitos de funcionamento da VU são especificados no anexo I B, secção III.

A típica unidade-veículo é ilustrada pelo esquema seguinte:

Figura 2

Unidade-veículo típica (...) opcional



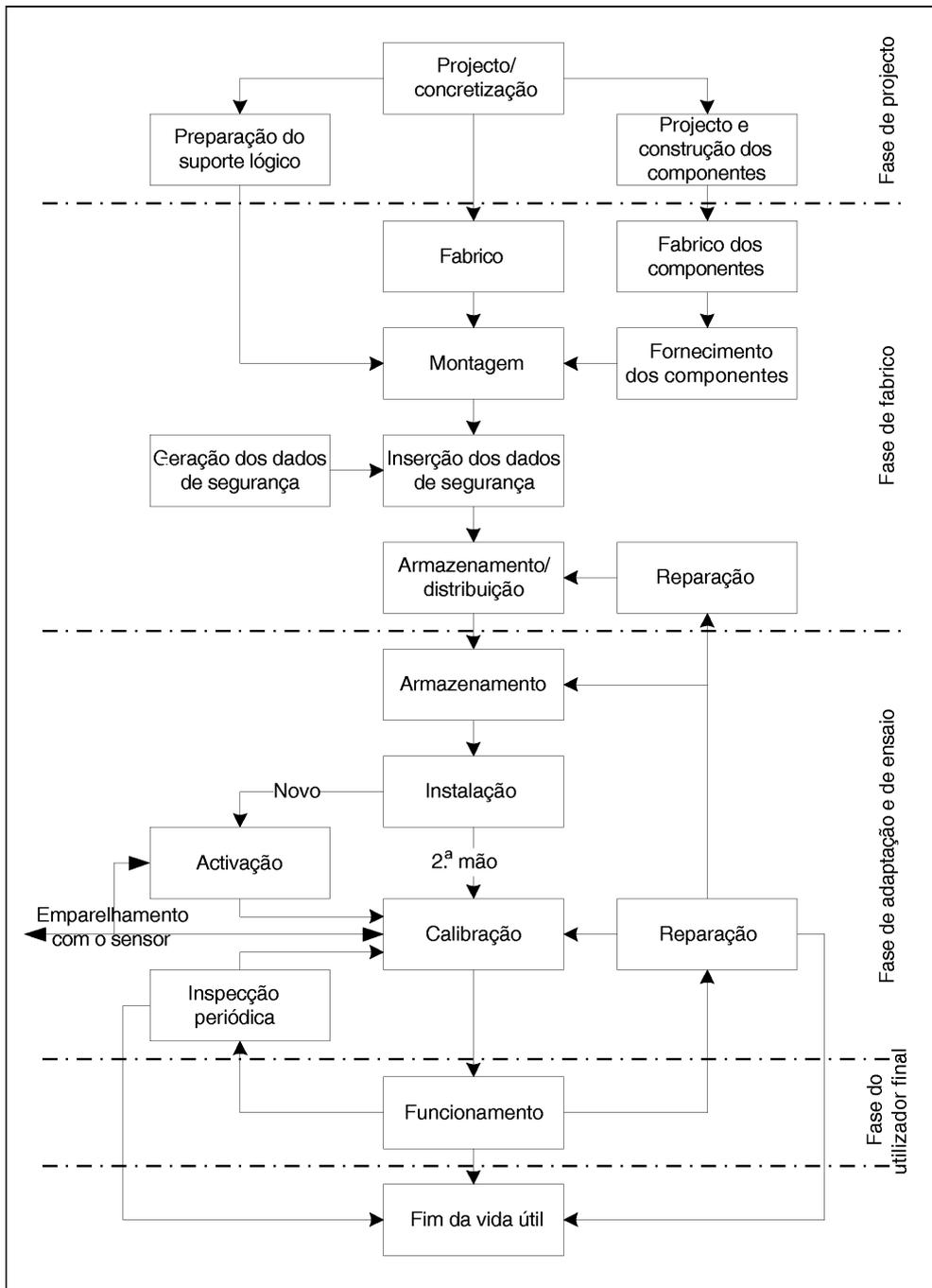
De notar que, embora o mecanismo da impressora faça parte do TOE (objectivo de avaliação), o mesmo não acontece com o documento produzido em papel.

3.2. *Ciclo de vida de uma unidade-veículo*

O típico ciclo de vida da VU é ilustrado pelo esquema seguinte:

Figura 3

Ciclo de vida típico de uma unidade-veículo



3.3. *Ameaças*

Nesta secção, referem-se as ameaças susceptíveis de se apresentarem à VU.

3.3.1. *Ameaças às políticas de identificação e de controlo do acesso*

- T.Access Possibilidade de o utilizador tentar acesso a funções que lhe são defesas (por exemplo, obter acesso à função de calibração)
- T.Identification Possibilidade de o utilizador tentar utilizar diversas identificações ou nenhuma identificação

3.3.2. Ameaças relacionadas com a concepção

T.Faults	Falhas no equipamento informático, no suporte informático (suporte lógico) ou no processo de comunicação podem colocar a VU em condições imprevistas, comprometendo a sua segurança
T.Tests	O recurso a modos de ensaio não validados ou a estratégias pode comprometer a segurança da VU
T.Design	Possibilidade de o utilizador tentar obter conhecimento ilícito de elementos conceptuais, através quer do material do fabricante (por furto, suborno, etc.) quer de desmontagem da unidade-veículo

3.3.3. Ameaças relacionadas com o funcionamento

T.Calibration_Parameters	Possibilidade de o utilizador tentar utilizar equipamento mal calibrado (por modificação dos dados de calibração ou falhas de organização)
T.Card_Data_Exchange	Possibilidade de o utilizador tentar modificar dados durante o seu intercâmbio entre a VU e os cartões tacográficos (adição, modificação, apagamento ou reprodução de sinal)
T.Clock	Possibilidade de o utilizador tentar modificar o relógio interno
T.Environment	Possibilidade de o utilizador comprometer a segurança da VU através de ataques ambientais (térmicos, electromagnéticos, ópticos, químicos, mecânicos, etc.)
T.Fake_Devices	Possibilidade de o utilizador tentar conectar (ou seja, ligar) dispositivos falsificados (sensor de movimentos, cartões inteligentes) à VU
T.Hardware	Possibilidade de o utilizador tentar modificar o equipamento informático da VU
T.Motion_Data	Possibilidade de o utilizador tentar modificar os dados relativos ao movimento do veículo (adição, alteração, eliminação ou apagamento, reprodução do sinal)
T.Non_Activated	Possibilidade de o utilizador utilizar equipamento não activado
T.Output_Data	Possibilidade de o utilizador tentar modificar os dados saídos (para impressão, visualização ou descarregamento)
T.Power_Supply	Possibilidade de o utilizador tentar anular os objectivos de segurança da VU mediante a modificação (por corte, redução ou acréscimo) da sua alimentação energética
T.Saturation	Possibilidade de o utilizador tentar saturar a memória de dados (ainda que em utilização lícita), com o objectivo de apagar dados
T.Security_Data	Possibilidade de o utilizador tentar obter conhecimento ilícito dos dados de segurança durante a geração, o transporte ou a memorização deles no equipamento
T.Software	Possibilidade de o utilizador tentar modificar o suporte lógico instalado na VU
T.Stored_Data	Possibilidade de o utilizador tentar modificar os dados memorizados (dados de segurança ou dados de utilização)

3.4. Objectivos de segurança

É o seguinte o principal objectivo de segurança do sistema tacográfico digital:

O.Main	Os dados a verificar pelas autoridades responsáveis pelo controlo devem estar disponíveis e reflectir plenamente e com rigor as actividades dos condutores e dos veículos sujeitos a controlo, no atinente a condução, trabalho, disponibilidade, períodos de repouso e velocidade do veículo
--------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Portanto, o objectivo de segurança da VU, que contribui para o objectivo de segurança genérico, é o seguinte:

O.VU_Main	Os dados a medir e registar e posteriormente a verificar pelas autoridades responsáveis pelo controlo devem estar disponíveis e reflectir plenamente e com rigor as actividades dos condutores e dos veículos sujeitos a controlo, no atinente a condução, trabalho, disponibilidade, períodos de repouso e velocidade do veículo
O.VU_Export	A VU deve poder exportar dados para meios externos de memorização de modo a possibilitar a verificação das suas integridade e autenticidade

3.5. Objectivos de segurança próprios das tecnologias da informação

São os seguintes os objectivos de segurança da VU, próprios das IT, que contribuem para os seus objectivos principais de segurança:

O.Access	VU deve controlar o acesso dos utilizadores a funções e dados
O.Accountability	VU deve recolher dados de responsabilização rigorosos
O.Audit	A VU deve inspecionar tentativas de sabotagem da sua segurança e detectar a correspondente relação com utilizadores associados
O.Authentication	A VU deve autenticar os utilizadores e as entidades conectadas (se tiver de ser estabelecida uma via de confiança entre entidades)
O.Integrity	A VU deve manter a integridade dos dados memorizados
O.Output	A VU deve garantir que a transmissão ou saída (output) de dados reflecta com rigor os dados medidos ou memorizados
O.Processing	A VU deve garantir o rigor do processo de entrada de dados de utilização
O.Reliability	A VU deve proporcionar um serviço fiável
O.Secured_Data_Exchange	A VU deve garantir segurança no intercâmbio de dados com os cartões tacográficos

3.6. Meios físicos, humanos e processuais

Nesta secção, referem-se os requisitos físicos, humanos e processuais que contribuem para a segurança da VU.

