



Instituto da Mobilidade
e dos Transportes Terrestres, I.P.

SPTD **Sistema Português do Tacógrafo** **Digital**

Política da **Autoridade Portuguesa**

Controlo de versão

Versão	Data	Ação	Nomes
1.0	Março 2006	Elaboração Submetido para aprovação pela Autoridade Europeia	--
1.0	Março 2006	Aprovação	--
1.1	Abril 2006	Alteração do texto de acordo com a comunicação G07-TRVA/JB/jb/(2006)D	--
1.2	Fevereiro 2008	Alteração do texto para adaptação à substituição da DGTTF pelo IMTT,IP	--

1.	Introdução	6
1.1.	Organizações responsáveis	6
1.2.	Aprovação	7
1.3.	Disponibilidade e contactos	7
2.	Âmbito e aplicabilidade.....	8
3.	Disposições gerais	9
3.1.	Obrigações.....	9
3.1.1.	Obrigações da Autoridade Portuguesa e da Autoridade Portuguesa Emissora de Cartões	9
3.1.2.	Obrigações da Autoridade Portuguesa de Certificação	9
3.1.3.	Obrigações do Centro de Personalização	10
3.1.4.	Obrigações das Empresas Colaboradoras	10
3.1.5.	Obrigações dos Titulares	10
3.1.6.	Obrigações dos Fabricantes de Unidades de Veículo.....	10
3.1.7.	Obrigações dos Fabricantes de Sensores de Movimento	11
3.2.	Responsabilidade	11
3.2.1.	Responsabilidade da Autoridade Portuguesa e da Autoridade Portuguesa Emissora de Cartões perante os titulares e organismos relacionados.	12
3.2.2.	Responsabilidade da Autoridade Portuguesa de Certificação e do Centro de Personalização perante a Autoridade Portuguesa e a Autoridade Portuguesa Emissora de Cartões.....	12
3.3.	Interpretação e aplicação	12
3.4.	Confidencialidade.....	12
3.4.1.	Informação considerada confidencial	12
3.4.2.	Informação não considerada confidencial	13
4.	Disposições práticas.....	14
5.	Gestão de equipamentos: cartões e tacógrafos	15
6.	Gestão de chaves	16
6.1.	Chave pública da ERCA	16
6.2.	Par de chaves da Autoridade Portuguesa	16
6.2.1.	Geração do par de chaves da Autoridade Portuguesa	17
6.2.2.	Período de validade das chaves	17
6.2.3.	Armazenamento da chave privada da Autoridade Portuguesa.....	18
6.2.4.	Cópia de segurança da chave privada da Autoridade Portuguesa	18
6.2.5.	Delegação de confiança da chave privada da Autoridade Portuguesa	18
6.2.6.	Comprometimento das chaves da Autoridade Portuguesa	18
6.2.7.	Fim de validade das chaves	18
6.3.	Chaves do sensor de movimentos	18
6.4.	Chaves de transporte	19
7.	Chaves dos equipamentos (assimétricas)	21
7.1.	Aspectos genéricos sobre a Autoridade Portuguesa de Certificação, Centro de Personalização e os fabricantes de unidades de veículo	21
7.2.	Geração das chaves dos equipamentos	21
7.2.1.	Validade das chaves dos equipamentos	22
7.2.2.	Protecção e armazenamento das chaves privadas de cartões	22
7.2.3.	Protecção e armazenamento das chaves privadas de unidades de veículo	22
7.2.4.	Delegação de confiança e arquivo de chaves privadas de equipamentos	22

7.2.5.	Arquivo de chaves públicas de equipamentos	22
8.	Gestão dos certificados dos equipamentos	22
8.1.	Entrada de dados	22
8.2.	Certificados dos cartões tacográficos.....	23
8.2.1.	Certificados de condutor	23
8.2.2.	Certificados de centro de ensaio	23
8.2.3.	Certificados de controlo	23
8.2.4.	Certificados de empresa	23
8.3.	Certificados das unidades de veículo	23
8.4.	Validade temporal dos certificados dos equipamentos.....	23
8.5.	Emissão dos certificados dos equipamentos	24
8.6.	Renovação e actualização dos certificados dos equipamentos	24
8.7.	Tarefas informativas da autoridade nacional de certificação.....	24
9.	Segurança da informação	25
9.1.	Gestão da informação da Autoridade Portuguesa de Certificação e do Centro de Personalização	25
9.2.	Classificação e gestão dos recursos da Autoridade Portuguesa de Certificação e do Centro de Personalização	25
9.3.	Controlos de segurança relativos a pessoal da Autoridade Portuguesa de Certificação e do Centro de Personalização	25
9.3.1.	Perfis de confiança	25
9.3.2.	Separação de perfis	27
9.3.3.	Identificação e autenticação para cada perfil	27
9.3.4.	Qualificações, experiência e autorização	27
9.3.5.	Requisitos de formação	27
9.4.	Controlos de segurança relativos aos sistemas da Autoridade Portuguesa de Certificação e do Centro de Personalização	27
9.4.1.	Requisitos técnicos de segurança dos equipamentos informáticos.....	28
9.4.2.	Classificação de segurança dos equipamentos informáticos.....	28
9.4.3.	Controlo de desenvolvimento do sistema	28
9.4.4.	Controlo da gestão de segurança	28
9.4.5.	Network Security Controls	28
9.5.	Procedimentos de auditoria de segurança	28
9.5.1.	Tipos de eventos registados	28
9.5.2.	Frequência do processamento do registo de auditoria	29
9.5.3.	Período de conservação do registo de auditoria.....	29
9.5.4.	Protecção do registo de auditoria	29
9.5.5.	Cópias de segurança do registo de auditoria	29
9.5.6.	Sistemas de recolha de eventos (interno vs. externo)	29
9.6.	Arquivamento de registos	29
9.6.1.	Tipos de eventos armazenados pela Autoridade Portuguesa Emissora de Cartões.....	29
9.6.2.	Tipos de eventos armazenados pela Autoridade Portuguesa de Certificação e pelo Centro de Personalização	30
9.6.3.	Período de conservação do arquivo	30
9.6.4.	Procedimentos para obter e verificar informação arquivada	30
9.7.	Plano de continuidade.....	31
9.7.1.	Comprometimento das chaves nacionais	31
9.7.2.	Recuperação de dados	31
9.8.	Controlo de segurança física	31
9.8.1.	Acesso físico.....	31

10.	Cessação de actividade	33
10.1.	Finalização dos serviços.....	33
10.2.	Transferência de responsabilidades	33
11.	Auditoria.....	34
11.1.	Frequência de auditoria de conformidade das entidades	34
11.2.	Tópicos abrangidos pela auditoria	34
11.3.	Entidade que deve efectuar a auditoria	34
11.4.	Medidas a serem tomadas em caso de deficiência.....	34
11.5.	Comunicação de resultados	34
12.	Procedimentos de alteração da política da autoridade nacional	35
12.1.	Itens alteráveis sem notificação	35
12.2.	Alterações com notificação	35
12.2.1.	Notificação	35
12.2.2.	Período de comentários	35
12.2.3.	Entidades a informar	35
12.3.	Alterações que requerem a aprovação de uma nova política da autoridade nacional.....	35
13.	Conformidade com a política da ERCA	36
14.	Referências	44
	Glossário/Definições e abreviaturas	45
14.1.	Glossário/Definições.....	45
14.2.	Lista de abreviaturas.....	45

1. Introdução

Este documento estabelece a política da Autoridade Portuguesa¹. Esta política aplicar-se-á no funcionamento do sistema do tacógrafo digital.

A política da Autoridade Portuguesa é um documento em que se incluem os requisitos para garantir a segurança da gestão de chaves, certificados e os seus equipamentos associados.

Esta política está conforme com:

- 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
- O Regulamento (CE) n.º 2135/98 do sistema do tacógrafo digital do Conselho de 24 de Setembro de 1998, que altera o Regulamento 3821/85.
- O Regulamento n.º 1360/2002 da Comissão, de 13 de Junho de 2002, que adapta o Regulamento n.º 3821/85 ao progresso técnico
- A política da Autoridade Raiz Europeia (ERCA Policy)

1.1. Organizações responsáveis

O gráfico seguinte mostra a organização do sistema do tacógrafo digital:

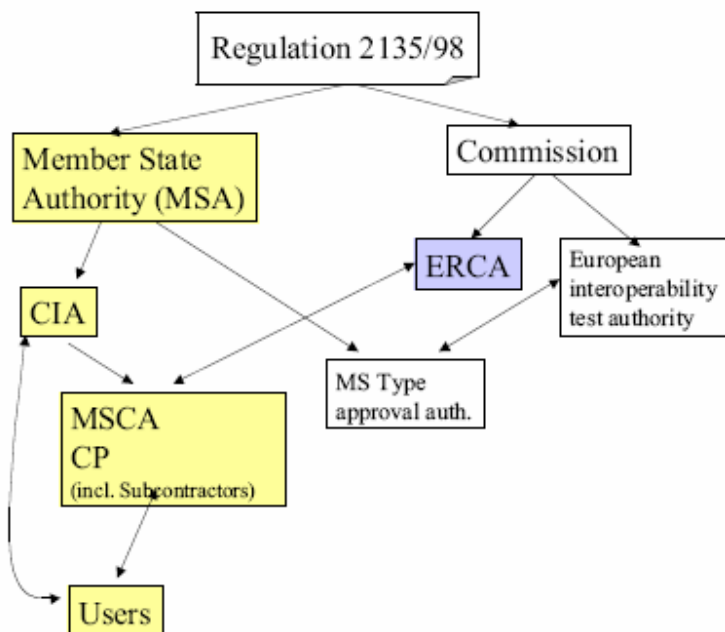


Figura 1 - Organização do sistema do tacógrafo digital

¹ A política da Autoridade de Certificação é uma terminologia comum que estabelece os requisitos para garantir a segurança da gestão de chaves, certificados e, usualmente, cartões para uma determinada CA (Autoridade de Certificação)

A Autoridade Portuguesa responsável por estabelecer as directrizes da presente política é:

IMTT
Instituto da Mobilidade e dos Transportes Terrestres
Av. das Forças Armadas, 40
1649-022 Lisboa

O IMTT assumirá também a função de Autoridade Portuguesa Emissora de Cartões.

