

DIRECTIVA 2003/127/CE DA COMISSÃO
de 23 de Dezembro de 2003
que altera a Directiva 1999/37/CE do Conselho relativa aos documentos de matrícula dos veículos
(Texto relevante para efeitos do EEE)

A COMISSÃO DAS COMUNIDADES EUROPEIAS,

Tendo em conta o Tratado que institui a Comunidade Europeia,

Tendo em conta a Directiva 1999/37/CE do Conselho, de 29 de Abril de 1999, relativa aos documentos de matrícula dos veículos ⁽¹⁾ e, nomeadamente, o seu artigo 6.º,

Considerando o seguinte:

- (1) A Directiva 1999/37/CE estabelece as regras harmonizadas aplicáveis aos certificados de matrícula dos veículos sujeitos a registo na Comunidade.
- (2) Dada a crescente introdução de equipamentos electrónicos e telemáticos nos veículos, os anexos da Directiva 1999/37/CE devem ser adaptados ao progresso científico e técnico, para que os Estados-Membros possam emitir documentos de matrícula dos veículos sob a forma de cartões inteligentes com microprocessador em vez de documentos em papel.
- (3) A Directiva 1999/37/CE deverá, por conseguinte, ser alterada em conformidade.
- (4) As medidas previstas na presente directiva estão em conformidade com o parecer do Comité instituído pelo artigo 8.º da Directiva 96/96/CE do Conselho ⁽²⁾.
- (5) Os Estados-Membros devem tomar as medidas necessárias para assegurar que a recolha e o tratamento dos dados pessoais necessários à emissão dos documentos de matrícula dos veículos sob a forma de cartões inteligentes estejam em conformidade com a 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 ⁽³⁾,

ADOPTOU A PRESENTE DIRECTIVA:

Artigo 1.º

Os anexos da Directiva 1999/37/CE são substituídos pelo texto que figura em anexo à presente directiva.

Artigo 2.º

1. Os Estados-Membros devem pôr em vigor as disposições legislativas, regulamentares e administrativas necessárias para dar cumprimento à presente directiva o mais tardar 12 meses após a sua publicação no *Jornal Oficial da União Europeia*. Os Estados-Membros devem imediatamente comunicar à Comissão o texto das referidas disposições, bem como um quadro de correspondência entre as disposições da presente directiva e as disposições nacionais aprovadas.

Quando os Estados-Membros aprovarem essas disposições, estas devem incluir uma referência à presente directiva ou ser acompanhadas dessa referência na publicação oficial. As modalidades dessa referência serão estabelecidas pelos Estados-Membros.

2. Os Estados-Membros devem comunicar à Comissão o texto das principais disposições de direito interno que adoptarem no domínio regido pela presente directiva.

Artigo 3.º

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

Artigo 4.º

Os Estados-Membros são os destinatários da presente directiva.

Feito em Bruxelas, em 23 de Dezembro de 2003.

Pela Comissão
Loyola DE PALACIO
Vice-Presidente

⁽¹⁾ JO L 138 de 1.6.1999, p. 57.

⁽²⁾ JO L 46 de 17.2.1997, p. 1.

⁽³⁾ JO L 281 de 23.11.1995, p. 31.

ANEXO

«ANEXO I

PARTE I DO CERTIFICADO DE MATRÍCULA ⁽¹⁾

- I. A presente parte poderá ser implementada num dos dois formatos seguintes: documento em papel ou cartão inteligente. As características da versão papel são especificadas no capítulo II e as do cartão inteligente no capítulo III.

II. Especificações da parte I do certificado de matrícula em papel

- II.1. As dimensões totais do certificado de matrícula não devem exceder as dimensões do formato A4 (210 × 297 mm) ou de um desdobrável de formato A4.
- II.2. O papel utilizado para a parte I do certificado de matrícula deve ser protegido contra a falsificação por meio da utilização de, pelo menos, duas das técnicas seguintes:

- grafismos,
- marca de água,
- fibras fluorescentes, ou
- impressões fluorescentes.

Os Estados-Membros são livres de introduzir elementos de segurança adicionais.

- II.3. A parte I do certificado de matrícula pode ser composta de várias páginas. Os Estados-Membros determinarão o número de páginas necessárias de acordo com as informações contidas no documento e a sua apresentação gráfica.

- II.4. A primeira página da parte I do certificado de matrícula deve conter as informações seguintes:

- nome do Estado-Membro emissor da parte I do certificado de matrícula,
- sinal distintivo do Estado-Membro emissor da parte I do certificado de matrícula, ou seja:
 - 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
- nome da autoridade competente,
- menção “Parte I do Certificado de Matrícula” ou, se o certificado tiver apenas uma única parte, a menção “Certificado de Matrícula”, impressa em corpo grande na língua ou línguas do Estado-Membro emissor do certificado de matrícula; esta menção pode ainda estar presente a uma distância adequada, impressa em corpo pequeno, nas outras línguas da Comunidade Europeia,
- menção “Comunidade Europeia”, impressa na língua ou línguas do Estado-Membro emissor da parte I do certificado de matrícula,
- número do documento.

⁽¹⁾ O certificado composto de uma só parte ostentará a menção “Certificado de Matrícula”, não sendo feita qualquer referência à “parte I”

- II.5. A parte I do certificado de matrícula deve igualmente conter as informações seguintes, precedidas dos respectivos códigos comunitários harmonizados:
- (A) Número de matrícula;
 - (B) Data da primeira matrícula do veículo;
 - (C) Dados pessoais,
 - (C.1) Titular do certificado de matrícula:
 - (C.1.1) Apelido(s) ou denominação comercial,
 - (C.1.2) Outro(s) nome(s) ou inicial(ais) (quando aplicável),
 - (C.1.3.) Morada no Estado-Membro de matrícula na data de emissão do documento,
 - (C.4) Se as informações do ponto II.6, código C.2, não constarem do certificado de matrícula, referência do facto de o titular do certificado de matrícula:
 - a) ser o proprietário do veículo,
 - b) não ser o proprietário do veículo,
 - c) não estar identificado no certificado de matrícula como proprietário do veículo;
 - (D) Veículo:
 - (D.1) marca,
 - (D.2) modelo,
 - variante (se disponível),
 - versão (se disponível);
 - (D.3) denominação(ões) comercial(ais);
 - (E) Número de identificação do veículo;
 - (F) Massa:
 - (F.1) massa máxima em carga tecnicamente admissível, excepto para motociclos;
 - (G) Massa do veículo em serviço com carroçaria e, no caso de um veículo tractor de qualquer categoria que não a categoria M1 [kg], com dispositivo de engate;
 - (H) Validade da matrícula, caso não seja ilimitada;
 - (I) Data da matrícula a que se refere o certificado;
 - (K) Número de homologação do modelo (se disponível),
 - (P) Motor:
 - (P.1) cilindrada (em cm³);
 - (P.2) potência útil máxima (em kW) (se disponível),
 - (P.3) tipo de combustível ou fonte de energia;
 - (Q) Relação potência/peso (em kW/kg) (apenas para os motociclos);
 - (S) Lotação:
 - (S.1) número de lugares sentados, incluindo o lugar do condutor,
 - (S.2) número de lugares em pé (se aplicável).
- II.6. A parte I do certificado de matrícula poderá ainda incluir os seguintes dados, precedidos dos respectivos códigos comunitários harmonizados:
- (C) Dados pessoais:
 - (C.2) proprietário do veículo (repetir o número de vezes correspondente ao número de proprietários):
 - (C.2.1) apelido ou denominação comercial,
 - (C.2.2) outro(s) nome(s) ou inicial(ais) (se aplicável),
 - (C.2.3) morada no Estado-Membro de matrícula na data de emissão do documento,