3.6.1. Concepção do equipamento

M.Development	No decurso do processo de criação, os criadores de unidades-veículo devem assegurar a atribuição de responsabilidades numa perspectiva de manutenção da segurança IT
M.Manufacturing	No decurso do processo de fabrico, os fabricantes de unidades-veículo devem assegurar a atribuição de responsabilidades numa perspectiva de manutenção da segurança IT, bem como a protecção das VU contra ataques físicos susceptíveis de comprometer a segurança IT

3.6.2. Entrega e activação do equipamento

M.Delivery	Os fabricantes de unidades-veículo, os fabricantes e adaptadores de veículos e os centros de ensaio devem assegurar o manuseamento das VU não activadas de modo a não comprometer a segurança IT
M.Activation	Uma vez instalada, a VU deve ser activada pelos fabricantes e adaptadores de veículos ou pelos centros de ensaio, antes de o veículo deixar a oficina onde foi efectuada a instalação

3.6.3. Geração e entrega dos dados de segurança

M.Sec_Data_Generation	Os algoritmos de geração dos dados de segurança devem ser acessíveis exclusivamente a pessoal autorizado
M.Sec_Data_Transport	Os dados de segurança devem ser gerados, transportados e inseridos na VU de um modo que preserve as suas confidencialidade e integridade

3.6.4. Entrega de cartões

M.Card_Availability	Os cartões tacográficos devem ser disponibilizados e entregues exclusivamente a pessoal autorizado
M.Driver_Card_Uniqueness	Um condutor nunca pode ter em sua posse mais de um cartão válido de condutor
M.Card_Traceability	A entrega de cartões deve ser rastreável (listas brancas, listas negras), com utilização de listas negras durante auditorias de segurança

3.6.5. Instalação, calibração e inspecção do aparelho de controlo

M.Approved_Workshops	A instalação, a calibração e a reparação do aparelho de controlo devem ser efectuadas por agentes adaptadores ou centros de ensaio providos da devida autorização
M.Regular_Inspections	O aparelho de controlo deve ser sujeito a inspecção e calibração periódicas
M.Faithful_Calibration	Os parâmetros pertinentes do veículo devem ser introduzidos no aparelho de controlo, durante a calibração, por agentes adaptadores ou centros de ensaio providos da devida autorização

3.6.6. Funcionamento do equipamento

M.Faithful_Drivers	Os condutores devem cumprir a regulamentação e agir responsabilmente (por exemplo, utilizar os respectivos cartões, seleccionar correctamente as actividades em caso de selecção manual, etc.)
--------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

3.6.7. Controlo da aplicação da legislação

M.Controls	Devem ser efectuados, com regularidade e aleatoriamente, controlos que incluam auditorias relativas à aplicação da legislação
------------	-------------------------------------------------------------------------------------------------------------------------------

3.6.8. Actualização do suporte lógico

M.Software_Upgrade	Antes de executadas nas VU, as revisões do suporte lógico devem ser sujeitas a uma certificação de segurança
--------------------	--------------------------------------------------------------------------------------------------------------

4. Funções de concretização da segurança

4.1. Identificação e autenticação

4.1.1. Identificação e autenticação do sensor de movimentos

UIA_201 A VU deve poder estabelecer, em qualquer interacção, a identidade do sensor de movimentos ao qual esteja conectada.

UIA_202 A identidade do sensor de movimentos conectado consiste nos seus números de homologação e de série.

UIA_203 A VU deve autenticar o sensor de movimentos a que esteja ligada:

- ao ser efectuada a ligação do sensor,
- a cada calibração do aparelho de controlo,
- ao ser restabelecida a alimentação energética.

A autenticação deve ser mútua e despoletada pela VU.

UIA_204 A VU deve periodicamente (periodicidade TBD pelo fabricante, mas superior a uma vez por hora) reidentificar e reautenticar o sensor de movimentos a que esteja conectada e assegurar que o sensor identificado durante a última calibração do aparelho de controlo não foi alterado.

UIA_205 A VU deve detectar e impedir a utilização de dados de autenticação que tenham sido copiados e reproduzidos.

UIA_206 Se forem detectadas (TBD pelo fabricante, mas não mais de 20) tentativas consecutivas de autenticação infrutífera, e/ou se se detectar que a identidade do sensor de movimentos foi alterada em contexto não autorizado (isto é, fora de uma calibração do aparelho de controlo), a SEF deve:

- gerar um registo de auditoria do incidente,
- avisar (alertar) o utilizador,
- continuar a aceitar e a utilizar dados de movimento não securizados enviados pelo sensor de movimentos.

4.1.2. Identificação e autenticação do utilizador

UIA_207 A VU deve seguir permanente e selectivamente a identidade de dois utilizadores, acompanhando os cartões tacográficos inseridos no aparelho de controlo, respectivamente na ranhura do condutor e na ranhura do ajudante.

UIA_208 A identidade do utilizador consiste em:

- grupo do utilizador:
 - DRIVER (cartão de condutor)
 - CONTROLLER (cartão de controlador)
 - WORKSHOP (cartão de centro de ensaio)
 - COMPANY (cartão de empresa)
 - UNKNOWN (nenhum cartão inserido)
- ID do utilizador, composta de:
 - código do Estado-Membro emissor do cartão e número do cartão
 - UNKNOWN, se o grupo do utilizador for UNKNOWN (desconhecido).

As identidades UNKNOWN podem ser conhecidas implícita ou explicitamente.

UIA_209 A VU deve autenticar os seus utilizadores ao serem inseridos os respectivos cartões.

UIA_210 A VU deve reautenticar os seus utilizadores:

- ao ser restabelecida a alimentação energética,
- periodicamente ou após a ocorrência de incidentes específicos (periodicidade TBD pelos fabricantes, mas superior a uma vez por dia).

UIA_211 A autenticação deve ser efectuada por comprovação em como o cartão inserido é um cartão tacográfico válido, detentor de dados de segurança que somente o sistema poderia distribuir. A autenticação deve ser mútua e despoletada pela VU.

UIA_212 Para além do supradispuesto, os centros de ensaio devem ser autenticados com êxito mediante uma verificação do PIN. Os PIN devem ter um mínimo de 4 caracteres de comprimento.

Nota: caso o PIN seja transferido para a VU a partir de um aparelho externo localizado nas vizinhanças da VU, a sua confidencialidade não carece de protecção durante a transferência.

UIA_213 A VU deve detectar e impedir a utilização de dados de autenticação que tenham sido copiados e reproduzidos.

UIA_214 Logo que sejam detectadas 5 tentativas consecutivas de autenticação infrutífera, a SEF deve:

- gerar um registo de auditoria do incidente,
- avisar (alertar) o utilizador,
- considerar que o utilizador é UNKNOWN e o cartão não válido (definição z no anexo IB e requisito 007).

4.1.3. *Identificação e autenticação de empresa conectada à distância*

A capacidade de ligar uma empresa à distância é opcional. Por conseguinte, a presente secção aplica-se somente se tal opção for concretizada.

- UIA_215 Em cada interacção com uma empresa ligada à distância, a VU deve poder estabelecer a identidade da empresa.
- UIA_216 A identidade da empresa conectada à distância deve consistir no código do Estado-Membro emissor do cartão da empresa e no número deste cartão.
- UIA_217 Antes de permitir a exportação de quaisquer dados para uma empresa conectada à distância, a VU deve autenticar a empresa com êxito.
- UIA_218 A autenticação deve ser efectuada por comprovação em como a empresa é titular de um cartão válido, detentor de dados de segurança que somente o sistema poderia distribuir.
- UIA_219 A VU deve detectar e impedir a utilização de dados de autenticação que tenham sido copiados e reproduzidos.
- UIA_220 Logo que sejam detectadas 5 tentativas consecutivas de autenticação infrutífera, a VU deve:
- avisar (alertar) a empresa conectada à distância.

4.1.4. *Identificação e autenticação de dispositivo de gestão*

Os fabricantes de unidades-veículo podem prever dispositivos dedicados para funções adicionais de gestão das VU (por exemplo, reclassificação ou actualização do suporte lógico, recarga dos dados de segurança, etc.). Por conseguinte, a presente secção aplica-se somente se tal opção for concretizada.

- UIA_221 Em cada interacção com um dispositivo de gestão, a VU deve poder estabelecer a identidade do mesmo.
- UIA_222 Antes de permitir qualquer nova interacção, a VU deve autenticar com êxito o dispositivo de gestão.
- UIA_223 A VU deve detectar e impedir a utilização de dados de autenticação que tenham sido copiados e reproduzidos.

4.2. **Controlo do acesso**

Os controlos do acesso asseguram que a informação seja lida do TOE, criada no TOE ou modificada para o TOE apenas por agente devidamente autorizado.

De notar que, embora apresentem características de privacidade e sensibilidade comercial, os dados de utilizador registados pela VU não têm natureza confidencial. Por conseguinte, o requisito de funcionamento relacionado com direitos de acesso à leitura de dados (requisito 011) não é objecto de qualquer função de concretização da segurança.

4.2.1. *Política de controlo do acesso*

- ACC_201 A VU deve gerir e verificar os direitos de acesso a funções e dados.

4.2.2. *Direitos de acesso a funções*

- ACC_202 A VU deve aplicar as regras de selecção do modo de funcionamento (requisitos 006 a 009).
- ACC_203 A VU deve utilizar o modo de funcionamento correspondente à aplicação das regras de controlo do acesso às funções (requisito 010).

4.2.3. *Direitos de acesso a dados*

- ACC_204 A VU deve aplicar as regras de acesso à escrita dos dados da sua identificação (requisito 076).
- ACC_205 A VU deve aplicar as regras de acesso à escrita dos dados de identificação do sensor de movimentos emparelhado (requisitos 079 e 155).
- ACC_206 Uma vez activada, a VU deve garantir que dados de calibração possam ser introduzidos e armazenados na sua memória somente em modo de calibração (requisitos 154 e 156).
- ACC_207 Uma vez activada, a VU deve aplicar as regras de acesso à escrita e ao apagamento dos dados de calibração (requisito 097).

ACC_208 Uma vez activada, a VU deve garantir que dados de ajustamento do tempo possam ser introduzidos e armazenados na sua memória somente em modo de calibração (requisito não aplicável a pequenos ajustamentos do tempo autorizados pelos requisitos 157 e 158).

ACC_209 Uma vez activada, a VU deve aplicar as regras de acesso à escrita e ao apagamento dos dados de ajustamento do tempo (requisito 100).

ACC_210 A VU deve aplicar os devidos direitos de acesso à leitura e à escrita de dados de segurança (requisito 080).

4.2.4. *Estrutura de ficheiro e condições de acesso*

ACC_211 A estrutura dos ficheiros de dados de aplicação e as condições de acesso devem ser criadas durante o processo de fabrico, bloqueando-se em seguida a possibilidade de quaisquer modificações ou apagamento subsequentes.

4.3. **Responsabilização**

ACT_201 A VU deve assegurar a responsabilização dos condutores pelas suas actividades (requisitos 081, 084, 087, 105a, 105b, 109 e 109a).

ACT_202 A VU deve guardar dados permanentes de identificação (requisito 075).

ACT_203 A VU deve assegurar a responsabilização dos centros de ensaio pelas suas actividades (requisitos 098, 101 e 109).

ACT_204 A VU deve assegurar a responsabilização dos controladores pelas suas actividades (requisitos 102, 103 e 109).

ACT_205 A VU deve registar os dados odométricos (requisito 090) e os dados pormenorizados relativos à velocidade (requisito 093).

ACT_206 A VU deve assegurar que, uma vez registados, os dados de utilização (ou de utilizador) relacionados com os requisitos 081 a 093 e 102 a 105b, inclusive, não sejam modificados, excepto se atingirem antiguidade que justifique a sua substituição por dados novos.