A Autoridade Portuguesa de Certificação designada é:

ISQ – Instituto de Soldadura e Qualidade

TagusPark
Av. Prof. Dr. Cavaco Silva, 33
2740-120 Porto Salvo

O Centro de Personalização designado é:

Imprensa Nacional-Casa da Moeda, SA

Av. António José de Almeida
1000-042 Lisboa

1.2. Aprovação

A política da Autoridade Portuguesa foi actualizada pelo Instituto da Mobilidade e dos Transportes Terrestres

1.3. Disponibilidade e contactos

A política da Autoridade Portuguesa está disponível em <http://www.imtt.pt/>.

Quaisquer questões relativas a esta política devem ser dirigidas a:

IMTT
Instituto da Mobilidade e dos Transportes Terrestres
Av. das Forças Armadas, 40
1649-022 Lisboa

2. Âmbito e aplicabilidade

- [1] A política da Autoridade Portuguesa é válida apenas para o sistema do tacógrafo digital.
- [2] As chaves e certificados emitidos pela Autoridade Portuguesa apenas serão utilizados no sistema do tacógrafo digital.
- [3] Os cartões emitidos pelo sistema serão utilizados apenas no sistema do tacógrafo digital.

O diagrama seguinte resume o processo de certificação seguido pela Autoridade Portuguesa de Certificação para o sistema do tacógrafo digital:

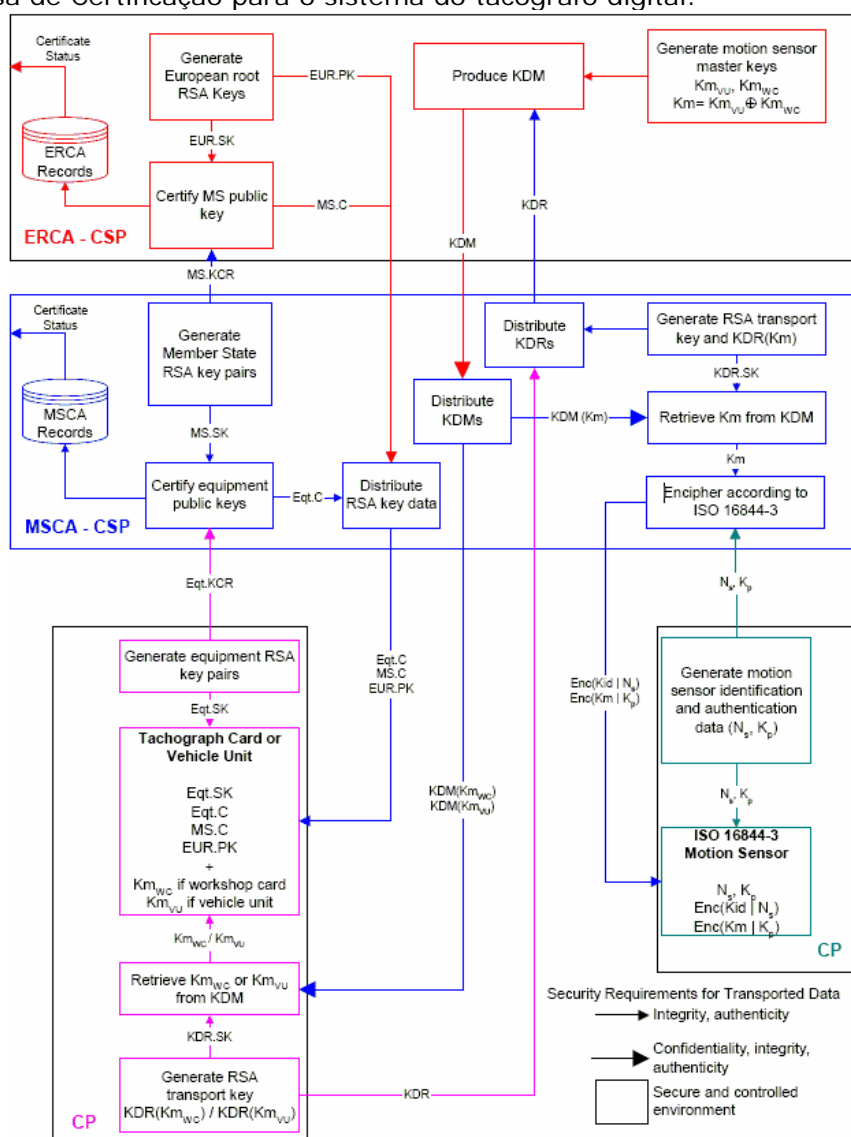


Figura 2 - Gestão de chaves, certificados e equipamentos do sistema do tacógrafo digital

3. Disposições gerais

3.1. Obrigações

Esta secção contém as disposições relativas às obrigações das seguintes entidades:

- Autoridade Portuguesa e Autoridade Portuguesa Emissora de Cartões
- Autoridade Portuguesa de Certificação
- Centro de Personalização
- Utilizadores (titulares, fabricantes de unidades de veículo e fabricantes de sensores de movimento)

3.1.1. Obrigações da Autoridade Portuguesa e da Autoridade Portuguesa Emissora de Cartões

[4] É responsabilidade da Autoridade Portuguesa:

- a) Manter a política nacional
- b) Designar a Autoridade Portuguesa de Certificação e o Centro de Personalização
- c) Auditar a Autoridade Portuguesa de Certificação e o Centro de Personalização
- d) Aprovar as disposições práticas da Autoridade Portuguesa de Certificação e do Centro de Personalização
- e) Informar as entidades designadas acerca desta política
- f) Informar os fabricantes de unidades de veículo e os fabricantes de sensores de movimento acerca desta política
- g) Evitar o uso não autorizado das chaves privadas geradas, armazenadas e utilizadas ao abrigo desta política
- h) Fazer aprovar a presente política pela Comissão

[5] É responsabilidade da Autoridade Portuguesa Emissora de Cartões:

- a) Assegurar que os dados relevantes resultantes dos processos de requisição são correctamente enviados para a Autoridade Portuguesa de Certificação e o Centro de Personalização
- b) Informar os utilizadores (titulares, fabricantes de unidades de veículo e fabricantes de sensores de movimento), dos requisitos definidos nesta política relacionados com a utilização do sistema

3.1.2. Obrigações da Autoridade Portuguesa de Certificação

[6] É responsabilidade da Autoridade Portuguesa de Certificação:

- a) Seguir a presente política
- b) Publicar o documento de Disposições Práticas da Autoridade Portuguesa de Certificação, com referência à presente política, a ser aprovado pela Autoridade Portuguesa
- c) Manter os suficientes recursos organizacionais e financeiros para operar em conformidade com os requisitos definidos na presente política, em particular para fazer face a prejuízos causados por responsabilidade civil.

- [7] A Autoridade Portuguesa de Certificação deve garantir o cumprimento de todos os requisitos definidos na presente política.
- [8] A Autoridade Portuguesa de Certificação é responsável pela conformidade com os procedimentos estabelecidos na presente política.

3.1.3. Obrigações do Centro de Personalização

- [9] É responsabilidade do Centro de Personalização:
- a) Seguir a presente política
 - b) Publicar o documento de Disposições Práticas do Centro de Personalização, com referência à presente política, a ser aprovado pela Autoridade Portuguesa
 - c) Manter os suficientes recursos organizacionais e financeiros para operar em conformidade com os requisitos definidos na presente política, em particular para fazer face a prejuízos causados por responsabilidade civil.
- [10] O Centro de Personalização deve garantir o cumprimento de todos os requisitos definidos na presente política.
- [11] O Centro de Personalização é responsável pela conformidade com os procedimentos estabelecidos na presente política.

3.1.4. Obrigações das Empresas Colaboradoras

- [12] As empresas colaboradoras assumirão as obrigações expressas na presente política através de acordos contratuais estabelecidos com a Autoridade Portuguesa de Certificação, o Centro de Personalização e os utilizadores.

3.1.5. Obrigações dos Titulares

- [13] A Autoridade Portuguesa Emissora de Cartões obrigará, mediante formulário assinado, os utilizadores (ou organizações a que estes pertençam) ao cumprimento das seguintes obrigações:
- a) Fornecer informação verdadeira nos formulários de requisição
 - b) Assegurar que o cartão é utilizado de forma apropriada, apenas para o fim a que se destina e evitar o seu uso indevido, especialmente por terceiros
 - c) Os titulares de um Cartão de Condutor possuirão apenas um cartão válido deste tipo.
 - d) Não utilizar cartões caducados ou danificados
 - e) Informar a autoridade responsável acerca do extravio, furto, dano ou utilização indevida do cartão e/ou da respectiva chave privada

3.1.6. Obrigações dos Fabricantes de Unidades de Veículo

- [14] A Autoridade Portuguesa exigirá, mediante acordo assinado, aos fabricantes de unidades de veículo o cumprimento das seguintes obrigações:

- a) Fornecer informação completa e precisa à Autoridade Portuguesa de acordo com os requisitos estabelecidos na presente política, concretamente no que se refere aos dados de registo
- b) Usar as chaves e certificados exclusivamente no sistema do tacógrafo digital
- c) Usar a chave privada do equipamento exclusivamente na unidade de veículo
- d) Evitar o uso não autorizado da chave privada do equipamento
- e) Notificar de imediato a Autoridade Portuguesa Emissora de Cartões, dentro do período de validade que consta no certificado, se a chave privada do equipamento se perdeu ou se de alguma forma se encontra comprometida

[15] A Autoridade Portuguesa de Certificação poderá suspender, reactivar ou revogar a permissão de utilização do certificado e informar posteriormente a Autoridade Portuguesa.

3.1.7. Obrigações dos Fabricantes de Sensores de Movimento

[16] A Autoridade Portuguesa exigirá, mediante acordo assinado, aos fabricantes de sensores de movimento o cumprimento das seguintes obrigações:

- a) Fornecer informação completa e precisa à Autoridade Portuguesa de acordo com os requisitos estabelecidos na presente política, concretamente no que se refere aos dados de registo
- b) Usar as chaves exclusivamente no sensor de movimentos
- c) Notificar de imediato a Autoridade Portuguesa se a chave se perdeu ou se de alguma forma se encontra comprometida

[17] A Autoridade Portuguesa de Certificação poderá suspender, reactivar ou revogar a permissão de utilização da chave e informar posteriormente a Autoridade Portuguesa.

