AUTENTICAÇÃO.GOV
CHAVE MÓVEL DIGITAL

Declaração de Práticas de Certificação da EC de Chave Móvel Digital de Assinatura Qualificada do Cartão de Cidadão

Políticas

PJ.CMDA_33

Identificação do Projeto: Chave Móvel Digital

Identificação da CA: CMD

Nível de Acesso: Público

Versão: 1.0

Data: 25/02/2018

Identificador do documento: PJ.CMDA_33

Palavras-chave: Cartão de Cidadão, Declaração de Práticas de Certificação, EC do Cidadão

Tipologia documental: Políticas

Título: Declaração de Práticas de Certificação da EC de Chave Móvel Digital de Assinatura Qualificada do Cartão de Cidadão

Língua original: Português

Língua de publicação: Português

Nível de acesso: Público

Data: 25/02/2018

Periodicidade de Revisão: 1ano

Versão atual: 1.0

Identificação do Projeto: Chave Móvel Digital

Identificação da CA: CMD

Cliente: AMA

Histórico de Versões

Versão	Data	Detalhes	Autor(es)
1.0	Fevereiro 2018	Versão Aprovada	AMA

Documentos Relacionados

ID Documento	Detalhes	Autor(es)
PJ.CMDA_36	Política de Certificado da Sub-EC de CMD de Assinatura Qualificada	MULTICERT
PJ.CMDA_34	Política de Certificado de Chave Móvel de Assinatura	MULTICERT

Apêndices

ID	Detalhes	Autor(es)
PJ.CMDA_30	Formulário de emissão de certificado de equipamento tecnológico pela EC CMD	MULTICERT
PJ.CMDA_31	Formulário de receção de certificado de equipamento tecnológico emitido pela EC CMD	MULTICERT
PJ.CMDA_44	Formulário de revogação de certificado de equipamento tecnológico emitido pela EC CMD	MULTICERT

Resumo Executivo

Decorrente da implementação de vários programas públicos para a promoção das tecnologias de informação e comunicação e a introdução de novos processos de relacionamento em sociedade, entre cidadãos, empresas, organizações não-governamentais e o Estado, com vista ao fortalecimento da sociedade de informação e do governo eletrónico (*eGovernment*), o Cartão de Cidadão fornece os mecanismos necessários para a autenticação digital forte da identidade do Cidadão perante os serviços da Administração Pública, assim como as assinaturas eletrónicas indispensáveis aos processos de desmaterialização que estão a ser disponibilizados pelo Estado.

A infraestrutura da Entidade de Certificação do Cartão de Cidadão (ou Entidade de Certificação do Cidadão) fornece uma hierarquia de confiança, que promoverá a segurança eletrónica do Cidadão no seu relacionamento com o Estado. A Entidade de Certificação do Cidadão estabelece uma estrutura de confiança eletrónica que proporciona a realização de transações eletrónicas seguras, a autenticação forte, um meio de assinar eletronicamente transações ou informações e documentos eletrónicos, assegurando a sua autoria, integridade e não repúdio, e assegurando a confidencialidade das transações ou informação.

A hierarquia de confiança da Entidade de Certificação do Cartão de Cidadão encontra-se englobada na hierarquia do Sistema de Certificação Eletrónica do Estado Português[1] (SCEE) – Infraestrutura de Chaves Públicas do Estado.

A Entidade de Certificação do Cartão de Cidadão está devidamente credenciada pela Autoridade Nacional de Segurança, encontrando-se o seu registo na Lista de Serviços de Confiança (TSL - *Trust Service List*), emitida por esta entidade, como previsto na legislação portuguesa e europeia. O URL onde poderá ser validada esta informação é: http://www.gns.gov.pt/media/1891/TSLPTHR.pdf.

Este documento define os procedimentos e práticas utilizadas pela Entidade de Certificação de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão no suporte à sua atividade de certificação digital, sendo referenciado como o documento de Declaração de Práticas de Certificação da EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão.

[1] *cf.* SCEE 2.16.620.1.1.1.2.1.1.0. 2006, Política de Certificados da SCEE e Requisitos mínimos de Segurança.

Sumário

Introdução

Objetivos

O objetivo deste documento é definir os procedimentos e práticas utilizadas pela Entidade de Certificação (EC) de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão no suporte à sua atividade de certificação digital.

Público-Alvo

Este documento deve ser lido por:

- Recursos humanos atribuídos aos grupos de trabalho da EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão,
- Terceiras partes encarregues de auditar a EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão,
- Cidadão titular de um certificado emitido pela EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão,
- Todo o público, em geral.

Estrutura do Documento

Assume-se que o leitor é conhecedor dos conceitos de criptografia, infraestruturas de chave pública e assinatura eletrónica. Caso esta situação não se verifique recomenda-se o aprofundar de conceitos e conhecimento nos tópicos anteriormente focado antes de proceder com a leitura do documento.

Este documento segue a estrutura definida e proposta pelo grupo de trabalho PKIX do IETF, no documento RFC 3647[2], de acordo também com a estrutura recomendada pelo SCEE[1].

Os primeiros sete capítulos são dedicados a descrever os procedimentos e práticas mais importantes no âmbito da certificação digital da EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão. O capítulo 8 descreve auditorias de conformidade e outras avaliações. O capítulo 9 descreve matérias legais.

[2] *cf.* RFC 3647. 2003, Internet X.509 *Public Key Infrastructure Certificate Policy and Certification Practices Framework.*

1 Contexto Geral

O presente documento é uma Declaração de Práticas de Certificação, ou DPC, cujo objetivo prende-se com a definição de um conjunto de práticas para a emissão e validação de Certificados e para a garantia de fiabilidade desses mesmos certificados. Não se pretende nomear regras legais ou obrigações, mas antes informar, pretendendo-se assim que este documento seja simples, direto e entendido por um público alargado, incluindo pessoas sem conhecimentos técnicos ou legais.

Este documento descreve as práticas gerais de emissão e gestão de Certificados seguidas pela Entidade de Certificação Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão (EC CMD) e, explica o que um Certificado fornece e significa, assim como os procedimentos que deverão ser seguidos por Partes Confiantes e por qualquer outra pessoa interessada para confiarem nos Certificados emitidos pela EC CMD. Este documento pode sofrer atualizações regulares.

Os Certificados emitidos pela EC CMD contêm uma referência à DPC de modo a permitir que Partes confiantes e outras pessoas interessadas possam encontrar informação sobre o certificado e sobre a entidade que o emitiu.

1.1 Visão Geral

As práticas de criação, assinatura e de emissão de Certificados, assim como de revogação de certificados inválidos levadas a cabo por uma Entidade de Certificação (EC) são fundamentais para garantir a fiabilidade e confiança de uma Infraestrutura de Chaves Públicas (ou PKI – *Public Key Infrastructure*).

Esta DPC aplica-se especificamente à EC CMD (Entidade de Certificação de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão, de acordo com a estrutura recomendada pelo SCEE[1]) e respeita e implementa os seguintes *standards*:

- RFC 3647: *Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework*;
- RFC 5280: *Internet X.509 PKI - Certificate and CRL Profile*.

Esta DPC satisfaz os requisitos impostos pela Declaração de Práticas de Certificação da SCEE[1] e específica como implementar os seus procedimentos e controlos, e ainda como a EC CMD atinge os requisitos especificados.

1.2 Designação e Identificação do Documento

Este documento é a Declaração de Práticas de Certificação da EC CMD. A DPC é representada num certificado através de um número único designado de "identificador de objeto" (OID), sendo o valor do OID associado a este documento o **2.16.620.1.1.1.2.4.3.0.7**.

Este documento é identificado pelos dados constantes na seguinte tabela:

INFORMAÇÃO DO DOCUMENTO	
Nome do Documento	Declaração de Práticas de Certificação da EC de Chave Móvel Digital de Assinatura Qualificada do Cartão de Cidadão
Versão do Documento	Versão 1.0
Estado do Documento	Aprovado
Data de Emissão	Janeiro de 2018
Validade	1 Ano
Localização	http://pki.cartaodecidadao.pt/publico/politicas/dpc/cc_sub-ec_cidadao_cmd_dpc.html

1.3 Participantes na Infraestrutura de Chave Pública

1.3.1 Entidades Certificadoras

A EC CMD insere-se na hierarquia de confiança da SCEE (Sistema de Certificação Eletrónica do Estado), constituindo-se numa sub-entidade Certificadora do Estado, sendo o seu certificado assinado pela entidade certificadora do Cartão de Cidadão (i.e., por uma Entidade Certificadora do Estado[1]). Deste modo, a EC CMD encontra-se dois níveis abaixo da EC Raiz do Estado Português.

A principal função da EC CMD é a gestão de serviços de certificação: emissão, suspensão, revogação para os seus subscritores.

A EC CMD emite certificados de:

- CMD de Assinatura Qualificada do Cidadão
- Serviços necessários no âmbito da EC CMD:
    - Validação *on-line* OCSP.

1.3.1.1 A EC Raiz do Estado

A EC Raiz do Estado é a entidade de Certificação de primeiro nível. Tem como função o estabelecimento da raiz da cadeia de confiança da infraestrutura de chaves públicas (ICP) do Estado Português, denominada de Entidade de Certificação Eletrónica do Estado (ECEE). O certificado da ECRaizEstado poderá ser consultado em https://www.scee.gov.pt/rep/certificados/. A informação previamente descrita consta da Política de Certificados

da SCEE. Visto não ter existido qualquer alteração à data de aprovação desta DPC todos os pressupostos referidos anteriormente mantêm-se válidos.

1.3.1.2 As ECEstado

As ECEstado são as entidades que se encontram no nível imediatamente abaixo da ECRaizEstado, sendo, no caso presente, a EC do Cartão de Cidadão (EC CC) uma ECEstado e cuja função principal é promover a gestão de serviços de certificação: emissão, suspensão e revogação de certificados para as SubECEstado.

A EC CC emite os certificados digitais, em formato X509 v3, das Entidades Certificadoras de Assinatura Digital Qualificada do Cartão de Cidadão, de Autenticação do Cidadão, de Chave Móvel Digital de Assinatura Digital Qualificada do Cidadão e, de Controlo de Acessos, sendo adicionalmente responsável pela emissão dos seguintes certificados digitais, em formato X509 v3, específicos:

- Certificados para assinatura digital de dados colocados no chip do Cartão de Cidadão, a ser utilizada pela Entidade de Certificação de Documentos do Cartão de Cidadão (ECD);
- Certificados para o Serviço de Validação OCSP;
- Certificados para o Serviço de Selo Temporal.

A EC CC é detentora de oito certificados X509 v3 no seguimento das renovações a que foi sujeito, sendo a distribuição dos mesmos, realizada em consonância com os seus respetivos objetivos:

- 4 (quatro) auto-assinados;
- 4 (quatro) assinados pela ECEE, traduzindo-se numa EC Estado, podendo ser consultado em https://pki.cartaodecidadao.pt/publico/certificado/cc_ec_cidadao/

1.3.1.3 As SubECEstado

Estas são entidades que se encontram no nível imediatamente abaixo das ECEstado têm como função a prestação de serviços de certificação para o utilizador final. O seu certificado é assinado por uma ECEstado, que no caso da EC CMD será a EC CC.

1.3.1.3.1 EC CMD

Esta EC é responsável pela emissão dos certificados digitais de assinatura qualificada, em formato X509 v3, de ativação facultativa, por cidadãos de idade igual ou superior a 16 anos, que não se encontrem interditos ou inabilitados, conforme ponto 13 do artigo 2º da Lei 37/2014 republicada com as alterações introduzidas pela Lei 32/2017.

O certificado desta EC é renovado a cada dois anos. A informação de cada um deles poderá ser consultada em https://pki.cartaodecidadao.pt/publico/certificado/cc_ec_cidadao_cmd/

1.3.2 Entidades de Registo

A Entidade de Registo (ER) é a entidade que aprova os nomes distintos (DN) dos titulares dos certificados e mediante avaliação do pedido, aceita ou rejeita a solicitação do mesmo. Para além disso, a ER também tem autoridade para aprovar a revogação ou suspensão de certificados.

Esta entidade materializa-se pelos postos de atendimento da AMA, do IRN (Lojas do Cidadão, a uma conservatória do registo civil, outras entidades que hajam celebrado um protocolo com o Instituto dos Registos e do Notariado, I. P.), para a receção dos pedidos de emissão, renovação e cancelamento do cartão de cidadão, e por outras entidades da Administração Pública que celebrem um protocolo com a AMA para este efeito, conforme o número 6 do artigo 2º da Lei 37/2014 republicada com as alterações introduzidas pela Lei 32/2017.

Adicionalmente, a ER também está disponível online através do serviço AUTENTICAÇÃO.GOV que identifica o titular através do certificado de autenticação do seu Cartão de Cidadão ou através da Chave Móvel Digital.

1.3.3 Titulares de Certificados

No contexto deste documento o termo subscritor/titular aplica-se a todos os utilizadores finais a quem tenham sido atribuídos certificados por uma EC do Estado ou EC subordinada do Estado.

De acordo com as regras da SCEE[1], são considerados titulares de certificados emitidos pela EC CMD, aqueles cujo nome está inscrito no campo *Subject* do certificado e utilizam o certificado e respetiva chave privada de acordo com o estabelecido nas diversas políticas de certificado descritas neste documento, sendo emitidos certificados de CMD de Assinatura Digital Qualificada, para as seguintes categorias de titulares, nos termos do ponto 13 do artigo 2º da Lei 37/2014 republicada com as alterações introduzidas pela Lei 32/2017:

- Cidadão portador de Cartão de Cidadão;
- Cidadão portador do Bilhete de Identidade.

Os Certificados CMD de Assinatura Digital Qualificada são de ativação facultativa, por cidadãos de idade igual ou superior a 16 anos, que não se encontrem interditos ou inabilitados.

1.3.3.1 Patrocinador

A EC CMD emite também um certificado para Equipamento Tecnológico, cujo titular é designado por Patrocinador. A Entidade designada por Patrocinador é responsável por garantir a correta gestão de certificados para equipamentos tecnológicos sempre que a sua emissão seja efetuada manualmente.
O patrocinador aceita o certificado e é responsável pela sua correta utilização, bem como pela proteção e salvaguarda da sua chave privada.
A EC CMD emite o seguinte certificado de equipamento tecnológico:

- Validação *on-line* OCSP.

1.3.4 Partes Confiantes

As partes confiantes ou destinatários são pessoas singulares, entidades ou equipamentos que confiam na validade dos mecanismos e procedimentos utilizados no processo de associação do nome do titular com a sua chave pública, ou seja confiam que o certificado corresponde na realidade a quem diz pertencer.

Nesta DPC, considera-se uma parte confiante, aquela que confia no teor, validade e aplicabilidade do certificado emitido no "ramo" da EC CMD da hierarquia de confiança da SCEE, podendo ser titular de certificados da comunidade SCEE ou não.

1.3.5 Outros participantes

1.3.5.1 Conselho Gestor

O Conselho Gestor[3] (CG) é a entidade responsável pela gestão global e administração de toda a Infraestrutura de Chaves Públicas, pela aprovação da integração das Entidades Certificadoras do Estado, e a quem cabe pronunciar-se sobre as políticas e práticas de certificação das entidades certificadoras que integram a SCEE.

Compete especialmente ao Conselho Gestor[3]:

a) Definir e aprovar, de acordo com as normas ou especificações internacionalmente reconhecidas, as políticas e as práticas de certificação a observar pelas Entidades Certificadoras que integram a SCEE;

b) Garantir que as declarações de práticas de certificação das várias Entidades Certificadoras do Estado, incluindo a Entidade Certificadora Raiz, estão em conformidade com as Políticas de Certificado da SCEE;

c) Definir e publicar os critérios para aprovação das entidades certificadoras que pretendam integrar a SCEE;

d) Aprovar a integração na SCEE das Entidades Certificadoras do Estado que obedeçam aos requisitos estabelecidos no presente diploma e que se enquadrem nos critérios previamente estabelecidos e referidos na alínea anterior;

e) O Conselho Gestor deverá obter da Entidade Supervisora um parecer de auditoria e conformidade sobre as Entidades Certificadoras que se pretendam constituir como Entidades Certificadoras do Estado;

f) Aferir da conformidade dos procedimentos seguidos pelas Entidades Certificadoras do Estado com as políticas e diretivas aprovadas, sem prejuízo das competências legalmente cometidas à Entidade Supervisora;

[3] Em falta deste, o Grupo de Trabalho de Gestão do Cartão de Cidadão

g) Decidir pela exclusão da SCEE das Entidades Certificadoras do Estado em caso de não conformidade com as políticas e práticas aprovadas, comunicando tal fato à Entidade Supervisora;

h) Pronunciar-se sobre as melhores práticas internacionais no exercício das atividades de certificação eletrónica e propor a sua aplicação.

Compete ainda ao Conselho Gestor a promoção e coordenação das atividades para o estabelecimento de acordos de interoperabilidade, com base em certificação cruzada, com outras Infraestruturas de Chaves Públicas, de natureza privada ou pública, nacionais ou internacionais, nomeadamente:

a) Dar indicações à Entidade Certificadora Raiz do Estado para atribuição e revogação de certificados emitidos com base em certificação cruzada;
b) Definir os termos e condições para início, suspensão ou finalização aos processos de interoperabilidade com outras Infraestruturas de chaves públicas.

A definição do detalhe, composição e funcionamento estão definidos em documentação e legislação própria.

1.3.5.2 Entidade Supervisora

Entidade Supervisora é a entidade competente para a credenciação e fiscalização das entidades certificadoras. De uma forma geral o papel da Entidade Supervisora, exercida em Portugal pela Autoridade Nacional de Segurança (ANS), está relacionado com a auditoria/inspeção de conformidade, no sentido de aferir se os processos utilizados pelas EC, nas suas atividades de certificação, estão conformes, de acordo com os requisitos mínimos estabelecidos na legislação portuguesa e europeia, assim como com o estabelecido nesta DPC.
A Entidade Supervisora é uma das "peças" que contribui para a confiabilidade dos Certificados Qualificados, pelas competências que exerce sobre as EC que os emitem. No âmbito das suas funções, exerce os seguintes papéis relativamente às EC:

a) Credenciação: procedimento de aprovação da EC para exercer a sua atividade, com base numa avaliação feita a parâmetros tão diversificados como a segurança física, HW e SW, procedimentos de acesso e de operação;

b) Registo: procedimento sem o qual a EC não poderá emitir os Certificados Qualificados;

c) Fiscalização: procedimento assente em inspeções efetuadas às EC, com vista a regularmente verificar parâmetros de conformidade.

1.3.5.3 Autoridades de Validação

As Autoridades de Validação (AV), têm como função comprovar o estado dos certificados emitidos, através da utilização do protocolo *Online Certificate Status Protocol*[4] (OCSP), de forma a determinar o estado atual do certificado a pedido de uma entidade sem necessidade de recorrer à verificação do estado através da consulta das LRC.

[4] *cf.* RFC 6960. 2013, X.509 *Internet Public Key Infrastructure Online Certificate Status Protocol* – OCSP.

1.3.5.4 Entidades externas de prestação de serviços

As Entidades que prestam serviços de suporte à PKI da EC CMD, têm as suas responsabilidades definidas, através de contratos estabelecidos com as mesmas.