ACT_207 A VU deve assegurar que não modificará dados já memorizados num cartão tacográfico (requisitos 109 e 109a), excepto para substituição de dados antigos por dados novos (requisito 110) ou no caso referido no apêndice 1 (secção 2.1, nota).

4.4. **Auditoria**

A capacidade de auditoria só é exigível em relação a incidentes que possam indicar manipulação ou tentativa de violação da segurança. Não é exigível para o exercício normal de direitos, ainda que com importância na perspectiva da segurança.

AUD_201 A VU deve registar, juntamente com os dados correlatos, os incidentes que ponham em causa a sua segurança (requisitos 094, 096 e 109).

AUD_202 Incidentes susceptíveis de afectar a segurança da VU:

— Tentativas de violação da segurança:

— falha da autenticação do sensor de movimentos

— falha da autenticação do cartão tacográfico

— mudança não autorizada de sensor de movimentos

— erro de integridade na introdução de dados relativos a um cartão

— erro de integridade de dados memorizados relativos a um utilizador

— erro de transferência interna de dados

— abertura não autorizada da caixa

— sabotagem do equipamento informático (hardware),

- Última sessão de cartão incorrectamente encerrada
- Incidente “erro nos dados de movimento”
- Incidente “interrupção da alimentação energética”
- Falha interna da VU.

AUD_203 A VU deve aplicar as regras de memorização dos registos de auditoria (requisitos 094 e 096).

AUD_204 A VU deve armazenar na sua memória (isto é, memorizar) os registos de auditoria gerados pelo sensor de movimentos.

AUD_205 Deve ser possível imprimir, visualizar e descarregar registos de auditoria.

4.5. *Reutilização de objectos*

REU_201 A VU deve assegurar que objectos de memorização temporária possam ser reutilizados sem que tal implique fluxos de informação inadmissíveis.

4.6. *Precisão*

4.6.1. *Política de controlo do fluxo de informação*

ACR_201 A VU deve assegurar que os dados de utilização (ou de utilizador) relacionados com os requisitos 081, 084, 087, 090, 093, 102, 104, 105, 105a e 109 só possam ser processados a partir das fontes correctas de entrada (ou seja, de input):

- dados de movimento do veículo,
- relógio de tempo real da VU,
- parâmetros de calibração do aparelho de controlo,
- cartões tacográficos,
- entradas do utilizador.

ACR_201a A VU deve assegurar que os dados de utilização aferentes ao requisito 109a só possam ser introduzidos relativamente ao período “última retirada/actual inserção do cartão” (requisito 050a).

4.6.2. *Transferências internas de dados*

O disposto nesta secção aplica-se somente se a VU for composta por peças fisicamente separadas.

ACR_202 Se forem transferidos entre peças da VU fisicamente separadas, os dados devem ser protegidos contra o risco de modificação.

ACR_203 Se se detectar algum erro durante uma transferência interna de dados, a transmissão deve ser repetida e a SEF gerará um registo de auditoria do incidente.

4.6.3. *Integridade dos dados memorizados*

ACR_204 A VU deve verificar a ocorrência de erros de integridade nos dados de utilização armazenados na sua memória.

ACR_205 Se detectar algum erro de integridade nos dados de utilização memorizados, a SEF deve gerar um registo de auditoria.

4.7. *Fiabilidade do serviço*

4.7.1. *Ensaaios*

RLB_201 Os comandos, acções e pontos de teste específicos dos requisitos de ensaio na fase de fabrico da VU devem ser todos desactivados ou removidos antes da activação da VU, não devendo ser possível restaurá-los para posterior reutilização.

RLB_202 A VU deve executar auto-ensaaios de funcionamento correcto quer durante o arranque quer durante o funcionamento normal. Os auto-ensaaios da VU incluirão uma verificação da integridade dos dados de segurança e uma verificação da integridade do código executável memorizado (se não estiver na ROM).

RLB_203 Se for detectada alguma falha interna no decurso dos auto-ensaaios, a SEF deve:

- gerar um registo de auditoria (falha interna da VU), excepto em modo de calibração
- preservar a integridade dos dados memorizados.

4.7.2. Suporte lógico

RLB_204 Não deve haver possibilidade de analisar ou esmiuçar (debug) o suporte lógico (software) no campo, depois de activada a VU.

RLB_205 As entradas (inputs) de fontes externas não devem ser aceites como código executável.

4.7.3. Protecção física

RLB_206 Se tiver sido projectada de modo a poder ser aberta, a VU deve detectar qualquer abertura da caixa, excepto em modo de calibração, mesmo sem alimentação energética externa durante um mínimo de 6 meses. Neste caso, a SEF gerará um registo de auditoria do incidente (é aceitável que o registo de auditoria seja gerado e memorizado após o restabelecimento da alimentação energética).

Se por concepção não puder ser aberta, a VU deve ser projectada de modo a poderem ser facilmente detectadas (por exemplo, por inspecção visual) tentativas de fraude física.

RLB_207 Uma vez activada, a VU deve detectar sabotagens (TBD pelo fabricante) do hardware (ou seja, do equipamento informático).

RLB_208 No caso *supra*, a SEF deve gerar um registo de auditoria e a VU deve: (TBD pelo fabricante).

4.7.4. Interrupções da alimentação energética

RLB_209 A VU deve detectar desvios dos valores especificados para a alimentação energética, incluindo o corte.

RLB_210 No caso *supra*, a SEF deve:

- gerar um registo de auditoria (excepto em modo de calibração)
- preservar o estado de segurança da VU
- manter as funções de segurança relacionadas com componentes ou processos ainda operacionais,
- preservar a integridade dos dados memorizados.

4.7.5. Condições de restabelecimento (reset)

RLB_211 Na eventualidade de interrupção na alimentação energética ou de paragem prematura de uma transacção, ou ainda em quaisquer situações de restabelecimento (reset conditions), a VU deve ser restaurada ou restabelecida (reset) sem choque.

4.7.6. Disponibilidade dos dados

RLB_212 A VU deve assegurar o acesso, sempre que requerido, aos recursos, e que os recursos não sejam requeridos nem retidos desnecessariamente.

RLB_213 A VU deve assegurar que os cartões não possam ser libertados antes de neles memorizados os dados pertinentes (requisitos 015 e 016).

RLB_214 No caso *supra*, a SEF deve gerar um registo de auditoria do incidente.

4.7.7. Aplicações múltiplas

RLB_215 Se a VU proporcionar aplicações para além da aplicação tacográfica, todas elas devem ser física e/ou logicamente separadas umas das outras. Estas aplicações não devem partilhar dados de segurança. Em cada momento, estará activada uma só função.

4.8. Intercâmbio de dados

A presente secção incide no intercâmbio de dados entre a VU e dispositivos a ela ligados.

4.8.1. Intercâmbio de dados com o sensor de movimentos

DEX_201 A VU deve verificar a integridade e a autenticidade dos dados de movimento importados do sensor de movimentos.

DEX_202 Ao ser detectado um erro de integridade ou autenticidade nos dados de movimento, a SEF deve:

- gerar um registo de auditoria
- continuar a utilizar os dados importados.

4.8.2. Intercâmbio de dados com os cartões tacográficos

DEX_203 A VU deve verificar a integridade e a autenticidade dos dados de movimento importados dos cartões tacográficos.

DEX_204 Ao ser detectado um erro de integridade ou autenticidade nos dados de um cartão, a SEF deve:

- gerar um registo de auditoria
- rejeitar a utilização dos dados.

DEX_205 A exportação de dados de movimento da VU para um cartão tacográfico inteligente deve ser efectuada com atributos de segurança associados, de modo a que o cartão possa verificar a integridade e a autenticidade desses dados.

4.8.3. Intercâmbio de dados com meios externos de memorização (função de descarregamento)

DEX_206 A VU deve gerar uma prova de origem dos dados descarregados para meios externos.

DEX_207 A VU deve proporcionar capacidade de verificação da prova de origem dos dados descarregados para o receptor.

DEX_208 O descarregamento de dados da VU para meios externos de memorização deve ser efectuado com atributos de segurança associados, de modo a poderem ser verificadas a integridade e a autenticidade desses dados.

4.9. Apoio criptográfico

O disposto nesta secção aplica-se somente quando necessário, dependendo dos mecanismos de segurança utilizados e das soluções do fabricante.

CSP_201 As operações criptográficas executadas pela VU devem obedecer a um algoritmo especificado e a uma dimensão especificada de chave criptográfica.

CSP_202 A eventual geração de chaves criptográficas pela VU deve obedecer a algoritmos especificados de geração e a dimensões especificadas das chaves.

CSP_203 A eventual distribuição de chaves criptográficas pela VU deve obedecer a métodos especificados de distribuição das chaves.

CSP_204 O eventual acesso a chaves criptográficas pela VU deve obedecer a métodos especificados de acesso às chaves.

CSP_205 A eventual destruição de chaves criptográficas pela VU deve obedecer a métodos especificados de destruição das chaves.

5. Definição de mecanismos de segurança

Os mecanismos de segurança requeridos são especificados no apêndice 11.

Todos os restantes mecanismos de segurança devem ser definidos pelos fabricantes.

6. Energia mínima dos mecanismos de segurança

A energia mínima dos mecanismos de segurança do sensor de movimentos é High ("elevada"), conforme definição da norma ITSEC.

7. Nível de garantia

O nível objectivado de garantia para a unidade-veículo é o nível ITSEC E3, conforme definição da norma ITSEC.

8. Síntese lógica

As matrizes que se seguem contêm uma síntese lógica das SEF, indicando:

- as SEF ou os meios e as correspondentes ameaças a que se contrapõem
- as SEF e os correspondentes objectivos de segurança IT por elas cumpridos.