3.2. Responsabilidade

A Autoridade Portuguesa de Certificação e o Centro de Personalização não terão qualquer responsabilidade perante os utilizadores finais do sistema, apenas a terá perante a Autoridade Portuguesa e a Autoridade Portuguesa Emissora de Cartões.

Qualquer assunto sobre responsabilidade perante os utilizadores finais do sistema será da competência da Autoridade Portuguesa ou da Autoridade Portuguesa Emissora de Cartões.

[18] Os cartões tacográficos, chaves e certificados são para utilização exclusiva no sistema do tacógrafo digital. A presença de quaisquer outros certificados nos cartões constituirá uma violação da presente política e consequentemente nem a Autoridade Portuguesa, nem a Autoridade Portuguesa Emissora de Cartões, nem a Autoridade Portuguesa de Certificação nem o Centro de Personalização serão responsáveis por tal presença ou qualquer uso que lhes sejam dados.

3.2.1. Responsabilidade da Autoridade Portuguesa e da Autoridade Portuguesa Emissora de Cartões perante os titulares e organismos relacionados

- [19] A Autoridade Portuguesa e a Autoridade Portuguesa Emissora de Cartões serão responsáveis pelos danos causados pelo não cumprimento das suas obrigações apenas se tiverem actuado de forma negligente. Se a Autoridade Portuguesa e a Autoridade Portuguesa Emissora de Cartões tiverem actuado de acordo com a presente política ou qualquer outro documento pertinente, tal actuação não será considerada negligente.

3.2.2. Responsabilidade da Autoridade Portuguesa de Certificação e do Centro de Personalização perante a Autoridade Portuguesa e a Autoridade Portuguesa Emissora de Cartões

- [20] A Autoridade Portuguesa de Certificação e o Centro de Personalização serão responsáveis pelos danos causados pelo não cumprimento das suas obrigações apenas se tiverem actuado de forma negligente. Se a Autoridade Portuguesa de Certificação e o Centro de Personalização tiverem actuado de acordo com a presente política e as correspondentes disposições práticas, tal actuação não será considerada negligente.

3.3. Interpretação e aplicação

- [21] Os conflitos que possam surgir da interpretação ou execução da presente política serão resolvidos (...)

3.4. Confidencialidade

A confidencialidade está delimitada pela Lei n.º 67/98, de 26 de Outubro, que transpõe para a ordem jurídica portuguesa a Directiva 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995.

3.4.1. Informação considerada confidencial

- [22] Qualquer informação pessoal ou empresarial detida pela Autoridade Portuguesa de Certificação ou pelo Centro de Personalização e que não esteja presente nos cartões ou certificados emitidos é confidencial e não será divulgada sem o consentimento prévio do utilizador, nem sem (quando aplicável) sem o consentimento prévio da entidade empregadora do utilizador ou seus representantes, excepto quando especificado em contrário pela legislação.
- [23] Todas as chaves privadas e secretas utilizadas ou manejadas durante as operações da Autoridade Portuguesa de Certificação e o Centro de Personalização, no âmbito da presente política, serão confidenciais.
- [24] Todas as chaves privadas e secretas utilizadas ou manejadas durante as operações dos fabricantes de unidades de veículo, no âmbito da presente política, serão confidenciais.

- [25] Todas as chaves privadas e secretas utilizadas ou manejadas durante as operações dos fabricantes de sensores de movimento, no âmbito da presente política, serão confidenciais.
- [26] Os arquivos de auditoria e os registos não serão disponibilizados por inteiro, excepto quando requerido por lei.

3.4.2. Informação não considerada confidencial

- [27] Os certificados não são considerados confidenciais.
- [28] A informação de identificação ou outra qualquer informação pessoal ou empresarial presente nos cartões ou certificados não se considera confidencial, salvo se disposições ou acordos especiais assim o estipulem.

4. Disposições práticas

[29] A Autoridade Portuguesa de Certificação e o Centro de Personalização terão um documento que enumere um conjunto de disposições práticas e procedimentos a seguir para cumprir os requisitos estabelecidos nesta política, adiante designados por Disposições Práticas. A Autoridade Portuguesa deverá aprovar tais documentos.

Em particular:

- a) O documento deve identificar as obrigações de todas as entidades externas que suportem serviços da Autoridade Portuguesa de Certificação ou do Centro de Personalização incluindo as políticas e práticas aplicáveis.
- b) O documento deve ser tratado como informação restrita e disponibilizado à Autoridade Portuguesa. O conteúdo do documento de Disposições Práticas pode no entanto ser disponibilizado aos utilizadores do sistema do tacógrafo digital e outras entidades relacionadas com este (e.g. organismos de controlo) sempre que tal seja considerado necessário.

Em qualquer caso, não será geralmente necessário que a Autoridade Portuguesa de Certificação ou o Centro de Personalização tornem públicos todos os detalhes das suas práticas.

- c) Os órgãos gestores da Autoridade Portuguesa de Certificação e do Centro de Personalização têm a responsabilidade de garantir que as práticas e procedimentos descritos no documento de Disposições Práticas estão devidamente implementados;
- d) A Autoridade Portuguesa de Certificação e o Centro de Personalização definirão um processo de revisão para o PS;
- e) A Autoridade Portuguesa de Certificação e o Centro de Personalização notificarão as autoridades competentes sobre quaisquer alterações que se proponham fazer aos documentos de Disposições Práticas e, logo que aprovado, disponibilizará de forma imediata o documento revisto.

5. Gestão de equipamentos: cartões e tacógrafos

- [30] A Autoridade Portuguesa de Certificação assegurar-se-á, segundo instruções da Autoridade Portuguesa, de que os certificados produzidos e as chaves secretas correspondem ao seu propósito e serão utilizados unicamente em cartões e tacógrafos que cumpram o Regulamento (EC) 2135/98.
- [31] A Autoridade Portuguesa de Certificação recusará a emissão de chaves e certificados se existir o risco de estes serem utilizados indevidamente.
- [32] A Autoridade Portuguesa Emissora de Cartões e o Centro de Personalização garantirão o cumprimento dos procedimentos e instruções do Regulamento (EC) 2135/98.
- [33] A Autoridade Portuguesa Emissora de Cartões e o Centro de Personalização garantirão que a emissão de cartões de substituição ou renovação ocorrerá apenas aquando se verificarem os requisitos mencionados no Regulamento (EC) 2135/98 e que os respectivos prazos estabelecidos serão cumpridos.
- [34] O Centro de Personalização garantirá que a personalização dos cartões se leva a cabo segundo as instruções do Regulamento (EC) 2135/98. A integridade dos dados inseridos deve ser especialmente respeitada.
- [35] A Autoridade Portuguesa de Certificação e o Centro de Personalização garantirão que as chaves privadas e secretas serão armazenadas e utilizadas num ambiente seguro.
- [36] A Autoridade Portuguesa Emissora de Cartões disporá de dados suficientes para associar cada cartão a um utilizador ou titular.
- [37] A Autoridade Portuguesa Emissora de Cartões garantirá que os cartões serão entregues de acordo com o mencionado no Regulamento (EC) 2135/98 e que o utilizador seja identificado num qualquer momento do processo de pedido de emissão de cartão ou na entrega do mesmo.
- [38] O Centro de Personalização garantirá que os cartões de centro de ensaio terão associado um PIN que cumpra as instruções do Regulamento (EC) 2135/98.
- [39] O PIN será gerado num ambiente seguro, de acesso controlado, que garanta a sua associação a apenas um cartão de centro de ensaio. Uma vez gerado será impresso e enviado ao seu destinatário por via segura e nunca a acompanhar o cartão correspondente.
- [40] A reconstrução do PIN deve ser impossível.

6. Gestão de chaves

Esta secção contém as disposições para a gestão de:

- Chave raiz europeia, chave pública da ERCA
- Chaves do Estado Português
- Chaves do Sensor de Movimentos
- Chaves de transporte (entre a ERCA e a Autoridade Portuguesa de Certificação)

A chave pública da ERCA é utilizada para verificar os certificados portugueses.

As chaves do Estado Português são as chaves assinadas de Portugal e também podem ser denominadas chaves raiz portuguesas.

As chaves do sensor de movimentos são as chaves simétricas que se colocam nos cartões de centro de ensaio, nas unidades de veículo e nos sensores de movimentos para reconhecimento mútuo. A Autoridade Portuguesa de Certificação recebe as chaves do sensor de movimentos da ERCA, armazena-as e distribui-as aos fabricantes homologados.

As chaves de transporte são pares de chaves assimétricas empregues para o intercâmbio seguro de informação entre a ERCA e a Autoridade Portuguesa de Certificação.

Se a Autoridade Portuguesa de Certificação necessitar de outras chaves criptográficas distintas das referidas anteriormente, estas não são consideradas parte do sistema do tacógrafo digital e não serão objecto da presente política.

6.1. Chave pública da ERCA

- [41] A Autoridade Portuguesa de Certificação deve manter a chave pública da ERCA (EUR.PK) de forma a garantir a sua permanente integridade e disponibilidade.
- [42] A Autoridade Portuguesa de Certificação deve reconhecer o formato de distribuição de certificados descrito no Anexo B da política da ERCA.
- [43] O Centro de Personalização e os fabricantes de equipamentos garantirão a inserção da EUR.PK em todos os cartões tacográficos e unidades de veículo que estejam sob a sua responsabilidade.

6.2. Par de chaves da Autoridade Portuguesa

As chaves portuguesas são utilizadas para assinar todos os certificados gerados para os equipamentos. Este par de chaves consiste em uma chave pública (P.PK) e uma chave privada ou secreta (P.SK).