- (C.3) pessoa singular ou colectiva autorizada a utilizar o veículo em virtude de um direito legal que não a propriedade do veículo:
- (C.3.1) apelido ou denominação comercial,
- (C.3.2) outros(s) nome(s) ou inicial(ais) (se aplicável),
- (C.3.3) morada no Estado-Membro de matrícula na data de emissão do documento;
- (C.5), (C.6), (C.7) e (C.8): Se a alteração dos dados pessoais a que se referem os pontos II.5, código C.1, II.6, código C.2 e/ou II.6, código C.3, não der lugar à emissão de um novo certificado de matrícula, os novos dados pessoais correspondentes podem ser inseridos com os códigos (C.5), (C.6), (C.7) ou (C.8); nessa altura serão desagregados de acordo com as referências constantes dos pontos II.5, código C.1, II.6, código C.2, II.6, código C.3 e II.5, código C.4;
- (F) Massa:
- (F.2) massa máxima em carga admissível do veículo em serviço no Estado-Membro de matrícula,
- (F.3) massa máxima em carga admissível do conjunto em serviço no Estado-Membro de matrícula;
- (J) Categoria do veículo;
- (L) Número de eixos;
- (M) Distância entre eixos (em mm);
- (N) No caso dos veículos com uma massa total superior a 3 500 kg, distribuição entre os eixos da massa máxima em carga tecnicamente admissível:
- (N.1) eixo 1 (em kg),
- (N.2) eixo 2 (em kg), quando aplicável,
- (N.3) eixo 3 (em kg), quando aplicável,
- (N.4) eixo 4 (em kg), quando aplicável,
- (N.5) eixo 5 (em kg), quando aplicável;
- (O) Massa máxima rebocável tecnicamente admissível:
- (O.1) reboque travado (em kg),
- (O.2) reboque destravado (em kg);
- (P) Motor:
- (P.4) regime nominal (em min⁻¹),
- (P.5) número de identificação do motor;
- (R) Cor do veículo;
- (T) Velocidade máxima (em km/h);
- (U) Nível sonoro:
- (U.1) estacionário [em dB(A)],
- (U.2) regime do motor (em min⁻¹),
- (U.3) em circulação [em dB(A)];
- (V) Gases de escape:
- (V.1) CO (em g/km ou g/kWh),
- (V.2) HC (em g/km ou g/kWh),
- (V.3) NOx (em g/km ou g/kWh),

- (V.4) HC + NO_x (em g/km),
- (V.5) partículas no caso dos motores *diesel* (em g/km ou g/kWh),
- (V.6) coeficiente de absorção corrigido no caso dos motores *diesel* (em min-1),
- (V.7) CO₂ (em g/km),
- (V.8) consumo de combustível em ciclo combinado (em l/100 km),
- (V.9) indicação da classe ambiental de homologação CE;
referência da versão aplicável por força da Directiva 70/220/CEE ⁽¹⁾ ou da Directiva 88/77/CEE ⁽²⁾

(W) Capacidade do(s) depósito(s) de combustível (em l).

II.7. Os Estados-Membros podem incluir informações complementares (na parte I do certificado de matrícula), designadamente acrescentando, entre parênteses, aos códigos de identificação, conforme estabelecido nos pontos II.5 e II.6, códigos nacionais adicionais.

III. **Especificações da parte I do certificado de matrícula sob a forma de cartão inteligente** (Alternativa ao modelo em papel descrito no capítulo II)

III.1. *Formato do cartão e dados legíveis a olho nu*

Dado incorporar um microprocessador, o cartão com circuito integrado deve ser concebido de acordo com as normas constantes do capítulo III.5. A leitura dos dados armazenados no cartão devem poder ser efectuada com a ajuda de equipamentos de leitura de uso corrente (tal como para os cartões tacográficos).

A frente e o verso do cartão devem ter impressos, pelo menos, os dados especificados nos capítulos II.4 e II.5; esses dados devem ser legíveis a olho nu (altura mínima dos caracteres: 6 pontos) e impressos conforme abaixo indicado (ver exemplos de possíveis apresentações gráficas na figura 1, no final da presente secção).

A. Bloco de dados de base

Os dados de base devem incluir o seguinte:

Frente

a) À direita do circuito integrado:

- na(s) língua(s) do Estado-Membro emissor do certificado de matrícula
 - a menção “Comunidade Europeia”,
 - o nome do Estado-Membro emissor do certificado de matrícula,
 - a menção “Parte I do Certificado de Matrícula” ou, se o certificado apenas for composto de uma parte, a menção “Certificado de Matrícula”, impressa em corpo grande,
 - outra denominação do documento equivalente (por exemplo, a anterior designação nacional) (opcional),
 - o nome da autoridade competente (alternativamente, também sob a forma de dados específicos como indicado na secção B),
 - o número sequencial e inequívoco do documento, conforme utilizado no Estado-Membro (alternativamente, também sob a forma de dados específicos como indicado na secção B);

b) Na zona acima do circuito integrado:

A sigla distintiva do Estado-Membro emissor do certificado de matrícula, a branco, num rectângulo azul e rodeada por 12 estrelas amarelas;

B Bélgica

DK Dinamarca

D Alemanha

GR Grécia

E Espanha

F França

⁽¹⁾ Directiva 70/220/CEE do Conselho, de 20 de Março de 1970, relativa à aproximação das legislações dos Estados-Membros respeitantes às medidas a tomar contra a poluição do ar pelos gases provenientes dos motores de ignição comandada que equipam os veículos a motor (JO L 76 de 6.4.1970, p. 1), com a última redacção que lhe foi dada pela Directiva 2002/80/CE da Comissão (JO L 291 de 28.10.2002, p. 20)

⁽²⁾ Directiva 88/77/CEE do Conselho, de 3 de Dezembro de 1987, relativa à aproximação das legislações dos Estados-Membros respeitantes às medidas a tomar contra a emissão de gases poluentes pelos motores diesel utilizados em veículos (JO L 36 de 9.2.1988, p. 33), com a última redacção que lhe foi dada pela Directiva 2001/27/CE da Comissão (JO L 107 de 18.4.2001, p. 10)

IRL Irlanda
 I Itália
 L Luxemburgo
 NL Países Baixos
 A Áustria
 P Portugal
 FIN Finlândia
 S Suécia
 UK Reino Unido

- c) Os Estados-Membros poderão equacionar a possibilidade de aditamento, no bordo inferior, em corpo pequeno, e na(s) sua(s) língua(s) nacional(ais), da menção: "O presente documento deve ser exibido mediante pedido de qualquer pessoa com poderes para o efeito."
- d) A cor de base do cartão é o verde (Pantone 362); alternativamente, é possível a transição do verde para o branco.
- e) No canto inferior esquerdo da face do cartão, deverá ser impresso um símbolo representativo de uma roda (ver representação gráfica proposta na figura 1).

Em tudo o mais, devem ser observadas as disposições do capítulo III.13.

B. Bloco de dados específicos

O bloco de dados específicos deve conter as informações seguintes:

Frente

- a) o nome da autoridade competente — ver também secção Aa);
- b) o nome da autoridade emissora do certificado de matrícula (opcional);
- c) o número sequencial e inequívoco do documento, conforme utilizado no Estado-Membro (ver também secção Aa);
- d) os dados do capítulo II.5 mencionados abaixo; conforme indicado no capítulo II.7, os códigos comunitários harmonizados podem ser acompanhados de códigos nacionais.

<i>Código</i>	<i>Referência</i>
(A)	número de matrícula (número oficial da autorização);
(B)	data da primeira matrícula do veículo;
(I)	data da matrícula a que se refere o presente certificado.