	Ameaças																Objectivos IT												
	T.Access	T.Identification	T.Faults	T.Tests	T.Design	T.Calibration_Parameters	T.Card_Data_Exchange	T.Clock	T.Environment	T.Fake_Devices	T.Hardware	T.Motion_Data	T.Non_Activated	T.Output_Data	T.Power_Supply	T.Saturation	T.Security_Data	T.Software	T.Stored_Data	O.Access	O.Accountability	O.Audit	O.Authentication	O.Integrity	O.Output	O.Processing	O.Reliability	O.Secured_Data_Exchange	
Meios físicos, humanos ou processuais																													
Desenvolvimento			X	X	X																								
Fabrico				X	X																								
Entrega													X																
Activação	X											X																	
Geração de dados de segurança																	X												
Transporte de dados de segurança																	X												
Disponibilidade do cartão	X																												
Cartão de um só condutor	X																												
Rastreabilidade do cartão	X																												
Centros de ensaio homologados					X	X																							
Inspeção/calibração regular					X	X			X				X				X												
Centros de ensaio de confiança					X	X																							
Condutores de confiança	X																												
Controlos de aplicação da lei	X				X	X	X	X	X	X	X	X	X	X	X	X	X	X											
Actualizações do software																	X												
Funções de concretização da segurança																													
Identificação e autenticação																													
UIA_201 Identificação do sensor									X	X												X							X
UIA_202 Identidade do sensor								X	X													X							
UIA_203 Autenticação do sensor								X	X													X							X
UIA_204 Reidentificação e reautenticação do sensor								X	X													X							X
UIA_205 Autenticação infalsificável								X	X													X							
UIA_206 Falha da autenticação								X	X													X					X		
UIA_207 Identificação do utilizador	X	X						X										X				X							X
UIA_208 Identidade do utilizador	X	X						X										X				X							
UIA_209 Autenticação do utilizador	X	X						X										X				X							X
UIA_210 Reautenticação do utilizador	X	X						X										X				X							X
UIA_211 Meios de autenticação	X	X						X										X				X							
UIA_212 Verificações do PIN	X	X			X	X												X				X							
UIA_213 Autenticação infalsificável	X	X						X										X				X							

	Ameaças																Objectivos IT											
	T.Access	T.Identification	T.Faults	T.Tests	T.Design	T.Calibration_Parameters	T.Card_Data_Exchange	T.Clock	T.Environment	T.Fake_Devices	T.Hardware	T.Motion_Data	T.Non_Activated	T.Output_Data	T.Power_Supply	T.Saturation	T.Security_Data	T.Software	T.Stored_Data	O.Access	O.Accountability	O.Audit	O.Authentication	O.Integrity	O.Output	O.Processing	O.Reliability	O.Secured_Data_Exchange
UIA_214 Falha da autenticação	x	x							x												x							
UIA_215 Identificação de utilizador à distância	x	x																	x			x						x
UIA_216 Identidade de utilizador à distância	x	x																	x			x						
UIA_217 Autenticação de utilizador à distância	x	x																	x			x						x
UIA_218 Meios de autenticação	x	x																	x			x						
UIA_219 Autenticação infalsificável	x	x																	x			x						
UIA_220 Falha da autenticação	x	x																										
UIA_221 Identificação de dispositivo de gestão	x	x																	x			x						
UIA_222 Autenticação de dispositivo de gestão	x	x																	x			x						
UIA_223 Autenticação infalsificável	x	x																	x			x						
Controlo do acesso																												
ACC_201 Política de controlo do acesso	x					x	x										x		x	x								
ACC_202 Direitos de acesso a funções	x					x	x														x							
ACC_203 Direitos de acesso a funções	x					x	x														x							
ACC_204 ID da VU																				x	x							
ACC_205 ID do sensor conectado									x											x	x							
ACC_206 Dados de calibração	x					x														x	x							
ACC_207 Dados de calibração						x															x	x						
ACC_208 Dados ajustamento tempo							x														x	x						
ACC_209 Dados ajustamento tempo							x															x	x					
ACC_210 Dados de segurança																				x		x	x					
ACC_211 Estrutura do ficheiro e condições de acesso	x					x												x		x	x							
Responsabilização																												
ACT_201 Responsabilização de condutores																						x						
ACT_202 Dados de ID da VU																						x	x					
ACT_203 Responsabilização de centros de ensaio																						x						
ACT_204 Responsabilização de controladores																						x						
ACT_205 Responsabilização do movimento do veículo																						x						
ACT_206 Modificação de dados de responsabilização																					x				x			x
ACT_207 Modificação de dados de responsabilização																					x				x			x

OBJECTIVO GENÉRICO DE SEGURANÇA DO CARTÃO TACOGRÁFICO

1. Introdução

O presente documento contém uma descrição do cartão tacográfico (cartão de tacógrafo), das ameaças contra as quais ele deve poder actuar e dos objectivos de segurança que ele deve cumprir. Especifica igualmente as funções exigíveis de concretização da segurança, bem como a energia mínima dos mecanismos de segurança e o necessário nível de garantia no desenvolvimento e na avaliação do cartão.

Os requisitos referidos neste documento são os que constam do anexo I B. Por motivos de clareza na leitura, registam-se algumas duplicações entre os requisitos do anexo I B e os requisitos dos objectivos de segurança. Em caso de ambiguidade entre um requisito dos objectivos de segurança e o requisito do anexo I B referido por esse requisito dos objectivos de segurança, prevalece o requisito do anexo I B.

Os requisitos do anexo I B não referidos por objectivos de segurança não são objecto de funções de concretização da segurança.

Um cartão de tacógrafo é um cartão inteligente normalizado que comporta uma aplicação tacográfica dedicada e que deve cumprir os requisitos actualizados de segurança e funcionalidade aplicáveis aos cartões inteligentes. Por conseguinte, este objectivo de segurança incorpora apenas os requisitos extraordinários de segurança necessários à aplicação tacográfica.

Às ameaças, aos objectivos, aos meios processuais e às especificações de funções de concretização da segurança foram assignadas etiquetas únicas, para efeitos de rastreabilidade dos documentos de desenvolvimento e avaliação.

2. Abreviaturas, definições e referências**2.1. Abreviaturas**

IC	Integrated circuit (circuito integrado: componente electrónico destinado a executar funções de processamento e/ou memorização)
OS	Operating system (sistema operativo)
PIN	Personal identification number (número de identificação pessoal)
ROM	Read only memory (memória exclusivamente de leitura; memória morta)
SFP	Security functions policy (política das funções de segurança)
TBD	To be defined (a definir)
TOE	Target of evaluation (objectivo de avaliação)
TSF	TOE security function (função de segurança do TOE)
VU	Vehicle unit (unidade-veículo; unidade montada num veículo)

2.2. Definições

Tacógrafo digital	Aparelho de controlo
Dados sensíveis	Dados memorizados pelo cartão tacográfico e que têm de ser protegidos para efeitos de integridade, modificação não autorizada e confidencialidade (se aplicável a dados de segurança). Os dados sensíveis incluem os dados de segurança e os dados de utilização
Dados de segurança	Os dados específicos necessários para apoiar as funções de concretização da segurança (por exemplo, chaves criptadas)
Sistema	Equipamento, pessoas ou organizações que de algum modo tenham a ver com o aparelho de controlo
Utilizador	Qualquer entidade (pessoa ou entidade IT externa), exterior ao TOE mas que interage com ele

Dados de utilização	Dados sensíveis memorizados no cartão tacográfico, com excepção dos dados de segurança. Os dados de utilização incluem os dados de identificação e os dados de actividade
Dados de identificação	Os dados de identificação incluem os dados de identificação do cartão e os dados de identificação do titular do cartão
Dados de identificação do cartão	Dados de utilização relativos à identificação do cartão, conforme definição nos requisitos 190, 191, 192, 194, 215, 231 e 235
Dados de identificação do titular do cartão	Dados de utilização relativos à identificação do titular do cartão, conforme definição nos requisitos 195, 196, 216, 232 e 236
Dados de actividade	Os dados de actividade incluem os dados relativos às actividades do titular do cartão, os dados relativos a incidentes e falhas e os dados relativos à actividade de controlo
Dados de actividade do titular do cartão	Dados de utilização relativos às actividades executadas pelo titular do cartão, conforme definição nos requisitos 197, 199, 202, 212, 212a, 217, 219, 221, 226, 227, 229, 230a, 233 e 237
Dados relativos a incidentes e falhas	Dados de utilização relativos a incidentes ou falhas, conforme definição nos requisitos 204, 205, 207, 208 e 223
Dados relativos à actividade de controlo	Dados de utilização relativos à aplicação da regulamentação, conforme definição nos requisitos 210 e 225

2.3. Referências

ITSEC	ITSEC Information Technology Security Evaluation Criteria ("Critérios de Avaliação da Segurança nas Tecnologias da Informação"), 1991
IC PP	Smartcard Integrated Circuit Protection Profile — versão 2.0 — edição de Setembro de 1998. Registado no organismo francês de certificação com o número PP/9806
ES PP	Smart Card Integrated Circuit With Embedded Software Protection Profile — versão 2.0 — edição de Junho de 1999. Registado no organismo francês de certificação com o número PP/9911.

3. Características do produto

3.1. Descrição e método de utilização do cartão tacográfico

Um cartão tacográfico é um cartão inteligente (ver referências IC PP e ES PP) que comporta uma aplicação destinada à sua utilização com o aparelho de controlo.

Funções básicas do cartão tacográfico:

- Memorizar os dados de identificação do cartão e do seu titular. Estes dados são utilizados pela unidade-veículo (VU) para identificar o titular do cartão, facultar correspondentemente funções e direitos de acesso a dados e assegurar a responsabilização do titular do cartão pelas suas actividades.
- Memorizar os dados relativos às actividades do titular do cartão, a incidentes e falhas e às actividades de controlo relacionadas com o titular.

Por conseguinte, um cartão tacográfico destina-se a ser utilizado por um dispositivo de interface na VU. Pode também ser utilizado por qualquer leitor de cartões (por exemplo, um computador pessoal), o qual deve dispor de direitos plenos de acesso à leitura de dados de utilização.

Na fase de utilizador final do ciclo de vida de um cartão tacográfico (fase 7 do ciclo, ver referência ES PP), as unidades-veículo podem somente escrever dados de utilização no cartão.

Os requisitos de funcionamento de um cartão tacográfico são especificados no anexo I B e no apêndice 2.

3.2. Ciclo de vida de um cartão tacográfico

O ciclo de vida de um cartão tacográfico corresponde ao descrito na referência ES PP.

3.3. Ameaças

Para além das ameaças gerais aos cartões inteligentes enunciadas nas referências IC PP e ES PP, o cartão tacográfico pode enfrentar as seguintes:

3.3.1. Intenções últimas

A intenção última de um ataque consistirá em modificar os dados de utilização memorizados no TOE.

T.Ident_Data	Uma modificação bem sucedida nos dados de identificação guardados pelo TOE (por exemplo, dados sobre o tipo e o prazo de validade do cartão ou sobre a identificação do seu titular) permitiria a utilização fraudulenta do TOE e constituiria uma ameaça drástica ao objectivo global de segurança do sistema.
T.Activity_Data	Uma modificação bem sucedida nos dados de actividade memorizados no TOE constituiria uma ameaça à segurança do TOE.
T.Data_Exchange	Uma modificação bem sucedida (adição, apagamento, alteração) nos dados relativos à actividade, durante as suas importação ou exportação, constituiria uma ameaça à segurança do TOE.