1.4 Utilização do Certificado

Os certificados emitidos no domínio da EC CMD são utilizados, pelos diversos sistemas, aplicações, mecanismos e protocolos, com o objetivo de garantir serviços de segurança:

Tipo de Certificado	Uso Apropriado
Certificado CMD de Assinatura Qualificada	Assinatura Eletrónica Qualificada
Certificados OCSP	Serviço de Estado de Revogações dos certificados

Estes serviços são obtidos com recurso à utilização de criptografia de chave pública, através da sua utilização na estrutura de confiança que a EC CMD e SCEE proporcionam.

1.4.1 Utilização adequada

Os requisitos e regras definidos neste documento, aplicam-se a todos os certificados emitidos pela EC CMD.

Os certificados atribuídos a pessoas singulares, têm como objetivo a sua utilização em qualquer aplicação para efeitos de Assinatura digital qualificada.

Os certificados emitidos para equipamentos tecnológicos, têm como objetivo a sua utilização em serviços de autenticação e no estabelecimento de canais cifrados.

Os certificados emitidos para efeitos de utilização por serviços de confidencialidade, emitidos com base nas regras aqui definidas, podem ser utilizados para processar informação classificada até o grau de RESERVADO quando utilizados sobre redes públicas (p.e. Internet). Na sua utilização em redes proprietárias, o grau de classificação da informação deverá ser definido pelo organismo nacional com responsabilidades no âmbito do tratamento da informação/matéria classificada.

Os certificados emitidos pela EC CMD são também utilizados pelas Partes Confiantes para verificação da cadeia de confiança de um certificado emitido sob a EC CMD, assim como para garantir a autenticidade e identidade do emissor de uma assinatura digital gerada pela chave privada correspondente à chave pública contida num certificado emitido sob a EC CMD.

1.4.2 Utilização não autorizada

Os certificados poderão ser utilizados noutros contextos apenas na extensão do que é permitido pelas regras da SCEE[1] e pela legislação aplicável.

Os certificados emitidos pela EC CMD não poderão ser utilizados para qualquer função fora do âmbito das utilizações descritas anteriormente.

Os serviços de certificação oferecidos pela EC CMD, não foram desenhados nem estão autorizados a ser utilizados em atividades de alto risco ou que requeiram uma atividade isenta de falhas, como as relacionadas com o funcionamento de instalações hospitalares, nucleares, controlo de tráfego aéreo, controlo de tráfego ferroviário, ou qualquer outra atividade onde uma falha possa levar à morte, lesões pessoais ou danos graves para o meio ambiente.

1.5 Gestão das Políticas

1.5.1 Entidade responsável pela gestão do documento

A gestão desta política de certificados é da responsabilidade do AMA.

1.5.2 Contacto

Nome:	AMA – Agência para a Modernização Administrativa IP
Morada:	Rua Abranches Ferrão, 10 - 3º G 1600 - 001 Lisboa
Correio Eletrónico:	ama@ama.pt
Telefone:	217 231 200

1.5.3 Entidade responsável pela determinação da conformidade da DPC relativamente à Política

O Grupo de Trabalho de Políticas, em conjunto com o Grupo de Gestão de Informação, determina a conformidade e aplicação interna desta DPC (e/ou respetiva PCs) no que diz respeito a legislação e normas aplicáveis.

1.5.4 Atualização da DPC

O Grupo de Trabalho de Políticas é responsável pela constante atualização desta DPC garantindo que a mesma é revista pelo menos 1 vez por ano.

Sempre que for registada necessidade de alterações, as mesmas devem ser feitas pelo Grupo de Trabalho de Políticas e analisadas pelo Grupo de Gestão de Informação.

1.5.5 Procedimentos para Aprovação da DPC

A aprovação interna desta DPC (e/ou respetivas PCs) e seguintes correções (ou atualizações) deverão ser levadas a cabo pelos Grupos de Trabalho de Políticas e Gestão da Informação. Correções (ou atualizações) deverão ser publicadas sob a forma de novas versões desta DPC (e/ou respetivas PCs), substituindo qualquer DPC (e/ou respetivas PCs) anteriormente definida. O Grupo de Trabalho da Política deverá ainda determinar quando é que as alterações na DPC (e/ou respetivas PCs) levam a uma alteração nos identificadores dos objetos (OID) da DPC (e/ou respetivas PCs).

Após a aprovação interna, a DPC (e/ou respetivas PCs) é submetido ao Grupo de Gestão. Por sua vez o Grupo de Gestão deve submeter o mesmo documento, após a sua aprovação, o Conselho Gestor (CG) – órgão competente para determinar a adequação das DPC (e/ou respetivas PCs) das diversas entidades, com a Política de Certificados definida pela SCEE – para aprovação.

1.6 Definições e Acrónimos

Ver Anexo A.

2 Responsabilidade de Publicação e Repositório

2.1 Repositórios

A AMA é responsável pelas funções de repositório da EC CMD, publicando, entre outras, informação relativa às práticas adotadas e o estado dos certificados emitidos (LRC).

A plataforma tecnológica do repositório está configurada de acordo com os seguintes indicadores e métricas:

- Disponibilidade de serviços da plataforma de 99,5%, em período 24hx7d, excluindo manutenções necessárias efetuadas em horário de menor utilização, garantindo-se durante o tempo da disponibilidade:
  - Mínimo de 99,990% de respostas a pedidos de obtenção da LRC;
  - Mínimo de 99,990% de respostas a pedidos do documento da DPC;
- Número máximo de pedidos de LRC: 50 pedidos/minuto;
- Número máximo de pedidos da DPC: 50 pedidos/minuto;
- Número médio de pedidos de LRC: 20 pedidos/minuto;
- Número médio de pedidos da DPC: 20 pedidos/minuto.

O acesso à informação disponibilizada pelo repositório é efetuado através do protocolo HTTPS e HTTP, estando implementado os seguintes mecanismos de segurança:

- LRC e DPC só podem ser alterados através de processos e procedimentos bem definidos;
- Plataforma tecnológica do repositório encontra-se devidamente protegida pelas técnicas mais atuais de segurança física e lógica;
- Os recursos humanos que gerem a plataforma têm formação e treino adequado para o serviço em questão.

2.2 Publicação de informação de certificação

A AMA mantém um repositório em ambiente web, permitindo que as Partes Confiantes efetuem pesquisas *on-line* relativas à revogação e outra informação referente ao estado dos Certificados.

A SCEE[1] disponibiliza a sua política de certificado em https://www.scee.gov.pt/media/1709/ECRaizEstado.crt.

A AMA disponibiliza 24hx7d a seguinte informação pública *on-line*:

- Cópia eletrónica deste DPC e Políticas de Certificados (PC) mais atuais da EC CMD, assinada eletronicamente pelo Grupo de Gestão:
    - DPC da EC CMD disponibilizada no URI: http://pki.cartaodecidadao.pt/publico/politicas/dpc/cc_sub-ec_cidadao_cmd_dpc.html;
    - PC de certificado de assinatura digital qualificada disponibilizada no URI: http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_sub-ec_cidadao_cmd_pc.html;
    - PC de certificado de validação *on-line* OCSP disponibilizada no URI: http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_sub-ec_cidadao_cmd_OCSP_pc.html.
- LRC da EC CMD – URI:

  http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_cmd_crl<ID_CA>.crl;
- Delta-LRC da EC CMD – URI:

  http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_cmd_crl<ID_CA>_delta.crl;
- Certificado da EC CMD – URI: http://pki.cartaodecidadao.pt/publico/certificado/cc_ec_cidadao_cmd;
- Outra informação relevante – URI: http://pki.cartaodecidadao.pt/publico/info/cc_ec_cidadao_cmd.

Adicionalmente, serão conservadas todas as versões anteriores das PCs e DPC da EC CMD, disponibilizando-as a quem as solicite (desde que justificado), ficando, no entanto fora do repositório público de acesso livre.

2.3 Periodicidade de publicação

As atualizações a esta DPC e respetivas PCs serão publicadas imediatamente após a sua aprovação pelo Conselho Gestor[3] (CG), de acordo com a secção 9.12. Será considerado como prazo máximo para atualização da informação desta DPC, 1 ano.

O certificado da EC CMD é publicado imediatamente após a emissão. A LRC da EC CMD será publicada, no mínimo, uma vez por semana. A Delta-LRC da EC CMD será publicada, no mínimo, todos os dias.

2.4 Controlo de acesso aos repositórios

A informação publicada pela AMA estará disponível na Internet, sendo sujeita a mecanismos de controlo de acesso (acesso somente para leitura). A AMA implementou medidas de segurança lógica e física para impedir que pessoas não autorizadas possam adicionar, apagar ou modificar registos do repositório.

3 Identificação e Autenticação

3.1 Atribuição de Nomes

A atribuição de nomes segue a convenção determinada pelo SCEE[1], i.e., aos certificados de pessoa singular é atribuído o nome real do titular, enquanto, que aos certificados de equipamentos tecnológicos é atribuído o nome qualificado do domínio e/ou o âmbito da sua utilização ("Serviços do Cartão de Cidadão").

A operação dos certificados emitidos pela EC CMD está sempre na dependência da AMA. O patrocinador dos certificados de equipamentos tecnológicos será um colaborador devidamente identificado de um organismo na dependência da AMA.

3.1.1 Tipos de nomes

O certificado da EC CMD assim com os certificados emitidos pela EC CMD é identificado por um nome único (DN – *Distinguished Name*) de acordo com *standard* X.500:

Campo	Valor
***Common Name* – CN**	EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão <nnnn>[5]
Organization Unit - OU	subECEstado,
Organization Unit - OU	Cartão de Cidadão
Organization - O	AMA - AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA I. P.
Country - C	PT

3.1.2 Necessidade de nomes significativos

A EC CMD irá assegurar, dentro do seu "ramo" da hierarquia de confiança do SCEE:

- A não existência de certificados que, tendo o mesmo nome único, identifiquem entidades (equipamento) distintas;
- A relação entre o titular e a organização a que pertence é a mesma que consta no certificado e é facilmente percetível e identificável pelos Humanos.

[5] <nnnn> identifica o número sequencial a atribuir a cada renovação de certificado da EC CMD

3.1.3 Anonimato ou pseudónimo de titulares

Não é permitida a emissão de certificados com base no conceito de anonimato ou de pseudónimo.

3.1.4 Interpretação de formato de nomes

As regras utilizadas pela EC CMD para interpretar o formato dos nomes seguem o estabelecido no RFC 5280[6], assegurando que todos os atributos *DirectoryString* dos campos *issuer* e *subject* do certificado são codificados numa *UTF8String*, com exceção dos atributos *country* e *serialnumber* que são codificados numa *PrintableString*.

3.1.5 Unicidade de nomes

Os identificadores do tipo DN são únicos para cada titular de certificado emitido dentro da EC CMD e de cada uma das suas Entidades de Certificação subordinadas, não induzindo em ambiguidades.

De acordo com os seus processos de emissão, a EC CMD e as suas EC subordinadas rejeitam, dentro de cada EC, a emissão de certificados com o mesmo DN para titulares distintos. Quando ocorrer tal situação, é permitido a adição de caracteres numéricos ao nome original de cada entidade, de forma a assegurar a unicidade do campo, desde que tal não induza uma parte confiante em ambiguidade.

3.1.6 Reconhecimento, autenticação, e função das marcas registadas

As entidades requisitantes de certificados, devem demonstrar que têm direito à utilização do nome requisitado, não podendo as designações usadas nos certificados emitidos pela EC CMD e pelas EC subordinadas infringir os direitos de propriedade intelectual de outros indivíduos ou entidades.

No procedimento de autenticação e identificação do titular do certificado, prévio à emissão do mesmo, a entidade requisitante do certificado terá que apresentar os documentos legais que demonstrem o direito à utilização do nome requisitado.

3.2 Validação de Identidade no registo inicial

Para os certificados emitidos no domínio da SCEE[1], é obrigatório que o registo inicial seja efetuado presencialmente, ou seja, a validação inicial da identidade do requerente é feita pelo método de "cara-a-cara".

A validação de Identidade do cidadão é sempre efetuada com base no Cartão de Cidadão ou Bilhete de Identidade, quer nos balcões físicos da Entidade de Registo como online (cf. secção 1.3.2), originando procedimentos diferenciados, descritos de seguida:

[6] *cf.* RFC 5280. 2002, Internet X.509 *Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

- Nos balcões físicos da Entidade de Registo, o funcionário do serviço valida pelo método "cara-a-cara", comparando a fotografia no Cartão do Cidadão ou Bilhete de Identidade, com o cidadão na sua presença, confirmando e validando através de reconhecimento facial que o requerente é quem diz ser;
- No balcão online da Entidade de Registo, a validação é efetuada com base:
    - no certificado de autenticação do Cartão de Cidadão do requerente, tendo previamente sido utilizado o método "cara-a-cara" para emitir o mesmo;
    - na Chave Móvel Digital de autenticação, tendo a validação de identidade do registo inicial da mesma sido efetuada por um dos dois métodos anteriores.

3.2.1 Método de comprovação da posse de chave privada

No caso das pessoas singulares, o par de chaves e certificado é guardado em ambiente criptográfico seguro pelo serviço de Chave Móvel Digital. A posse da chave privada é garantida pelo processo de emissão e guarda do par de chaves e certificado, garantindo que,

1. O cidadão requerente do certificado é autenticado com base no seu Cartão de Cidadão ou Bilhete de Identidade, conforme indicado nas secções 3.2.3 e 4.1.2;
2. O par de chaves é gerado em *hardware* criptográfico;
3. A chave pública é enviada à Entidade de Certificação para emissão do certificado digital correspondente;
4. O par de chaves e o certificado digital correspondente são guardados em ambiente criptográfico seguro, protegidos por palavra-passe fornecida pelo requerente/titular do certificado;
5. A comprovação da titularidade da chave e certificado, para posterior acesso às mesmas, é efetuada de acordo com o CEN 419241:2014.

No caso do equipamento tecnológico, quando emitido manualmente, a comprovação da posse da chave privada será garantida através da presença física do patrocinador (ver 1.3.3.1), que apresentará o pedido de certificado no formato PKCS#10, cf. secção 3.2.2.

3.2.2 Autenticação da identidade de uma pessoa coletiva

O processo de autenticação da identidade de uma pessoa coletiva, deve obrigatoriamente garantir que a pessoa coletiva para quem vai ser emitido o certificado é quem na realidade diz ser e que a criação de assinatura, através de dispositivo de criação de assinatura, exige a intervenção de pessoas singulares que, estatutariamente, representam essa pessoa coletiva.

3.2.2.1 Certificado de equipamento tecnológico

Sempre que o certificado de equipamento tecnológico seja emitido manualmente, a AMA guarda toda a documentação utilizada para verificação da identidade do patrocinador, garantindo que o mesmo tem os poderes

bastantes de representante nomeado pela entidade para a emissão do certificado digital. O documento[7] que serve de base ao registo do pedido do certificado de equipamento tecnológico contém, entre outros, os seguintes elementos:

- Denominação legal da pessoal coletiva (i.e., AMA ou organismo da dependência da AMA);
- Número de pessoa coletiva, sede, objeto social, nome dos titulares dos corpos sociais e de outras pessoas com poderes para a obrigarem e número de matrícula na conservatória do registo comercial;
- Nome completo, número do bilhete de identidade ou qualquer outro elemento que permita a identificação inequívoca das pessoas singulares que, estatutária ou legalmente, a representam;
- Endereço e outras formas de contacto;
- Indicação de que o certificado digital de equipamento tecnológico é emitido para a entidade, na hierarquia de confiança da SCEE, de acordo com a presente DPC;
- Nome único (DN) a ser atribuído ao certificado;
- Informação relativa à identificação e aos poderes do(s) patrocinador(es) nomeados pela entidade para efetuar presencialmente o pedido do certificado digital de equipamento tecnológico (apresentado mediante o preenchimento de formulário próprio[7] e do fornecimento do pedido de certificado no formato PKCS#10);
- Outras informações relativas ao formato do pedido de certificado, assim como ao conteúdo do DN do certificado.

O certificado e restantes dados necessários serão entregues ao patrocinador pelo método "cara-a-cara", sendo tal ato registado através do preenchimento e assinatura de formulário[8] que é arquivado pela EC CMD.

3.2.3 Autenticação da identidade de uma pessoa singular

O processo de autenticação da identidade de uma pessoa singular, garante que a pessoa singular para quem vai ser emitido o certificado é quem na realidade diz ser.

Este processo é efetuado pela Entidade de Registo, tanto nos seus balcões físicos como online (cf. secção 1.3.2) e, suporta as atividades relacionadas com a recolha e validação de dados biográficos e biométricos do cidadão, de modo a registar o pedido para geração do par de chaves e emissão de certificado digital – note-se que todos os dados de identificação e validade a constar no certificado CMD de Assinatura Qualificada são obtidos do Cartão de Cidadão ou Bilhete de Identidade. Prevê também as funcionalidades de suporte à ocorrência de erros nas diversas ações de validação, de modo a suportar os procedimentos a realizar em cada situação, pelo funcionário, pelo sistema e/ou pelo Cidadão.

Os métodos de validação de identidade são descritos na secção 3.2.

[7] cf. PJ.CMDA_30, Formulário de emissão de certificado de equipamento tecnológico pela EC CMD.
[8] cf. PJ.CMDA_31, Formulário de receção de certificado de equipamento tecnológico emitido pela EC CMD.

3.2.4 Informação de subscritor/titular não verificada

Toda a informação descrita nos pontos 3.2.2 e 3.2.3 é verificada.

3.2.5 Validação de Autoridade

A intervenção dos representantes legais no pedido de emissão de certificado de Assinatura Qualificada, não é permitida.

3.2.6 Critérios para interoperabilidade

A EC opera exclusivamente no domínio do Cartão de Cidadão, não estando portanto contemplada a certificação cruzada.

3.3 Identificação e autenticação para pedidos de renovação de chaves

A identificação e autenticação para a renovação de certificados são realizadas utilizando os procedimentos para a autenticação e identificação inicial.

3.3.1 Identificação e autenticação para renovação de chaves, de rotina

Não existe renovação de chaves, de rotina. A renovação de certificados utiliza os procedimentos para a autenticação e identificação inicial, onde são gerados novos pares de chaves.

3.3.2 Identificação e autenticação para renovação de chaves, após revogação

Após revogação de certificado, a geração de novo par de chaves e respetiva emissão de certificado segue os procedimentos para a autenticação e identificação inicial.

3.4 Identificação e autenticação para pedido de revogação

O processo de identificação e autenticação para pedido de revogação de certificado de pessoa singular, está disponível nas Entidades de registo (cf. secção 1.3.2), assim como online através do serviço

AUTENTICAÇÃO.GOV (https://www.autenticacao.gov.pt/), sendo guardadas as evidências necessárias da ocorrência do pedido.

O pedido poderá ser efetuado nesse serviço, após uma das seguintes formas de autenticação:

- Mediante autenticação com certificado de autenticação do Cartão de Cidadão do titular do certificado CMD de Assinatura Qualificada,
- Mediante autenticação com Chave Móvel Digital de autenticação do titular do certificado CMD de Assinatura Qualificada,
- Mediante preenchimento de formulário, por pessoa legalmente habilitada a pedir a revogação.