Dados pessoais

- (C.1) titular do certificado de matrícula,
 - (C.1.1) apelido ou denominação comercial,
 - (C.1.2) outros nome(s) ou inicial(ais) (quando aplicável),
 - (C.1.3) morada no Estado-Membro de matrícula na data de emissão do documento;
- (C.4) se as informações especificadas no capítulo II.6, código C.2, não constarem do certificado de matrícula, conforme definido nas secções A e B, referência do facto de o titular do certificado de matrícula:
 - a) ser o proprietário do veículo;
 - b) não ser o proprietário do veículo;
 - c) não estar identificado no certificado de matrícula como proprietário do veículo;

Verso

O verso do cartão deve incluir, pelo menos, os restantes dados especificados no capítulo II.5; conforme indicado no capítulo II.7, os códigos comunitários harmonizados podem ser acompanhados de códigos nacionais.

Mais especificamente, esses dados são os seguintes:

*Código**Referência*

Dados do veículo (tendo em conta as notas do capítulo II.5)

- | | |
|-------|---|
| (D.1) | marca, |
| (D.2) | modelo (variante/versão, quando aplicável), |
| (D.3) | denominação(ções) comercial(ais), |
| (E) | número de identificação do veículo, |
| (F.1) | massa máxima em carga tecnicamente admissível, excepto para os motociclos [kg], |
| (G) | massa do veículo em serviço com carroçaria e, no caso de um veículo tractor de qualquer categoria que não a categoria M1 [kg], com dispositivo de engate, |
| (H) | prazo de validade da matrícula, caso não seja ilimitado, |
| (K) | número de homologação do modelo (se disponível): |
| (P.1) | cilindrada [cm ³], |
| (P.2) | potência nominal [kW], |
| (P.3) | tipo de combustível ou fonte de energia, |
| (Q) | relação potência/peso [em kW/kg] (apenas para os motociclos), |
| (S.1) | número de lugares sentados, incluindo o lugar do condutor |
| (S.2) | número de lugares em pé (quando aplicável) |

Acessoriamente, podem ser acrescentados, no verso do cartão, os dados complementares constantes dos capítulos II.6 (com os códigos harmonizados) e II.7.

C. Elementos de segurança física do cartão inteligente

As ameaças à segurança física dos documentos são as seguintes:

- fabrico de cartões falsos: criação de um objecto novo, que mantém uma grande semelhança com o documento inicial, de raiz ou mediante a realização de cópias de um documento original,
- alteração do material: alteração de uma propriedade de um documento original, modificando, por exemplo, alguns dos dados impressos no documento.

O material utilizado na parte i do certificado de matrícula deve ser protegido contra a falsificação por meio da utilização de, pelo menos, três das técnicas seguintes:

- microcaracteres,
- guilhoché*,
- impressão iridescente,
- gravura a *laser*,
- tinta fluorescente sob luz ultravioleta,
- tintas com cor dependente do ângulo de visão*,
- tintas com cor dependente da temperatura*,
- hologramas*,
- imagens *laser* variáveis,
- imagens de impressão variável (OVI).

Os Estados-Membros são livres de introduzir elementos de segurança adicionais.

Como ponto de partida, deve ser dada preferência às técnicas indicadas com um asterisco, pois permitem a verificação da validade do cartão pelos serviços responsáveis pela aplicação da lei sem recurso a quaisquer meios especiais.

Figura 1: Exemplos de possíveis representações gráficas dos dados obrigatórios
(é possível acrescentar dados opcionais e adicionais no verso do cartão)

III.2. Armazenamento e protecção dos dados

Precedidos dos códigos comuns harmonizados (quando aplicável acompanhados dos códigos dos Estados-Membros, em conformidade com o capítulo II.7), os dados a seguir devem ou podem ser armazenados, a título complementar, na superfície do cartão que leva a informação legível, de acordo com o Capítulo III.1:

A. Dados de acordo com os capítulos II.4 e II.5

Os dados especificados nos capítulos II.4 e II.5 devem ser obrigatoriamente armazenados no cartão.

B. Outros dados de acordo com o capítulo II.6

Além disso, os Estados-Membros são livres de armazenar dados adicionais de acordo com o capítulo II.6, na medida do necessário.

C. Outros dados de acordo com o capítulo II.7

Podem ser armazenadas informações adicionais no cartão, a título facultativo.

Os dados constantes das secções A e B são armazenados em dois ficheiros correspondentes com uma estrutura transparente (ver ISO/CEI 7816-4). Os Estados-Membros podem definir os seus próprios requisitos de armazenamento dos dados indicados na secção C.

Esses ficheiros não apresentam restrições à leitura.

O acesso aos ficheiros para escrita deve ser limitado às autoridades nacionais competentes do Estado-Membro emissor do cartão inteligente (e suas agências autorizadas).

O acesso para escrita apenas será autorizado após uma autenticação assimétrica através da troca de chaves de sessão, de modo a proteger a sessão entre o cartão de matrícula do veículo e um módulo de segurança (por exemplo, um cartão com módulo de segurança) das autoridades nacionais competentes (ou suas agências autorizadas). O processo de autenticação é, por conseguinte, antecedido da troca de certificados verificáveis do cartão, em conformidade com a norma ISO/CEI 7816-8. Os certificados verificáveis do cartão contêm as respectivas chaves públicas, que devem ser recuperadas e utilizadas no processo de autenticação subsequente. Esses certificados são assinados pelas autoridades nacionais competentes e contêm um objecto de autorização (autorização do titular do certificado) em conformidade com a norma ISO/CEI 7816-9, de modo a codificar uma autorização específica de função para o cartão. Esta autorização de função está associada à autoridade nacional competente (por exemplo, para actualizar um campo de dados).

As chaves públicas correspondentes das autoridades nacionais competentes são armazenadas no cartão enquanto âncoras de confiança (chave pública de raiz).

A especificação dos ficheiros e dos comandos necessários aos processos de autenticação e de escrita é da competência dos Estados-Membros. A garantia de segurança deve ser aprovada através de uma avaliação assente em critérios comuns de acordo com a certificação EAL4+. Os elementos adicionais são os seguintes: (1) AVA_MSU.3 Análise e ensaio para detecção de estados sem segurança; (2) AVA_VLA.4 Elevada resistência.

D. Dados de verificação da autenticidade dos dados de matrícula

A autoridade emissora calcula a sua assinatura electrónica relativa a todos os dados de um ficheiro que contenha as informações especificadas nas secções A ou B e armazena essas informações num ficheiro correspondente. Essas assinaturas permitem verificar a autenticidade dos dados em memória. Os cartões devem conter os dados seguintes:

- assinatura electrónica dos dados de matrícula relacionados com a secção A,
- assinatura electrónica dos dados de matrícula relacionados com a secção B.

Para verificação dessas assinaturas electrónicas, o cartão deve conter:

- os certificados da autoridade emissora que calcula as assinaturas relativas aos dados das secções A e B.

Não deve haver restrições à leitura das assinaturas electrónicas e dos certificados. O acesso para escrita, quer às assinaturas electrónicas quer aos certificados, deve ficar restringido às autoridades nacionais competentes.

III.3. Interface

Os contactos externos devem funcionar como interfaces. A combinação de contactos externos com um emissor-respondedor (*transponder*) é facultativa.

III.4. Capacidade de armazenamento do cartão

O cartão deverá ter capacidade de armazenamento suficiente para guardar os dados mencionados no capítulo III.2.

III.5. Normas

O cartão com circuito integrado e os dispositivos de leitura devem satisfazer as normas seguintes:

- ISO 7810: Normas para cartões de identificação (cartões plastificados): Características físicas,
- ISO 7816-1 e -2: Características físicas dos cartões com circuito integrado; dimensões e localização dos contactos,
- ISO 7816-3: Características eléctricas dos contactos, protocolos de transmissão,
- ISO 7816-4: Conteúdo das comunicações, estrutura dos dados dos cartões com circuito integrado, arquitectura de segurança, mecanismos de acesso,
- ISO 7816-5: Estrutura dos identificadores de aplicação, selecção execução dos identificadores de aplicação, processo de registo dos identificadores de aplicação (sistema de numeração),
- ISO 7816-6: Elementos de dados intersectoriais para intercâmbio,
- ISO 7816-8: Cartões com circuito(s) integrado(s) com contactos, Comandos de segurança intersectoriais,
- ISO 7816-9: Cartões com circuito(s) integrado(s) com contactos, Comandos intersectoriais optimizados.