3.3.2. Vias de ataque

Os activos do TOE podem ser atacados através das seguintes vias:

- tentativa de obtenção de conhecimento ilícito sobre o equipamento informático e o suporte lógico do TOE e, em especial, sobre os seus dados ou funções de segurança. O conhecimento ilícito pode ser obtido por meio de ataques ao material de projecto ou de fabrico (furto, suborno, etc.) ou por meio do exame directo do TOE (ensaio físico, análise de inferência, etc.);
- aproveitamento de fragilidades na concepção ou na construção do TOE (erros no equipamento informático e no suporte lógico, falhas de transmissão, erros induzidos no TOE por pressões ambientais, vulnerabilidades nas funções de segurança, como procedimentos de autenticação, controlo do acesso a dados, operações criptográficas, etc.);
- modificação do TOE ou das suas funções de segurança por meio de ataques físicos, eléctricos ou lógicos ou combinações deles.

3.4. Objectivos de segurança

É o seguinte o principal objectivo de segurança do sistema tacográfico digital:

O.Main	Os dados a verificar pelas autoridades responsáveis pelo controlo devem estar disponíveis e reflectir plenamente e com rigor as actividades dos condutores e dos veículos sujeitos a controlo, no atinente a condução, trabalho, disponibilidade, períodos de repouso e velocidade do veículo.
--------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Portanto, o objectivo de segurança do TOE, que contribui para aquele objectivo de segurança genérico, é o seguinte:

O.Card_Identification_Data	O TOE deve preservar os dados de identificação do cartão e do titular do cartão, memorizados durante o processo de personalização do cartão.
O.Card_Activity_Storage	O TOE deve preservar os dados de utilização memorizados no cartão pelas unidades-veículo.

3.5. Objectivos de segurança próprios das tecnologias da informação

Para além dos objectivos genéricos de segurança dos cartões inteligentes, enunciados nas referências IC PP e ES PP, são os seguintes os objectivos de segurança do TOE, próprios das IT, que contribuem para os objectivos genéricos de segurança do TOE durante a fase de utilizador final do seu ciclo de vida:

O.Data_Access	O TOE deve limitar a unidades-veículo autenticadas os direitos de acesso à escrita de dados de utilização.
O.Secure_Communications	Sempre que a aplicação o exija, o TOE deve poder apoiar protocolos e procedimentos de comunicação segura entre o cartão e o dispositivo de interface.

3.6. Meios físicos, humanos e processuais

Os requisitos físicos, humanos e processuais que contribuem para a segurança do TOE constam das referências IC PP e ES PP (capítulos relativos aos objectivos de segurança para o ambiente).

4. Funções de concretização da segurança

A presente secção explica algumas das operações permitidas, como a atribuição ou instrução (assignment) e a selecção (selection), da referência ES PP, e apresenta alguns requisitos adicionais para o funcionamento da SEF.

4.1. Cumprimento dos perfis de protecção

CPP_301 O TOE deve cumprir o disposto na referência IC PP.

CPP_302 O TOE deve cumprir o disposto na referência ES PP, conforme explicação adiante.

4.2. Identificação e autenticação do utilizador

O cartão deve identificar a entidade na qual está inserido e saber se se trata ou não de uma VU autenticada. Pode exportar quaisquer dados de utilização independentemente da entidade à qual estiver conectado, excepto se se tratar de um cartão de controlo, que pode exportar dados de identificação do titular unicamente para unidades-veículo autenticadas (de modo a um controlador, vendo o seu nome no visor ou na impressão, poder certificar-se de que a VU não está falsificada).

4.2.1. Identificação do utilizador

Assignment (FIA_UID.1.1) *Lista de acções mediadas pelo TSF*: nenhuma.

Assignment (FIA_ATD.1.1) *Lista de atributos de segurança*:

- USER_GROUP: VEHICLE_UNIT, NON_VEHICLE_UNIT,
- USER_ID: Número de registo do veículo (VRN) e código do Estado-Membro de registo (USER_ID é conhecido somente quando USER_GROUP = VEHICLE_UNIT).

4.2.2. Autenticação do utilizador

Assignment (FIA_UAU.1.1) *Lista de acções mediadas pelo TSF*:

- Cartões de condutor e de centro de ensaio: exportação de dados de utilização com atributos de segurança (função de descarregamento de dados do cartão),
- Cartão de controlo: exportação de dados de utilização sem atributos de segurança, com excepção dos dados de identificação do titular.

UIA_301 A autenticação de uma VU deve ser efectuada por comprovação em como a unidade é detentora de dados de segurança que somente o sistema poderia distribuir.

Selection (FIA_UAU.3.1 e FIA_UAU.3.2): evitar.

Assignment (FIA_UAU.4.1) *Mecanismo(s) identificado(s) de autenticação*: qualquer mecanismo de autenticação.

UIA_302 O cartão de centro de ensaio deve proporcionar um mecanismo adicional de autenticação mediante a verificação de um código PIN (mecanismo destinado a que a VU assegure a identidade do titular do cartão, e não a proteger o conteúdo deste último).

4.2.3. Falhas na autenticação

As atribuições ou instruções (assignments) que se seguem descrevem a reacção do cartão a cada falha na autenticação de um utilizador:

Assignment (FIA_AFL.1.1) *Número: 1, lista de incidentes de autenticação*: autenticação de um dispositivo de interface de cartão.

Assignment (FIA_AFL.1.2) *Lista de acções*:

- avisar (alertar) a entidade conectada,
- considerar o utilizador como NON_VEHICLE_UNIT.

As atribuições ou instruções (assignments) que se seguem descrevem a reacção do cartão em caso de falha do mecanismo adicional de autenticação requerido em UIA_302:

Assignment (FIA_AFL.1.1) *Número: 5, lista de incidentes de autenticação*: verificações do código PIN (cartão de centro de ensaio).

Assignment (FIA_AFL.1.2) *Lista de acções:*

- avisar (alertar) a entidade conectada,
- bloquear o procedimento de verificação do PIN de modo a falhar qualquer subsequente tentativa de verificação do PIN,
- poder indicar a utilizadores subsequentes a razão do bloqueamento.

4.3. **Controlo do acesso**

4.3.1. *Política de controlo do acesso*

Na fase de utilizador final do seu ciclo de vida, o cartão tacográfico é objecto de uma só Security Function Policy (“política de função de segurança” ou SFP) para controlo do acesso, designada AC_SFP.

Assignment (FDP_ACC.2.1) *SFP de controlo do acesso:* AC_SFP.

4.3.2. *Funções de controlo do acesso*

Assignment (FDP_ACF.1.1) *Controlo do acesso:* AC_SFP.

Assignment (FDP_ACF.1.1) *Grupo nomeado de atributos de segurança:* USER_GROUP.

Assignment (FDP_ACF.1.2) *Regras de acesso entre sujeitos controlados e objectos controlados que efectuam operações controladas sobre objectos controlados:*

- GENERAL_READ: Os dados de utilização podem ser lidos do TOE por qualquer utilizador, com excepção dos dados de identificação do titular do cartão, que só podem ser lidos dos cartões de controlo por VEHICLE_UNIT.
- IDENTIF_WRITE: Os dados de identificação só podem ser escritos uma vez e antes da fase 6 do ciclo de vida do cartão. Nenhum utilizador pode escrever ou modificar dados de identificação durante a fase de utilizador final do referido ciclo.
- ACTIVITY_WRITE: Os dados de actividade só podem ser escritos no TOE por VEHICLE_UNIT.
- SOFT_UPGRADE: Nenhum utilizador pode reformar (upgrade) o suporte lógico (software) do TOE.
- FILE_STRUCTURE: A estrutura dos ficheiros e as condições de acesso devem ser criadas antes de terminar a fase 6 do ciclo de vida do TOE, bloqueando-se em seguida a possibilidade de quaisquer modificações ou apagamento subsequentes.

4.4. **Responsabilização**

ACT_301 O TOE deve guardar dados permanentes de identificação.

ACT_302 Deve ser dada uma indicação sobre a hora e a data da personalização do TOE. Essa indicação deve permanecer inalterável.

4.5. **Auditoria**

O TOE deve acompanhar (monitor) os incidentes que indiquem potencial violação da sua segurança.

Assignment (FAU_SAA.1.2) *Subconjunto de incidentes definidos passíveis de auditoria:*

- falha na identificação do titular do cartão (5 verificações sucessivas e infrutíferas do PIN),
- erro de auto-ensaio,
- erro de integridade dos dados memorizados,
- erro de integridade dos dados de actividade introduzidos.

4.6. **Precisão**

4.6.1. *Integridade dos dados memorizados*

Assignment (FDP_SDI.2.2) *Acções a emprender:* alertar a entidade conectada.

4.6.2. *Autenticação de dados de base*

Assignment (FDP_DAU.1.1) *Lista de objectos ou tipos de informação:* Dados de actividade.

Assignment (FDP_DAU.1.2) *Lista de sujeitos:* Quaisquer.

4.7. *Fiabilidade do serviço*

4.7.1. *Ensaaios*

Selection (FPT_TST.1.1): no arranque e periodicamente durante o funcionamento normal.

Nota: “no arranque” significa antes de executado o código (e não necessariamente durante o procedimento Answer To Reset).

RLB_301 Os auto-ensaaios do TOE devem incluir a verificação da integridade de todos os códigos informáticos não memorizados na ROM.

RLB_302 Ao detectar um erro de auto-ensaio, a TSF deve alertar a entidade conectada.

RLB_303 Terminado o ensaio do sistema, os comandos e acções específicos de ensaio devem ser todos desactivados ou removidos. Não deve ser possível contornar estes controlos ou restaurá-los para reutilização. Durante uma determinada fase do ciclo de vida, nunca deve ser possível o acesso a um comando associado exclusivamente a outra fase.

4.7.2. *Suporte lógico*

RLB_304 Não deve haver possibilidade de analisar, esmiuçar (debug) ou modificar o suporte lógico (software) do TOE no campo.

RLB_305 As entradas (inputs) de fontes externas não devem ser aceites como código executável.

4.7.3. *Alimentação energética*

RLB_306 O TOE deve preservar um estado de segurança durante cortes ou variações na alimentação energética.

4.7.4. *Condições de restabelecimento (reset)*

RLB_307 Na eventualidade de interrupção (ou de variação) na alimentação energética do TOE ou de paragem prematura de uma transacção, ou ainda em quaisquer situações de restabelecimento (reset conditions), o TOE deve ser restaurado ou restabelecido (reset) sem choque.

4.8. *Intercâmbio de dados*

4.8.1. *Intercâmbio de dados com uma unidade-veículo*

DEX_301 O TOE deve verificar a integridade e a autenticidade dos dados importados de uma VU.

DEX_302 Ao ser detectado um erro de integridade em dados importados, o TOE deve:

- alertar a entidade conectada,
- renunciar a utilizar os dados.

DEX_303 O TOE deve exportar dados de utilização para a VU com atributos de segurança associados, para que a VU possa verificar a integridade e a autenticidade deles.