Salienta-se que o Cartão de Cidadão e os certificados constantes do mesmo continuam válidos, após a revogação do certificado CMD de Assinatura Qualificada. De igual modo, após o cancelamento do Cartão de Cidadão e/ou a revogação de um (ou todos) certificado(s) do Cartão de Cidadão, o certificado CMD de Assinatura Qualificada permanece válido.

A EC CMD guarda toda a documentação, referente a revogações de certificados de equipamento tecnológico, utilizada para verificação da identidade e autenticidade da entidade que efetua o pedido de revogação, que podem ser, entre outros:

- Patrocinador nomeado pela entidade, no caso de certificado de equipamento tecnológico;
- Representante legal da AMA, com poderes de representação para o pedido de revogação de certificados;
- Parte confiante, sempre que demonstre que o certificado foi utilizado com fins diferente dos previstos.

O pedido de revogação de certificado de equipamento tecnológico tem um formulário próprio[9] associado que, contém, entre outros, os seguintes elementos de identificação da entidade que inicia o pedido de revogação:

- Denominação legal;
- Número de pessoa coletiva, sede, objeto social, nome dos titulares dos corpos sociais e de outras pessoas com poderes para a obrigarem e número de matrícula na conservatória do registo comercial;
- Nome completo, número do bilhete de identidade ou qualquer outro elemento que permita a identificação inequívoca da entidade (ou seu representante) que inicia o pedido de revogação;
- Endereço e outras formas de contacto;
- Indicação de pedido de revogação, indicando o nome único (DN) atribuído ao certificado, assim como a sua validade;
- Indicação do motivo para revogação do certificado.

[9] *cf.* PJ.CMDA_33, Formulário de revogação de certificado de equipamento tecnológico emitido pela EC CMD.

4 Requisitos Operacionais do Ciclo de Vida do Certificado

4.1 Pedido de Certificado

4.1.1 Quem pode subscrever um pedido de certificado

O Serviço de Chave Móvel Digital (SCMD) é a única entidade que pode aceitar pedidos de certificados de pessoa singular referidos na secção 1.3.3.

Relativamente a certificados de Equipamento Tecnológico, o patrocinador é a única entidade que pode subscrever estes pedidos de certificados desde que sejam utilizados no âmbito do SCMD e sempre que sejam emitidos manualmente.

4.1.2 Processo de registo e responsabilidades

O processo de registo de certificado de pessoa singular é da única e total responsabilidade do SCMD.

Os pedidos de certificados, quando chegam à EC CMD, já se encontram com os titulares devidamente identificados e autenticados pela Entidade de Registo, sendo o registo inicial do requerente efetuado tal como descrito na secção 3.2.

O Certificado CMD de Assinatura Qualificada e o respetivo par de chaves são guardados em ambiente criptográfico seguro, protegidos por palavra-passe fornecida pelo requerente/titular do certificado, no estado ativo (i.e., pronto a ser utilizado para assinatura qualificada).

Faz prova de emissão do Certificado CMD de Assinatura Qualificada, a disponibilização dessa informação na conta do cidadão no serviço AUTENTICAÇÃO.GOV.

No ato do pedido de emissão do Certificado CMD de Assinatura Qualificada é fornecido ao titular informação sobre a utilização do Certificado (no âmbito das "Condições Gerais de utilização do serviço SCMD"), sendo que este deve aceitar os termos de utilização do mesmo (cf. seção 4.4.1).

No caso de certificado de equipamento tecnológico e de este ser emitido manualmente, o processo de registo é constituído pelos seguintes passos, a serem efetuados pela entidade de certificação subordinada requerente:

- Geração do par de chaves (chave pública e privada) pela EC subordinada (patrocinador, no caso de certificado de equipamento tecnológico);
- Geração do PKCS#10 correspondente pela EC subordinada (patrocinador, no caso de certificado de equipamento tecnológico);

- Geração do *hash* (SHA-256[10]) do PKCS#10, em formato PEM, pela EC subordinada (patrocinador, no caso de certificado de equipamento tecnológico);
- Arquivo do PKCS#10 e *hash* num CD/DVD, pela EC subordinada (patrocinador, no caso de certificado de equipamento tecnológico);
- Preenchimento pela EC subordinada (patrocinador, no caso de certificado de equipamento tecnológico) de documento de validação da identidade da entidade, de acordo com secção 3.2;
- Envio do CD/DVD e do documento corretamente preenchido ao contato da EC CMD indicado na secção 1.5.2.

4.2 Processamento do pedido de certificado

Os pedidos de certificado, depois de recebidos pela EC CMD através do SCMD, são considerados válidos se os seguintes requisitos forem cumpridos:

a) Validação da origem do pedido de certificado – o pedido só pode ser efetuado pelo SCMD –;

b) Verificação da exatidão e integridade do pedido de certificado.

As secções 3.2, 4.2.1 e 4.3 descrevem detalhadamente todo o processo.

4.2.1 Processos para a identificação e funções de autenticação

4.2.1.1 Certificado de pessoa singular

O SCMD é responsável por todos os processos para a identificação e funções de autenticação, de acordo com as secções 3.2, 3.2.3, 3.2.4.

4.2.1.2 Certificado de equipamento tecnológico

O Patrocinador é responsável pela candidatura para um certificado de equipamento tecnológico quando emitido manualmente, sempre que os seguintes critérios são preenchidos:

- Identificação e autenticação bem, sucedida de toda a informação necessária nos termos da secção 3.2.2 – toda a documentação utilizada para verificação da identidade e de poderes de representação é guardada;
- Formulário de pedido de emissão corretamente preenchido;
- PKCS#10 válido.

[10] *cf.* NIST FIPS PUB 180-2. 2002, Secure Hash Standard, U. S. Department of Commerce, Technology Administration, National Institute of Standards and Technology.

Em qualquer outra situação, será rejeitada a candidatura para emissão de certificado.

Após a emissão manual do certificado, este é entregue ao patrocinador pelo método "cara-a-cara" – tal ato é registado através do preenchimento e assinatura de formulário[8].

4.2.2 Aprovação ou recusa de pedidos de certificado

O pedido de certificado de pessoa singular enviado pelo SCMD é sempre aceite.

A aprovação de certificado de equipamento tecnológico, emitido manualmente, passa pelo cumprimento dos requisitos exigidos nas secções 4.2 e 4.2.1. Quando tal não se verifique, é recusada a emissão do certificado.

4.2.3 Prazo para processar o pedido de certificado

Após a aprovação do pedido de certificado, o certificado deverá ser emitido em, não mais do que:

- 10 horas, no caso de certificado de pessoa singular;
- Cinco (5) dias úteis, no caso de certificado de equipamento tecnológico.

4.3 Emissão de Certificado

4.3.1 Procedimentos para a emissão de certificado

4.3.1.1 Certificado de pessoa singular

A emissão do certificado é efetuada como resposta ao pedido do SCMD.

A emissão dos certificados por parte da EC CMD, indica que todos os procedimentos de processamento do pedido foram concluídos com sucesso.

A EC CMD utiliza um procedimento de geração de certificados, que vincula de forma segura o certificado com a informação de registo, incluindo a chave pública, e protege a confidencialidade e integridade dos dados de registo.

O par de chaves é gerado em *hardware* criptográfico, após autenticação do requerente com base no seu Cartão de Cidadão, conforme indicado nas secções 3.2.3 e 4.1.2. A chave pública é enviada à Entidade de Certificação, pelo SCMD, para emissão do certificado digital correspondente. O par de chaves e o certificado digital correspondente são guardados em ambiente criptográfico seguro do SCMD, protegidos por palavra-passe fornecida pelo requerente/titular do certificado.

Quando a EC CMD emite um certificado, efetuará as notificações que se estabelecem no ponto 4.3.2.

Os certificados são emitidos no estado ativo, iniciando a sua vigência no momento da sua emissão.

O período de vigência dos certificados está sujeito a uma possível extinção antecipada definitiva (revogação), quando se expliquem as causas que a motivem.

Todos os procedimentos relacionados com a emissão e com o estado de certificados são registados e arquivados.

4.3.1.2 Certificado de equipamento tecnológico

O certificado de equipamento tecnológico é emitido automaticamente. No entanto, sempre que não se possa garantir este processo, procede-se ao plano alternativo, que inclui a emissão do certificado manualmente garantindo assim a continuidade do processo.

Neste caso, a emissão do certificado é efetuada por meio de uma cerimónia que decorre na zona de alta segurança da EC CMD e, em que se encontram presentes:

- O patrocinador;
- Quatro (4) membros dos Grupo de Trabalho já que a segregação de funções não possibilita a presença de um número inferior de elementos;
- Quaisquer observadores, aceites simultaneamente pelos membros do Grupo de Trabalho e pelo patrocinador.

A cerimónia de emissão de certificado é constituída pelos seguintes passos:

- Identificação e autenticação de todas as pessoas presentes na cerimónia, garantindo que o patrocinador e os membros dos Grupos de Trabalho têm os poderes necessários para os atos a praticar;
- O patrocinador entrega, em mão, o CD/DVD e o formulário de emissão do certificado aos membros do Grupo de Trabalho da EC CMD. O formulário é datado e assinado pelos membros do Grupo de Trabalho que o devolvem ao patrocinador;
- Os membros do Grupo de Trabalho da EC CMD efetuam o procedimento de acesso ao EC CMD e emitem o certificado (correspondente ao PKCS#10 fornecido no CD/DVD) em formato PEM;
- Os membros do Grupo de Trabalho da EC CMD arquivam o certificado em formato PEM num CD/DVD e preenchem o formulário de receção e aceitação de certificado[8] em duplicado;
- Após a assinatura de ambas as cópias do formulário de receção e aceitação de certificado pelo patrocinador e pelos membros do Grupo de Trabalho, os membros do Grupo de Trabalho entregam o CD/DVD com o certificado em formato PEM ao patrocinador;
- A cerimónia de emissão fica terminada com a execução do procedimento de saída da EC CMD, pelos membros do Grupo de Trabalho da EC CMD.

O certificado emitido inicia a sua vigência no momento da sua emissão.

4.3.2 Notificação da emissão do certificado ao titular

A conta do cidadão no serviço AUTENTICAÇÃO.GOV indica ao cidadão o estado da emissão do Certificado CMD de Assinatura Qualificada.

Relativamente a certificados de Equipamento Tecnológico, a emissão do certificado, quando manual, é efetuada de forma presencial, de acordo com secção anterior.

4.4 Aceitação do Certificado

4.4.1 Procedimentos para a aceitação de certificado

Antes de ser disponibilizado o certificado ao seu titular, e consequentemente lhe serem disponibilizadas todas as funcionalidades na utilização da chave privada e certificado, é garantido que,

- O titular toma conhecimento dos seus direitos e responsabilidades;
- O titular toma conhecimento das funcionalidades e conteúdo do certificado;
- O titular toma conhecimento das suas condições de utilização, onde constam os procedimentos necessários em caso de expiração, revogação e renovação do certificado, bem como os termos, condições e âmbito de utilização do mesmo.

A tomada de conhecimento dos direitos, funcionalidades e condições de utilização, nos termos acima referidos, bem como a aceitação das condições de utilização do certificado, de que depende a utilização do mesmo, são sempre efetuados online mediante o acesso obrigatório pelo titular ao site do SCMD.

4.4.1.1 Certificado de pessoa singular

O SCMD suporta as atividades associadas ao pedido de emissão do certificado à EC CMD, assim como a sua guarda (em conjunto com o respetivo par de chaves) em ambiente criptográfico seguro, protegidos por palavra-passe fornecida pelo requerente/titular do certificado. São previstas também as funcionalidades de suporte à ocorrência de erros nas diversas atividades associadas a esta, de modo a suportar os procedimentos a realizar em cada situação, quer pelo SCMD, quer pelo Titular do certificado, comunicando com outros sistemas como a EC que emitiu o certificado.

Assume-se a aceitação do certificado pelo titular, após o mesmo ter fornecido a palavra-passe de proteção no ambiente criptográfico seguro.

4.4.1.2 Certificado de equipamento tecnológico

Sempre que o certificado é emitido manualmente, este considera-se aceite após a assinatura do formulário de emissão e aceitação de certificado pelo patrocinador, de acordo com cerimónia de emissão (conforme secção 4.3.1).

4.4.2 Publicação do certificado

A EC CMD não publica os certificados emitidos

4.4.3 Notificação da emissão de certificado a outras entidades

Nada a assinalar.

4.5 Uso do certificado e par de chaves

4.5.1 Uso do certificado e da chave privada pelo titular

Os titulares de certificados utilizarão a sua chave privada apenas e só para o fim a que estas se destinam (conforme estabelecido no campo do certificado "*keyUsage*") e sempre com propósitos legais.

A sua utilização apenas é permitida:

- A quem estiver designado no campo "*Subject*" do certificado;
- De acordo com as condições definidas nas secções 1.4.1 e 1.4.2;
- Enquanto o certificado se mantiver válido e não estiver na LRC da EC CMD.

Adicionalmente:

- O certificado CMD de Assinatura Qualificada atribuído a pessoa singular tem como objetivo a sua utilização para efeitos de assinatura digital qualificada, em aplicações identificadas no serviço AUTENTICAÇÃO.GOV;
- O certificado de Validação *on-line* OCSP tem como objetivo a sua utilização em servidores OCSP[4]

4.5.2 Uso do certificado e da chave pública pelas partes confiantes

Na utilização do certificado e da chave pública, as partes confiantes apenas podem confiar nos certificados, tendo em conta apenas o que é estabelecido nesta DPC e na respetiva Política de Certificação. Para isso devem, entre outras, garantir o cumprimento das seguintes condições:

- Ter conhecimento e perceber a utilização e funcionalidades proporcionadas pela criptografia de chave pública e certificados;
- Ser responsável pela sua correta utilização;
- Ler e entender os termos e condições descritos nas Políticas e práticas de certificação;
- Verificar os certificados (validação de cadeias de confiança) e LRC, tendo especial atenção às suas extensões marcadas como críticas e propósito das chaves;
- Confiar nos certificados, utilizando-os sempre que estes estejam válidos.

4.6 Renovação de Certificados

A renovação de um certificado é o processo em que a emissão de um novo certificado utiliza os dados anteriores do certificado, não havendo alteração das chaves ou qualquer outra informação, com exceção do período de validade do certificado.

Esta prática não é suportada na SCEE.

4.6.1 Motivos para renovação de certificado

Nada a assinalar.

4.6.2 Quem pode submeter o pedido de renovação de certificado

Nada a assinalar.

4.6.3 Processamento do pedido de renovação de certificado

Nada a assinalar.

4.6.4 Notificação de emissão de novo certificado ao titular

Nada a assinalar.

4.6.5 Procedimentos para aceitação de certificado

Nada a assinalar.

4.6.6 Publicação de certificado após renovação

Nada a assinalar.

4.6.7 Notificação da emissão do certificado a outras entidades

Nada a assinalar.

4.7 Renovação de certificado com geração de novo par de chaves

A renovação de chaves do certificado (*certificate re-key*) é o processo em que um titular (ou patrocinador) gera um novo par de chaves e submete o pedido para emissão de novo certificado que certifica a nova chave pública. Este processo, no âmbito da SCEE, é designado por renovação de certificado com geração de novo par de chaves.

A renovação de certificado com geração de novo par de chaves é feita de acordo com o estabelecido na secção 4.3.

4.7.1 Motivo para a renovação de certificado com geração de novo par de chaves

É motivo válido para a renovação de certificado com geração de novo par de chaves, sempre e quando se verifique que:

a) O certificado anterior expirou;

b) O certificado anterior foi revogado.

4.7.2 Quem pode submeter o pedido de certificação de uma nova chave pública

Tal como na secção 4.1.1.

4.7.3 Processamento do pedido de renovação de certificado com geração de novo par de chaves

Tal como na secção 4.1.2 e 4.2.

4.7.4 Notificação da emissão de novo certificado ao titular

Tal como na secção 4.3.2.

4.7.5 Procedimentos para aceitação de um certificado renovado com geração de novo par de chaves

Tal como na secção 4.4.1.

4.7.6 Publicação de certificado renovado com geração de novo par de chaves

Tal como na secção 4.4.2.

4.7.7 Notificação da emissão de certificado renovado a outras entidades

Tal como na secção 4.4.3.

4.8 Modificação de certificados

A alteração de certificados é o processo em que é emitido um certificado para um titular (ou patrocinador), mantendo as respetivas chaves, havendo apenas alterações na informação do certificado.

Esta prática não é suportada pela EC CMD.

4.8.1 Motivos para alteração do certificado

Nada a assinalar.

4.8.2 Quem pode submeter o pedido de alteração de certificado

Nada a assinalar.

4.8.3 Processamento do pedido de alteração de certificado

Nada a assinalar.

4.8.4 Notificação da emissão de certificado alterado ao titular

Nada a assinalar.

4.8.5 Procedimentos para aceitação de certificado alterado

Nada a assinalar.

4.8.6 Publicação do certificado alterado

Nada a assinalar.

4.8.7 Notificação da emissão de certificado alterado a outras entidades

Nada a assinalar.

4.9 Suspensão e revogação de certificado

Na prática, a revogação e suspensão de certificados é uma ação através da qual o certificado deixa de estar válido antes do fim do seu período de validade, perdendo a sua operacionalidade.

Os certificados depois de revogados não podem voltar a ser válidos, enquanto, que os certificados suspensos podem recuperar a sua validade.

4.9.1 Motivos para revogação

No caso do Certificado de pessoa singular, este pode ser revogado por uma das seguintes razões:

a) Informação do titular, contida no certificado, sofreu alterações;

b) Incapacidade superveniente do titular;

c) Perda da palavra-chave fornecida para guardar par de chaves e certificado em ambiente criptográfico seguro;

d) Fim de validade do certificado CMD de Assinatura Qualificada;

e) Morte do titular do certificado.

No caso de certificado de equipamento tecnológico, este pode ser revogado por uma das seguintes razões:

a) Comprometimento ou suspeita de comprometimento da chave privada;

b) Inexatidões graves nos dados fornecidos;

c) Equipamento tecnológico deixa de ser utilizado no âmbito do Cartão de Cidadão.

Para qualquer certificado emitido pela EC CMD podem ser causas para a sua revogação:

a) Comprometimento ou suspeita de comprometimento da chave privada da EC CMD ou de outra EC no "caminho" até à ECRaizEstado;

b) Perda, destruição ou deterioração do dispositivo de suporte da chave privada (por exemplo, hardware criptográfico);

c) Revogação do certificado da EC CMD ou de outra EC no "caminho" até à ECRaizEstado;

d) Incumprimento por parte da EC CMD ou titular das responsabilidades previstas na presente DPC;

e) Sempre que haja razões credíveis que induzam que os serviços de certificação possam ter sido comprometidos, de tal forma que coloquem em causa a fiabilidade dos certificados;

f) Sempre que haja razões credíveis que o certificado foi utilizado com fins diferente dos previstos;

g) Por resolução judicial ou administrativa.