- [44] A chave pública da Autoridade Portuguesa será certificada pela ERCA, mas será gerada pela Autoridade Portuguesa de Certificação.
- [45] A Autoridade Portuguesa deverá ter em conta o prazo necessário para a certificação de chaves requerido pela ERCA.
- [46] A Autoridade Portuguesa deverá utilizar o formato para solicitação de certificados definido no Anexo A da política da ERCA.
- [47] A Autoridade Portuguesa assegurar-se-á que as chaves serão utilizadas exclusivamente para:
 - Assinaturas digitais dos equipamentos do sistema do tacógrafo digital,
 - Geração da solicitação de certificação para a ERCA,
 - Emissão de listas de revogação de certificados.

6.2.1. Geração do par de chaves da Autoridade Portuguesa

- [48] A geração do(s) par(es) de chaves da Autoridade Portuguesa ocorrerá num equipamento que:
 - obedeça aos requisitos identificados no FIPS 140-2 (ou 140-1) nível 3 ou superior; ou
 - obedeça aos requisitos identificados no CEN Workshop Agreement 14167-2; ou
 - seja um sistema confiável que garanta o cumprimento da EAL4 ou superior de acordo com a ISO 15408, ou E3 ou superior na ITSEC, ou
 - demonstre que disponibiliza um nível de segurança equivalente.
- [49] A Autoridade Portuguesa de Certificação assinará os certificados dos equipamentos no mesmo equipamento utilizado para armazenar as chaves privadas.
- [50] O equipamento utilizado e os requisitos cumpridos serão especificados no documento de Disposições Práticas da Autoridade Portuguesa de Certificação.
- [51] A geração de pares de chaves da Autoridade Portuguesa obrigará à participação activa de duas pessoas. Pelo menos uma delas terá a função de administrador da Autoridade de Certificação.
- [52] A Autoridade Portuguesa de Certificação terá pelo menos duas (2) e no máximo cinco (5) pares de chaves e os seus certificados respectivos para assegurar a continuidade.

6.2.2. Período de validade das chaves

- [53] Cada par de chaves da Autoridade Portuguesa será utilizado por um período máximo de dois anos a partir da certificação da correspondente chave pública, e será destruído pela Autoridade Portuguesa para prevenir o seu uso futuro.

6.2.3. Armazenamento da chave privada da Autoridade Portuguesa

- [54] As chaves privadas serão armazenadas e utilizadas num equipamento devidamente protegido que:
- obedeça aos requisitos identificados no FIPS 140-2 (ou 140-1) nível 3 ou superior; ou
 - seja um sistema confiável que garanta o cumprimento da EAL4 ou superior de acordo com a ISO 15408, ou E3 ou superior na ITSEC, ou
 - demonstre que disponibiliza um nível de segurança equivalente.
- [55] Nenhuma pessoa possuirá individualmente os meios necessários para aceder ao ambiente onde as chaves privadas se encontram armazenadas.

6.2.4. Cópia de segurança da chave privada da Autoridade Portuguesa

- [56] Poderão existir cópias de segurança das chaves privadas utilizando um procedimento de recuperação que exija controlo dual. O procedimento utilizado deverá ser especificado no documento de Disposições Práticas da Autoridade Portuguesa de Certificação. No entanto, se forem utilizadas chaves como definido em [52], as cópias de segurança são desnecessárias.

6.2.5. Delegação de confiança da chave privada da Autoridade Portuguesa

- [57] Não é permitida a delegação de confiança das chaves privadas da Autoridade Portuguesa.

6.2.6. Comprometimento das chaves da Autoridade Portuguesa

- [58] Existirão instruções escritas, incluídas no documento de Disposições Práticas da Autoridade Portuguesa de Certificação, que descrevam as providências a tomar pelos utilizadores e responsáveis de segurança da autoridade de certificação se as chaves privadas tiverem sido expostas ou se se considerar ou suspeitar que as mesmas foram comprometidas.
- [59] Neste caso, a Autoridade Portuguesa de Certificação deverá informar a Autoridade Portuguesa, a ERCA e todas as outras autoridades de certificação dos restantes estados membros.

6.2.7. Fim de validade das chaves

- [60] A Autoridade Portuguesa de Certificação deverá ter mecanismos que garantam que possui sempre um par de chaves nacional certificado.
- [61] Uma vez terminada a utilização de um par de chaves, a chave pública será arquivada e a correspondente chave privada será destruída de forma a impossibilitar a sua recuperação.

6.3. Chaves do sensor de movimentos

- [62] A Autoridade Portuguesa de Certificação solicitará à ERCA, conforme necessárias, as chaves do sensor de movimentos Km, Kmvu, e Kmwc (Anexo IB, Apêndice 11:3.1.3).
- [63] A solicitação das chaves simétricas para o sensor de movimentos utilizando o protocolo definido no Anexo D da política da ERCA.

- [64] A Autoridade Portuguesa de Certificação, quando solicitado pelo fabricante, encriptará os dados do sensor de movimentos (emparelhando a chave Kp com o número de série Ns) utilizando a chave Km (Anexo IB, Apêndice 11:3.1.3). A Autoridade Portuguesa de Certificação assegurará que a chave Km é utilizada apenas para este fim.
- [65] A Autoridade Portuguesa de Certificação enviará aos fabricantes de unidades de veículo, utilizando meios adequadamente seguros, a chave Kmvu para inserção nas unidades de veículo (Anexo IB, Apêndice 11:3.1.3).
- [66] A Autoridade Portuguesa de Certificação enviará ao Centro de Personalização a chave Kmwc para inserção nos cartões de centro de ensaio.
- [67] O Centro de Personalização assegurará a função da Autoridade Portuguesa de Certificação de garantir que a chave Kmwc é inserida em todos os cartões de centro de ensaio emitidos (Anexo IB, Apêndice 11:3.1.3).
- [68] A Autoridade Portuguesa de Certificação e o Centro de Personalização devem prevenir o uso não autorizado das chaves do sensor de movimentos e, durante o seu armazenamento, utilização e distribuição protegê-las com controlos de segurança físicos e lógicos. As chaves deverão ser armazenadas e utilizadas num equipamento devidamente protegido que:
- obedeça aos requisitos identificados no FIPS 140-2 (ou 140-1) nível 3 ou superior; ou
 - seja um sistema confiável que garanta o cumprimento da EAL4 ou superior de acordo com a ISO 15408, ou E3 ou superior na ITSEC, ou
 - demonstre que disponibiliza um nível de segurança equivalente.

6.4. Chaves de transporte

- [69] Para garantir a segurança das comunicações, a Autoridade Portuguesa de Certificação emitirá chaves assimétricas especiais para transporte. Durante o armazenamento, utilização e distribuição será protegida a parte privada destas chaves com controlos que garantam a segurança física e lógica. As chaves deverão ser armazenadas e utilizadas num equipamento devidamente protegido que:
- obedeça aos requisitos identificados no FIPS 140-2 (ou 140-1) nível 3 ou superior; ou
 - seja um sistema confiável que garanta o cumprimento da EAL4 ou superior de acordo com a ISO 15408, ou E3 ou superior na ITSEC, ou
 - demonstre que disponibiliza um nível de segurança equivalente.
- [70] A Autoridade Portuguesa assegurará que o identificador de chave (KID) e o módulo das chaves de transporte submetidas à ERCA para certificação e distribuição das chaves do sensor de movimentos são únicos no domínio da Autoridade Portuguesa de Certificação.

- [71] A Autoridade Portuguesa assegurar-se-á de que os meios físicos empregues no transporte da solicitação da certificação de chaves da Autoridade Portuguesa de Certificação, dos certificados da Autoridade Portuguesa de Certificação, da chave pública da ERCA e das chaves do sensor de movimentos são os descritos no Anexo C da política da ERCA.

7. Chaves dos equipamentos (assimétricas)

As chaves dos equipamentos são chaves assimétricas geradas nalgum ponto do processo de emissão/produção, e certificadas pela Autoridade Portuguesa de Certificação para os equipamentos do sistema do tacógrafo digital:

- Cartões tacográficos
- Unidades de veículo

7.1. Aspectos genéricos sobre a Autoridade Portuguesa de Certificação, Centro de Personalização e os fabricantes de unidades de veículo

- [72] Na inicialização dos equipamentos (cartões e unidades de veículo), a inserção da chave e a personalização será levada a cabo num ambiente fisicamente seguro e controlado. O acesso a esta área será estritamente regulado, controlável individualmente, e requerendo a presença de pelo menos duas pessoas para operar o sistema. Serão guardados registos dos acessos e operações efectuadas no sistema.
- [73] Nenhuma informação confidencial contida no sistema de geração de chaves sairá do mesmo de alguma forma que viole a política estabelecida neste documento.
- [74] Nenhuma informação confidencial contida nos sistemas de personalização sairá dos mesmos de alguma forma que viole a política estabelecida neste documento.

7.2. Geração das chaves dos equipamentos

- [75] A entidade que proceder à geração das chaves garantirá que estas são geradas de uma forma segura e que as chaves privadas dos equipamentos são mantidas secretas.
- [76] A geração das chaves ocorrerá num equipamento que:
- obedeça aos requisitos identificados no FIPS 140-2 (ou 140-1) nível 3 ou superior; ou
 - obedeça aos requisitos identificados no CEN Workshop Agreement 14167-2; ou
 - seja um sistema confiável que garanta o cumprimento da EAL4 ou superior de acordo com a ISO 15408, ou E3 ou superior na ITSEC, ou
 - demonstre que disponibiliza um nível de segurança equivalente.
- [77] Os processos de geração e armazenamento da chave privada prevenirão que a mesma seja exposta fora do ambiente que a criou. Para além disso, a chave privada deve ser apagada do sistema imediatamente após a sua inserção no equipamento a que se destina.

- [78] Os pedidos de certificação de chaves que dependam do transporte de chaves privadas não são permitidos.
- [79] É responsabilidade da entidade que procede à geração das chaves tomar as providências necessárias para assegurar a unicidade da chave pública no seu domínio antes de ocorrer o processo de certificação.

7.2.1. Validade das chaves dos equipamentos

- [80] O uso de chaves privadas de equipamentos relacionadas com os certificados emitidos no âmbito desta política não excederá nunca o fim da validade do certificado.