III.6. Características técnicas e protocolos de transmissão

Deverá ser adoptado o formato ID-1 (dimensão normal, ver ISO/CEI 7810). O cartão deverá suportar o protocolo de transmissão T = 1, em conformidade com a norma ISO/CEI 7816-3. Adicionalmente, poderá suportar outros protocolos de transmissão, como T = 0, USB ou "sem contactos".

Para a transmissão dos dados, deverá ser utilizada a "convenção directa" (ver ISO/CEI 7816-3).

A. Tensão de alimentação, tensão de programação

O cartão deve funcionar com $V_{cc} = 3V (+/- 0.3V)$ ou com $V_{cc} = 5V (+/- 0.5V)$. Não deve carecer de tensão de programação no pino C6.

B. Resposta à restauração (*Reset*)

O *byte* presente no cartão que indica a dimensão do campo de informação deve ser apresentado em ATR em caracteres TA3. Este valor será de, pelo menos, "80h" (= 128 bytes).

C. Selecção dos parâmetros do protocolo

O sistema deve obrigatoriamente suportar a selecção de parâmetros de protocolo (PPS) em conformidade com a norma ISO/CEI 7816-3. Será usado para seleccionar T = 1, no caso de T = 0 também constar do cartão, e para negociar os parâmetros Fi/Di, de modo a obter taxas de transmissão mais elevadas.

D. Protocolo de transmissão T = 1

O suporte da formação de cadeia (*chaining*) é obrigatório:

São permitidas as simplificações seguintes:

- Byte NAD: não utilizado (NAD deve ser posto a "00"),
- ABORT — bloco-S: não utilizado,
- Erro de estado VPP — bloco-S: não utilizado.

A dimensão do campo de informação do dispositivo (IFSD) deve ser indicada pelo IFD imediatamente após ATR, ou seja, o IFD transmite o pedido de IFS — bloco-S após ATR e o cartão reenvia IFS — bloco-S. O valor recomendado para o IFSD é de 254 bytes.

III.7. Amplitude térmica

O certificado de matrícula sob a forma de cartão inteligente deve poder funcionar correctamente nas condições climáticas habitualmente verificadas no território da União Europeia e, pelo menos, na gama de temperaturas especificada na norma ISO 7810. Os cartões tacográficos devem poder funcionar correctamente com níveis de humidade entre 10 % e 90 %.

III.8. *Período de vida física*

Se for utilizado em conformidade com as especificações ambientais e eléctricas, o cartão deve funcionar correctamente durante um período de 10 anos. Os materiais utilizados no cartão devem ser seleccionados de forma a garantir esse período de vida.

III.9. *Características eléctricas*

Durante o seu funcionamento, os cartões devem cumprir o disposto na Directiva 95/54/CE da Comissão, relativa à compatibilidade electromagnética ⁽¹⁾ e estar protegidos contra as descargas electrostáticas.

III.10. *Estrutura do ficheiro*

O quadro 1 enumera os ficheiros de base obrigatórios (EF) da aplicação DF (ver ISO/CEI 7816-4) DF. Registration. Esses ficheiros apresentam todos uma estrutura transparente. As condições de acesso constam do capítulo III.2. A dimensão dos ficheiros é estabelecida pelos Estados-Membros de acordo com os seus requisitos.

Quadro 1

Nome do ficheiro	Identificador de ficheiro	Descrição
EF.Registration_A	"D001"	Dados de matrícula de acordo com os capítulos II.4 e II.5
EF.Signature_A	"E001"	Assinatura electrónica relativa a todo o conteúdo de EF.Registration_A
EF.C.IA_A.DS	"C001"	Certificado X.509v3 da autoridade emissora que calcula as assinaturas para EF.Signature_A
EF.Registration_B	"D011"	Dados de matrícula de acordo com o capítulo II.6
EF.Signature_B	"E011"	Assinatura electrónica relativa a todo o conteúdo de EF.Registration_B
EF.C.IA_B.DS	"C011"	Certificado X.509v3 da autoridade emissora que calcula as assinaturas para EF.Signature_B

III.11. *Estrutura dos dados*

Os certificados são armazenados no formato X.509v3 em conformidade com a norma ISO/CEI 9594-8. As assinaturas electrónicas são armazenadas de forma transparente.

Os dados de matrícula são armazenados como objectos de dados BER-TLV (ver ISO/CEI 7816-4) nos ficheiros de base correspondentes. Os campos de valores são codificados como caracteres ASCII, conforme especificado na norma ISO/CEI 8824-1, os valores "C0"-FF" são definidos pela norma ISO/CEI 8859-1 (jogo de caracteres Latino 1), ISO/CEI 8859-7 (jogo de caracteres Grego) ou ISO/CEI 8859-5 (jogo de caracteres Cirílico). O formato das datas é AAAAMMDD.

O quadro 2 enumera as etiquetas (Tags) que identificam os objectos de dados correspondentes aos dados de matrícula constantes dos capítulos II.4 e II.5, juntamente com os dados adicionais do capítulo III.1. Salvo indicação em contrário, os objectos de dados constantes do quadro 2 são obrigatórios. Os objectos de dados facultativos podem ser omitidos. A coluna correspondente à etiqueta indica o nível de encastramento (*nesting*).

Quadro 2

Etiqueta				Descrição
"78"				autoridade que atribui etiquetas compatíveis; encastra o objecto "4F" (ver ISO/CEI 7816-4 e ISO/CEI 7816-6)
	"4F"			identificador de aplicação (ver norma ISO/CEI 7816-4)
"71"				modelo intersectorial (ver ISO/CEI 7816-4 e ISO/CEI 7816-6) correspondente aos dados obrigatórios da parte 1 do certificado de matrícula; encastra todos os objectos subsequentes

⁽¹⁾ Directiva 95/54/CE da Comissão, de 31 de Outubro de 1995, que adapta ao progresso técnico a Directiva 72/245/CEE do Conselho relativa à aproximação das legislações dos Estados-Membros respeitantes à supressão das interferências radioeléctricas produzidas pelos motores de ignição comandada que equipam os veículos a motor e que altera a Directiva 70/156/CEE relativa à aproximação das legislações dos Estados-Membros respeitantes à recepção dos veículos a motor e seus reboques (JO L 266 de 08.11.1995, p. 1).