4.9.2 Quem pode submeter o pedido de revogação

Está legitimado para submeter o pedido de revogação, sempre que se verifiquem alguma das condições descritas no ponto 4.9.1, os seguintes:

- No caso de certificado para pessoa singular este pode ser revogado a pedido de um dos seguintes elementos:
  - O titular do certificado;
  - A pessoa legalmente habilitada em caso de falecimento do titular;
  - O SCMD.
- No caso de Certificado de equipamento tecnológico este pode ser revogado a pedido de um dos seguintes elementos:
  - O patrocinador do certificado;
  - A EC CMD;
  - O Conselho Gestor (CG);
  - Uma parte confiante, sempre que demonstre que o certificado foi utilizado com fins diferente dos previstos.

A EC CMD guarda toda a documentação utilizada para verificação da identidade e autenticidade da entidade que efetua o pedido de revogação de certificados de equipamento tecnológico.

4.9.3 Procedimento para o pedido de revogação

4.9.3.1 Certificado de pessoa singular

No âmbito do processo de revogação, o SCMD suportará as atividades relacionadas com o registo dos pedidos de revogação do certificado, devido aos motivos indicados na secção 4.9.1, comunicando o pedido de revogação à EC CMD.

A forma de pedido de revogação poderá ser consultada na secção 3.4.

4.9.3.2 Certificado de equipamento tecnológico

Os procedimentos seguidos no pedido de revogação de certificado são os seguintes:

- Todos os pedidos de revogação devem ser endereçados para a EC CMD por escrito ou por mensagem eletrónica assinada digitalmente, em formulário de pedido de revogação[9]**;**
- Identificação e autenticação da entidade que efetua o pedido de revogação, conforme secção 4.4;
- Registo e arquivo do formulário de pedido de revogação;
- Análise do pedido de revogação pelo Grupo de Trabalho de Gestão da EC CMD, que propõe ao responsável do organismo que tutela a EC CMD a aprovação ou recusa do pedido de revogação;
- Mediante o parecer do Grupo de trabalho de Gestão da EC CMD, o responsável do organismo que tutela a EC CMD, decide a aprovação ou recusa do pedido de revogação do certificado;
- Sempre que se decidir revogar um certificado, a revogação é publicada na respetiva LRC.

Em qualquer dos casos, é arquivada a descrição pormenorizada de todo o processo de decisão, ficando documentado:

- Data do pedido de revogação;
- Nome do titular do certificado;
- Exposição pormenorizada dos motivos para o pedido de revogação;
- Nome e funções da pessoa que solicita a revogação;
- Informação de contacto da pessoa que solicita a revogação;
- Assinatura da pessoa que solicita a revogação.

4.9.4 Produção de efeitos da revogação

A revogação será feita de forma imediata. Após terem sido efetuados todos os procedimentos a revogação é efetivada e irreversível, sendo tal informação disponibilizada na conta do cidadão no serviço AUTENTICAÇÃO.GOV.

4.9.5 Prazo para processar o pedido de revogação

O pedido de revogação deve ser tratado de forma imediata, pelo que em caso algum poderá ser superior a 24 horas.

4.9.6 Requisitos de verificação da revogação pelas partes confiantes

Antes de utilizarem um certificado, as partes confiantes têm como responsabilidade verificar o estado de todo os certificados, através das LRC ou num servidor de verificação do estado *on-line* (via OCSP).

4.9.7 Periodicidade da emissão da lista de certificados revogados (LRC)

A EC CMD publica uma nova LRC no repositório, sempre que haja uma revogação. Quando não haja alterações ao estado de validade dos certificados, ou seja, se nenhuma revogação se tiver produzido a EC CMD disponibiliza nova LRC todas as semanas.

4.9.8 Período máximo entre a emissão e a publicação da LRC

O período máximo entre a emissão e publicação da LRC não deverá ultrapassar os 30 minutos.

4.9.9 Disponibilidade de verificação *on-line* do estado / revogação de certificado

A EC CMD dispõe de serviços de validação OCSP[4] do estado dos certificados de forma *on-line*. Esse serviço poderá ser acedido em http://ocsp.cmd.cartaodecidadao.pt/publico/ocsp.

O período máximo entre a revogação e a disponibilização através do serviço de validação OCSP não deverá ultrapassar os 10 minutos.

4.9.10 Requisitos de verificação *on-line* de revogação

As partes confiantes deverão dispor de *software* capaz de operar o protocolo OCSP[4], de forma a obter a informação sobre o estado do certificado.

4.9.11 Outras formas disponíveis para divulgação de revogação

Nada a assinalar.

4.9.12 Requisitos especiais em caso de comprometimento de chave privada

Apenas quando se trate do comprometimento da chave privada de uma EC. Neste caso deverão ser adotados os procedimentos descritos na secção 5.7.3.

4.9.13 Motivos para suspensão

A EC CMD não suspende certificados.

4.9.14 Quem pode submeter o pedido de suspensão

Nada a assinalar.

4.9.15 Procedimentos para pedido de suspensão

Nada a assinalar.

4.9.16 Limite do período de suspensão

Nada a assinalar.

4.10 Serviços sobre o estado do certificado

4.10.1 Caraterísticas operacionais

O estado dos certificados emitidos está disponível publicamente através das LRC.

4.10.2 Disponibilidade do serviço

O Serviço sobre o estado do certificado está disponível 24 horas por dia, 7 dias por semana.

4.10.3 Caraterísticas opcionais

Nada a assinalar.

4.11 Fim de subscrição

O fim da operacionalidade de um certificado acontece quando se verificarem uma das seguintes situações:

a) Revogação do certificado;

b) Por ter caducado o prazo de validade do certificado.

4.12 Retenção e recuperação de chaves (*Key escrow*)

A EC CMD só efetua a retenção da sua chave privada.

4.12.1 Políticas e práticas de recuperação de chaves

A chave privada da EC CMD é armazenada num *token hardware* de segurança, sendo efetuada uma cópia de segurança utilizando uma ligação direta *hardware* a *hardware* entre dois *tokens* de segurança. A geração da cópia de segurança é o último passo da emissão de um novo par de chaves da EC CMD.

A cerimónia de cópia de segurança utiliza um HSM com autenticação de dois fatores (consola de autenticação portátil e chaves PED – pequenos *tokens* de identificação digital, com o formato de chaves físicas – identificadoras de diferentes papéis no acesso à HSM), em que várias pessoas, cada uma delas possuindo uma chave PED, são obrigadas a autenticar-se antes que seja possível efetuar a cópia de segurança.

O *token hardware* de segurança com a cópia de segurança da chave privada da EC CMD é colocado num cofre seguro em instalações seguras secundárias, e acessível apenas aos membros autorizados dos Grupos de Trabalho. O controlo de acesso físico a essas instalações impede a outras pessoas de obterem acesso não autorizado às chaves privadas.

A cópia de segurança da chave privada da EC CMD pode ser recuperada no caso de mau funcionamento da chave original. A cerimónia de recuperação da chave utiliza os mesmos mecanismos de autenticação de dois fatores e com múltiplas pessoas, que foram utilizados na cerimónia de cópia de segurança.

4.12.2 Políticas e práticas de encapsulamento e recuperação de chaves de sessão

Nada a assinalar.

5 Medidas de segurança física, de gestão e operacionais

A AMA implementou várias regras e políticas incidindo sobre controlos físicos, procedimentais e humanos, que suportam os requisitos de segurança constantes desta DPC. Esta secção descreve sucintamente os aspetos não técnicos de segurança que possibilitam, de modo seguro, realizar as funções de geração de chaves, autenticação dos titulares, emissão de certificados, revogação de certificados, auditorias e arquivo. Todos estes controlos não técnicos de segurança são críticos para garantir a confiança nos certificados, pois qualquer falta de segurança pode comprometer as operações da EC.

5.1 Medidas de segurança física

5.1.1 Localização física e tipo de construção

As instalações da EC CMD são desenhadas de forma a proporcionar um ambiente capaz de controlar e auditar o acesso aos sistemas de certificação, estando fisicamente protegidas do acesso não autorizado, dano, ou interferência. A arquitetura utiliza o conceito de defesa em profundidade, ou seja, por níveis de segurança, garantindo-se que o acesso a um nível de segurança mais elevado só é possível quando previamente se tenha alcançado o nível imediatamente anterior, nunca sendo possível, em qualquer local das instalações, aceder ao nível de segurança (n) a partir de outro que não seja o nível (n-1).

As operações da EC CMD são realizadas numa sala numa zona de alta segurança, inserida noutra zona também de alta segurança e, dentro de um edifício que reúne diversas condições de segurança, nomeadamente o controlo total de acessos que previne, deteta e impede acessos não autorizados, baseado em múltiplos níveis de segurança física.

As duas zonas de alta segurança são áreas que obedecem às seguintes características:

- Paredes em alvenaria, betão ou tijolo;
- Teto e pavimento com construção similar à das paredes;
- Inexistência de janelas;
- Porta de segurança, com chapa em aço, com as dobradiças fixas e ombreira igualmente em aço, com fechadura de segurança acionável eletronicamente, características corta – fogo e funcionalidade antipânico.

Adicionalmente, as seguintes condições de segurança são garantidas no ambiente da EC CMD:

- Perímetros de segurança claramente definidos;

- Paredes, chão e teto em alvenaria, sem janelas, que impedem acessos não autorizados;
- Trancas e fechaduras antirroubo de alta segurança nas portas de acesso ao ambiente de segurança.
- O perímetro do edifício é estanque na medida em que não existem portas, janelas ou outras brechas não controladas, que possibilitem acessos não autorizados;
- Acesso ao ambiente passa obrigatoriamente por áreas de controlo humano, e por outros meios de controlo que restringem o acesso físico apenas a pessoal devidamente autorizado.

5.1.2 Acesso físico ao local

Os sistemas da EC CMD estão protegidos por um mínimo de 4 níveis de segurança física hierárquicos (edifício em si, bloco de alta segurança, área de alta segurança, sala de alta segurança) de acordo com a NT D-02[11], garantindo-se que o acesso a um nível de segurança mais elevado só é possível quando previamente se tenha alcançado os privilégios necessários ao nível imediatamente anterior.

Atividades operacionais sensíveis da EC, criação e armazenamento de material criptográfico, quaisquer atividades no âmbito do ciclo de vida do processo de certificação como autenticação, verificação e emissão ocorrem dentro da zona mais restrita de alta segurança. O acesso a cada nível de segurança requer o uso de um cartão magnético de autenticação (amarelo para o edifício, e vermelho para os outros níveis). Acessos físicos são automaticamente registados e gravados em circuito fechado de TV para efeitos de auditorias.

O acesso ao cartão de identificação vermelho obriga a um duplo controlo de autenticação de acesso individual. A pessoal, não acompanhado, incluindo colaboradores ou visitantes não autenticados não é permitida a sua entrada e permanência em áreas de segurança. A não ser que todo o pessoal que circule dentro destas áreas de segurança seja garantidamente reconhecido por todos, é obrigatório o uso do respetivo cartão de acesso de modo visível, assim como garantir que não circulam indivíduos não reconhecidos sem o respetivo cartão de acesso visível.

O acesso à zona mais restrita de alta segurança requer controlo duplo, cada um deles utilizando dois fatores de autenticação, incluindo autenticação biométrica. O *hardware* criptográfico e *tokens* físicos seguros dispõem de proteção adicional, sendo guardados em cofres e armários seguros. O acesso à zona mais restrita de alta segurança, assim como ao *hardware* criptográfico e aos *tokens* físicos seguros é restrito, de acordo com as necessidades de segregação de responsabilidades dos vários Grupos de Trabalho.

5.1.3 Energia e ar condicionado

O ambiente seguro da AMA possui equipamento redundante, que garante condições de funcionamento 24 horas por dia / 7 dias por semana, de:

[11] GNS/NT D-02 – Requisitos mínimos de Segurança Física de Instalações de Entidades Certificadoras

- Alimentação de energia garantindo alimentação contínua ininterrupta com a potência suficiente para manter autonomamente a rede elétrica durante períodos de falta de corrente e para proteger os equipamentos face a flutuações elétricas que os possam danificar (o equipamento redundante consiste em baterias de alimentação ininterrupta de energia, e geradores de eletricidade a diesel); e
- Refrigeração/ventilação/ar condicionado que controlam os níveis de temperatura e humidade, garantindo condições adequadas para o correto funcionamento de todos os equipamentos eletrónicos e mecânicos presentes dentro do ambiente. Um sensor de temperatura, ativa um alerta GSM, sempre que a temperatura atinge valores anormais. Este alerta GSM consiste em telefonemas com uma mensagem previamente gravada, para os elementos da equipa de manutenção.

5.1.4 Exposição à água

As zonas de alta segurança têm instalado os mecanismos devidos (detetores de inundação) para minimizar o impacto de inundações nos sistemas da EC CMD.

5.1.5 Prevenção e proteção contra incêndio

O ambiente seguro da AMA tem instalado os mecanismos necessários para evitar e apagar fogos ou outros incidentes derivados de chamas ou fumos. Estes mecanismos estão em conformidade com os regulamentos existentes:

- Sistemas de deteção e alarme de incêndio estão instalados nos vários níveis físicos de segurança;
- Equipamento fixo e móvel de extinção de incêndios estão disponíveis, colocados em sítios estratégicos e de fácil acesso de modo a poderem ser rapidamente usados no início de um incêndio e extingui-lo com sucesso;
- Procedimentos de emergência bem definidos, em caso de incêndio.

5.1.6 Salvaguarda de suportes de armazenamento

Todos os suportes de informação sensível contendo *software* e dados de produção, informação para auditoria, arquivo ou cópias de segurança são guardados em cofres e armários de segurança dentro da zona de alta segurança, assim como num ambiente distinto externo ao edifício com controlos de acessos físicos e lógicos apropriados para restringir o acesso apenas a elementos autorizados dos Grupos de Trabalho. Para além das restrições de acessos, também tem implementado mecanismos de proteção contra acidentes (e.g., causados por água ou fogo).

Quando, para efeito de arquivo de cópias de segurança, informação sensível é transportada da zona de alta segurança para o ambiente externo, o processo é executado sob supervisão de pelo menos 2 (dois) elementos do Grupo de Trabalho que têm por obrigação garantir o transporte seguro da informação até ao local de destino.

A informação (ou o *token* de transporte da informação) deverá estar sempre sob controlo visual dos membros do Grupo de Trabalho.

Em situações que implique a deslocação física de *hardware* de armazenamento de dados (i.e., discos rígidos,...) para fora da zona de alta segurança, por motivos que não o arquivo de cópias de segurança, cada elemento do *hardware* deverá ser verificado para garantir que não contém dados sensíveis. Nestas situações, a informação tem de ser eliminada usando todos os meios necessários para o efeito (formatar o disco rígido, *reset* do *hardware* criptográfico ou mesmo destruição física do equipamento de armazenamento).

5.1.7 Eliminação de resíduos

Documentos e materiais em papel que contenham informação sensível deverão ser triturados antes da sua eliminação.

É garantido que não é possível recuperar nenhuma informação dos suportes de informação utilizados para armazenar ou transmitir informação sensível (através de formatação "segura" de baixo nível ou destruição física), antes dos mesmos serem eliminados. Equipamentos criptográficos ou chaves físicas de acesso lógico são fisicamente destruídos ou seguem as recomendações de destruição do respetivo fabricante, antes da sua eliminação. Outros equipamentos de armazenamento (discos rígidos, tapes,...) deverão ser devidamente limpos de modo a não ser possível recuperar nenhuma informação (através de formatações seguras, ou destruição física dos equipamentos).

5.1.8 Instalações externas (alternativa) para recuperação de segurança

Todas as cópias de segurança são guardadas em ambiente seguro em instalações externas, ficando alojadas em cofres e armários seguros situados em zonas com controlos de acesso físicos e lógicos, de modo a restringir o acesso apenas a pessoal autorizado, garantindo também a proteção contra danos acidentais (e.g., causados por água ou fogo).

5.2 Medida de segurança dos processos

A atividade de uma Entidade Certificadora (daqui em diante denominada por EC) depende da intervenção coordenada e complementar de um extenso elenco de recursos humanos, nomeadamente porque:

- Dados os requisitos de segurança inerentes ao funcionamento de uma EC é vital garantir uma adequada segregação de responsabilidades, que minimize a importância individual de cada um dos intervenientes;
- É necessário garantir que a EC apenas poderá ser sujeita a ataques do tipo *denial-of-service* mediante o conluio de um número significativo de intervenientes;

- Quando uma mesma entidade é detentora de várias EC de diferentes níveis de segurança ou hierarquia, por vezes é desejável que os recursos humanos associados a uma EC não acumulem funções (ou pelo menos as mesmas) numa EC distinta.

Pelo exposto, nesta secção, descrevem-se os requisitos necessários para reconhecer os papéis de confiança e responsabilidades associadas a cada um desses papéis. Esta secção inclui também a separação de deveres, em termos dos papéis que não podem ser executados pelos mesmos indivíduos.

5.2.1 Grupos de Trabalho

Definem-se como pessoas autenticadas todos os colaboradoras, fornecedores e consultores que tenham acesso ou que controlem operações criptográficas ou de autenticação.

A AMA estabeleceu que os papéis de confiança fossem agrupados em sete categorias diferentes (que correspondem a nove Grupos de Trabalho distintos) de modo a garantir que as operações sensíveis sejam efetuadas por diferentes pessoas autenticadas, eventualmente pertencentes a diferentes Grupos de Trabalho.

5.2.1.1 Grupo de Trabalho de Inicialização

É responsável pela instalação e configuração de base (*hardware* e *software*) da EC até à sua inicialização. Este grupo deve ter pelo menos 1 (um) membro.

As responsabilidades deste grupo são:

- Instalar e configurar o *software* de base da EC;
- Instalar, interligar e configurar o *hardware* da EC;
- Configurar palavras-passe iniciais que irão ser alteradas posteriormente pelo Grupo de Trabalho de Autenticação e,
- Preparar comunicados sobre:
    - As palavras-passe iniciais;
    - Identificação dos membros do Grupo de Trabalho de Instalação;
    - *Hash* do(s) CD(s) de instalação utilizados e,
    - A lista de todos os artefactos (univocamente identificados) indispensáveis à inicialização e operação da EC.

5.2.1.2 Grupo de Gestão de Informação

É responsável por assegurar que toda a informação indispensável ao funcionamento e auditoria da EC se encontra disponível ao longo do tempo. Este Grupo deve ter um mínimo de 3 (três membros)

Este grupo tem como responsabilidades:

- Gerir o Ambiente de Informação;
- Assegurar que todos os documentos relevantes e relacionados, direta ou indiretamente, com o funcionamento da EC e existentes em formato papel[12] se encontram armazenados no Ambiente de Informação;

5.2.1.3 Grupo de Trabalho da Política

É responsável por propor todas as políticas da EC, assegurando que se encontram atualizadas. Este grupo deve ter um mínimo de 3 (três) membros.

As responsabilidades deste grupo incluem:

- Gerir o "Ambiente de Informação"
- Definir todas as políticas da EC e garantir que se encontram atualizadas, adaptadas à realidade desta e disponíveis;
- Assumir o papel de "Administrador de Segurança" e,
- Assegurar que as PCs da EC são suportadas pela DPC da EC.

5.2.1.4 Grupo de Trabalho de Auditoria

É responsável por efetuar a auditoria interna a todas as ações relevantes e necessárias para assegurar a operacionalidade da EC. Este grupo deve ter um mínimo de 2 (dois) membros.