7.2.2. Protecção e armazenamento das chaves privadas de cartões

- [81] O Centro de Personalização assegurará que a chave privada esteja protegida por, e restrita a, um cartão que tenha sido entregue ao seu titular de acordo com os procedimentos definidos na presente política.
- [82] Serão mantidas cópias da chave privada apenas no cartão tacográfico. Caso o seu uso seja necessário durante o processo de personalização, as chaves devem ser mantidas encriptadas.

7.2.3. Protecção e armazenamento das chaves privadas de unidades de veículo

- [83] O fabricante de unidades de veículo assegurará que a chave privada esteja protegida por, e restrita a, uma unidade de veículo.
- [84] Serão mantidas cópias da chave privada apenas na unidade de veículo. Caso o seu uso seja necessário durante o processo de personalização, as chaves devem ser mantidas encriptadas.

7.2.4. Delegação de confiança e arquivo de chaves privadas de equipamentos

- [85] A caução e o arquivamento de chaves privadas de equipamentos não são permitidos.

7.2.5. Arquivo de chaves públicas de equipamentos

- [86] Todas as chaves públicas certificadas serão arquivadas pela Autoridade Portuguesa de Certificação.

8. Gestão dos certificados dos equipamentos

Esta secção descreve o ciclo de vida dos certificados, incluindo o seu registo, emissão, distribuição, utilização, renovação e fim de período de validade.

8.1. Entrada de dados

- [87] Na emissão dos certificados dos equipamentos, a Autoridade Portuguesa de Certificação verificará a unicidade do número de referência do titular do certificado (CHR).

8.2. Certificados dos cartões tacográficos

8.2.1. Certificados de condutor

[88] Só serão emitidos certificados de condutor para as solicitações comprovadamente correctas de um cartão de condutor.

8.2.2. Certificados de centro de ensaio

[89] Só serão emitidos certificados de centro de ensaio para as solicitações comprovadamente correctas de um cartão de centro de ensaio.

8.2.3. Certificados de controlo

[90] Só serão emitidos certificados de controlo para as solicitações comprovadamente correctas de um cartão de controlo.

8.2.4. Certificados de empresa

[91] Só serão emitidos certificados de empresa para as solicitações comprovadamente correctas de um cartão de empresa.

8.3. Certificados das unidades de veículo

[92] A Autoridade Portuguesa de Certificação apenas emitirá certificados a fabricantes de unidades de veículo e para unidades de veículo homologadas em Portugal.

[93] Para obter os certificados das unidades de veículo os fabricantes deverão fornecer pelo menos:

- os dados identificativos do dispositivo (por exemplo, homologação e número de série) ou um CRI (*Certificate Request Identifier* – Identificador de Pedido de Certificado) no caso em que o dispositivo não esteja identificado;
- o nome completo do fabricante;
- um número de identificação reconhecido em Portugal, ou quaisquer outros atributos que possam ser utilizados para, tanto quanto possível, distinguir o fabricante de outros com o mesmo nome.

8.4. Validade temporal dos certificados dos equipamentos

[94] Os certificados não terão um período de validade superior à validade do equipamento correspondente:

- os certificados de condutor terão um período de validade não superior a 5 anos (Regulamento 14.4.a).
- os certificados de centro de ensaio terá um período de validade não superior a 1 ano (Regulamento 12.1).
- os certificados de controlo terão uma validade não superior a 5 anos.
- os certificados de empresa terão uma validade não superior a 5 anos.

- os certificados das unidades de veículo terão uma validade não superior a 30 anos.

8.5. Emissão dos certificados dos equipamentos

[95] A Autoridade Portuguesa de Certificação assegurar-se-á de que emite os certificados de modo a que seja mantida a sua integridade e autenticidade. O conteúdo dos certificados está definido pelo Anexo IB do Regulamento, apêndice 11.

8.6. Renovação e actualização dos certificados dos equipamentos

Dado que os certificados e os cartões têm o mesmo tempo de validade, serão tratados em conjunto. É assumido que o tempo de vida dos equipamentos é mais curto que aquele dos certificados.

8.7. Tarefas informativas da autoridade nacional de certificação

- [96] A Autoridade Portuguesa de Certificação será responsável pela transferência de todos os dados respeitantes aos certificados tanto para o Centro de Personalização como para os fabricantes para que certificados, equipamentos bem como cartões e titulares estejam inequivocamente relacionados.
- [97] No caso de que algumas autoridades tenham um interesse legítimo em informação acerca do funcionamento da Autoridade Portuguesa de Certificação ou suas empresas colaboradoras, e não existindo qualquer norma ou consideração de segurança que a impeça de proporcionar essa informação, a Autoridade Portuguesa de Certificação deve disponibilizá-la tão depressa quanto possível em coordenação com a Autoridade Portuguesa.
- [98] O funcionamento da Autoridade Portuguesa de Certificação será considerado confidencial. A informação por ela gerida apenas poderá ser consultada nas instalações da própria Autoridade Portuguesa de Certificação, mediante acordo prévio da Autoridade Nacional, sempre e quando exista um interesse legítimo demonstrado e quando a confidencialidade da informação seja adequadamente protegida junto do receptor da mesma.
- [99] A Autoridade Portuguesa de Certificação manterá e disponibilizará informação sobre o estado dos certificados.

9. Segurança da informação

9.1. Gestão da informação da Autoridade Portuguesa de Certificação e do Centro de Personalização

- [100] A Autoridade Portuguesa de Certificação e o Centro de Personalização assegurarão que os procedimentos administrativos e de gestão aplicados são adequados e correspondam a standards reconhecidos.
- [101] A Autoridade Portuguesa de Certificação e o Centro de Personalização serão responsáveis por todos os aspectos referentes aos serviços de certificação de chaves ainda que algumas funções sejam subcontratadas a outras entidades. A responsabilidade destas entidades deve ser claramente definida e devem ser tomadas as necessárias providências para assegurar que estas entidades estejam obrigadas a implementar quaisquer controlos requeridos pela Autoridade Portuguesa de Certificação ou pelo Centro de Personalização.
- [102] A infra-estrutura de segurança necessária à adequada gestão da informação da Autoridade Portuguesa de Certificação e do Centro de Personalização deve ser mantida permanentemente. Qualquer alteração que impacte com o nível de segurança disponível deve ser aprovada pela Autoridade Portuguesa.
- [103] A Autoridade Portuguesa de Certificação e o Centro de Personalização adoptarão um sistema de gestão de segurança equivalente à ISO 17799. Não é requerida a certificação formal.

9.2. Classificação e gestão dos recursos da Autoridade Portuguesa de Certificação e do Centro de Personalização

- [104] A Autoridade Portuguesa de Certificação e o Centro de Personalização assegurar-se-ão de que os seus recursos e informação têm um nível adequado de protecção.

Concretamente:

- a) A Autoridade Portuguesa de Certificação e o Centro de Personalização levarão a cabo uma análise de risco para avaliar e determinar as medidas de segurança necessárias e os procedimentos operacionais.
- b) A Autoridade Portuguesa de Certificação e o Centro de Personalização manterão um inventário com todos os seus recursos de informação e atribuir-lhes-ão uma classificação quanto aos requisitos de protecção aplicáveis a esses recursos consistente com a análise de risco.

9.3. Controlos de segurança relativos a pessoal da Autoridade Portuguesa de Certificação e do Centro de Personalização

9.3.1. Perfis de confiança

- [105] A Autoridade Portuguesa de Certificação e o Centro de Personalização, de acordo com esta política, estabelecerão três perfis diferentes de utilizadores, que se descrevem seguidamente.

[106] Para garantir que nenhuma pessoa individualmente possa ultrapassar as salvaguardas de segurança, as atribuições nos sistemas da Autoridade Portuguesa de Certificação e do Centro de Personalização serão desempenhadas por múltiplos perfis e indivíduos. Cada conta no sistema terá limitadas as suas capacidades de acordo com o perfil do proprietário da conta.

[107] Os perfis são:

- a) Certification Authority Administrator or Personalization Administrator (CAA/PA)
- b) System Administrator (SA)
- c) Information System Security Officer (ISSO)

[108] O perfil CAA/PA inclui:

- a) A geração de chaves
- b) A geração de certificados
- c) Personalização e distribuição segura de equipamentos
- d) Funções administrativas associadas à manutenção da base de dados da Autoridade Portuguesa de Certificação e do Centro de Personalização e o acompanhamento de investigações a eventuais quebras de segurança

[109] O perfil SA inclui:

- a) A configuração inicial do sistema incluindo mecanismos seguros de inicialização e shut down
- b) A configuração inicial de todas as novas contas
- c) A configuração inicial da rede
- d) A criação de suportes para a reinicialização do sistema em caso de perda do mesmo
- e) A execução de cópias de segurança do sistema, actualizações e recuperação de software, incluindo o armazenamento seguro e a distribuição de cópias de segurança para uma localização remota. As cópias de segurança serão efectuadas pelo menos semanalmente, e o sistema deve ser reinicializado após a execução desta para que sejam efectuados os testes de integridade do hardware.

[110] O perfil ISSO inclui:

- a) A atribuição de privilégios de segurança e controlos de acesso aos CAA/PA
- b) A definição de *passwords* para todas as novas contas
- c) O arquivamento dos necessários registos de sistema
- d) A análise dos registos de auditoria do sistema para verificar o cumprimento pelos CAA/PA da política de segurança do sistema. Esta análise será feita pelo menos semanalmente
- e) A condução ou supervisão de um inventário anual dos registos da Autoridade Portuguesa de Certificação e do Centro de Personalização
- f) A participação na geração das chaves nacionais

9.3.2. Separação de perfis

[111] Na Autoridade Portuguesa de Certificação e no Centro de Personalização devem ser nomeados indivíduos distintos para cada um dos três perfis acima descritos.

9.3.3. Identificação e autenticação para cada perfil

[112] Os mecanismos de identificação e autenticação dos CAA/PA, SA e ISSO devem ser adequados e consistentes com as práticas, procedimentos e condições estabelecidos nesta política.