Etiqueta				Descrição
	"80"			versão da definição da etiqueta
	"9F33"			nome do Estado-Membro emissor do certificado de matrícula, parte 1
	"9F34"			outra designação do documento equivalente (anterior designação nacional) (opcional)
	"9F35"			nome da autoridade competente
	"9F36"			nome da autoridade emissora do certificado de matrícula (opcional)
	"9F37"			jogo de caracteres utilizado: "00": ISO/CEI 8859-1 (latino 1) "01": ISO/CEI 8859-5 (cirílico) "02": ISO/CEI 8859-7 (grego)
	"9F38"			número sequencial e inequívoco do documento, conforme utilizado no Estado-Membro
	"81"			número de matrícula
	"82"			data da primeira matrícula
	"A1"			dados pessoais; encastra os objectos "A2" e "86"
		"A2"		titular do certificado de matrícula; encastra os objectos "83", "84" e "85"
			"83"	apelido ou denominação comercial
			"84"	outros nomes ou iniciais (facultativo)
			"85"	morada no Estado-Membro
		"86"		"00": é o proprietário do veículo "01": não é o proprietário do veículo "02": não é identificado como proprietário do veículo
	"A3"			veículo; encastra os objectos "87", "88" e "89"
		"87"		marca do veículo
		"88"		modelo do veículo
		"89"		descrições comerciais do veículo
	"8A"			número de identificação do veículo
	"A4"			massa; encastra "8B"
		"8B"		massa máxima em carga tecnicamente admissível
	"8C"			massa do veículo em serviço com carroçaria
	"8D"			período de validade
	"8E"			data da matrícula a que se refere o presente certificado
	"8F"			número de homologação do modelo
	"A5"			motor; encastra os objectos "90", "91" e "92"
		"90"		cilindrada do motor
		"91"		potência útil máxima do motor

Etiqueta				Descrição
		"92"		tipo de combustível do motor
	"93"			relação potência/peso
	"A6"			lotação; encastra os objectos "94" e "95"
		"94"		número de lugares sentados
		"95"		número de lugares em pé

O quadro 3 enumera as etiquetas que identificam os objectos de dados correspondentes aos dados de matrícula constantes do capítulo II.6. Os objectos de dados constantes do quadro 3 são facultativos.

Quadro 3

Etiqueta				Descrição
"78"				autoridade que atribui etiquetas compatíveis; encastra o objecto "4F" (ver norma ISO/CEI 7816-4 e ISO/CEI 7816-6)
	"4F"			identificador de aplicação (ver norma ISO/CEI 7816-4)
"72"				modelo intersectorial (ver ISO/CEI 7816-4 e ISO/CEI 7816-6) correspondente a dados facultativos do certificado de matrícula — parte 1, capítulo II.6; encastra todos os objectos subsequentes
	"80"			versão da definição de etiqueta
	"A1"			dados pessoais; encastra os objectos "A7", "A8" e "A9"
		"A7"		proprietário do veículo; encastra os objectos "83", "84" e "85"
			..	
		"A8"		segundo proprietário do veículo; encastra os objectos "83", "84" e "85"
			..	
		"A9"		pessoa autorizada a utilizar o veículo em virtude de um direito legal que não a propriedade; encastra os objectos "83", "84" e "85"
			..	
	"A4"			massa; encastra "96" e "97"
		"96"		massa máxima em carga admissível do veículo em serviço
		"97"		massa máxima em carga admissível do conjunto em serviço
	"98"			categoria do veículo
	"99"			número de eixos
	"9A"			distância entre eixos
	"AD"			distribuição entre os eixos da massa máxima em carga admissível; encastra os objectos "9F1F", "9F20", "9F21", "9F22" e "9F23"
		"9F1F"		eixo 1

Etiqueta				Descrição
		"9F20"		eixo 2
		"9F21"		eixo 3
		"9F22"		eixo 4
		"9F23"		eixo 5
	"AE"			massa máxima rebocável tecnicamente admissível; encastra os objectos "9B" e "9C"
		"9B"		reboque travado
		"9C"		reboque destravado
	"A5"			motor; encastra os objectos "9D" e "9E"
		"9D"		velocidade nominal
		"9E"		número de identificação do motor
	"9F24"			cor do veículo
	"9F25"			velocidade máxima
	"AF"			nível sonoro; encastra os objectos "DF26", "DF27" e "DF28"
		"9F26"		estacionário
		"9F27"		velocidade do motor
		"9F28"		em circulação
	"B0"			gases de escape; encastra os objectos "9F29", "9F2A", "9F2B", "9F2C", "9F2D", "9F2E", "9F2F", "9F30" e "9F31"
		"9F29"		CO
		"9F2-A"		HC
		"9F2B"		NOX
		"9F2C"		HC+NOX
		"9F2-D"		partículas no caso dos motores <i>diesel</i>
		"9F2E"		coeficiente de absorção corrigido no caso dos motores <i>diesel</i>
		"9F2F"		CO ₂
		"9F30"		consumo de combustível em ciclo combinado
		"9F31"		indicação da classe ambiental de homologação CE
	"9F32"			capacidade dos depósitos de combustível

A estrutura e o formato dos dados serão definidos pelos Estados-Membros, em conformidade com o capítulo II.7.

III.12. *Leitura dos dados de matrícula*

A. *Seleccção da aplicação*

A aplicação "Matrícula do veículo" deve poder ser seleccionada usando o comando SELECT DF (por nome, ver ISO/CEI 7816-4), através do seu identificador de aplicação (AID). O valor a atribuir a AID será solicitado a um laboratório seleccionado pela Comissão Europeia.

B. *Leitura dos dados dos ficheiros*

Os ficheiros correspondentes ao capítulo II, secções A, B e D, devem poder ser seleccionados através do comando SELECT (ver ISO/CEI 7816-4), pondo o parâmetro de comando P1 com o valor "02", P2 com "04" e o campo de dados de comando com o identificador de ficheiro (ver capítulo X, quadro 1). O modelo de FCP apresentado contém a dimensão do ficheiro, o que pode ser útil para a leitura.

A leitura dos ficheiros deve poder ser efectuada usando o comando READ BINARY (ver ISO/CEI 7816-4) com um campo de dados de comando ausente e L_c configurado para o comprimento dos dados pretendidos, usando um L_c curto.

C. *Verificação da autenticidade dos dados*

Para verificar a autenticidade dos dados de matrícula armazenados, deve ser verificada a assinatura electrónica correspondente. Isto significa que, além de permitir a leitura dos dados de matrícula, o cartão de matrícula deve ainda permitir a leitura da assinatura electrónica correspondente.

A chave pública para verificação da assinatura pode ser extraída do cartão procedendo à leitura do certificado da autoridade emissora correspondente. Os certificados contêm a chave pública e a identificação da autoridade correspondente. A verificação da assinatura pode ser efectuada utilizando outro sistema que não o cartão de matrícula.

Os Estados-Membros são livres de proceder à extracção das chaves públicas e dos certificados para verificação do certificado da autoridade emissora.

III.13. *Disposições especiais*

Independentemente das disposições acima, os Estados-Membros são livres de, após terem notificado a Comissão Europeia, acrescentar cores, marcas ou símbolos. Além disso, no caso de certos dados do capítulo III.2, secção C, os Estados-Membros podem autorizar a utilização do formato XML e do acesso via TCP/IP.

Os Estados-Membros podem ainda, com a autorização da Comissão Europeia, acrescentar outras aplicações relativamente às quais ainda não existam normas ou documentos harmonizados a nível da União Europeia (por exemplo, certificado de controlo técnico), no cartão de matrícula do veículo, tendo em vista serviços adicionais relacionados com o veículo.

ANEXO II

PARTE II DO CERTIFICADO DE MATRÍCULA ⁽¹⁾

- I. A presente parte poderá ser implementada num dos dois formatos: documento em papel ou cartão inteligente. As características da versão papel são especificadas no Capítulo II e as do cartão inteligente no capítulo III.

II. Especificações da parte II do certificado de matrícula em papel

- II.1. As dimensões totais do certificado de matrícula não devem exceder as dimensões do formato A4 (210 × 297 mm) ou de um desdobrável de formato A4.

- II.2. O papel utilizado para a parte II do certificado de matrícula deve ser protegido contra a falsificação por meio da utilização de, pelo menos, duas das técnicas seguintes:

- grafismos,
- marca de água,
- fibras fluorescentes, ou
- impressões fluorescentes.

Os Estados-Membros são livres de introduzir elementos de segurança adicionais.

- II.3. A parte II do certificado de matrícula pode ser composta de várias páginas. Os Estados-Membros determinarão o número de páginas necessárias de acordo com as informações contidas no documento e a sua apresentação gráfica.