As responsabilidades deste grupo são:

- Auditar a execução e confirmar a exatidão dos processos e cerimónias da EC;
- Registar todas as operações sensíveis;
- Investigar suspeitas de fraudes procedimentais;
- Verificar periodicamente a funcionalidade dos controlos de segurança (dispositivos de alarme, de controlo de acessos, sensores de fogo, etc.) existentes nos vários ambientes;
- Registar todos os procedimentos passíveis de auditoria;
- Registar os resultados de todas as ações por si realizadas;
- Assumir o papel de "Auditor de Sistema";
- Validar que todos os recursos usados são seguros.

[12] Os procedimentos a adotar em relação aos documentos em formato eletrónico serão definidos após a concretização do *Business Continuity Plan*.

5.2.1.5 Grupo de Trabalho de Operação

É responsável por executar as tarefas de rotina essenciais ao bom funcionamento e operacionalidade da EC. Note-se que, no sentido de assegurar a disseminação de conhecimento aprofundado sobre a operação da EC, este grupo subdivide-se em 2 (dois) subgrupos, compostos por pelo menos 4 (quatro) membros cada, que deverão revezar-se na participação nas cerimónias da EC. Cada membro apenas pode pertencer exclusivamente a um único subgrupo.

As responsabilidades deste grupo são:

- Gestão do "Ambiente de Produção" e do "Ambiente Operação";
- Realizar as tarefas de rotina da EC, incluindo operações de cópias de segurança dos seus sistemas;
- Execução de tarefas de monitorização dos sistemas EC;
- Monitorizar, reportar e quantificar todos os incidentes e avarias de *software* e *hardware*, despoletando os processos apropriados à correção das mesmas;
- Assumir o papel de "Operador de Sistema"; e
- Assumir o papel de "Administrador de Registo".

5.2.1.6 Grupo de Trabalho de Autenticação

É responsável por assegurar a gestão, guarda e disponibilidade (nas situações previstas) das palavras-passe (não pessoais) e dos *tokens* de autorização. Note-se que, no sentido de assegurar altos níveis de segurança e de continuidade de negócio, este grupo subdivide-se em 2 (dois) subgrupos, compostos por pelo menos 3 (três) membros cada, que deverão revezar-se na participação nas cerimónias da EC. Cada membro apenas pode pertencer exclusivamente a um único subgrupo.

Nenhum membro deste grupo está autorizado a entrar no "Ambiente de Operação" sem a presença de um membro do "Grupo de Trabalho de Operação" e/ou do "Grupo de Trabalho de Auditoria".

As responsabilidades deste grupo são:

- Gestão do "Ambiente de Autenticação";
- Gestão de todas as palavras-passe não pessoais;
- Manter um inventário atualizado de todos os *tokens* de autenticação usados no "Ambiente de Operação", e quando os *tokens* estão à responsabilidade de algum(ns) membro(s), registar a identificação desse(s) membro(s), e guardar estes registos no "Ambiente de Autenticação";

- Manter um inventário atualizado de todas as palavras-passe usadas no "Ambiente de Operação", e quando as palavras-passe estão à responsabilidade de algum(ns) membro(s), registar a identificação desse(s) membro(s), e guardar estes registos no "Ambiente de Autenticação";
- Garantir que cada membro dos restantes grupos não detém mais *tokens* de autenticação do que os estritamente necessários à execução das responsabilidades de que está incumbido;
- Garantir que cada membro dos restantes grupos não detém mais palavras-passe de autenticação do que as estritamente necessárias para a execução das responsabilidades de que está incumbido;
- Registar a devolução dos *tokens* de autenticação usados pelos membros dos restantes grupos;
- Registar trocas de palavras-passe de autenticação usadas pelos membros dos restantes grupos;
- Registar a perca de *tokens* de autenticação, descrevendo adequadamente a situação que lhe deu origem;
- Registar sempre que uma palavra-passe de autenticação é comprometida, descrevendo adequadamente a situação que o originou;
- Avaliar os riscos de negócio resultantes da perca de um *token* ou o comprometimento de uma palavra-passe de autenticação;
- Tomar medidas ativas de modo a não comprometer cada Ambiente de Produção derivado da perca de um *token*, ou do comprometimento de alguma palavra-passe de autenticação e,
- Avaliar pedidos de replicação de documentação.
- Assumir o papel de *Administrador de Sistema*;
- Assumir o papel de "Administrador de Registo".

5.2.1.7 Grupo de Trabalho de Monitorização e Controlo

É responsável por monitorizar e controlar os pontos de controlo de segurança de todos os recursos utilizados no Ambiente de Produção da PKI do Cartão de Cidadão, que podem dar origem a eventos, alarmes e incidentes.

As responsabilidades deste grupo são:

- Consolidar e analisar a monitorização dos recursos utilizados no Ambiente de Produção da PKI do Cartão de Cidadão;
- Monitorizar o funcionamento dos mecanismos de alarme existentes;
- Monitorizar eventos, gerir alarmes e classificar incidentes;
- Definir, apoiar a implementação e a melhoria contínua de procedimentos para resposta a incidentes.

5.2.1.8 Grupo de Gestão

É responsável pela nomeação dos membros dos restantes grupos[13] e pela guarda de alguns artefactos sensíveis (*tokens* de autenticação, etc.). Este membro deve ter um mínimo de 4 (quatro) membros.

[13] À exceção do Grupo de Trabalho de Instalação, do Grupo de Trabalho de Auditoria e do Grupo de Trabalho de Custódia

As responsabilidades deste grupo são:

- Gestão do "Ambiente de Gestão";
- Rever e aprovar as políticas propostas pelo Grupo de Trabalho de Política;
- Designar os membros dos restantes grupos de trabalho;
- Disponibilizar a identificação de todos os indivíduos que pertencem aos vários Grupos de Trabalho, em um ou mais pontos de acesso facilmente acessíveis pelos indivíduos autorizados.

5.2.1.9 Grupo de Trabalho de Custódia

É responsável pela custódia de alguns artefactos sensíveis (*tokens* de autenticação, etc.), que podem ser levantados pelos membros dos outros grupos mediante a satisfação de determinadas condições[14]. Note-se que, no sentido de melhorar os níveis de segurança, operacionalidade e continuidade de negócio da EC, poderão existir várias instâncias deste grupo, cada qual encarregue da custódia de um conjunto distinto de artefactos. Este grupo deve fazer uso dos vários ambientes seguros disponibilizados para a guarda deste tipo de itens.

As responsabilidades deste grupo são:

- Gestão do "Ambiente de Custódia" respetivo;
- Custódia de artefactos sensíveis (*tokens* de autenticação, etc.) usando os meios adequados que respondam às necessidades de segurança respetivas e,
- Disponibilização segura destes itens a membros de grupos autorizados e explicitamente indicados com permissões de acesso a esses itens, após o cumprimento dos procedimentos apropriados de segurança.

5.2.2 Número de pessoas exigidas por tarefa

Existem rigorosos procedimentos de controlo que obrigam à divisão de responsabilidades baseada nas especificidades de cada Grupo de Trabalho, e de modo a garantir que tarefas sensíveis apenas podem ser executadas por um conjunto múltiplo de pessoas autenticadas.

Os procedimentos de controlo interno foram elaborados de modo a garantir um mínimo de 2 indivíduos autenticados para se ter acesso físico ou lógico aos equipamentos de segurança. O acesso ao *hardware* criptográfico da EC segue procedimentos estritos envolvendo múltiplos indivíduos autorizados a aceder-lhe durante o seu ciclo de vida, desde a receção e inspeção até à destruição física e/ou lógica do *hardware*. Após a ativação de um módulo com chaves operacionais, controlos adicionais de acesso são utilizados de modo a garantir que os acessos físicos e lógicos ao *hardware* só são possíveis com um mínimo de 2 indivíduos autenticados. Indivíduos com acesso físico aos módulos, não detêm as chaves de ativação e vice-versa.

[14] Definidas para cada um dos artefactos à sua guarda

5.2.3 Funções que requerem separação de responsabilidades

A matriz seguinte define as incompatibilidades (assinaladas por ✖) entre a pertença ao grupo/subgrupo identificado na coluna esquerda e a pertença ao grupo/subgrupo identificado na primeira linha, no contexto desta EC:

Se pertence ao Grupo/Subgrupo ...	Pode pertencer ao Grupo/Subgrupo ... ?	Instalação	Políticas	Operação		Autenticação		Auditoria	Monitorização e Controlo	Custódia	Gestão	Gestão da Informação
				Subgrupo 1	Subgrupo 2	Subgrupo 1	Subgrupo 2					
Instalação								✖		✖	✖	
Políticas						✖	✖	✖	✖	✖	✖	
Operação	**Subgrupo 1**				✖	✖	✖	✖		✖	✖	
	Subgrupo 2			✖		✖	✖	✖		✖	✖	
Autenticação	**Subgrupo 1**		✖	✖	✖		✖	✖		✖	✖	✖
	Subgrupo 2		✖	✖	✖	✖		✖		✖	✖	✖
Auditoria		✖	✖	✖	✖	✖	✖		✖	✖	✖	✖
Monitorização e Controlo			✖					✖		✖	✖	✖
Custódia		✖	✖	✖	✖	✖	✖	✖	✖		✖	✖
Gestão		✖	✖	✖	✖	✖	✖	✖	✖	✖		✖
Gestão da Informação						✖	✖	✖	✖	✖	✖	

5.3 Medidas de Segurança de Pessoal

5.3.1 Requisitos relativos às qualificações, experiência, antecedentes e credenciação

Todo o pessoal que desempenhe funções de confiança na EC CMD deve cumprir os seguintes requisitos:

- Ter sido nomeado formalmente para a função a desempenhar;
- Apresentar provas de antecedentes, qualificações e experiência necessárias para a realização das tarefas inerentes à função;
- Ter credenciação mínima Nacional Confidencial (ou equivalente);

- Ter formação e treino adequado para o desempenho da respetiva função;
- Garantir confidencialidade, relativamente a informação sensível da EC ou dados de identificação dos titulares;
- Garantir o conhecimento dos termos e condições para o desempenho da respetiva função e,
- Garantir que não desempenhar funções que possam causar conflito com as suas responsabilidades nas atividades da EC.

5.3.2 Procedimento de verificação de antecedentes

A verificação de antecedentes decorre do processo de credenciação dos indivíduos nomeados para exercer cargos em qualquer uma das funções de confiança. A verificação de antecedentes inclui:

- Confirmação de identificação, usando documentação emitida por fontes fiáveis e,
- Investigação de registos criminais.

5.3.3 Requisitos de formação e treino

É ministrado aos membros dos Grupos de Trabalho formação e treino adequado de modo a realizarem as suas tarefas satisfatória e competentemente.

Os elementos dos Grupos de Trabalho, estão adicionalmente sujeitos a um plano de formação e treino, englobando os seguintes tópicos:

a) Certificação digital e Infraestruturas de Chave Pública;
b) Conceitos gerais sobre segurança da informação;
c) Formação específica para o desempenho das suas funções;
d) Funcionamento do *software* e/ou *hardware* usado pela EC;
e) Política de Certificados e Declaração de Práticas de Certificação;
f) Recuperação face a desastres;
g) Procedimentos para a continuidade da atividade e,
h) Aspetos legais básicos relativos à prestação de serviços de certificação.

5.3.4 Frequência e requisitos para ações de reciclagem

Sempre que necessário será ministrado treino e formação complementar aos membros dos Grupos de Trabalho, de modo a garantir o nível pretendido de profissionalismo para a execução competente e satisfatória das suas responsabilidades. Em particular,

- Sempre que exista qualquer alteração tecnológica, introdução de novas ferramentas ou modificação de procedimentos, é levada a cabo a adequada formação para todo o pessoal afeto às EC;
- Sempre que são introduzidas alterações nas Politicas de Certificação ou Declaração de Práticas de Certificação são realizadas sessões de reciclagem aos elementos das EC.

5.3.5 Frequência e sequência da rotação de funções

Nada a assinalar.

5.3.6 Sanções para ações não autorizadas

Consideram-se ações não autorizadas todas as ações que desrespeitem a Declaração de Práticas de Certificação e as Políticas de Certificação, quer sejam realizadas de forma deliberada ou sejam ocasionadas por negligência.

São aplicadas sanções de acordo com as regras da AMA e das leis de segurança nacional, a todos os indivíduos que realizem ações não autorizadas ou que façam uso não autorizado dos sistemas.

5.3.7 Requisitos para prestadores de serviços

Consultores ou prestadores de serviços independentes tem permissão de acesso à zona de alta segurança desde de que estejam sempre acompanhados e diretamente supervisionados pelos membros do Grupo de Trabalho, sendo a sua identidade confirmada através da verificação de documentação emitida por fontes confiáveis.

5.3.8 Documentação fornecida ao pessoal

É disponibilizado aos membros dos Grupos de Trabalho toda a informação adequada para que estes possam realizar as suas tarefas de modo competente e satisfatório.

5.4 Procedimentos de auditoria de segurança

5.4.1 Tipo de eventos registados

Eventos significativos geram registos auditáveis. Estes incluem, pelo menos os seguintes:

- Tentativas de acesso (com e sem sucesso) para solicitar, gerar, assinar, emitir ou revogar chaves de certificados;
- Tentativas de acesso (com e sem sucesso) para criar, modificar ou apagar informação dos titulares dos certificados;

- Tentativas de acesso (com e sem sucesso) e alterações dos parâmetros de segurança do sistema operativo;
- Emissão e publicação de LRC's;
- Arranque e paragem de aplicações;
- Tentativas de acesso (com e sem sucesso) de início e fim de sessão;
- Tentativas de acesso (com e sem sucesso) de criar, modificar, apagar contas do sistema;
- Cópias de segurança, recuperação ou arquivo dos dados;
- Alterações ou atualizações de *software* e *hardware*;
- Manutenção dos sistemas;
- Operações realizadas por membros dos Grupos de Trabalho;
- Alteração de Recursos Humanos;
- Tentativas de acesso (com e sem sucesso) às instalações por parte de pessoal autorizado ou não;
- A cerimónia de geração de chaves e sistemas envolvidos na mesma, tais como servidores aplicacionais, base de dados e sistema operativo.

As entradas nos registos incluem a informação seguinte:

- Número de série do evento;
- Data e hora do evento;
- Identidade do sujeito que causou o evento;
- Categoria do evento;
- Descrição do evento.

5.4.2 Frequência da auditoria de registos

Os registos são analisados, pelo menos, uma vez por ano pelos elementos do grupo de trabalho de Auditoria, e adicionalmente sempre que haja suspeitas ou atividades anormais ou ameaças de algum tipo. Ações tomadas, baseadas na informação dos registos são também documentadas.

5.4.3 Período de retenção dos registos de auditoria

Os registos são mantidos disponíveis durante pelo menos 2 (dois) meses após processamento, e depois arquivados nos termos descritos na secção 5.5.

5.4.4 Proteção dos registos de auditoria

Os registos são analisados exclusivamente por membros do Grupo de Trabalho de Auditoria e reportados ao Grupo de Gestão.

Os registos são protegidos por mecanismos eletrónicos auditáveis de modo a detetar e impedir a ocorrência de tentativas de modificação, remoção ou outros esquemas de manipulação não autorizada dos dados.

A destruição de um arquivo de auditoria só pode ser levada a cabo na presença de, no mínimo dois elementos, um elemento de autenticação e um de auditoria. Estes só podem ser destruídos com autorização expressa do Grupo de Gestão.

5.4.5 Procedimentos para a cópia de segurança dos registos

Cópias de segurança dos arquivos são efetuadas de modo incremental ou total e guardados em dispositivos de memória terciária.

5.4.6 Sistema de recolha de registos (Interno / Externo)

O processo de tratamento e recolha de registos de auditoria é constituído por uma combinação de processos automáticos e manuais, executados pelos sistemas operativos, pelas aplicações da EC CMD e pelo pessoal que as opera. Todos os registos de auditoria são armazenados nos sistemas internos da EC CMD.

5.4.7 Notificação de agentes causadores de eventos

Eventos auditáveis são registados no sistema de auditoria e guardados de modo seguro, sem haver notificação ao sujeito causador da ocorrência do evento.

5.4.8 Avaliação de vulnerabilidades

Os registos auditáveis são regularmente analisados de modo a minimizar e eliminar potenciais tentativas de quebrar a segurança do sistema.

São realizados dois testes de intrusão por ano de forma a verificar e avaliar vulnerabilidades.

O resultado da análise é reportado ao Grupo de Gestão para rever e aprovar um plano de implementação e correção das vulnerabilidades detetadas.

5.5 Arquivo de registos

5.5.1 Tipo de dados arquivados

Todos os dados auditáveis são arquivados (conforme indicado na secção 5.4.1), assim como informação de pedidos de certificados e documentação de suporte ao ciclo de vida das várias operações.

As informações e eventos que são registados e arquivados são:

- Os registos de auditoria especificados na secção 5.4.1 desta DPC;

- As cópias de segurança dos sistemas que compõem a infraestrutura da EC CMD;

- Toda a documentação relativa ao ciclo de vida dos certificados, designadamente:

    - Procedimentos de emissão e revogação de certificados;

    - Formulários de emissão e receção dos certificados de equipamento tecnológico.

- Acordos de confidencialidade;

- Protocolos estabelecidos com as Entidades Subscritoras;

- Contratos estabelecidos entre a EC e outras entidades encontram-se armazenados em local seguro e poderão ser disponibilizados a quem solicitar a sua visualização, após avaliação e aprovação prévia do pedido;

- Autorizações de acesso aos sistemas de informação;

- Acessos aos artefactos existentes nas custódias;

- Autorizações de acesso aos sistemas de informação.

5.5.2 Período de retenção em arquivo

Os dados sujeitos a arquivo são retidos pelo período de tempo definido pela legislação nacional.

5.5.3 Proteção dos arquivos

O arquivo é protegido de modo a que:

- Apenas membros autorizados dos Grupos de Trabalho possam consultar e ter acesso ao arquivo;
- O arquivo é protegido contra qualquer modificação ou tentativa de o remover;
- O arquivo é protegido contra a deterioração do media onde é guardado, através de migração periódica para media novo;

- O arquivo é protegido contra a obsolescência do *hardware*, sistemas operativos e outros *software*, pela conservação do *hardware*, sistemas operativos e outros *software* que passam a fazer parte do próprio arquivo, de modo a permitir o acesso e uso dos registos guardados, de modo intemporal e,
- Os arquivos são guardados de modo seguro em ambientes externos seguros.

5.5.4 Procedimentos para as cópias de segurança do arquivo

Cópias de segurança dos arquivos são efetuadas de modo incremental ou total e guardados em dispositivos de memória terciária.

5.5.5 Requisitos para validação cronológica dos registos

Algumas das entradas dos arquivos contêm informação de data e hora. Tais informações de data e hora não têm por base uma fonte de tempo segura.

5.5.6 Sistema de recolha de dados de arquivo (Interno / Externo)

Os sistemas de recolha de dados de arquivo são internos.

5.5.7 Procedimentos de recuperação e verificação de informação arquivada

Apenas membros autorizados dos Grupos de Trabalho têm acesso aos arquivos para verificação da sua integridade.

São realizadas de forma automática verificações de integridade dos arquivos eletrónicos (cópias de segurança) na altura da sua criação, em caso de erros ou comportamentos imprevistos, realiza-se novo arquivo.