9.3.4. Qualificações, experiência e autorização

[113] Todo o pessoal da Autoridade Portuguesa de Certificação e do Centro de Personalização que ocupe cargos sensíveis, incluindo pelo menos todas as posições de CAA/PA e ISSO deverão:

- a) Não terem outras tarefas que possam entrar em conflito com os seus deveres e responsabilidades enquanto CAA/PA e ISSO
- b) Não terem sido previamente dispensados de outros cargos por motivo de negligência ou não cumprimento de deveres
- c) Ter recebido formação adequada ao desempenho das suas funções

[114] A Autoridade Portuguesa de Certificação e o Centro de Personalização podem também especificar requisitos adicionais como por exemplo cidadania, qualificação e ausência de antecedentes criminais. Tais requisitos deverão estar detalhados no correspondente documento de Disposições Práticas.

9.3.5. Requisitos de formação

[115] Todo o pessoal deverá ter formação adequada ao seu perfil e funções.

9.4. Controlos de segurança relativos aos sistemas da Autoridade Portuguesa de Certificação e do Centro de Personalização

[116] A Autoridade Portuguesa de Certificação e o Centro de Personalização assegurar-se-ão de que os seus sistemas sejam operados de forma segura e correcta, com um risco mínimo de falha.

Em particular:

- a integridade dos sistemas e da informação será protegida contra vírus, *software* malicioso e não autorizado
- os danos causados por incidentes de segurança ou mau funcionamento serão minimizados mediante a utilização de mecanismos de resposta e informação de incidentes

[117] Os sistemas da Autoridade Portuguesa de Certificação e do Centro de Personalização disponibilizarão os controlos de segurança adequados para fazer cumprir a separação de perfis descrita nesta política o no correspondente documento de Disposições Práticas.

9.4.1. Requisitos técnicos de segurança dos equipamentos informáticos

[118] A inicialização dos sistemas em que são utilizadas as chaves privadas de certificação da Autoridade Portuguesa de Certificação requer a co-operação por pelo menos dois operadores, sendo ambos autenticados pelo sistema.

9.4.2. Classificação de segurança dos equipamentos informáticos

[119] Os sistemas da Autoridade Portuguesa de Certificação e do Centro de Personalização não necessitam qualquer classificação formal desde que cumpram todos os requisitos desta secção.

9.4.3. Controlo de desenvolvimento do sistema

[120] Será levada a cabo uma análise dos requisitos de segurança durante a fase de desenho e especificação de requisitos em qualquer projecto de desenvolvimento de sistemas levado a cabo pela Autoridade Portuguesa de Certificação ou pelo Centro de Personalização ou em seu nome para garantir que esses requisitos estarão implementados nos sistemas de informação.

[121] Estarão definidos procedimentos de controlo de alterações para novas versões ou modificações a qualquer *software* operacional.

9.4.4. Controlo da gestão de segurança

[122] Os perfis de sistema serão implementados e obrigatoriamente utilizados.

9.4.5. Network Security Controls

[123] Serão implementados controlos (por exemplo, firewalls) de forma a proteger os domínios de rede internos da Autoridade Portuguesa de Certificação e do Centro de Personalização de domínios de rede externos acessíveis por terceiros.

[124] Os dados considerados sensíveis serão protegidos quando transmitidos sobre redes não seguras.

9.5. Procedimentos de auditoria de segurança

Os procedimentos de auditoria de segurança descritos nesta secção são válidos para todas os componentes do sistema que afectem o resultado dos processos de emissão de chaves, certificados e equipamentos abrangidos por esta política.

9.5.1. Tipos de eventos registados

[125] As funções de auditoria de segurança dos sistemas da Autoridade Portuguesa de Certificação e do Centro de Personalização registarão:

- a) A criação de contas
- b) Os pedidos de execução de transacções junto com a conta que os solicitou, tipo de pedido, indicação se a transacção se concluiu e a eventual causa da não conclusão da transacção
- c) Instalação ou actualização de software
- d) Data e hora, bem como qualquer outra informação descritiva acerca de todas as cópias de segurança

- e) Shutdowns e reinicializações do sistema.
- f) Data e hora de todas as actualizações de hardware
- g) Data e hora da descarga de registos de auditoria
- h) Data e hora da descarga de arquivos de transacções

9.5.2. Frequência do processamento do registo de auditoria

[126] O registo de auditoria será processado regularmente e analisado para evitar utilização maliciosa ou fraudulenta. Os procedimentos respectivos serão descritos no documento de Disposições Práticas.

9.5.3. Período de conservação do registo de auditoria

[127] O registo de auditoria será conservado pelo prazo de pelo menos 2 anos.

9.5.4. Protecção do registo de auditoria

[128] A integridade dos registo de auditoria será adequadamente protegida. Todas as entradas terão um timestamp associado (sendo suficiente o tempo do sistema).

[129] Os registos de auditoria serão verificados e consolidados pelo menos mensalmente. Pelo menos duas pessoas com perfil SA ou ISSO estarão presentes durante este procedimento.

9.5.5. Cópias de segurança do registo de auditoria

[130] As cópias de segurança do registo de auditoria serão protegidas contra o acesso não autorizado.

9.5.6. Sistemas de recolha de eventos (interno vs. externo)

[131] Apenas é necessário um sistema de recolha de eventos interno.

9.6. Arquivamento de registos

9.6.1. Tipos de eventos armazenados pela Autoridade Portuguesa Emissora de Cartões

[132] Os registos incluirão todos os factos e documentos relevantes na posse da Autoridade Portuguesa Emissora de Cartões:

- a) Solicitação de certificados e mensagens relacionadas intercambiadas com a Autoridade Portuguesa de Certificação, o Centro de Personalização, utilizadores e o directório
- b) Os formulários assinados dos pedidos de emissão de cartões e certificados pelos utilizadores, incluindo a identificação da pessoa responsável por aceitar o pedido
- c) A aceitação assinada da entrega dos cartões
- d) Acordos contratuais relativos aos certificados e cartões associados
- e) Renovação de certificados e todas as mensagens trocadas com o utilizador
- f) Mensagens trocadas com o originador do pedido e/ou o utilizador
- g) Documentos relativos à política actual e às implementadas anteriormente

9.6.2. Tipos de eventos armazenados pela Autoridade Portuguesa de Certificação e pelo Centro de Personalização

[133] Os registos incluirão todos os factos e documentos relevantes na posse da Autoridade Portuguesa de Certificação e do Centro de Personalização:

- a) Conteúdo dos certificados emitidos
- b) Documentos informativos de auditoria que incluam registos das auditorias anuais ao cumprimento pela Autoridade Portuguesa de Certificação e pelo Centro de Personalização das respectivas disposições práticas
- c) Documentos relativos à política actual e às implementadas anteriormente

[134] Os registos de todos os pedidos electrónicos assinados digitalmente feitos por pessoal da Autoridade Portuguesa de Certificação e do Centro de Personalização (CAA/PA) devem incluir a identificação do administrador responsável por cada pedido conjuntamente com toda a informação necessária à não repudição enquanto o registo for conservado.

9.6.3. Período de conservação do arquivo

[135] Os arquivos deverão ser conservados e protegidos contra alteração ou destruição por um período definido no documento de Disposições Práticas aplicável.

9.6.4. Procedimentos para obter e verificar informação arquivada

[136] A Autoridade Portuguesa de Certificação e o Centro de Personalização actuarão em cumprimento dos requisitos relativos a confidencialidade definidos na secção 3.4.

[137] Os registos de transacções individuais podem ser disponibilizados a pedido de qualquer uma das entidades envolvida na transacção, ou um seu representante.

[138] A Autoridade Portuguesa de Certificação e o Centro de Personalização disponibilizarão, após pedido justificado, documentação relativa ao seu cumprimento das disposições práticas aplicáveis, de acordo com a secção 11.5.

[139] De forma regulada, poderia cobrar-se uma taxa razoável para cobrir os custos de recuperação de registos.

[140] A Autoridade Portuguesa de Certificação e o Centro de Personalização garantirão a disponibilidade do arquivo e que a informação arquivada terá um formato legível durante o seu período de conservação, ainda que as suas operações sejam interrompidas, suspensas ou terminadas.

[141] No caso em que os serviços da Autoridade Portuguesa de Certificação ou do Centro de Personalização sejam interrompidos, suspensos ou terminados, esses organismos deverão notificar todas as organizações clientes de forma a garantir a disponibilidade ininterrupta do arquivo. Todos os pedidos de acesso a informação arquivada serão dirigidos à Autoridade Portuguesa de

Certificação ou ao Centro de Personalização ou às entidades por estes indicadas antes do termo dos seus serviços.

9.7. Plano de continuidade

[142] A Autoridade Portuguesa de Certificação e o Centro de Personalização terão um plano de continuidade de negócio (BCP). Este incluirá (mas não está limitado a) eventos tais como:

- Comprometimento das chaves
- Perda catastrófica de dados devida a, por exemplo, furto, incêndio, falha de *hardware* ou *software*
- Outro tipo de falhas do sistema

9.7.1. Comprometimento das chaves nacionais

O comprometimento das chaves nacionais foi tratado na secção 6.2.6.

9.7.2. Recuperação de dados

[143] A Autoridade Portuguesa de Certificação, o Centro de Personalização e as empresas colaboradoras disporão de procedimentos estabelecidos para prevenir e minimizar os efeitos de desastres no sistema. Tais procedimentos incluirão cópias de segurança dos dados armazenadas segura e remotamente, processos de recuperação de dados, etc., a serem detalhados no BCP.

9.8. Controlo de segurança física

[144] Serão implementados mecanismos de controlo de segurança física para controlar o acesso ao hardware e software da Autoridade Portuguesa de Certificação e do Centro de Personalização. Será mantido um registo com todos os acessos físicos a estas áreas.

[145] As chaves nacionais para certificação serão mantidas protegidas física e logicamente conforme descrito nas disposições práticas.

[146] As instalações da Autoridade Portuguesa de Certificação e do Centro de Personalização terão um local para armazenamento das cópias de segurança e dos suportes de distribuição de dados de forma a evitar a perda, manipulação ou o uso não autorizado dos dados armazenados. As cópias de segurança deverão ser também guardadas em locais distintos àqueles em que encontram os sistemas das entidades acima referidas para facilitar a recuperação no caso de um desastre naqueles locais

[147] Uma verificação de segurança às instalações onde se encontram os sistemas centrais da Autoridade Portuguesa de Certificação e do Centro de Personalização terá lugar, pelo menos, uma vez por semana.