- II.4. A primeira página da parte II do certificado de matrícula deve conter as informações seguintes:

- nome do Estado-Membro emissor da parte II do certificado de matrícula,
- sinal distintivo do Estado-Membro emissor da parte II do certificado de matrícula, ou seja:
 - B Bélgica
 - DK Dinamarca
 - D Alemanha
 - GR Grécia
 - E Espanha
 - F França
 - IR Irlanda
 - I Itália
 - L Luxemburgo
 - NL Países Baixos
 - A Áustria
 - P Portugal
 - FIN Finlândia
 - S Suécia
 - UK Reino Unido
- nome da autoridade competente,
- menção “parte II do certificado de matrícula”, impressa em corpo grande na língua ou línguas do Estado-Membro emissor do certificado de matrícula, esta menção pode ainda estar presente a uma distância adequada, impressa em corpo pequeno, nas outras línguas da Comunidade Europeia,
- menção “Comunidade Europeia”, impressa na língua ou línguas do Estado-Membro emissor da parte II do certificado de matrícula,
- número do documento.

⁽¹⁾ O presente anexo refere-se apenas aos certificados de matrícula compostos das partes I e II.

- II.5. A parte II do certificado de matrícula deve igualmente conter as informações seguintes, precedidas dos respectivos códigos comunitários harmonizados:
- (A) Número de matrícula
 - (B) Data da primeira matrícula do veículo
 - (D) Veículo:
 - (D.1) marca,
 - (D.2) modelo,
 - variante (se disponível),
 - versão (se disponível),
 - (D.3) denominação(ões) comercial(ais)
 - (E) Número de identificação do veículo
 - (K) Número de homologação do modelo (se disponível)
- II.6. A parte II do certificado de matrícula poderá, ainda, incluir os dados seguintes, precedidos dos respectivos códigos comunitários harmonizados:
- (C) Dados pessoais:
 - (C.2) proprietário do veículo
 - (C.2.1) apelido(s) ou denominação comercial
 - (C.2.2) outros(s) nome(s) ou inicial(ais) (se aplicável)
 - (C.2.3) morada no Estado-Membro de matrícula na data de emissão do documento
 - (C.3) pessoa singular ou colectiva autorizada a utilizar o veículo em virtude de um direito legal que não a propriedade do veículo:
 - (C.3.1) apelido(s) ou denominação comercial,
 - (C.3.2) outros(s) nome(s) ou inicial(ais) (se aplicável),
 - (C.3.3) morada no Estado-Membro de matrícula na data de emissão do documento,
 - (C.5) e (C.6): Se a alteração dos dados pessoais a que se referem os pontos II.6, código C.3 não der lugar à emissão de uma nova parte II do certificado de matrícula, os novos dados pessoais correspondentes podem ser inseridos com os códigos (C.5) ou (C.6); sendo desagregados de acordo com os pontos II.6, código C.2 e II.6, código C.3.
 - (J) Categoria do veículo
- II.7. Os Estados-Membros podem incluir informações complementares na parte II do certificado de matrícula designadamente, acrescentando, entre parênteses, aos códigos de identificação, conforme estabelecido nos pontos II.5 e II.6, códigos nacionais adicionais.
- III. **Especificações da parte II do certificado de matrícula sob a forma de cartão inteligente** (Alternativa ao modelo em papel descrito no capítulo II)
- III.1. *Formato do cartão e dados legíveis a olho nu*

Dado incorporar um microprocessador, o cartão com circuito integrado deve ser concebido de acordo com as normas constantes do capítulo III.5.

A frente e o verso do cartão devem ter impressos, pelo menos, os dados especificados nos capítulos II.4 e II.5; esses dados devem ser legíveis a olho nu (altura mínima dos caracteres: 6 pontos) e impressos como segue (ver exemplos de possíveis apresentações gráficas na figura 2, no final da presente secção).

A. Bloco de dados de base

Os dados de base devem incluir o seguinte:

Frente

a) À direita do circuito integrado:

- na(s) língua(s) do Estado-Membro emissor do certificado de matrícula
 - a menção “Comunidade Europeia”,
 - o nome do Estado-Membro emissor do certificado de matrícula,
 - a menção “Parte II do Certificado de Matrícula”, impresso em corpo grande,
 - outra denominação do documento equivalente (anterior designação nacional) (opcional),
 - o nome da autoridade competente (em alternativa, também sob a forma de dados específicos como indicado na secção B),
 - o número sequencial e inequívoco do documento, conforme utilizado no Estado-Membro (em alternativa, também sob a forma de dados específicos, como indicado na secção B),

b) Na zona acima do circuito integrado:

A sigla distintiva do Estado-Membro emissor do certificado de matrícula, a branco, num rectângulo azul e rodeada por 12 estrelas amarelas;

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

- c) Os Estados-Membros poderão equacionar a possibilidade de aditamento, no bordo inferior, em corpo pequeno e na(s) sua(s) língua(s) nacional(ais), da menção: “O presente documento deve ser guardado num local seguro fora do veículo”;
- d) A cor de base do cartão é o vermelho (Pantone 194); alternativamente, é possível a transição do vermelho para o branco;
- e) No canto inferior esquerdo da face do cartão, deverá ser impresso um símbolo representativo de uma roda (ver representação gráfica proposta).

Em tudo o mais, devem ser observadas as disposições do capítulo III.13.

B. Bloco de dados específicos

O bloco de dados específicos deve conter as seguintes informações:

Frente

- a) Nome da autoridade competente — ver também secção Aa);
- b) Nome da autoridade emissora do certificado de matrícula (opcional);
- c) O número sequencial e inequívoco do documento, conforme utilizado no Estado-Membro (ver também a secção Aa);

- d) Os dados do capítulo II.5 mencionados abaixo; conforme indicado no capítulo II.7, os códigos comunitários harmonizados podem ser acompanhados de códigos nacionais.

<i>Código</i>	<i>Referência</i>
A	número de matrícula (número oficial da autorização)
B	data da primeira matrícula do veículo

Verso

O verso do cartão deve incluir, pelo menos, os restantes dados especificados no capítulo II.5; conforme indicado no capítulo II.7, os códigos comunitários harmonizados podem ser acompanhados de códigos nacionais.

Mais especificamente, esses dados são os seguintes:

<i>Código</i>	<i>Referência</i>
---------------	-------------------

Dados do veículo (tendo em conta as notas do capítulo II.5)

D.1	marca
D.2	modelo (variante/versão, quando aplicável)
D.3	denominação(ções) comercial(ais)
E	número de identificação do veículo
K	número de homologação do modelo (se disponível)

Acessoriamente, podem ser acrescentados, no verso do cartão, os dados complementares constantes dos capítulos II.6 (com os códigos harmonizados) e II.7.

C. Elementos de segurança física do cartão inteligente

As ameaças à segurança física dos documentos são as seguintes:

- fabrico de cartões falsos: criação de um objecto novo, que mantém uma grande semelhança com o documento inicial, de raiz ou mediante a realização de cópias de um documento original,
- alteração do material: alteração de uma propriedade de um documento original, modificando, por exemplo, alguns dos dados impressos no documento.

O material usado na parte II do certificado de matrícula deve ser protegido contra a falsificação por meio da utilização de, pelo menos, três das técnicas seguintes:

- microcaracteres,
- guilhoché*,
- impressão iridescente,
- gravura a *laser*,
- tinta fluorescente sob luz ultravioleta,
- tintas com cor dependente do ângulo de visão*,
- tintas com cor dependente da temperatura*,
- hologramas*,
- imagens *laser* variáveis,
- imagens de impressão variável (OVI).

Os Estados-Membros são livres de introduzir elementos de segurança adicionais.

Como ponto de partida, deve ser dada preferência às técnicas indicadas com um asterisco, pois permitem a verificação da validade do cartão pelos serviços responsáveis pela aplicação da lei, sem recurso a quaisquer meios especiais.