5.6 Renovação de chaves

Nada a assinalar.

5.7 Recuperação em caso de desastre ou comprometimento

Esta secção descreve os requisitos relacionados com os procedimentos de notificação e de recuperação no caso de desastre ou de comprometimento.

5.7.1 Procedimentos em caso de incidente ou comprometimento

As cópias de segurança das chaves privadas da EC (geradas e mantidas de acordo com a secção 6.2.4) e dos registos arquivados (secção 5.5.1) são guardados em ambientes seguros externos e disponíveis em caso de desastre. No caso de comprometimento da chave privada da EC CMD, esta deverá tomar as seguintes ações:

- Proceder à sua revogação imediata;
- Revogar todos os certificados dela, dependentes;
- Informar todos os titulares dos seus certificados e terceiras partes conhecidas;
- Informar todas as Entidades que compõem a SCEE dependendo ou não da EC CMD.

5.7.2 Corrupção dos recursos informáticos, do *software* e/ou dos dados

No caso dos recursos informáticos, *software* e/ou dados estarem corrompidos ou existir suspeita de corrupção, as cópias de segurança da chave privada da EC e os registos arquivados podem ser obtidos para verificação da integridade dos dados originais.

Se for confirmado que os recursos informáticos, *software* e/ou dados estão corrompidos, devem ser tomadas medidas apropriadas de resposta ao incidente. A resposta ao incidente pode incluir o restabelecimento do equipamento/dados corrompidos, utilizando equipamento similar e/ou recuperando cópias de segurança e registos arquivados. Até que sejam repostas as condições seguras, a EC CMD suspenderá os seus serviços e notificará o CG. Caso se verifique que esta situação tenha afetado certificados emitidos, proceder-se-á a notificação dos titulares dos mesmos e à revogação dos respetivos certificados.

5.7.3 Procedimentos em caso de comprometimento da chave privada da entidade

No caso da chave privada da EC CMD ser comprometida ou haver suspeita do seu comprometimento, devem ser tomadas medidas apropriadas de resposta ao incidente. As respostas a esse incidente podem incluir:

- Informar a Autoridade Nacional de Segurança (ANS);
- Revogação do certificado da EC CMD e de todos os certificados emitidos no "ramo" da hierarquia de confiança da EC CMD;
- Notificação do CG, todas as entidades que compõem a SCEE e todos os titulares de certificados emitidos no "ramo" da hierarquia de confiança da EC CMD;
- Geração de novo par de chaves para a EC CMD, e pedido de novo certificado à EC CC,
- Renovação de todos os certificados emitidos no "ramo" da hierarquia de confiança da EC CMD.

5.7.4 Capacidade de continuidade da atividade em caso de desastre

Em caso de desastre, os serviços serão retomados após estarem reunidas todas as condições de segurança.

5.8 Procedimentos em caso de extinção de EC ou ER

Em caso de cessação de atividade como prestador de serviços de Certificação, a EC CMD deve, atempadamente, com uma antecedência mínima de três meses, proceder às seguintes ações descritas na secção 9.10.

6 Medidas de Segurança Técnicas

Esta secção define as medidas de segurança implementadas para a EC CMD de forma a proteger chaves criptográficas geradas por esta, e respetivos dados de ativação. O nível de segurança atribuído à manutenção das chaves deve ser máximo para que chaves privadas e chaves seguras assim como dados de ativação estejam sempre protegidos e sejam apenas acedidos por pessoas devidamente autorizadas.

6.1 Geração e instalação do par de chaves

A geração dos pares de chaves da EC CMD é processada de acordo com os requisitos e algoritmos definidos nesta política.

6.1.1 Geração do par de chaves

A geração de chaves criptográficas da EC CMD é feita por um Grupo de Trabalho, composto por elementos autorizados para tal, numa cerimónia planeada e auditada de acordo com procedimentos escritos das operações a realizar. Todas as cerimónias de geração de chaves ficam registadas, datadas e assinadas pelos elementos envolvidos no Grupo de Trabalho

O *hardware* criptográfico, usado para a geração de chaves da EC CMD, cumpre os requisitos FIPS 140-2 nível 3 e/ou *Common Criteria* EAL 4+ e, efetua a manutenção de chaves, armazenamento e todas as operações que envolvem chaves criptográficas utilizando exclusivamente o *hardware*. O acesso a chaves críticas é protegido por políticas de segurança, divisão de papéis entre os Grupos de Trabalho, assim como através de regras de acesso limitado de utilizadores. As cópias de segurança de chaves criptográficas são efetuadas apenas usando *hardware*, permitindo que estas cópias sejam devidamente auditadas e que na eventualidade de uma perca de dados, possa haver uma recuperação total e segura das chaves.

A geração do par de chaves da EC CMD é efetuada por elementos autorizados dos Grupos de trabalho num *hardware* criptográfico que cumpre os requisitos FIPS 140-2 nível 3 e/ou *Common Criteria* EAL 4+.

O funcionamento da EC CMD é efetua em modo *on-line*.

6.1.2 Entrega da chave privada ao titular

A EC CMD não gera a chave privada associada aos certificados que emite.

6.1.3 Entrega da chave pública ao emissor do certificado

A chave pública é entregue à EC CMD, de acordo com os procedimentos indicados na secção 4.3.1.

6.1.4 Entrega da chave pública da EC às partes confiantes

A chave pública da EC CMD será disponibilizada através do certificado da EC CMD, assinado pela EC do Estado, conforme secção 2.2.

6.1.5 Dimensão das chaves

O comprimento dos pares de chaves deve ter o tamanho suficiente, de forma a prevenir possíveis ataques de criptanálise que descubram a chave privada correspondente ao par de chaves no seu período de utilização. A dimensão das chaves é a seguinte:

- 4096 bits RSA para a chave da EC CMD.

6.1.6 Geração dos parâmetros da chave pública e verificação da qualidade

A geração dos parâmetros da chave pública e verificação da qualidade deverá ter sempre por base a norma que define o algoritmo.

As chaves da EC são geradas com base na utilização de processos aleatórios/pseudo aleatórios descritos no ANSI X9.17 (Anexo C), de acordo com o estipulado no PKCS#1.

6.1.7 Fins a que se destinam as chaves (campo "*key usage*" X.509 v3)

O campo "*keyUsage*" dos certificados, utilizado de acordo com o recomendado no *RFC 5280*[6] inclui a seguinte utilização.

a) *Non-repudiation*

6.2 Proteção da chave privada e características do módulo criptográfico

Nesta secção são considerados os requisitos para proteção da chave privada e para os módulos criptográficos da EC CMD. A AMA implementou uma combinação de controlos físicos, lógicos e procedimentos, devidamente documentados, de forma a assegurar confidencialidade e integridade das chaves privadas da EC CMD.

6.2.1 Normas e medidas de segurança do módulo criptográfico

Para a geração dos pares de chaves da EC CMD assim como para o armazenamento das chaves privadas, a AMA utiliza módulo criptográfico em *hardware* que cumpre as seguintes normas:

- Segurança Física
    - Common Criteria EAL 4+ e/ou
    - FIPS 140-2, nível 3
- Certificações Regulamentares
    - *U/L 1950 (EN60950) & CSA C22.2*
    - *FCC Part 15 - Class B*
    - *RoHS*
    - *BAC & EAC*
- Papéis
    - Autenticação de dois fatores
- Suporte de API
    - PKCS#11
    - Microsoft CryptoAPI
    - Java JCE/JCE CSP
    - Open SSL
- Geração de números aleatórios
    - ANSI X9.17 (Anexo C)
- Troca de chaves e chave de cifra assimétrica
    - RSA (512-4096 bit), PKCS#1 v1.5, OAEP PKCS#1 v2.0
    - Diffie-Hellman (512-1024 bit)
- Assinatura Digital
    - RSA (512-4096 bit)
    - DSA (512-1024 bit)
    - PKCS#1 v1.5
- Algoritmos de chave simétrica
    - DES

- 3DES (comprimento duplo e triplo)
- RC2
- RC4
- RC5
- AST
- CAST-3
- CAST-128

– Algoritmos de Hash

- SHA-1
- SHA-256
- MD-2
- MD-5

– Códigos de Autenticação de Mensagens (*Message Authentication Codes* - MAC)

- HMAC-MD5
- HMAC-SHA-1
- SSL3-MD5-MAC
- SSL3-SHA-1-MAC

6.2.2 Controlo multipessoal (*n* de *m*) para a chave privada

O controlo multipessoal apenas é utilizado para as chaves de EC, pois a chave privada dos certificados está sob exclusivo controlo do seu titular.

A AMA implementou um conjunto de mecanismos e técnicas que obrigam à participação de vários membros do Grupo de Trabalho para efetuar operações criptográficas sensíveis na EC.

Os dados de ativação necessários para a utilização da chave privada da EC CMD são divididos em várias partes (guardadas nas chaves PED – pequenos *token*s de identificação digital, com o formato de chaves físicas, identificadoras de diferentes papéis no acesso à HSM), acessíveis e à responsabilidade de diferentes membros do Grupo de Trabalho. Um determinado número destas partes (*n*) do total número de partes (*m*) é necessário para ativar a chave privada da EC CMD guardada no módulo criptográfico em *hardware*. São necessárias, no mínimo, duas (n) partes para a ativação da chave privada da EC CMD.

6.2.3 Retenção da chave privada (*key escrow*)

A retenção da chave privada da EC CMD é explicada em detalhe na secção 4.12.

6.2.4 Cópia de segurança da chave privada

A chave privada da EC CMD tem pelo menos uma cópia de segurança, com o mesmo nível de segurança que a chave original, conforme secção 4.12.

6.2.5 Arquivo da chave privada

As chaves privadas da EC CMD, alvo de cópias de segurança, são arquivadas conforme identificado na secção 4.12.

6.2.6 Transferência da chave privada para/do módulo criptográfico

As chaves privadas da EC CMD não são extraíveis a partir do *token* criptográfico FIPS 140-2 nível 3.

Se for realizada uma cópia de segurança das chaves privadas da EC CMD para um outro *token* criptográfico, essa cópia é efetuada diretamente, *hardware* para *hardware*, de uma forma que garante o transporte das chaves entre módulos numa transmissão cifrada.

6.2.7 Armazenamento da chave privada no módulo criptográfico

As chaves privadas da EC CMD são armazenadas de forma cifrada nos módulos do *hardware* criptográfico.

6.2.8 Processo para ativação da chave privada

A EC CMD é uma EC *on-line*, cuja chave privada é ativada quando o sistema da EC é ligado. Esta ativação é efectivada através da autenticação no módulo criptográfico pelos indivíduos indicados para o efeito, sendo obrigatória a utilização de autenticação de dois fatores (consola de autenticação portátil e chaves PED – pequenos *tokens* de identificação digital, com o formato de chaves físicas – identificadoras de diferentes papéis no acesso à HSM), em que várias pessoas (membros dos grupos de trabalho), cada uma delas possuindo uma chave PED, são obrigadas a autenticar-se antes que seja possível efetuar a cópia de segurança.

Para a ativação das chaves privadas da EC CMD é necessária, no mínimo, a intervenção de quatro elementos do Grupo de Trabalho. Uma vez a chave ativada, esta permanecerá assim até que o processo de desativação seja executado.

6.2.9 Processo para desativação da chave privada

A chave privada da EC CMD é desativada quando o sistema da EC é desligado.

Para a desativação das chaves privadas da EC CMD é necessária, no mínimo, a intervenção de quatro elementos do Grupo de Trabalho. Uma vez desativada, esta permanecerá inativa até que o processo de ativação seja executado.

6.2.10 Processo para destruição da chave privada

As chaves privadas da EC CMD (incluindo as cópias de segurança) são apagadas/destruídas num procedimento devidamente identificado e auditado no mínimo 30 dias após assim que terminada a sua data de validade (ou se revogadas antes deste período).

A destruição das chaves privadas garante que não será possível a recuperação/reconstrução da mesma. São executados procedimentos específicos disponibilizados pelo fabricante do *hardware* criptográfico que garantem a total destruição da chave privada da EC.

6.2.11 Avaliação/nível do módulo criptográfico

Descrito na secção 6.2.1.

6.3 Outros aspetos da gestão do par de chaves

6.3.1 Arquivo da chave pública

É efetuada uma cópia de segurança de todas as chaves públicas da EC CMD pelos membros do Grupo de Trabalho permanecendo armazenadas após a expiração dos certificados correspondentes, para verificação de assinaturas geradas durante seu prazo de validade.

6.3.2 Períodos de validade do certificado e das chaves

O período de utilização das chaves é determinado pelo período de validade do certificado, pelo que após expiração do certificado as chaves deixam de poder ser utilizadas, dando origem à cessação permanente da sua operacionalidade e da utilização que lhes foi destinada.

Neste sentido a validade dos diversos tipos de certificados e período em que os mesmos devem ser renovados, é o seguinte:

- O certificado de pessoa singular tem uma validade máxima de dez anos;

- Os certificados de equipamento tecnológico têm uma validade de cinco anos e dois meses, sendo utilizados durante o seu primeiro mês de validade, sendo reemitido após o primeiro mês de validade.

6.4 Dados de ativação

6.4.1 Geração e instalação dos dados de ativação

Os dados de ativação necessários para a utilização da chave privada da EC CMD são divididos em várias partes (guardadas em chaves PED – pequenos *tokens* de identificação digital, com o formato de chaves físicas – identificadoras de diferentes papéis no acesso à HSM), ficando à responsabilidade de diferentes membros do Grupo de Trabalho. As diferentes partes são geradas de acordo com o definido no processo/cerimónia de geração de chaves.

6.4.2 Proteção dos dados de ativação

Os dados de ativação (em partes separadas e/ou palavra-passe) são memorizados e/ou guardados em *tokens* que evidenciem tentativas de violação e/ou guardados em envelopes que são guardados em cofres seguros.

As chaves privadas da EC CMD são guardadas, de forma cifrada, em *token* criptográfico.

6.4.3 Outros aspetos dos dados de ativação

Se for preciso transmitir os dados de ativação das chaves privadas, esta transmissão será protegida contra perdas de informação, roubo, alteração de dados e divulgação não autorizada.

Os dados de ativação são destruídos (por formatação e/ou destruição física) quando a chave privada associada é destruída.

6.5 Medidas de segurança informáticas

6.5.1 Requisitos técnicos específicos

O acesso aos servidores da EC CMD é restrito aos membros dos Grupos de Trabalho com uma razão válida para esse acesso. A EC CMD tem um funcionamento *on-line*, sendo o pedido de emissão de certificados efetuado a partir do Sistema de Ciclo de Vida e da consola de operação (caso dos certificados de equipamento tecnológico).

A EC CMD e o Sistema de Ciclo de Vida dispõem de dispositivos de proteção de fronteira, nomeadamente sistema *firewall*, assim como cumprem os requisitos necessários para identificação, autenticação, controlo de

acessos, administração, auditorias, reutilização, responsabilidade e recuperação de serviços e troca de informação.

6.5.2 Avaliação/nível de segurança

Os vários sistemas e produtos utilizados pela EC CMD são fiáveis e protegidos contra modificações.

O módulo criptográfico em *Hardware* da EC CMD satisfaz a norma EAL 4+ *Common Criteria for Information Technology Security Evaluation* e/ou FIPS 140-2 nível 3.

6.6 Ciclo de vida das medidas técnicas de segurança

6.6.1 Medidas de desenvolvimento do sistema

As aplicações são desenvolvidas e implementadas por terceiros de acordo com as suas regras de desenvolvimento de sistemas e de gestão de mudanças.

É fornecido metodologia auditável que permite verificar que o *software* da EC CMD não foi alterado antes da sua primeira utilização. Toda a configuração e alterações do *software* são executadas e auditadas por membros do Grupo de Trabalho.

6.6.2 Medidas para a gestão da segurança

A AMA tem mecanismos e/ou Grupos de Trabalho, para controlar e monitorizar a configuração dos sistemas da EC. O sistema do EC CMD, quando utilizado pela primeira vez, será verificado para garantir que o *software* utilizado é fidedigno e legal e que não foi alterado depois da sua instalação.

6.6.3 Ciclo de vida das medidas de segurança

As operações de atualização e manutenção dos produtos e sistemas da EC CMD, seguem o mesmo controlo que o equipamento original e é instalado pelos membros do Grupo de Trabalho com adequada formação para o efeito, seguindo os procedimentos definidos para o efeito.

6.7 Medidas de Segurança da rede

A EC CMD encontra-se ligada a uma rede interna, protegida e isolada com vários perímetros físicos e lógicos de segurança.

6.8 Validação cronológica (*Time-stamping*)

Certificados, CRLs e outras entradas na base de dados contêm sempre informação sobre a data e hora dessa entrada. A informação cronológica é baseada em fontes de tempo confiáveis estando sincronizada com o padrão mundial da hora UTC, através de pelo menos duas fontes de tempo confiáveis externas, sendo escolhidas entre os vários laboratórios UTC(k) identificados pelo BIPM (Bureau International des Poids et Mesures) na sua Circular T (https://www.bipm.org/en/bipm-services/timescales/time-ftp/Circular-T.html), estando neste momento a ser utilizadas as seguintes:

- time-b-b.nist.gov – 132.163.96.2 - NIST, Boulder, Colorado
- ntp-p1.obspm.fr – 145.238.203.14 - Observatoire de Paris (LNE-SYRTE), Paris, France
- 200.20.186.75 – Observatório Nacional, Rio de Janeiro, Brazil.

A sincronização é efetuada pelo protocolo NTP em que o desvio máximo para o UTC é de um segundo. Esta precisão é monitorizada, dando origem a um evento a investigar, sempre que for ultrapassada.

7 Perfis de Certificado, CRL e OCSP

7.1 Perfil de Certificado

Os utilizadores de uma chave pública têm que ter confiança que a chave privada associada é detida pelo titular remoto correto (pessoa ou sistema) com o qual irão utilizar mecanismos de cifra ou assinatura digital. A confiança é obtida através do uso de certificados digitais X.509 v3, que são estrutura de dados que fazem a ligação entre a chave pública e o seu titular. Esta ligação é afirmada através da assinatura digital de cada certificado por uma EC de confiança. A EC pode basear esta afirmação em meios técnicos (por exemplo, prova de posse da chave privada através de um protocolo desafio-resposta), na apresentação da chave privada, ou no registo efetuado pelo titular.

Um certificado tem um período limitado de validade, indicado no seu conteúdo e assinado pela EC. Como a assinatura do certificado e a sua validade podem ser verificadas independentemente por qualquer *software* que utilize certificados, os certificados podem ser distribuídos através de linhas de comunicação e sistemas públicos, assim como podem ser guardados em qualquer tipo de unidades de armazenamento[6].

O utilizador de um serviço de segurança que requeira o conhecimento da chave pública do utilizador necessita, normalmente, de obter e validar o certificado que contém essa chave. Se o serviço não dispuser de uma cópia fidedigna da chave pública da EC que assinou o certificado, assim como do nome da EC e informação relacionada (tal como o período de validade), então poderá necessitar um certificado adicional para obter a chave pública da EC e validar a chave pública do utilizador. Em geral, para validar a chave pública de um utilizador, pode ser necessária uma cadeia de múltiplos certificados, incluindo o certificado da chave pública do utilizador assinado por uma EC e, zero ou mais certificados adicionais de ECs assinados por outras ECs[6].