4.8.2. *Exportação de dados para uma unidade não montada em veículo (função de descarregamento)*

DEX_304 O TOE deve gerar uma prova de origem dos dados descarregados para meios externos.

DEX_305 O TOE deve proporcionar capacidade de verificação da prova de origem dos dados descarregados para o receptor.

DEX_306 O descarregamento de dados do TOE para meios externos de memorização deve ser efectuado com atributos de segurança associados, de modo a poder ser verificada a integridade desses dados.

4.9. *Apoio criptográfico*

CSP_301 A eventual geração de chaves criptográficas de sessão pela TSF deve obedecer a algoritmos especificados de geração e a dimensões especificadas das chaves. As chaves geradas devem ter um número limitado de utilizações possíveis (TBD pelo fabricante, mas não mais de 240).

CSP_302 A eventual distribuição de chaves criptográficas pela TSF deve obedecer a métodos especificados de distribuição das chaves.

5. *Definição de mecanismos de segurança*

Os mecanismos de segurança requeridos são especificados no apêndice 11.

Todos os restantes mecanismos de segurança devem ser definidos pelo fabricante do TOE.

Apêndice 11

MECANISMOS COMUNS DE SEGURANÇA

1. GENERALIDADES

O presente apêndice especifica os mecanismos de segurança que garantem:

- a autenticação mútua entre unidades-veículo (VU) e cartões tacográficos, incluindo concordância entre chaves de sessão (session key agreement),
- a confidencialidade, a integridade e a autenticação dos dados transferidos entre as VU e os cartões tacográficos,
- a integridade e a autenticação dos dados descarregados das VU para meios de memorização externos,
- a integridade e a autenticação dos dados descarregados dos cartões tacográficos para meios de memorização externos.

1.1. Referências

No presente apêndice, são utilizadas as seguintes referências:

SHA-1	National Institute of Standards and Technology (Instituto Nacional de Normas e Tecnologia, USA NIST). FIPS Publication 180-1: Secure Hash Standard. Abril 1995
PKCS1	RSA Laboratories. PKCS # 1: RSA Encryption Standard. Versão 2.0. Outubro 1998
TDES	National Institute of Standards and Technology (NIST). FIPS Publication 46-3: Data Encryption Standard. Projecto de norma 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/CEI 7816-4	Tecnologia de Informação — Cartões de identificação — Cartões de circuito(s) integrado(s) com contactos — 4. ^a parte: Comandos para intercâmbio intersectorial. 1. ^a edição: 1995 + 1. ^a emenda: 1997
ISO/CEI 7816-6	Tecnologia de Informação — Cartões de identificação — Cartões de circuito(s) integrado(s) com contactos — 6. ^a parte: Elementos de dados intersectoriais. 1. ^a edição: 1996 + 1. ^a cor: 1998
ISO/CEI 7816-8	Tecnologia de Informação — Cartões de identificação — Cartões de circuito(s) integrado(s) com contactos — 8. ^a parte: Comandos intersectoriais de segurança. 1. ^a edição: 1999
ISO/CEI 9796-2	Tecnologia de Informação — Técnicas de segurança — Sistemas de assinatura digital para recuperação de mensagens — 2. ^a parte: Mecanismos que utilizam uma função de Hash. 1. ^a edição: 1997
ISO/CEI 9798-3	Tecnologia de Informação — Técnicas de segurança — Mecanismos de autenticação de entidades — 3. ^a parte: Autenticação da entidade por meio de um algoritmo de chave pública. 2. ^a edição: 1998
ISO 16844-3	Veículos rodoviários — Sistemas tacográficos — 3. ^a parte: Interface do sensor de movimentos

1.2. Notações e abreviaturas

No presente apêndice, são utilizadas as seguintes notações e abreviaturas:

(K_a, K_b, K_c)	Feixe de chaves utilizado pelo algoritmo triplo de criptagem dos dados
CA	Organismo certificador ou homologador
CAR	Referência do organismo certificador
CC	Soma criptográfica de controlo
CG	Criptograma
CH	Cabeçalho de comando
CHA	Autorização do titular de um certificado
CHR	Referência do titular de um certificado
D()	Decifragem com DES (Data Encryption Standard)
DE	Elemento de dados
DO	Objecto de dados
d	Chave privada/expoente privado RSA
e	Chave pública/expoente público RSA
E()	Criptagem com DES
EQT	Equipamento ou aparelho
Hash()	Valor Hash (saído de Hash)
Hash	Função de 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 centro de ensaio
m	Representante de mensagem (número inteiro entre 0 e $n-1$)
n	Chaves RSA, módulo
PB	Bytes de enchimento
PI	Byte indicador de enchimento (utilizado em criptograma para DO de confidencialidade)
PV	Valor simples (directo)
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
TDEA	Algoritmo triplo de criptagem dos dados
TLV	Comprimento dos marcadores ou etiquetas (tags)
VU	Unidade-veículo
X.C	Certificado do utilizador X, emitido por um organismo certificador
X.CA	Organismo certificador (ou homologador) 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 infix, cujo operando esquerdo é a chave pública de um organismo certificador, e cujo operando direito é o certificado emitido por esse organismo certificador. 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 uma informação I, utilizando a chave pública do utilizador X
X.SK	Chave privada RSA de um utilizador X
X.SK[I]	Cifragem RSA de uma informação 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 devem utilizar 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,
- assinatura digital de dados descarregados das VU ou dos cartões tacográficos para meios de memorização externos.

CSM_002 As unidades-veículo (VU) e os cartões tacográficos devem utilizar 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:

$$X.SK[m] = s = m^d \text{ mod } n$$

$$X.PK[s] = m = s^e \text{ mod } n$$

A referência PKCS1 contém uma descrição mais completa da função RSA.

2.2.2. Algoritmo Hash

CSM_004 Os mecanismos de assinatura digital devem utilizar o algoritmo Hash definido na referência SHA-1.

2.2.3. Algoritmo de criptagem dos dados

CSM_005 Os algoritmos de base DES devem ser utilizados no modo de funcionamento por cifragem progressiva.

3. CHAVES E CERTIFICADOS

3.1. Criação e distribuição de chaves

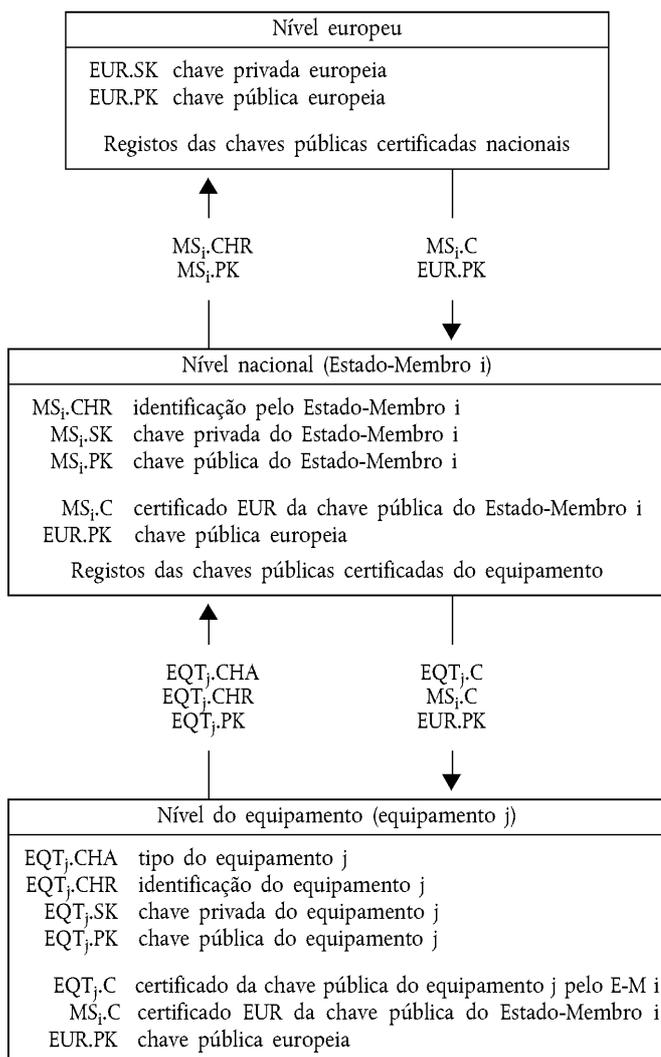
3.1.1. Criação e distribuição de chaves RSA

CSM_006 As chaves RSA devem ser criadas segundo três níveis hierárquicos de funcionamento:

- nível europeu,
- nível nacional,
- nível do equipamento ou aparelho.

- CSM_007 A nível europeu, é criado um único par de chaves (EUR.SK e EUR.PK). A chave privada europeia é utilizada para certificar (ou seja, homologar) as chaves públicas dos Estados-Membros. Devem ser mantidos registos de todas as chaves certificadas. Estas funções são asseguradas por um organismo europeu de certificação (ou de homologação), sob a autoridade e a responsabilidade da Comissão Europeia.
- CSM_008 A nível nacional (ou nível de Estado-Membro), é criado um par de chaves (MS.SK e MS.PK) para cada Estado-Membro. As chaves públicas dos Estados-Membros são certificadas pelo organismo europeu de certificação. A chave privada de um Estado-Membro é utilizada 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 um organismo nacional de certificação. Um Estado-Membro pode modificar regularmente o seu par 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. As chaves públicas do equipamento são certificadas pelo organismo nacional de certificação. 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 ser mantida a confidencialidade das chaves privadas.

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 (ensaio de interoperabilidade incluídos), o organismo europeu de certificação deve criar um outro par único de chaves europeias de ensaio e pelo menos dois pares de chaves nacionais de ensaio, cujas chaves públicas serão certificadas com a chave privada europeia de ensaio. Os fabricantes devem introduzir, no equipamento que é objecto 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 geração, o eventual transporte e o armazenamento.

Para que os aparelhos de controlo cumpram a norma ISO 16844, as autoridades competentes em matéria de certificação e a nível europeu e a nível de cada Estado-Membro devem, complementarmente, assegurar o seguinte:

CSM_036 A autoridade europeia de certificação gera $K_{m_{VU}}$ e $K_{m_{WC}}$, duas chaves Triple DES independentes e únicas, e gera K_m como:

$$K_m = K_{m_{VU}} \text{ XOR } K_{m_{WC}}$$

Mediante um procedimento adequadamente securizado, envia seguidamente estas chaves às autoridades de certificação de cada Estado-Membro, a seu pedido.

CSM_037 A autoridade de certificação de cada Estado-Membro:

- utiliza K_m 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 $K_{m_{VU}}$ aos fabricantes de unidades-veículo, para inserção nestas últimas,
- assegura a inserção de $K_{m_{WC}}$ em todos os cartões de centro de ensaio (`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 devem criar e intercambiar os dados necessários para elaborar uma chave de sessão DES tripla comum. A confidencialidade deste intercâmbio de dados deve ser protegida por meio de um mecanismo de criptagem RSA.