III.2. Armazenamento e protecção de dados

Precedidos dos códigos comuns harmonizados (quando aplicável acompanhados dos códigos dos Estados-Membros, em conformidade com o capítulo II.7), os dados a seguir devem ou podem ser armazenados, a título complementar, na superfície do cartão que leva a informação legível, de acordo com o capítulo III.1:

A. Dados de acordo com os capítulos II.4 e II.5

Os dados especificados nos capítulos II.4 e II.5 devem ser obrigatoriamente armazenados no cartão.

B. Outros dados de acordo com o capítulo II.6

Além disso, os Estados-Membros são livres de armazenar dados adicionais de acordo com o capítulo II.6, na medida do necessário.

C. Outros dados de acordo com o capítulo II.7

A título facultativo, podem ser armazenados no cartão mais dados de interesse geral relativos ao veículo.

Os dados constantes das secções A e B são armazenados em dois ficheiros correspondentes com uma estrutura transparente (ver ISO/IEC 7816-4). Os Estados-Membros podem definir os seus próprios requisitos de armazenamento dos dados indicados na secção C.

Esses ficheiros não apresentam restrições à leitura.

O acesso aos ficheiros para escrita deve ser limitado às autoridades nacionais competentes do Estado-Membro emissor do cartão inteligente (e suas agências autorizadas).

O acesso para escrita apenas será autorizado após uma autenticação assimétrica, através da troca de chaves de sessão, de modo a proteger a sessão entre o cartão de matrícula do veículo e o módulo de segurança (por exemplo, um cartão com módulo de segurança) das autoridades nacionais competentes (ou suas agências autorizadas). O processo de autenticação é, por conseguinte, antecedido da troca de certificados verificáveis do cartão, em conformidade com a norma ISO/CEI 7816-8. Os certificados verificáveis do cartão contêm as respectivas chaves públicas, que devem ser recuperadas e utilizadas no processo de autenticação subsequente. Esses certificados são assinados pelas autoridades nacionais competentes e contêm um objecto de autorização (autorização do titular do certificado) em conformidade com a norma ISO/CEI 7816-9, de modo a codificar uma autorização específica de função para o cartão. Esta autorização de função está associada à autoridade nacional competente (por exemplo, para actualizar um campo de dados).

As chaves públicas correspondentes das autoridades nacionais competentes são armazenadas no cartão enquanto âncoras de confiança (chave pública de raiz).

A especificação dos ficheiros e dos comandos necessários aos processos de autenticação e de escrita é da competência dos Estados-Membros. A garantia de segurança deve ser aprovada através de uma avaliação assente em critérios comuns de acordo com a certificação EAL4+. Os elementos adicionais são os seguintes: (1) AVA_MSU.3 Análise e ensaio para detecção de estados sem segurança; (2) AVA_VLA.4 Elevada resistência.

D. Dados de verificação da autenticidade dos dados de matrícula

A autoridade emissora calcula a sua assinatura electrónica relativa a todos os dados de um ficheiro que contenha as informações especificadas na secções A ou B e armazena essas informações num ficheiro correspondente. Essas assinaturas permitem verificar a autenticidade dos dados em memória. Os cartões devem conter os seguintes dados:

- assinatura electrónica dos dados de matrícula relacionados com a secção A,
- assinatura electrónica dos dados de matrícula relacionados com a secção B,

Para verificação dessas assinaturas electrónicas, o cartão deve conter:

- os certificados da autoridade emissora que calcula as assinaturas relativas aos dados das secções A e B.

Não deve haver restrições à leitura das assinaturas electrónicas e dos certificados. O acesso para escrita, quer às assinaturas electrónicas quer aos certificados, deve ficar restringido às autoridades nacionais competentes.

III.3. Interface

Os contactos externos devem funcionar como interfaces. A combinação de contactos externos com um emissor-respondedor (*transponder*) é facultativa.

III.4. Capacidade de armazenamento do cartão

O cartão deve ter capacidade de armazenamento suficiente para guardar os dados mencionados no capítulo III.2.

III.5. Normas

O cartão com circuito integrado e os dispositivos de leitura devem satisfazer as normas seguintes:

- ISO 7810: Normas para cartões de identificação (cartões plastificados): Características físicas,
- ISO 7816-1 e -2: Características físicas dos cartões com circuito integrado; dimensões e localização dos contactos,
- ISO 7816-3: Características eléctricas dos contactos, protocolos de transmissão,
- ISO 7816-4: Conteúdo das comunicações, estrutura dos dados dos cartões com circuito integrado, arquitectura de segurança mecanismos de acesso,
- ISO 7816-5: Estrutura dos identificadores de aplicação, selecção e execução dos identificadores de aplicação, processo de registo dos identificadores de aplicação (sistema de numeração),
- ISO 7816-6: Elementos de dados intersectoriais para intercâmbio,
- ISO 7816-8: Cartões com circuito(s) integrado(s) com contactos — Comandos de segurança intersectoriais,
- ISO 7816-9: Cartões com circuito(s) integrado(s) com contactos — Comandos intersectoriais optimizados.

III.6. Características técnicas e protocolos de transmissão

Deverá ser adoptado o formato ID-1 (dimensão normal, ver ISO/CEI 7810).

O cartão deverá suportar o protocolo de transmissão $T = 1$, em conformidade com a norma ISO/CEI 7816-3. Adicionalmente poderá suportar outros protocolos de transmissão, como $T = 0$, USB ou "sem contactos". Para a transmissão dos dados, deverá ser utilizada a "convenção directa" (ver ISO/CEI 7816-3).

A. Tensão de alimentação, tensão de programação

O cartão deve funcionar com $V_{cc} = 3V (+/- 0,3V)$ ou com $V_{cc} = 5V (+/- 0,5V)$. Não deve carecer de tensão de programação no pino C6.

B. Resposta à restauração (Reset)

O byte presente no cartão que indica a dimensão do campo de informação deve ser apresentado em ATR em caracteres TA3. Este valor será de, pelo menos, "80h" (= 128 bytes).

C. Selecção dos parâmetros do protocolo

O sistema deve obrigatoriamente suportar a selecção de parâmetros de protocolo (PPS) em conformidade com a norma ISO/CEI 7816-3E. Será usado para seleccionar $T = 1$, no caso de $T = 0$ também constar do cartão, e para negociar os parâmetros Fi/Di de modo a obter taxas de transmissão mais elevadas.

D. Protocolo de transmissão $T = 1$

O suporte da formação de cadeia (*chaining*) é obrigatório.

São permitidas as simplificações seguintes:

- Byte NAD: não utilizado (NAD deve ser posto a "00"),
- ABORT — bloco-S: não utilizado,
- Erro de estado VPP — bloco-S: não utilizado.

A dimensão do campo de informação do dispositivo (IFSD) deve ser indicada pelo IFD, imediatamente após ATR, ou seja, o IFD transmite o pedido de IFS bloco-S após ATR e o cartão reenvia IFS — bloco-S. O valor recomendado para o IFSD é de 254 bytes.

III.7. Amplitude térmica

O certificado de matrícula sob a forma de cartão inteligente deve poder funcionar correctamente nas condições climáticas habitualmente verificadas no território da União Europeia e, pelo menos, na gama de temperaturas especificada na norma ISO 7810. Os cartões tacográficos devem poder funcionar correctamente com níveis de humidade entre 10 % e 90 %.

III.8. *Período de vida física*

Se for utilizado em conformidade com as especificações ambientais e eléctricas o cartão deve funcionar correctamente durante um período de 10 anos. Os materiais utilizados no cartão devem ser seleccionados de forma a garantir este período de vida.

III.9. *Características eléctricas*

Durante o seu funcionamento, os cartões devem cumprir o disposto na Directiva 95/54/CE, relativa à compatibilidade electromagnética e estar protegidos contra as descargas electrostáticas.