9.8.1. Acesso físico

[148] O acesso ao local onde se encontram alojados os sistemas deve ser controlado através de uma lista de controlo de acessos. Uma pessoa

autorizada acompanhará outra que não esteja na lista de controlo. Se uma lista de controlo de acesso não for praticável para um local em particular, o material sensível relacionado com a Autoridade Portuguesa de Certificação ou o Centro de Personalização deverá ser guardado num local seguro quando não em utilização.

10. Cessação de actividade

10.1. Finalização dos serviços

A finalização dos serviços da Autoridade Portuguesa de Certificação ou do Centro de Personalização refere-se ao termo da sua actividade. Não se trata do caso em que o serviço é transferido de uma organização para outra ou quando se substitua o par de chaves nacionais por um novo o se substitua a chave da ERCA.

[149] A Autoridade Portuguesa garantirá que as tarefas enumeradas seguidamente se efectuem.

[150] Antes que a Autoridade Portuguesa de Certificação ou o Centro de Personalização finalizem os seus serviços terão que ser executados os seguintes procedimentos:

- a) Informar todos os utilizadores e entidades relacionadas com os quais a Autoridade Portuguesa de Certificação ou o Centro de Personalização mantenham acordos ou outro tipo de relação.
- b) Disponibilizar publicamente a informação relativa à sua dissolução com pelo menos 3 meses de antecedência em relação a esta.
- c) A Autoridade Portuguesa de Certificação e o Centro de Personalização porão fim a todas as autorizações a empresas colaboradoras para actuarem em nome daquelas entidades no processo de emissão de certificados.
- d) A Autoridade Portuguesa de Certificação e o Centro de Personalização disponibilizarão obrigatoriamente todos os meios para a manutenção e acesso contínuo a arquivos transferindo-os para a ERCA.

10.2. Transferência de responsabilidades

A transferência de responsabilidades da Autoridade Portuguesa de Certificação e do Centro de Personalização terá lugar quando a Autoridade Portuguesa decidir designar uma nova Autoridade Portuguesa de Certificação ou um novo Centro de Personalização para substituir os anteriores.

[151] A Autoridade Portuguesa assegurar-se-á que a transferência de responsabilidades e activos se efectua.

[152] A anterior Autoridade Portuguesa de Certificação transferirá todas as chaves para a nova Autoridade Portuguesa de Certificação de uma forma determinada pela Autoridade Portuguesa.

[153] A anterior Autoridade Portuguesa de Certificação destruirá todas as chaves nacionais que estejam em seu poder.

11. Auditoria

[154] A Autoridade Portuguesa será responsável por garantir que a Autoridade Portuguesa de Certificação e o Centro de Personalização sejam auditados.

11.1. Frequência de auditoria de conformidade das entidades

[155] Qualquer Autoridade Portuguesa de Certificação ou Centro de Personalização que actuem no âmbito desta política serão auditados no mínimo anualmente. Quando se proceda à auditoria do funcionamento das entidades referidas anteriormente, será especialmente verificada a conformidade com os requisitos da ERCA.

11.2. Tópicos abrangidos pela auditoria

[156] A auditoria abrangerá as práticas da Autoridade Portuguesa de Certificação e do Centro de Personalização.

[157] A auditoria abrangerá também a conformidade da Autoridade Portuguesa de Certificação e do Centro de Personalização com a presente política.

11.3. Entidade que deve efectuar a auditoria

[158] A Autoridade Portuguesa poderá encarregar uma entidade de certificação ou acreditação externa a aprovação dos documentos de Disposições Práticas da Autoridade Portuguesa de Certificação e do Centro de Personalização. Poderá ser também a própria Autoridade Portuguesa a encarregue de levar a cabo a auditoria.

11.4. Medidas a serem tomadas em caso de deficiência

[159] No caso de serem detectadas irregularidades na auditoria, a Autoridade Portuguesa tomará as providências adequadas de acordo com a sua gravidade.

11.5. Comunicação de resultados

[160] A Autoridade Portuguesa incluirá os resultados da auditoria num documento informativo em que definam as acções correctivas e a planificação para a sua implementação, conforme requerido pelas obrigações da Autoridade Portuguesa. Este documento será entregue, em inglês, à ERCA.

[161] Os resultados das auditorias de um determinado nível de segurança poderão ser consultados mediante pedido. Os relatórios detalhados das auditorias não poderão ser consultados excepto quando seja necessário o conhecimento pormenorizado da informação que contém.

12. Procedimentos de alteração da política da autoridade nacional

12.1. Itens alteráveis sem notificação

[162] As únicas alterações que poderão ser feitas a este documento sem notificação prévia são:

- a) Correções tipográficas ou editoriais
- b) Alterações aos contactos ou nomes das organizações

12.2. Alterações com notificação

12.2.1. Notificação

[163] Qualquer item desta política pode ser alterado desde que tal alteração seja comunicada com 90 dias de antecedência.

[164] As alterações a itens que no entender da Autoridade Portuguesa não afectem substancialmente a maioria dos utilizadores ou entidades envolvidas poderão ser alteradas bastando que tal alteração seja comunicada com 30 dias de antecedência.

12.2.2. Período de comentários

[165] Os utilizadores afectados pelas alterações poderão apresentar os seus comentários à Autoridade Portuguesa no prazo de 15 dias a contar da data da notificação.

12.2.3. Entidades a informar

[166] Informação acerca das alterações a esta política serão enviadas para:

- ERCA
- Centro de Personalização
- Fabricantes de unidades de veículo e fabricantes de sensores de movimentos afectados

[167] Se a alteração proposta for modificada como resultado de eventuais comentários, tal modificação será comunicada com uma antecedência de pelo menos 30 dias em relação à sua entrada em vigor.

12.3. Alterações que requerem a aprovação de uma nova política da autoridade nacional

[168] Se uma alteração de política for requerida pela Autoridade Portuguesa, esta submeterá a política revista à Comissão para aprovação.

13. Conformidade com a política da ERCA

Referência na ERCA policy	Requisito	Referência na política da Autoridade Portuguesa
5.3.1	The MSA Policy shall identify the entities in charge of operations.	1.1. Organizações responsáveis.
5.3.2	The MSCA key pairs for equipment key certification and for motion sensor master key distribution shall be generated and stored within a device which either: a) is certified to meet the requirements identified in FIPS 140-2 (or FIPS 140-1) level 3 or higher; b) is certified to be compliant with the requirements identified in the CEN Workshop Agreement 14167-2; c) is a trustworthy system which is assured to EAL4 or higher in accordance with ISO 15408; to level E3 or higher in ITSEC; or equivalent security criteria. These evaluations shall be to a protection profile or security target, d) is demonstrated to provide an equivalent level of security.	6.2.1. Geração do par de chaves da Autoridade Portuguesa. [48] 6.3. Chaves do sensor de movimentos. [68]
5.3.3	Member State Key Pair generation shall take place in a physically secured environment by personnel in trusted roles under, at least dual control.	6.2.1 Geração do par de chaves da Autoridade Portuguesa. [51] 9.3.1. Perfis de confiança. [105] a [110] 9.4. Controlos de segurança relativos aos sistemas da Autoridade Portuguesa de Certificação e do Centro de Personalização. [116] e [117] 9.8. Controlo de segurança física. [144] a [147] 9.8.1. Acesso físico. [148]
5.3.4	The Member State Key Pairs shall be used for a period of at most two years starting from certification by the ERCA.	6.2.2 Período de validade das chaves. [53]

Referência na ERCA policy	Requisito	Referência na política da Autoridade Portuguesa
5.3.5	The generation of new Member State Key Pairs shall take into account the one month turnaround time required for certification by the ERCA	6.2. Par de chaves da Autoridade Portuguesa. [45]
5.3.6	The MSA shall submit MSCA public keys for certification by the ERCA using the key certification request (KCR) protocol described in its Annex A.	6.2. Par de chaves da Autoridade Portuguesa. [46]
5.3.7	The MSA shall request motion sensor master keys from the ERCA using the key distribution request (KDR) protocol described in Annex D.	6.3. Chaves do sensor de movimentos. [63]
5.3.8	The MSA shall recognize the ERCA public key in the distribution format described in Annex B.	6.1. Chave pública da ERCA. [42]
5.3.9	The MSA shall use the physical media for key and certificate transport described in Annex C.	6.4. Chaves de transporte. [71]
5.3.10	The MSA shall ensure that the Key Identifier (KID) and modulus (n) of keys submitted to the ERCA for certification and for motion sensor key distribution are unique within the domain of the MSCA.	6.4. Chaves de transporte. [70]
5.3.11	The MSA shall ensure that expired keys are not used for any purpose. The Member State private key shall be either: destroyed so that the private key cannot be recovered or retained in a manner preventing its use.	6.2.2. Período de validade das chaves. [53]

Referência na ERCA policy	Requisito	Referência na política da Autoridade Portuguesa
5.3.12	<p>The MSA shall ensure that an equipment RSA key is generated, transported, and inserted into the equipment, in such a way as to preserve its confidentiality and integrity. For this purpose, the MSA shall:</p> <ul style="list-style-type: none"> • ensure that any relevant prescription mandated by security certification of the equipment is met. • ensure that both generation and insertion (if not onboard) takes place in a physically secured environment; • unless key generation was covered by the security certification of the equipment, ensure that specified and appropriate cryptographic key generation algorithms are used; <p>The last two of these requirements on generation shall be met by generating equipment keys within a device which either:</p> <ol style="list-style-type: none"> a) is certified to meet the requirements identified in FIPS 140-2 (or FIPS 140-1) level 3 or higher; b) is certified to be compliant with the requirements identified in the CEN Workshop Agreement 14167-2; c) is a trustworthy system which is assured to EAL4 or higher in accordance with ISO 15408; to level E3 or higher in ITSEC; or equivalent security criteria. These evaluations shall be to a protection profile or security target. d) is demonstrated to provide an equivalent level of security. 	<p>5. Gestão de equipamentos: cartões e tacógrafos. [35]</p> <p>7.1. Aspectos genéricos sobre a Autoridade Portuguesa de Certificação, Centro de Personalização e os fabricantes de unidades de veículo. [72]</p> <p>7.2. Geração das chaves dos equipamentos. [75] e [76]</p>