O perfil dos certificados emitidos pela EC CMD está de acordo com:

- Recomendação ITU.T X.509[15];
- RFC 5280[6] e,
- Política de Certificados da SCEE[1];
- Legislação nacional e Europeia, aplicável.

Os perfis dos certificados podem ser consultados nos documentos de Políticas de Certificados associadas a esta DPC.

[15] cf. ITU-T Recommendation X.509. 1997, (1997 E): Information Technology - Open Systems Interconnection – The Directory: Authentication Framework.

7.2 Perfil da lista de revogação de certificados

Quando um certificado é emitido, espera-se que seja utilizado durante todo o seu período de validade. Contudo, várias circunstâncias podem causar que um certificado se torne inválido antes da expiração do seu período de validade. Tais circunstâncias incluem a mudança de nome, mudança de associação entre o titular e os dados do certificado e, o compromisso ou suspeita de compromisso da chave privada correspondente. Sob tais circunstâncias, a EC tem que revogar o certificado[6].

O protocolo X.509 define um método de revogação do certificado, que envolve a emissão periódica, pela EC, de uma estrutura de dados assinada, a que se dá o nome de Lista de Revogação de Certificados (LRC). A LRC é uma lista com identificação temporal dos certificados revogados, assinada pela EC e disponibilizada livremente num repositório público. Cada certificado revogado é identificado na LRC pelo seu número de série. Quando uma aplicação utiliza um certificado (por exemplo, para verificar a assinatura digital de um utilizador remoto), a aplicação verifica a assinatura e validade do certificado, assim como obtém a LRC mais recente e verifica se o número de série do certificado não faz parte da mesma. Note-se que uma EC emite uma nova LRC numa base regular periódica[6].

O perfil da LRC está de acordo com:

- Recomendação ITU.T X.509[15];
- RFC 5280[6] e,
- Política de Certificados da SCEE[1];
- Legislação nacional e Europeia, aplicável.

Os perfis das LRC podem ser consultados nos documentos de Políticas de Certificados associadas a esta DPC, relativamente à EC CMD.

7.3 Perfil OCSP

O perfil dos certificados OCSP está de acordo com:

- Recomendação ITU.T X.509[15];
- RFC 5280[6] e,
- Política de Certificados da SCEE[1];
- Legislação nacional e Europeia, aplicável.

Os perfis dos certificados OCSP podem ser consultados no documento de Política de Certificados de Validação *on-line* OCSP associadas a esta DPC.

8 Auditoria e Avaliações de Conformidade

Uma inspeção regular de conformidade a esta DPC e a outras regras, procedimentos, cerimónias e processos será levada a cabo pelos membros do Grupo de Trabalho de Auditoria da EC CMD.

Para além de auditorias de conformidade, a AMA irá efetuar outras fiscalizações e investigações para assegurar a conformidade da EC CMD com a legislação nacional. A execução destas auditorias, fiscalizações e investigações poderá ser delegada a uma entidade externa de auditoria.

8.1 Frequência ou motivo da auditoria

As auditorias de conformidade são realizadas regularmente de acordo com o definido pelo regulamento (EU) nº 910/2014, caso não exista outra diretiva emitida pela Entidade Supervisora. A EC precisa de provar, com a auditoria e relatório de segurança (produzido por um organismo de avaliação de conformidade acreditado pelo Organismo Nacional de Acreditação), que a avaliação dos riscos foi assegurada, tendo sido identificado e implementado todas as medidas necessárias para a segurança de informação.

8.2 Identidade e qualificações do auditor

O auditor é uma pessoa ou organização, de reconhecida idoneidade, com experiência e qualificações comprovadas na área da segurança da informação e dos sistemas de informação, infraestruturas de chaves pública, familiarizado com as aplicações e programas de certificação digital e na execução de auditorias de segurança. A sua missão é auditar a infraestrutura da Entidade de Certificação, no que respeita a equipamentos, recursos humanos, processos, políticas e regras.

O Organismo Nacional de Acreditação (IPAC) é responsável pela acreditação dos Organismos de Avaliação de Conformidade estando estes capacitados para efetuar as avaliações de conformidade resultando dessa avaliação um Relatório de Conformidade (CAR) e a ser disponibilizado à Entidade Supervisora, para avaliar a continuidade de disponibilização de serviços de confiança.

8.3 Relação entre o auditor e a Entidade Certificadora

O auditor e membros da sua equipa são independentes, não atuando de forma parcial ou discriminatória em relação à entidade que é submetida à auditoria.

Na Relação entre o auditor e a entidade submetida a auditoria, deve estar garantido inexistência de qualquer vínculo contratual.

O Auditor e a parte auditada (Entidade Certificadora) não devem ter nenhuma relação, atual ou prevista, financeira, legal ou de qualquer outro género que possa originar um conflito de interesses.

O cumprimento do estabelecido na legislação em vigor sobre a proteção de dados pessoais, deve ser tida em conta por parte do auditor, na medida em que o auditor poderá aceder a dados pessoais dos ficheiros dos titulares das EC.

8.4 Âmbito da auditoria

O âmbito das auditorias e outras avaliações inclui a conformidade com a legislação nacional e com este DPC e outras regras, procedimentos e processos (especialmente os relacionados com operações de gestão de chaves, recursos, controlos de gestão e operação e, gestão de ciclo de vida de certificados).

8.5 Procedimentos após uma auditoria com resultado deficiente

Se duma auditoria resultarem irregularidades, o auditor procede da seguinte forma:

- Documenta todas as deficiências encontradas durante a auditoria;
- No final da auditoria reúne com os responsáveis da entidade submetida a auditoria e apresenta de forma resumida um relatório de primeiras impressões (RPI);
- Elabora o relatório auditoria. Este relatório deverá estar organizado de modo a que todas as deficiências sejam escalonadas por ordem decrescente de gravidade/severidade;
- Submete o relatório de auditoria à CG para apreciação;
- Depois de apreciado e consolidado, é remetida uma cópia do relatório de auditoria final (RAF), para a entidade;
- Tendo em conta a irregularidades constantes no relatório, a entidade submetida à auditoria enviará uma relatório de correção de irregularidades (RCI), para CG, no qual deve estar descrito quais as ações, metodologia e tempo necessário para corrigir as irregularidades encontradas;
- A CG e Entidade Supervisora depois de analisar este relatório tomam uma das três seguintes opções, consoante o nível de gravidade/severidade das irregularidades:
    a) Aceitam os termos, permitindo que a atividade seja desenvolvida até à próxima inspeção;
    b) Permitem que a entidade continue em atividade por um período máximo de 60 dias até à correção das irregularidades antes da revogação;
    c) Revogação imediata da atividade.

8.6 Comunicação de resultados

Os resultados devem ser comunicados à Entidade Supervisora.

9 Outras Situações e Assuntos Legais

Esta secção aborda aspetos de negócio e assuntos legais.

9.1 Taxas

9.1.1 Taxas por emissão ou renovação de certificados

Nada a assinalar.

9.1.2 Taxas para acesso a certificado

Nada a assinalar.

9.1.3 Taxas para acesso a informação do estado do certificado ou de revogação

O acesso a informação sobre o estado ou revogação dos certificados é livre e, gratuita.

9.1.4 Taxas para outros serviços

Nada a assinalar.

9.1.5 Política de reembolso

Nada a assinalar.

9.2 Responsabilidade financeira

9.2.1 Seguro de cobertura

Nada a assinalar.

9.2.2 Outros recursos

Nada a assinalar.

9.2.3 Seguro ou garantia de cobertura para utilizadores

Nada a assinalar.

9.3 Confidencialidade da informação processada

9.3.1 Âmbito da confidencialidade da informação

Declara-se expressamente como informação confidencial, aquela que não poderá ser divulgada a terceiros:

- As chaves privadas das EC CMD;
- Toda a informação relativa aos parâmetros de segurança, controlo e procedimentos de auditoria;
- Toda a informação de carácter pessoal proporcionada à EC CMD durante o processo de registo dos subscritores de certificados, salvo se houver autorização explícita para a sua divulgação;
- Planos de continuidade de negócio e recuperação;
- Registos de transações, incluindo os registos completos e os registos de auditoria das transações;
- Informação de todos os documentos relacionados com a EC CMD (regras, políticas, cerimónias, formulários e processos), incluindo conceitos organizacionais, constitui informação financeira/comercial secreta, confidencial e/ou privilegiada, sendo propriedade da AMA. Estes documentos são confiados aos recursos humanos dos Grupos de Trabalho da EC CMD com a condição de não serem usados ou divulgados para além do âmbito dos seus deveres nos termos estabelecidos, sem autorização prévia e explícita da AMA;
- Todas as palavras-chave, PINs e outros elementos de segurança relacionados com a EC CMD;
- A identificação dos membros dos grupos de trabalho da EC CMD;
- A localização dos ambientes da EC CMD e seus conteúdos.

9.3.2 Informação fora do âmbito da confidencialidade da informação

Considera-se informação de acesso público:

- Política de Certificados;
- Declaração de Práticas de Certificação;

- LRC e,
- Toda a informação classificada como "pública" (informação não expressamente considerada como "pública" será considerada confidencial).

A EC CMD permite o acesso a informação não confidencial sem prejuízo de controlos de segurança necessários para proteger a autenticidade e integridade da mesma.

9.3.3 Responsabilidade de proteção da confidencialidade da informação

Os elementos dos Grupos de Trabalho ou outras entidades que recebam informação confidencial são responsáveis por assegurar que esta não é copiada, reproduzida, armazenada, traduzida ou transmitida a terceiras partes por quaisquer meios sem antes terem o consentimento escrito da AMA.

9.4 Privacidade dos dados pessoais

A SCEE[1] mantém atualizada a sua Política de Privacidade nos seus repositórios, onde se declara o cumprimento das disposições estabelecidas na legislação de proteção de dados pessoais.

9.4.1 Medidas para garantia da privacidade

O SCMD é responsável pela implementação das medidas que garantem a privacidade dos dados pessoais, que estão de acordo com a Política de Certificação da Sistema de Certificação Electrónica do Estado[1].

9.4.2 Informação privada

De acordo com a Política de Certificação da Sistema de Certificação Electrónica do Estado[1].

9.4.3 Informação não protegida pela privacidade

De acordo com a Política de Certificação da Sistema de Certificação Electrónica do Estado[1].

9.4.4 Responsabilidade de proteção da informação privada

De acordo com a Política de Certificação da Sistema de Certificação Electrónica do Estado[1].

9.4.5 Notificação e consentimento para utilização de informação privada

De acordo com a Política de Certificação da Sistema de Certificação Electrónica do Estado[1].

9.4.6 Divulgação resultante de processo judicial ou administrativo

De acordo com a Política de Certificação da Sistema de Certificação Electrónica do Estado[1].

9.4.7 Outras circunstâncias para revelação de informação

Nada a assinalar.

9.5 Direitos de propriedade intelectual

Todos os direitos de propriedade intelectual, incluindo os que se referem a certificados e LRC emitidos, OID, DPC e PC, bem como qualquer outro documento propriedade da EC CMD pertencem à AMA.

As chaves privadas e as chaves públicas são propriedade do titular, independentemente do meio físico que se empregue para o seu armazenamento.

O Titular conserva sempre o direito sobre as marcas, produtos ou nome comercial contido no certificado

9.6 Representações e garantias

9.6.1 Representação e garantias das entidades certificadoras

A EC CMD está obrigada a:

- Realizar as suas operações de acordo com esta Política;
- Declarar de forma clara todas as suas Práticas de Certificação no documento apropriado;
- Proteger as suas chaves privadas;
- Emitir certificados de acordo com o *standard* X.509;
- Emitir certificados que estejam conformes com a informação conhecida no momento de sua emissão e livres de erros de entrada de dados;
- Garantir a confidencialidade no processo da geração dos dados da criação da assinatura e a sua entrega por um procedimento seguro ao titular;
- Utilizar sistemas e produtos fiáveis que estejam protegidos contra toda a alteração e que garantam a segurança técnica e criptográfica dos processos de certificação;
- Utilizar sistemas fiáveis para armazenar certificados reconhecidos que permitam comprovar a sua autenticidade e impedir que pessoas não autorizadas alterem os dados;
- Arquivar sem alteração os certificados emitidos;

- Garantir que podem determinar com precisão da data e hora em que emitiu ou extingui ou suspendeu um certificado;
- Empregar pessoal com qualificações, conhecimentos e experiência necessárias para a prestação de serviços de certificação;
- Revogar os certificados nos termos da Suspensão e Revogação de Certificados deste documento e publicar os certificados revogados na CRL do repositório da respetiva EC, com a frequência estipulada na secção 4.9.7;
- Publicar a sua DPC e as Políticas de Certificado aplicáveis no seu repositório garantindo o acesso às versões atuais assim como as versões anteriores;
- Notificar com a rapidez necessária, por correio eletrónico os titulares dos certificados em caso da EC proceder à revogação ou suspensão dos mesmos, indicando o motivo que originou esta ação;
- Colaborar com as auditorias dirigidas pelo CG, para validar a renovação das suas próprias chaves;
- Operar de acordo com a legislação aplicável;
- Proteger em caso de existirem as chaves que estejam sobre sua custódia;
- Garantir a disponibilidade da CRL de acordo com as disposições da secção 4.9.7;
- Em caso de cessar a sua atividade deverá comunicar com uma antecedência mínima de dois meses a todos os titulares dos certificados emitidos assim como à CG comunicando;
- Cumprir com as especificações contidas na norma sobre Proteção de Dados Pessoais;
- Conservar toda a informação e documentação relativa a um certificado reconhecido e as Declarações de Práticas de Certificação vigentes em cada momento e durante quinze anos desde o momento da emissão e,
- Disponibilizar os certificados da EC CMD.

9.6.2 Representação e garantias das Entidades de Registo

Nada a assinalar.

9.6.3 Representação e garantias dos titulares

É obrigação dos titulares dos certificados emitidos:

- Limitar e adequar a utilização dos certificados de acordo com as utilizações previstas nesta DPC e nas respetivas Políticas de Certificado;
- Tomar todos os cuidados e medidas necessárias para garantir a segurança da palavra-chave fornecida para proteger a sua chave privada;

- Solicitar de imediato a revogação de um certificado em caso de ter conhecimento ou suspeita de compromisso da palavra-chave fornecida para proteger a sua chave privada, de acordo com a secção 4.9.3;
- Não utilizar um certificado digital que tenha perdido a sua eficácia, quer por ter sido revogado, suspendido ou por ter expirado o período de validade;
- Submeter às Entidade de Registo (ER) a informação que considerem exata e completa com relação aos dados que estas solicitem para realizar o processo de registo. Deve informar a ER de qualquer modificação desta informação e,
- Não monitorizar, manipular ou efetuar ações de "engenharia inversa" sobre a implantação técnica (*hardware* e *software*) dos serviços de certificação, sem a devida autorização prévia, por escrito, da EC CMD.

9.6.4 Representação e garantias das partes confiantes

É obrigação das partes que confiem nos certificados emitidos pela EC CMD:

- Limitar a fiabilidade dos certificados às utilizações permitidas para os mesmos em conformidade com o expresso nesta DPC e na Politica de Certificado correspondente;
- Verificar a validade dos certificados no momento de realizar qualquer operação baseada nos mesmos;
- Assumir a responsabilidade na correta verificação das assinaturas digitais;
- Assumir a responsabilidade na comprovação da validade, revogação ou suspensão dos certificados em que confia;
- Ter pleno conhecimento das garantias e responsabilidades aplicáveis na aceitação e uso de certificados em que confia e aceitar sujeitar-se às mesmas;
- Notificar qualquer acontecimento ou situação anómala relativa ao certificado, que possa ser considerado como causa de revogação do mesmo, utilizando os meios que o SCMD publique no seu sítio *Web*, conforme seção 3.4.

9.6.5 Representação e garantias de outros participantes

Nada a assinalar.

9.7 Renúncia de garantias

A EC CMD recusa todas as garantias de serviço que não se encontrem vinculadas nas obrigações estabelecidas neste DPC.

9.8 Limitações às obrigações

- A EC CMD responde pelos danos e prejuízos que cause a qualquer pessoa em exercício da sua atividade de acordo com o Artº 26 do DL 62/2003.
- A EC CMD responde pelos prejuízos que cause aos titulares ou a terceiros pela falta ou atraso na inclusão no serviço de consulta sobre a vigência dos certificados, da revogação ou suspensão dum certificado, uma vez que tenha conhecimento dele.
- A EC CMD assume toda a responsabilidade mediante terceiros pela atuação dos titulares das funções necessárias à prestação de serviços de certificação.
- A responsabilidade da administração / gestão da EC CMD assenta sobre base objetiva e cobre todo o risco que os particulares sofram sempre que seja consequência do funcionamento normal ou anormal dos seus serviços
- A EC CMD só responde pelos danos e prejuízos causados pelo uso indevido do certificado reconhecido, quando não tenha consignado no certificado, de forma clara reconhecida por terceiros o limite quanto ao possível uso.
- A EC CMD não responde quando o titular superar os limites que figuram no certificado quanto as suas possíveis utilizações, de acordo com as condições estabelecidas e comunicadas ao titular.
- A EC CMD não responde se o destinatário dos documentos assinados eletronicamente não os comprovar e tiver em conta as restrições que figuram no certificado quanto às suas possíveis utilizações e
- A EC CMD não assume qualquer responsabilidade no caso de perca ou prejuízo:
    - Dos serviços que prestam, em caso de guerra, desastres naturais ou qualquer outro caso de força maior;
    - Ocasionados pelo uso dos certificados quando excedam os limites estabelecidos pelos mesmo na Política de Certificados e correspondente DPC:
    - Ocasionado pelo uso indevido ou fraudulento dos certificados ou LRC emitidos pela EC CMD.

9.9 Indemnizações

De acordo com a legislação em vigor

9.10 Termo e cessação da atividade

Em caso de decisão de términus de atividade são identificadas neste documento algumas ações a serem executadas.

9.10.1 Notificação de cessação de atividade

A primeira ação será a de Notificação, que pretende dar conhecimento a todas as entidades, singulares ou coletivas, que de alguma forma intervêm na atividade.

Desta forma a AMA deverá informar de forma imediata:

- Autoridade Nacional de segurança (GNS);
- Conselho Gestor do SCEE;
- Grupo Gestor da EC CC;
- Cidadão para quem tenham sido emitidos certificados e que ainda se encontrem válidos à data da decisão de cessação de atividade.

A notificação inclui, no mínimo, a seguinte informação:

- GNS e Conselho Gestor do SCEE:
  - Comunicação para efeitos de cancelamento das credenciações de segurança
- Cidadão:
  - Informar o cidadão de que os seus certificados, emitidos no âmbito do Cartão de Cidadão, irão ser revogados, deixando por isso de ser válidos para utilização.

9.10.2 Cessação de Relações contratuais

Serão cessadas as relações contratuais com todas as entidades terceiras que, de alguma forma, intervenham nas atividades inerentes ao SCMD.