III.10. *Estrutura do ficheiro*

O quadro 1 enumera os ficheiros de base obrigatórios (EF) da aplicação DF (ver ISO/CEI 7816-4) DF. Registration. Esses ficheiros apresentam todos uma estrutura transparente. As condições de acesso constam do capítulo III.2. A dimensão dos ficheiros é estabelecida pelos Estados-Membros de acordo com os seus requisitos.

Quadro 1

Nome do ficheiro	Identificador de ficheiro	Descrição
EF.Registration_A	"D001"	Dados de matrícula de acordo com os capítulos II.4 e II.5
EF.Signature_A	"E001"	Assinatura electrónica relativa a todo o conteúdo de EF.Registration_A
EF.C.IA_A.DS	"C001"	Certificado X.509v3 da autoridade emissora que calcula as assinaturas para EF.Signature_A
EF.Registration_B	"D011"	Dados de matrícula de acordo com o capítulo II.6
EF.Signature_B	"E011"	Assinatura electrónica relativa a todo o conteúdo de EF.Registration_B
EF.C.IA_B.DS	"C011"	Certificado X.509v3 da autoridade emissora que calcula as assinaturas para EF.Signature_B

III.11. *Estrutura dos dados*

Os certificados são armazenados no formato X.509v3 em conformidade com a norma ISO/CEI 9594-8.

As assinaturas electrónicas são armazenadas de forma transparente.

Os dados de matrícula são armazenados como objectos de dados BER-TLV (ver ISO/CEI 7816-4) nos ficheiros de base correspondentes. Os campos de valores são codificados como caracteres ASCII, conforme especificado na norma ISO/CEI 8824-1, os valores "C0"-FF" são definidos pela norma ISO/CEI 8859-1 (jogo de caracteres Latino 1), ISO/CEI 8859-7 (jogo de caracteres Grego) ou ISO/CEI 8859-5 (jogo de caracteres Cirílico). O formato das datas é AAAAMMDD.

O quadro 2 enumera as etiquetas (Tags) que identificam os objectos de dados correspondentes aos dados de matrícula constantes dos capítulos II.4 e II.5, juntamente com os dados adicionais do capítulo III.1. Salvo indicação em contrário, os objectos de dados constantes do quadro 2 são obrigatórios. Os objectos de dados facultativos podem ser omitidos. A coluna correspondente à etiqueta indica o nível de encastramento (*nesting*).

Quadro 2

Etiqueta	Descrição
"78"	autoridade que atribui etiquetas compatíveis; encastra o objecto "4F" (ver norma ISO/CEI 7816-4 e ISO/CEI 7816-6)
"4F"	identificador de aplicação (ver norma ISO/CEI 7816-4)
"73"	modelo intersectorial (ver ISO/CEI 7816-4 e ISO/CEI 7816-6) correspondente aos dados obrigatórios da parte 2 do certificado de matrícula; encastra todos os objectos subsequentes
"80"	versão da definição da etiqueta

Etiqueta				Descrição
	"9F33"			nome do Estado-Membro emissor do certificado de matrícula, parte 2
	"9F34"			outra designação do documento equivalente (anterior designação nacional) (opcional)
	"9F35"			nome da autoridade competente
	"9F36"			nome da autoridade emissora do certificado de matrícula (opcional)
	"9F37"			jogo de caracteres utilizado: "00": ISO/CEI 8859-1 (Latino 1) "01": ISO/CEI 8859-5 (Cirílico) "02": ISO/CEI 8859-7 (Grego)
	"9F38"			número sequencial e inequívoco do documento, conforme utilizado no Estado-Membro
	"81"			número de matrícula
	"82"			data da primeira matrícula
	"A3"			veículo; encastra os objectos "87", "88" e "89"
		"87"		marca do veículo
		"88"		modelo do veículo
		"89"		descrições comerciais do veículo
	"8A"			número de identificação do veículo
	"8F"			número de homologação do modelo

O quadro 3 enumera as etiquetas que identificam os objectos de dados correspondentes aos dados de matrícula constantes do capítulo II.6. Os objectos de dados constantes do quadro 3 são facultativos.

Quadro 3

Etiqueta				Descrição
"78"				autoridade que atribui etiquetas compatíveis; encastra o objecto "4F" (ver norma ISO/CEI 7816-4 e ISO/CEI 7816-6)
	"4F"			identificador de aplicação (ver norma ISO/CEI 7816-4)
"74"				modelo intersectorial (ver ISO/CEI 7816-4 e ISO/CEI 7816-6) correspondente a dados facultativos do certificado de matrícula — parte 1, capítulo II.6; encastra todos os objectos subsequentes
	"80"			versão da definição da etiqueta
	"A1"			dados pessoais; encastra os objectos "A7", "A8" e "A9"
		"A7"		proprietário do veículo; encastra os objectos "83", "84" e "85"
			"83"	apelido ou denominação comercial
			"84"	outros nomes ou iniciais (opcional)
			"85"	morada no Estado-Membro
		"A8"		segundo proprietário do veículo; encastra os objectos "83", "84" e "85"
			...	

Etiqueta				Descrição
		"A9"		pessoa autorizada a utilizar o veículo em virtude de um direito legal que não a propriedade; encastra os objectos "83", "84" e "85"
			...	
	"98"			categoria do veículo

A estrutura e o formato dos dados são definidos pelos Estados-Membros em conformidade com o capítulo II.7.

III.12. *Leitura dos dados de matrícula*

A. Seleção da aplicação

A aplicação "Matrícula do veículo" deve poder ser seleccionada usando o comando SELECT DF (por nome, ver ISO/CEI 7816-4), através do seu identificador de aplicação (AID). O valor de AID será solicitado a um laboratório seleccionado pela Comissão Europeia.

B. Leitura dos dados dos ficheiros

Os ficheiros correspondentes ao capítulo II, secções A, B e D, devem poder ser seleccionados usando o comando SELECT (ver ISO/CEI 7816-4) pondo o parâmetro de comando P1 com o valor "02", P2 com "04" e o campo de dados de comando com o identificador de ficheiro (ver capítulo X, quadro 1). O modelo de FCP apresentado contém a dimensão do ficheiro, o que pode ser útil para a leitura.

A leitura dos ficheiros deve poder ser efectuada usando o comando READ BINARY (ver ISO/CEI 7816-4) com um campo de dados de comando ausente e L_c configurado para o comprimento dos dados pretendidos, usando um L_c curto.

C. Verificação da autenticidade dos dados

Para verificar a autenticidade dos dados de matrícula armazenados, deve ser verificada a assinatura electrónica correspondente. Isto significa que, além de permitir a leitura dos dados de matrícula, o cartão de matrícula deve ainda permitir a leitura da assinatura electrónica correspondente.

A chave pública para verificação da assinatura pode ser extraída do cartão procedendo à leitura do certificado da autoridade emissora correspondente. Os certificados contêm a chave pública e a identificação da autoridade correspondente. A verificação da assinatura pode ser efectuada utilizando outro sistema que não o cartão de matrícula.

Os Estados-Membros são livres de proceder à extracção das chaves públicas e dos certificados para verificação do certificado da autoridade emissora.

III.13. *Disposições especiais*

Independentemente das disposições acima, os Estados-Membros são livres de, após terem notificado a Comissão Europeia, acrescentar cores, marcas ou símbolos. Além disso, no caso de certos dados do capítulo III.2, secção C, os Estados-Membros podem autorizar a utilização do formato XML e do acesso via TCP/IP. Os Estados-Membros podem ainda, com a autorização da Comissão Europeia, acrescentar outras aplicações relativamente às quais ainda não existam normas ou documentos harmonizados a nível da União Europeia (por exemplo, certificado de controlo técnico), no cartão de matrícula do veículo, tendo em vista serviços adicionais relacionados com o veículo.»