Referência na ERCA policy	Requisito	Referência na política da Autoridade Portuguesa
5.3.13	The MSA shall ensure confidentiality, integrity, and availability of the private keys generated, stored and used under control of the MSA Policy.	<p>3.4.1. Informação considerada confidencial. [23] a [25]</p> <p>5. Gestão de equipamentos: cartões e tacógrafos. [34]</p> <p>6.2.1. Geração do par de chaves da Autoridade Portuguesa. [49] e [52]</p> <p>6.2.3. Armazenamento da chave privada da Autoridade Portuguesa. [54] e [55]</p> <p>6.4. Chaves de transporte. [69]</p> <p>7.1. Aspectos genéricos sobre a Autoridade Portuguesa de Certificação, Centro de Personalização e os fabricantes de unidades de veículo. [73] e [74]</p> <p>7.2. Geração das chaves dos equipamentos. [75] a [78]</p> <p>7.2.2. Protecção e armazenamento das chaves privadas de cartões. [81] e [82]</p> <p>7.2.3. Protecção e armazenamento das chaves privadas de unidades de veículo. [83] e [84]</p>
5.3.14	The MSA shall prevent unauthorised use of the private keys generated, stored and used under control of the MSA Policy.	3.1.1. Obrigações da Autoridade Portuguesa e da Autoridade Portuguesa Emissora de Cartões. [4] g).
5.3.15	The Member State private keys may be backed up using a key recovery procedure requiring at least dual control.	6.2.4. Cópia de segurança da chave privada da Autoridade Portuguesa. [56]
5.3.16	Key certification requests that rely on transportation of private keys are not allowed.	7.2. Geração das chaves dos equipamentos. [78]

Referência na ERCA policy	Requisito	Referência na política da Autoridade Portuguesa
5.3.17	Key escrow is strictly forbidden	6.2.5. Delegação de confiança da chave privada da Autoridade Portuguesa. [57] 7.2.4. Delegação de confiança e arquivo de chaves privadas de equipamentos. [85]
5.3.18	The MSA shall prevent unauthorised use of its motion sensor keys.	3.4.1. Informação considerada confidencial. [25] 6.3. Chaves do sensor de movimentos. [68]
5.3.19	The MSA shall ensure that the motion sensor master key (Km) is used only to encrypt motion sensor data for the purposes of motion sensor manufacturers. The data to be encrypted is defined in the ISO / IEC 16844-3 standard.	6.3. Chaves do sensor de movimentos. [64]
5.3.20	The motion sensor master key (Km) shall never leave the secure and controlled environment of the MSA.	6.3. Chaves do sensor de movimentos. [64] e [68]
5.3.21	The MSA shall forward the workshop card motion sensor key (KmWC) to the component personaliser (in this case, the card personalisation service), by appropriately secured means, for the sole purpose of insertion into workshop cards.	6.3. Chaves do sensor de movimentos. [66]
5.3.22	The MSA shall forward the vehicle unit motion sensor key (KmVU) to the component personaliser (in this case, a vehicle unit manufacturer), by appropriately secured means, for the sole purpose of insertion into vehicle units.	6.3. Chaves do sensor de movimentos. [65]
5.3.23	The MSA shall maintain the confidentiality, integrity, and availability of its motion sensor key copies.	6.3. Chaves do sensor de movimentos. [68]

Referência na ERCA policy	Requisito	Referência na política da Autoridade Portuguesa
5.3.24	<p>The MSA shall ensure that its motion sensor key copies are stored within a device which either:</p> <p>a) is certified to meet the requirements identified in FIPS 140-2 (or FIPS 140-1) level 3 or higher;</p> <p>b) is a trustworthy system which is assured to EAL4 or higher in accordance with ISO 15408; to level E3 or higher in ITSEC ; or equivalent security criteria. These evaluations shall be to a protection profile or security target.</p>	6.3. Chaves do sensor de movimentos. [68]
5.3.25	The MSA shall possess different Member State Key Pairs for the production of vehicle unit and tachograph card equipment public key certificates.	Não aplicável.
5.3.26	The MSA shall ensure availability of its equipment public key certification service.	6.2.1. Geração do par de chaves da Autoridade Portuguesa. [52]
5.3.27	<p>The MSA shall only use the Member State Private Keys for:</p> <p>a) the production of Annex I(B) equipment key certificates using the ISO / IEC 9796-2 digital signature algorithm as described in Annex I(B) Appendix 11 Common Security Mechanisms;</p> <p>b) production of the ERCA key certification request as described in Annex A.</p> <p>c) issuing Certificate Revocation Lists if this method is used for providing certificate status information (see 5.3.30).</p>	6.2. Par de chaves da Autoridade Portuguesa. [47]
5.3.28	The MSA shall sign equipment certificates within the same device used to store the Member State Private Keys (see 5.3.2).	6.2.1 Geração do par de chaves da Autoridade Portuguesa. [49]

Referência na ERCA policy	Requisito	Referência na política da Autoridade Portuguesa
5.3.29	Within its domain, the MSA shall ensure that equipment public keys are identified by a unique key identifier which follows the prescriptions of Annex 1(B).	8.1. Entrada de dados. [87]
5.3.30	Unless key generation and certification is performed in the same physically secured Environment, the key certification request protocol shall provide proof of origin and integrity of certification requests, without revealing the private key.	7.2. Geração das chaves dos equipamentos. [75] a [78] 7.2.2. Protecção e armazenamento das chaves privadas de cartões. [81] e [82] 7.2.3. Protecção e armazenamento das chaves privadas de unidades de veículo. [83] e [84]
5.3.31	The MSA shall maintain and make certificate status Information available.	8.7. Tarefas informativas da autoridade nacional de certificação. [99]
5.3.32	The validity of a tachograph card certificate shall equal the validity of the tachograph card.	8.4. Validade temporal dos certificados dos equipamentos. [94]
5.3.33	The MSA shall prevent the insertion of undefined validity certificates into tachograph cards.	8.4. Validade temporal dos certificados dos equipamentos. [94]
5.3.34	The MSA may allow the insertion of undefined validity Member State certificates into vehicle units.	8.4. Validade temporal dos certificados dos equipamentos. [e94]
5.3.35	The MSA shall ensure that users of cards are identified at some stage of the card issuing process.	5. Gestão de equipamentos: cartões e tacógrafos. [37]
5.3.36	The MSA shall ensure that ERCA is notified without delay of loss, theft, or potential compromise of any MSA keys.	6.2.6. Comprometimento das chaves da Autoridade Portuguesa. [59]
5.3.37	The MSA shall implement appropriate disaster recovery mechanisms which do not depend on the ERCA response time.	6.2.1. Geração do par de chaves da Autoridade Portuguesa. [52] 9.7. Plano de continuidade. [140]

Referência na ERCA policy	Requisito	Referência na política da Autoridade Portuguesa
5.3.38	The MSA shall establish an information security management system (ISMS) based on a risk assessment for all the operations involved.	9.1. Gestão da informação da Autoridade Portuguesa de Certificação e do Centro de Personalização. [102]
5.3.39	The MSA shall ensure that the policies address personnel training, clearance and roles.	9.3. Controlos de segurança relativos a pessoal da Autoridade Portuguesa de Certificação e do Centro de Personalização. [105] a [115]
5.3.40	The MSA shall ensure that appropriate records of certification operations are maintained.	9.6.2. Tipos de eventos armazenados pela Autoridade Portuguesa de Certificação e pelo Centro de Personalização. [133] e [134]
5.3.41	The MSA shall include provisions for MSCA termination in the MSA Policy.	10.1. Finalização dos serviços. [149] e [150]
5.3.42	The MSA Policy shall include change procedures.	12. Procedimentos de alteração da política da autoridade nacional. [162] a [168]
5.3.43	The MSA audit shall establish whether the Requirements of this Section are being maintained.	11.1. Frequência de auditoria de conformidade das entidades. [155]
5.3.44	The MSA shall audit the operations covered by the approved policy at intervals of not more than 12 months.	11.1. Frequência de auditoria de conformidade das entidades. [155]
5.3.45	The MSA shall report the results of the audit as mentioned in 5.3.43 and provide the audit report, in English, to the ERCA.	11.5. Comunicação de resultados. [160]
5.3.46	The audit report shall define any corrective actions, including an implementation schedule, required to fulfil the MSA obligations.	11.5. Comunicação de resultados. [160]

14.Referências

- [1] Council Regulation (EC) No 2135/98 of 24th September 1998; Official Journal of the European Communities L274, 09.10.98.
- [2] Commission Regulation (EC) No 1360/2002 of 13th June 2002; Official Journal of the European Communities L207, 05.08.2002.
- [3] Common Security Guidelines, v1.0; Card Issuing Group SWG3.
- [4] Guideline and Template National CA Policy for the Digital Tachograph System, v1.0; Card Issuing Group SWG3.
- [5] ETSI TS 102 042 V1.1.1 (2002-04) Policy requirements for certification authorities issuing public key certificates
- [6] Commission Regulation (EC) No 1360/2002, Annex I(B) Appendix 11 - Common security mechanisms
- [7] ISO / IEC 17799:2000 Information technology – Code of practice for information security management
- [8] FIPS PUB 140-2 Security Requirements for Cryptographic Modules NIST, 2001
- [9] CEN Workshop Agreement 14167-2: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2 Cryptographic Module for CSP Signing Operations - Protection Profile (MCSO-PP)
- [10] ISO / IEC 15408 (Parts 1 to 3) Information technology – Security techniques – Evaluation criteria for IT security.
- [11] ITSEC Information Technology Security Evaluation Criteria 1991 v1.2
- [12] ISO / IEC 9794-8 | ITU-T Recommendation X.509 Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks
- [13] PKCS#1 v2.0: RSA Cryptography Standard, RSA Laboratories, October 1, 1998.
- [14] Digital Tachograph System European Root Policy, v2.0.

Glossário/Definições e abreviaturas

14.1. Glossário/Definições

14.2. Lista de abreviaturas