9.10.3 Revogação dos certificados

Todos os certificados emitidos no âmbito do SCMD, quer para o cidadão, quer para os sistemas inerentes, serão revogados. Assim, as atividades serão as seguintes:

1. Revogação de todos os certificados emitidos para o cidadão e para os equipamentos tecnológicos, que ainda se encontrem válidos;
2. Emissão e disponibilização pública das Listas de Certificados Revogados da EC CMD;
3. Destruição das Chaves Privadas da Entidades Certificadora CMD;

4. Garantir a transferência e manutenção para retenção por outra organização (se for o caso) de toda a informação relativa à atividade da EC, nomeadamente, documentação em arquivos (interno ou externo), repositórios e arquivos de registo de eventos, durante o período de tempo legalmente exigido.

Todas as Listas de Certificados Revogados serão mantidas acessíveis publicamente no repositório da EC CMD, até à expiração do último certificado emitido no âmbito do SCMD.

9.11 Notificação individual e comunicação aos participantes

Todos os participantes devem utilizar métodos razoáveis para comunicação. Esses métodos podem incluir correio eletrónico assinado digitalmente, fax, formulários assinados, ou outros, dependendo da criticidade e assunto da comunicação. No caso de comunicações a transmitir ao cidadão serão efetuadas através dos sites da AMA e do AUTENTICACAO.GOV.

9.12 Alterações

Os documentos relacionados com a EC (incluindo esta DPC) tornam-se efetivos assim que sejam aprovados pelo GG e apenas são eliminados ou alterados por sua ordem e/ou do Conselho Gestor.

Esta DPC entra em vigor desde o momento de sua publicação no repositório da EC e manter-se-á enquanto não for substituída pela emissão de uma nova versão.

9.12.1 Procedimento para alterações

No sentido de alterar este documento ou alguma das políticas de certificado, é necessário submeter um pedido formal ao Grupo de Trabalho das Políticas, indicando (pelo menos):

- A identificação da pessoa que submeteu o pedido de alteração;
- A razão do pedido.

As alterações pedidas.

O Grupo de Trabalho de Políticas vai rever o pedido feito e, se verificar a sua pertinência, procede às atualizações necessárias ao documento, resultando numa nova versão de rascunho do documento. O novo rascunho do documento é depois disponibilizado a todos os membros do Grupo de Trabalho e às partes afetadas (se alguma) para permitir o seu escrutínio. Contando a partir da data de disponibilização, as várias partes têm 15 dias úteis para submeter os seus comentários. Quando esse período terminar, o Grupo de Trabalho de Políticas tem mais 15 dias úteis para analisar todos os comentários recebidos e, se relevante, incorporá-los no documento. O documento é de seguida analisado pelo Grupo de Trabalho de Gestão da Informação e aprovado pelo Grupo de

Gestão. Depois da sua aprovação, o Grupo de Trabalho de Gestão de Informação solicita ao Grupo de Trabalho de Monitorização e Controlo a sua publicação no repositório público do cartão de cidadão, tornando-se as alterações finais e efetivas.

9.12.1.1 Substituição e revogação da DPC

O Grupo de Gestão pode decidir em favor substituição de um documento relacionado com a EC (incluindo esta DPC), quando:

- Os seus conteúdos são considerados incompletos, imprecisos ou erróneos;
- Os seus conteúdos foram comprometidos.

Neste caso o documento substituído será substituído por uma nova versão.

Após o Grupo de Gestão decidir em favor da substituição de um documento relacionado com a EC, o Grupo de Trabalho das Políticas tem 30 dias úteis para submeter para aprovação pelo Grupo de Trabalho de Gestão o(s) documento(s) substituto(s).

As obrigações e restrições que estabelece esta DPC, em referência a auditorias, informação confidencial, obrigações e responsabilidades da EC, nascidas sob sua vigência, serão substituídas por uma nova versão em tudo o que não se oponha a esta.

Sempre que um documento for considerado, pelo Grupo de Gestão, obsoleto, ou seja quando for considerada a sua existência desnecessária, será revogado e, quando este for um documento público, será retirado do repositório público, garantindo-se contudo que será conservado durante o período definido pelo regulamento (ER) nº 910/2014 ou, caso exista, pelo período indicado pela Entidade Supervisora.

9.12.2 Prazo e mecanismo de notificação

Sempre que as alterações à especificação possam afetar a aceitabilidade dos certificados para propósitos específicos, comunicar-se-á aos utilizadores dos certificados correspondentes que se efetuou uma mudança e que devem consultar a nova DPC no repositório estabelecido.

9.12.3 Motivos para mudar de OID

O Grupo de Trabalho da Política deve determinar se as alterações à DPC obrigam a uma mudança no OID da política de Certificados ou no URL que aponta para a DPC.

Nos casos em que, a julgamento do Grupo de Trabalho da Política, as alterações da DPC não afetem à aceitação dos certificados proceder-se-á ao aumento do número menor de versão do documento e o último número de Identificador de Objeto (OID) que o representa, mantendo o número maior da versão do documento, assim

como o resto de seu OID associado. Não se considera necessário comunicar este tipo de modificações aos utilizadores dos certificados.

No caso em que o Grupo de Trabalho da Política julgue que as alterações à especificação podem afetar à aceitabilidade dos certificados para propósitos específicos proceder-se-á ao aumento do número maior de versão do documento e colocado a zero o número menor da mesma. Também se modificarão os dois últimos números do Identificador de Objeto (OID) que o representa. Este tipo de modificações comunicar-se-á aos utilizadores dos certificados segundo o estabelecido na secção 9.11.

9.13 Disposições para resolução de conflitos

Todas reclamações entre utilizadores e EC CMD deverão ser comunicadas pela parte em disputa à Conselho Gestor[3] (CG), com o fim de tentar resolvê-lo entre as mesmas partes.

Para a resolução de qualquer conflito que possa surgir com relação a esta PC, as partes, com renúncia a qualquer outro foro que pudesse corresponder-lhes, submetem-se à Jurisdição de Contencioso Administrativo

9.14 Legislação aplicável

É aplicável à atividade das entidades certificadoras a seguinte legislação específica:

- Despacho nº 27008/2004, de 14 de Dezembro, publicado no D.R II, nº 302, de 28 de Dezembro;
- Portaria nº 1350/2004, de 23 de Outubro;
- Despacho nº 16445/2004, de 29 de Julho, publicado no D.R II, nº 190 de 13 de Agosto;
- Aviso nº 8134/2004, de 29 de Julho, publicado no D.R II, nº 190 de 13 de Agosto;
- Decreto Regulamentar nº. 25/2004, de 15 de Julho;
- Decreto-Lei nº 290-D/99, de 2 de Agosto com as alterações introduzidas pelo Decreto-Lei nº 62/2003, de 3 de Abril e Decreto-lei nº 165/2004, de 6 de Julho;
- Portaria nº 1370/2000, publicada no D.R. nº 211, II série de 12 de Setembro;
- Lei n.º 7/2007, de 5 de Fevereiro, alterada pela Lei n.º 91/2015, de 12 de Agosto
- Lei nº 37/2014 de 26 de Junho com as alterações introduzidas pela Lei n.º 32/2017, de 1 de Junho.
- Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014 relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno.

9.15 Conformidade com a legislação em vigor

Esta DPC é objeto de aplicação de leis nacionais e Europeias, regras, regulamentos, ordenações, decretos e ordens incluindo, mas não limitadas a, restrições na exportação ou importação de *software*, *hardware* ou informação técnica.

É responsabilidade da CG zelar pelo cumprimento da legislação aplicável listada na secção 9.14.

9.16 Providências várias

9.16.1 Acordo completo

Todas as partes confiantes assumem na sua totalidade o conteúdo da última versão desta DPC.

9.16.2 Independência

No caso que uma ou mais estipulações deste documento, sejam ou tendam a ser inválidas, nulas ou irreclamáveis, em termos jurídicos, deverão ser consideradas como não efetivas.

A situação anterior é valida, apenas e só nos casos em que tais estipulações não sejam consideradas essenciais. É responsabilidade da CG a avaliação da essencialidade das mesmas.

9.16.3 Severidade

Nada a assinalar.

9.16.4 Execuções (taxas de advogados e desistência de direitos)

Nada a assinalar.

9.16.5 Força Maior

Nada a assinalar.

9.17 Outras providências

Nada a assinalar.

Conclusão

Este documento define os procedimentos e práticas utilizadas pela EC CMD no suporte à sua atividade de certificação digital. A hierarquia de confiança da Entidade de Certificação do Cartão de Cidadão encontra-se englobada na hierarquia do Sistema de Certificação Electrónica do Estado Português (SCEE) – Infraestrutura de Chaves Públicas do Estado:

- Fornecendo uma hierarquia de confiança, que promoverá a segurança eletrónica do Cidadão no seu relacionamento com o Estado;
- Proporcionando a realização de transações eletrónicas seguras, a autenticação forte, um meio de assinar eletronicamente transações ou informações e documentos eletrónicos, assegurando a sua autoria, integridade e não repúdio, e assegurando a confidencialidade das transações ou informação.

Referências Bibliográficas

CEN/TS 419241:2014 – *Security Requirements for Trustworthy Systems Supporting Server*

Lei n.º 7/2007, de 5 de Fevereiro

Lei nº 37/2014 de 6 de Junho com as alterações introduzidas pela Lei n.º 32/2017, de 1 de Junho.

Regulamento (UE) nº910/2014 do Parlamento Europeu e do Conselho de 23 de Julho de 2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE

FIPS 140-2. 2001, *Security Requirements for Cryptographic Modules*.

ISO/IEC 3166. 1997, *Codes for the representation of names and countries and their subdivisions*.

ITU-T *Recommendation* X.509. 1997, (1997 E): *Information Technology - Open Systems Interconnection – The Diretory: Authentication Framework.*

NIST FIPS PUB 180-1. 1995, *The Secure Hash Algorithm (SHA-1). National Institute of Standards and Technology, "Secure Hash Standard", U.S. Department of Commerce*.

NIST FIPS PUB 180-2. 2002, *Secure Hash Standard, U. S. Department of Commerce, Technology Administration, National Institute of Standards and Technology.*RFC 1421. 1993, *Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures*.

RFC 1422. 1993, *Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management.*

RFC 1423. 1993, *Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers*.

RFC 1424. 1993, *Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services.*

RFC 2252. 1997, *Lightweight Diretory Access Protocol (v3).*

RFC 6960. 2013, X.*509 Internet Public Key Infrastructure Online Certificate Status Protocol* – OCSP.

RFC 2986. 2000, PKCS #10: *Certification Request Syntax Specification, version* 1.7.

RFC 3161. 2001, *Internet X.509 Public Key Infrastructure Time-Stamp Protocol* (TSP).

RFC 3279. 2002, *Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

RFC 5280. 2008, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*

RFC 3647. 2003, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.*

RFC 4210. 2005, *Internet X.509 Public Key Infrastructure Certificate Management Protocol* (CMP).

SCEE 2.16.620.1.1.1.2.1.1.0. 2006, Política de Certificados da SCEE e Requisitos mínimos de Segurança.

ETSI EN 319 401 v2.1.1 – Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;

ETSI EN 319 411-1 v1.1.1 – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;

ETSI EN 319 411-2 v2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part. 2: Requirements for Trust Service providers issuing EU qualified certificates;

ETSI EN 319 412-1 v1.1.1 – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures;

ETSI EN 319 412-2 v2.1.1 – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons;

ETSI EN 319 412-5 v2.1.1 – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements;

Anexo A – Definições e Acrónimos

Acrónimos

ANS	*Autoridade Nacional de Segurança*
ANSI	*American National Standards Institute*
C	*Country*
CA	*Certification Authority* (o mesmo que EC)
CMD	*Chave Móvel Digital*
CN	*Common Name*
CRL	Ver LRC
DL	Decreto-Lei
DN	*Distinguished Name*
DPC	Declaração de Práticas de Certificação
DR	Decreto Regulamentar
EC	Entidade de Certificação
ECD	Entidade Certificadora de Documentos
ER	Entidade de Registo
GMT	Tempo Médio de Greenwich (*Greenwich Mean Time*)
LRC	Lista de Revogação de Certificados
MAC	*Message Authentication Codes*
O	*Organization*

OCSP	*Online Certificate Status Protocol*
OID	Identificador de Objeto
PC	Política de Certificado
PKCS	*Public-Key Cryptography Standards*
PKI	*Public Key Infrastructure* (Infraestrutura de Chave Pública)
SHA	*Secure Hash Algorithm*
SCMD	Serviço Chave Móvel Digital
SSCD	*Secure Signature-Creation Device*
TSA	*Time-Stamping Authority* (o mesmo que EVC)

Definições

Assinatura Digital	Modalidade de assinatura eletrónica avançada baseada em sistema criptográfico assimétrico composto de um algoritmo ou série de algoritmos, mediante o qual é gerado um par de chaves assimétricas exclusivas e interdependentes, uma das quais privada e outra pública, e que permite ao titular usar a chave privada para declarar a autoria do documento eletrónico ao qual a assinatura é aposta e concordância com o seu conteúdo e ao destinatário usar a chave pública para verificar se a assinatura foi criada mediante o uso da correspondente chave privada e se o documento eletrónico foi alterado depois de aposta a assinatura.
Assinatura Eletrónica	Resultado de um processamento eletrónico de dados, suscetível de constituir objeto de direito individual e exclusivo e de ser utilizado para dar a conhecer a autoria de um documento eletrónico.
Assinatura Eletrónica Avançada	Assinatura eletrónica que preenche os seguintes requisitos: a) Identifica de forma unívoca o titular como autor do documento; b) A sua aposição ao documento depende apenas da vontade do titular;

	c) É criada com meios que o titular pode manter sob seu controlo exclusivo; d) A sua conexão com o documento permite detetar toda e qualquer alteração superveniente do conteúdo deste.
Assinatura Eletrónica Qualificada	Assinatura digital ou outra modalidade de assinatura eletrónica avançada que satisfaça exigências de segurança idênticas às da assinatura digital baseadas num certificado qualificado e criadas através de um dispositivo seguro de criação de assinatura.
Entidade Supervisora	Entidade competente para a credenciação e fiscalização das entidades certificadoras.
Cancelamento do Cartão de Cidadão	Ato de cancelar o Cartão de Cidadão de forma definitiva. O cancelamento do Cartão de Cidadão implica obrigatoriamente a revogação dos certificados.
Certificado	Documento eletrónico que liga os dados de verificação de assinatura ao seu titular e confirma a identidade desse titular.
Certificado Qualificado	Certificado que contém os elementos referidos no artigo 29.º do DL 62/2003 [7] e é emitido por entidade certificadora que reúne os requisitos definidos no artigo 24.º do DL 62/2003.
Certificado CMD de Assinatura Qualificada	Certificado Qualificado, conforme ponto 13 do artigo 2º da Lei 37/2014 republicada com as alterações introduzidas pela Lei 32/2017.
Chave Privada	Elemento do par de chaves assimétricas destinado a ser conhecido apenas pelo seu titular, mediante o qual se apõe a assinatura digital no documento eletrónico, ou se decifra um documento eletrónico previamente cifrado com a correspondente chave pública.
Chave Pública	Elemento do par de chaves assimétricas destinado a ser divulgado, com o qual se verifica a assinatura digital aposta no documento eletrónico pelo titular do par de chaves assimétricas, ou se cifra um documento eletrónico a transmitir ao titular do mesmo par de chaves.
Credenciação	Ato pelo qual é reconhecido a uma entidade que o solicite e que exerça a atividade de entidade certificadora o preenchimento dos requisitos definidos no presente diploma para os efeitos nele, previstos.

Dados de Criação de Assinatura	Conjunto único de dados, como chaves privadas, utilizado pelo titular para a criação de uma assinatura eletrónica.
Dados de Verificação de Assinatura	Conjunto de dados, como chaves públicas, utilizado para verificar uma assinatura eletrónica.
Delta LRC	*Delta LRCs* são listas que contêm apenas os certificados revogados desde a última emissão da Lista de Certificados Revogados da EC.
Dispositivo de Criação de Assinatura	Suporte lógico ou dispositivo de equipamento utilizado para possibilitar o tratamento dos dados de criação de assinatura.
Dispositivo Seguro de Criação de Assinatura	Dispositivo de criação de assinatura que assegure, através de meios técnicos e processuais adequados que, i) Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura só possam ocorrer uma única vez e que a confidencialidade desses dados se encontre assegurada; ii) Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura não possam, com um grau razoável de segurança, ser deduzidos de outros dados e que a assinatura esteja protegida contra falsificações realizadas através das tecnologias disponíveis; iii) Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura possam ser eficazmente protegidos pelo titular contra a utilização ilegítima por terceiros; iv) Os dados que careçam de assinatura não sejam modificados e possam ser apresentados ao titular antes do processo de assinatura.
Documento Eletrónico	Documento elaborado mediante processamento eletrónico de dados.
Endereço Eletrónico	Identificação de um equipamento informático adequado para receber e arquivar documentos eletrónicos.
Estampilha Temporal	Estrutura de dados que liga a representação eletrónica de um *datum* com uma data/hora particular, estabelecendo evidência de que o *datum* existia nessa data/hora.
Lista de Revogação de Certificados (LRC)	É uma lista completa, assinada digitalmente de certificados que foram revogados. Esta lista é publicada periodicamente e usada para verificar o estado de um certificado de revogação. Podendo esta lista atingir grandes

	dimensões, dependendo do número de certificados emitidos e revogados por uma EC, são publicadas umas listas de menor dimensão chamadas de *Delta LRCs*.
Parte Confiante	Recetor de uma estampilha temporal que confia na mesma.
Revogação de Certificado	Ato de invalidar definitivamente o certificado. Após revogado, o certificado, não voltará a ficar ativo.
Serviço Chave Móvel Digital	A Chave Móvel Digital (CMD) surgiu em 2015 como um meio simples e seguro de autenticação dos cidadãos em portais e sítios da Administração Pública na Internet, com dois fatores de segurança: uma palavra-chave e um código recebido por SMS. Tendo por base a importância da experiência de utilização, conjugado com as novas possibilidades de assinatura eletrónica qualificada "*server-side*" previstas no regulamento europeu 910/2014, o Serviço Chave Móvel Digital (SCMD) disponibiliza, desde Outubro de 2017, o serviço de assinatura qualificada "server-side". Neste contexto, o SCMD gere todos os fluxos de mensagem inerentes ao processo de emissão, ativação e revogação do certificado CMD de assinatura qualificada, assim como da sua utilização para assinatura qualificada "server-side" de documentos, de acordo com o número 13 do artigo 2º e o artigo 3º -A da Lei 37/2014, republicada com as alterações introduzidas pela Lei 32/2017.
Sistema TSA (*TSA System*)	Composição de produtos IT e componentes, organizados de modo a suportar o fornecimento de serviços de validação cronológica.
Suspensão de Certificado	Ato de invalidar o certificado por período determinado. O certificado poderá voltar a ficar válido.
UTC (*Coordinated Universal Time*)	Escala de tempo baseada no segundo, como definido na *ITU-R Recommendation TF.460-5* [10].
UTC(k)	Escala de tempo fornecida pelo laboratório "k" que garante ±100 ns em relação ao UTC (conforme *ITU-R Recommendation TF.536-1* [11])
Validação Cronológica	Declaração de uma EVC que atesta a data e hora da criação, expedição ou receção de um documento eletrónico.

Aprovação

VÍTOR JORGE DA SILVA CASTRO

Assinado de forma digital por VÍTOR JORGE DA SILVA CASTRO
Dados: 2018.03.22 23:22:22 Z