CSM_013 Esta chave será utilizada 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 ao cabo de 240 utilizações (uma utilização da chave = um comando que utilize o envio seguro de mensagens, transmitido ao cartão e seguido da correspondente resposta).

3.2. Chaves

CSM_014 Independentemente do nível, as chaves RSA devem ter os seguintes comprimentos: módulo n : 1024 bits; expoente público e : 64 bits no máximo; expoente privado d : 1024 bits.

CSM_015 As chaves triplas DES devem ter 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 detecção de erros de paridade.

3.3. Certificados

CSM_016 Os certificados de chaves públicas RSA devem ser non self descriptive ("não autodescritivos") e card verifiable ("verificáveis por cartão") (Ref.: ISO/CEI 7816-8).

3.3.1. *Conteúdo de um certificado*

CSM_017 Os certificados de chaves públicas devem conter 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 do organismo certificador
CHA	CADEIA DE OCTETOS	7	Autorização do titular do certificado
EOV	Tempo real	4	Prazo de validade do certificado. Opcional. Preenchido com 'FF' se não for utilizado
CHR	CADEIA DE OCTETOS	8	Referência do titular do certificado
<i>n</i>	CADEIA DE OCTETOS	128	Chave pública (módulo)
<i>e</i>	CADEIA DE OCTETOS	8	Chave pública (expoente público)
		164	

Notas:

- O “identificador de perfil do certificado” (CPI) indica a estrutura exacta 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 da lista extensa	Comprimento da lista	Marcador do CPI	Comprimento do CPI	Marcador da CAR	Comprimento da CAR	Marcador da CHA	Comprimento da CHA	Marcador do EOV	Comprimento do EOV	Marcador da CHR	Comprimento da CHR	Marcador da chave pública (constituído)	Comprimento de DO subsequentes	Marcador do módulo	Comprimento do módulo	Marcador do expoente público	Comprimento do exp. púb.

- A “referência do organismo certificador” (CAR) destina-se a identificar a autoridade emissora do certificado, de modo que o elemento de dado possa ser utilizado ao mesmo tempo como identificador de chave de autoridade para referenciar a chave pública do organismo certificador (relativamente à codificação, ver, adiante, identificador de chave).
- 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 dado EquipmentType, “00” para um Estado-Membro).
- A “referência do titular do certificado” (CHR) destina-se a identificar como único o titular do certificado, de modo que o elemento de dado possa ser utilizado ao mesmo tempo como identificador de chave de sujeito para referenciar a chave pública do titular do certificado.
- Os identificadores de chave identificam como únicos os titulares de certificados e os organismos certificadores. 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	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, ao organismo certificador do Estado-Membro competente. Deste modo, o certificado conterá a identificação do aparelho, e o fabricante deve velar por que chaves e certificado sejam inseridos no aparelho pertinente. 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, ao organismo certificador do Estado-Membro competente. 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	Codificação BCD	Codificação BCD mm aa	'FF'	Código do fabricante

5.2. Organismo certificador:

Dados	Identificação do organismo	Número de série da chave	Dados adicionais	Identificador
Comprimento	4 bytes	1 bytes	2 byte	1 byte
Valor	1 byte código numérico nacional 3 bytes código alfanumérico nacional	Inteiro	Codificação adicional (específica do 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 devem saber implicitamente que a chave pública certificada é uma chave RSA destinada a autenticação e a verificação e cifragem da assinatura digital para efeitos de confidencialidade (o certificado não contém qualquer identificador de objecto 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/CEI 9796-2, tendo apenas a "referência do organismo certificador".

$$X.C = X.CA.SK['6A' || C_r || Hash(Cc) || 'BC'] || C_n || X.CAR$$

$$\text{Conteúdo de certificado} = Cc = \begin{matrix} C_r & || & C_n \\ 106 \text{ bytes} & & 58 \text{ bytes} \end{matrix}$$

Notas:

1. Este certificado tem 194 bytes de comprimento.
2. A CAR oculta pela assinatura é também apenas a esta, de modo a que a chave pública do organismo certificador possa ser seleccionada para a verificação do certificado.
3. O verificador deve conhecer implicitamente o algoritmo utilizado pelo organismo certificador 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 de CV (constituído)	Comprimento de DO subsequentes	Marcador da assinatura	Comprimento da assinatura	Marcador remanescente	Comprimento remanescente	Marcador da CAR	Comprimento da CAR

3.3.3. Verificação e revelação de certificados

A verificação e a revelação de um certificado consiste em verificar se a assinatura obedece à norma ISO/CEI 9796-2, extraíndo o conteúdo do certificado e a chave pública contida ($X.PK = X.CA.PK_oX.C$) e verificando a validade do certificado.

CSM_019 Esta operação inclui os seguintes passos:

Verificação da assinatura e extracção do conteúdo:

— de X.C, extrair Sign, C_n' e CAR': $X.C = \begin{matrix} \text{Sign} \\ 128 \text{ bytes} \end{matrix} \parallel \begin{matrix} C_n' \\ 58 \text{ bytes} \end{matrix} \parallel \begin{matrix} \text{CAR}' \\ 8 \text{ bytes} \end{matrix}$

— a partir de CAR', seleccionar a pertinente chave pública do organismo certificador (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 Cr' e H' a partir de: $Sr' = \begin{matrix} '6A' \\ 106 \text{ bytes} \end{matrix} \parallel \begin{matrix} C_r' \\ 20 \text{ bytes} \end{matrix} \parallel \begin{matrix} H' \\ 20 \text{ bytes} \end{matrix} \parallel \begin{matrix} 'BC' \end{matrix}$

— recuperar o conteúdo do certificado $C' = C_r' \parallel C_n'$

— 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 aplicável, 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:

— $X.PK = n \parallel e$

— $X.KID = CHR$

— $X.CHA = CHA$

— $X.EOV = EOV$

4. MECANISMO DE AUTENTICAÇÃO MÚTUA

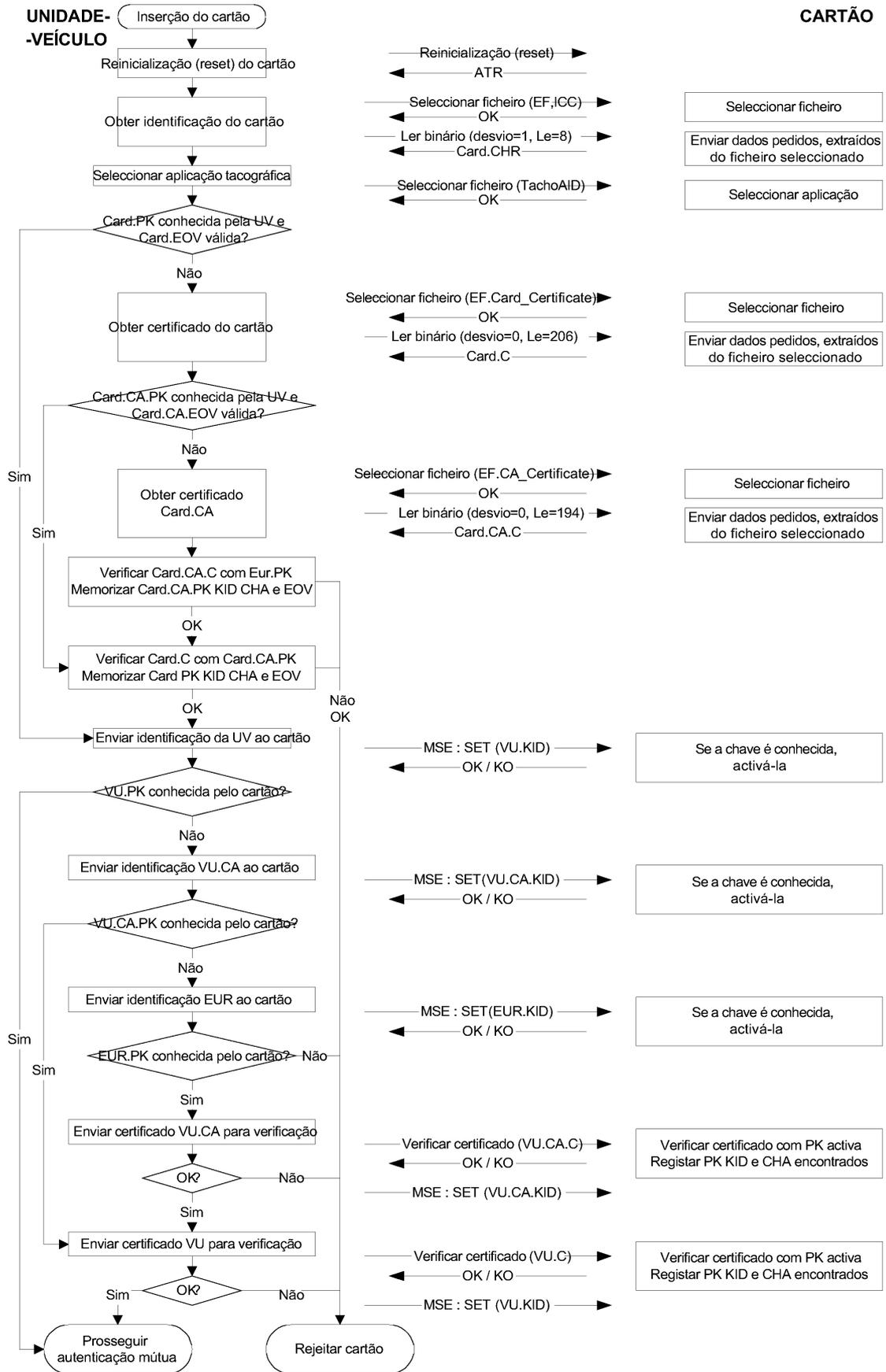
A autenticação mútua entre cartões e unidades-veículo baseia-se no seguinte princípio:

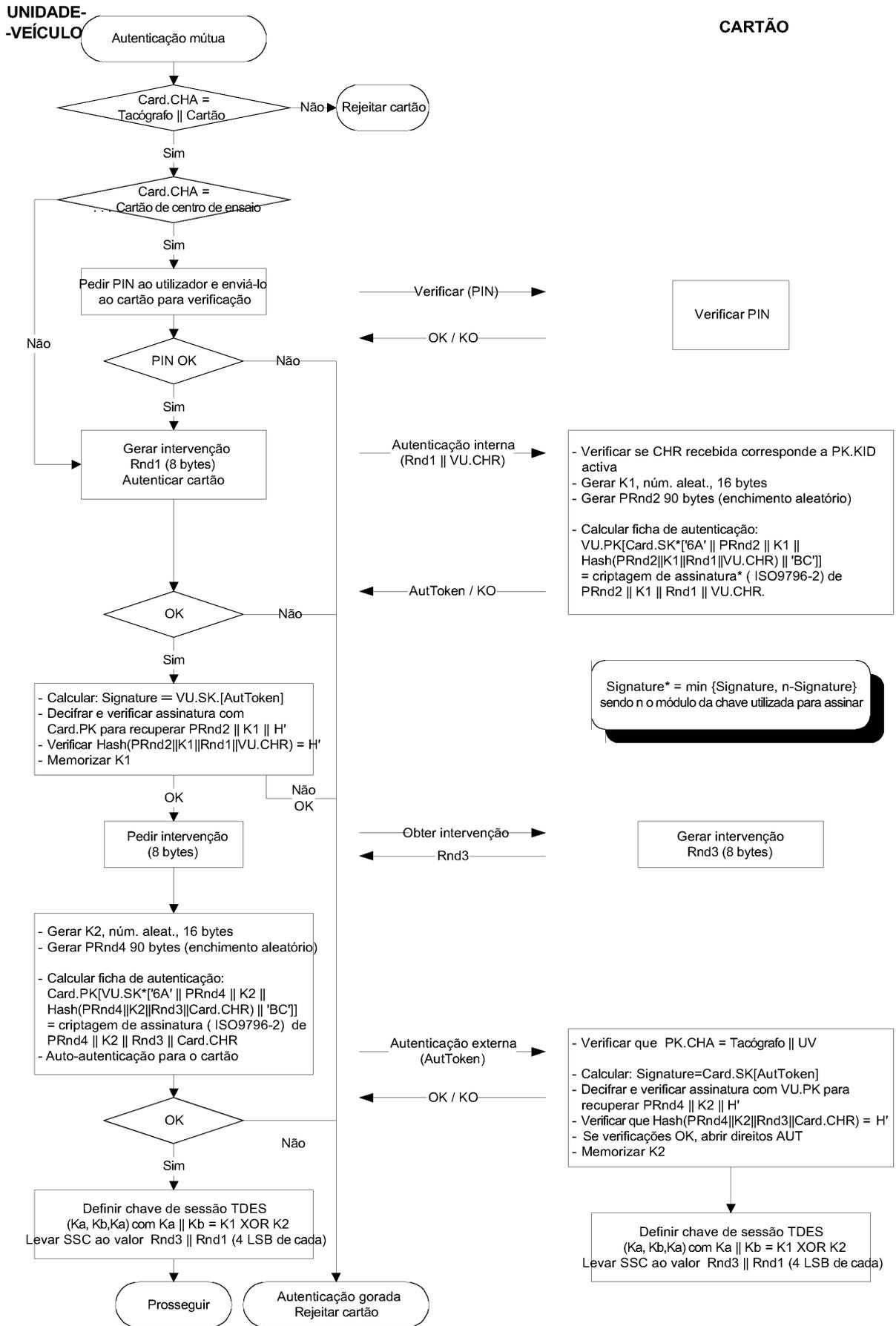
Cada parte deve demonstrar à outra parte que possui um par válido de chaves, no qual a chave pública foi certificada pelo organismo certificador do Estado-Membro pertinente, por sua vez certificado pelo organismo certificador europeu.

A demonstração é feita assinando com a chave privada um número aleatório enviado pela outra parte, a qual deve recuperar esse número quando verificar 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.

CSM_020 Utiliza-se o seguinte protocolo (as setas indicam comandos e dados intercambiados — ver apêndice 2):





5. MECANISMOS DE CONFIDENCIALIDADE, INTEGRIDADE E AUTENTICAÇÃO NA TRANSFERÊNCIA DE DADOS ENTRE UNIDADES-VEÍCULO E CARTÕES

5.1. **Segurança do envio de mensagens (envio seguro de mensagens)**

- CSM_021 A integridade das transferências de dados entre as VU e os cartões deve ser protegida mediante o mecanismo de segurança do envio de mensagens, em conformidade com as normas ISO/CEI 7816-4 e ISO/CEI 7816-8.
- CSM_022 Se for necessário proteger os dados durante a transferência, apende-se um objecto de dados “soma criptográfica de controlo”, incorporado no comando ou na resposta, aos objectos de dados enviados. A soma criptográfica de controlo deve ser verificada pelo receptor.
- CSM_023 A soma criptográfica de controlo dos dados enviados deve integrar o cabeçalho do comando no qual é incorporada e todos os objectos de dados enviados (= > CLA = '0C', e todos os objectos de dados devem ser encapsulados com marcadores nos quais b1 = 1).
- CSM_024 Os bytes de informação sobre a situação da resposta devem ser protegidos por uma soma criptográfica de controlo se a resposta não contiver campo de dados.
- CSM_025 As somas criptográficas de controlo devem ter 4 bytes de comprimento.

Se se recorrer ao envio seguro de mensagens, a estrutura dos comandos e das respostas será, portanto, a seguinte:

Os DO (objectos de dados) utilizados são um subconjunto dos DO de envio seguro de mensagens referidos na norma ISO/CEI 7816-4:

Marcador	Mnemónica	Significado
'81'	T _{PV}	Valor simples não codificado em BER-TLV (a proteger por CC)
'97'	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 controlo
'87'	T _{PI CG}	Byte indicador de enchimento Criptograma (valor simples não codificado em BER-TLV)

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]
'0C'	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	Cam- po de dados	'97'	'01'	L _e	'8E'	'04'	CC	

Dados a integrar na soma de controlo = CH || PB || T_{PV} || L_{PV} || PV || T_{LE} || L_{LE} || L_c || PB

P = bytes de enchimento (80 .. 00), segundo ISO-CEI 7816-4 e método 1 de ISO 9797.

Os objectos 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 mas 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 controlo = 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:

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 encaminhar pelo CG: dados não codificados em BER-TLV e bytes de enchimento.

Dados a integrar na soma de controlo = 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 controlo = 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/CEI 7816-4, definem-se os seguintes bytes de situação para indicar erros de SM:

'66 88': Falha na verificação da soma criptográfica de controlo

'69 87': Ausência de objectos de dados SM esperados

'69 88': Incorreção dos objectos 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 abortada pela VU.

5.3. Algoritmo para o cálculo de somas criptográficas de controlo

CSM_028 As somas criptográficas de controlo são constituídas com recurso a um controlo de acesso ao meio (MAC) pormenorizado, nos termos da norma ANSI X9.19 com DES:

- fase inicial: o bloco inicial de verificação y_0 é $E(K_a, SSC)$,
- fase sequencial: os blocos de verificação y_1, \dots, y_n são calculados com recurso a K_a ,
- fase final: a soma criptográfica de controlo é calculada com base no último bloco de verificação y_n , do seguinte modo: $E(K_a, D(K_b, y_n))$,

onde $E()$ representa a criptagem com DES, e $D()$ a descriptagem com DES.

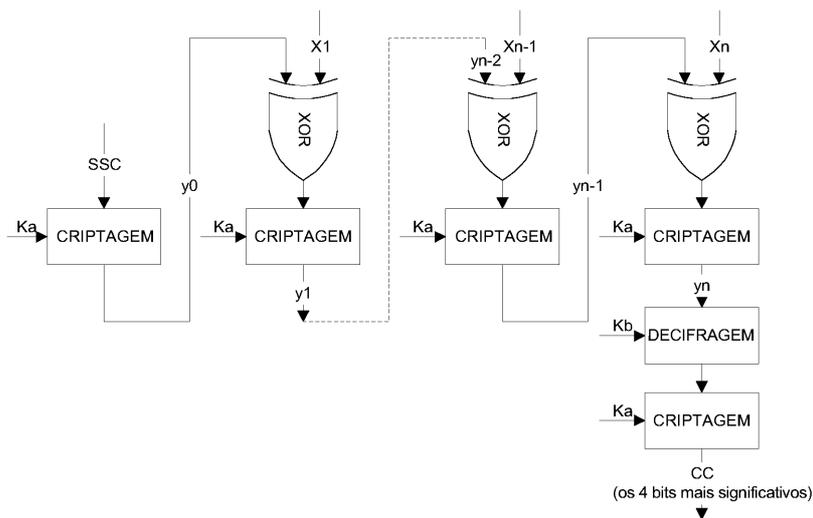
Os quatro bytes mais significativos da soma criptográfica de controlo são transferidos.

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 ser calculado cada MAC (ou seja, o SSC para o primeiro comando é SSC inicial + 1, o SSC para a primeira resposta é SSC inicial + 2).

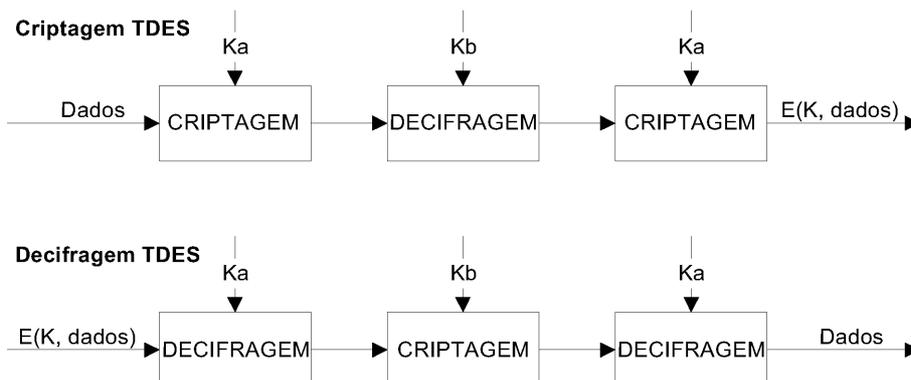
O esquema seguinte representa o cálculo do MAC pormenorizado:



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 vector nulo como bloco de valor inicial.

O esquema seguinte representa a aplicação de chaves em TDES:



6. MECANISMOS DE ASSINATURA DIGITAL DO DESCARREGAMENTO DE DADOS

- CSM_032 O equipamento inteligente afectado (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_iC e EQT.C. Contém as assinaturas digitais de blocos de dados, em conformidade com o apêndice 7 (Protocolos de Descarregamento de Dados).
- CSM_033 As assinaturas digitais dos dados descarregados devem utilizar 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 deve obedecer ao esquema de assinatura digital com apêndice, definido na referência PKCS1, com a função hash SHA-1:

$$\text{Assinatura} = \text{EQT.SK}[\text{'00'} \parallel \text{'01'} \parallel \text{PS} \parallel \text{'00'} \parallel \text{DER}(\text{SHA-1}(\text{dados}))]$$

PS = Cadeia de octetos de enchimento 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 deve obedecer 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.

