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

Políticas (POL#28)

Nível de Acesso: Público

Versão: 6.0

Data: Mar 2024

IRN – Instituto dos Registos e Notariado, I.P.
Av. D. João II, Lote 1.08.01, Edifício H, Parque das Nações 1990-097 Lisboa, Portugal
Telefone: +351 217 985 500 e-mail: geral@irn.mj.pt

Identificador do Documento: POL#28

Palavras-chave: PKI CC, Cartão de Cidadão, Declaração de Práticas de Certificação

Tipologia Documental: Políticas

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

Nível de acesso: Público

Autor: IRN - Instituto dos Registos e Notariado, I.P.

Data: Mar 2024

Versão atual: 6.0

Validade do Documento: 2 (dois) anos após a sua aprovação.

Histórico de Versões

Versão	Data	Detalhes
1.0	13/01/2007	Versão aprovada.
2.0	03/07/2018	Alterações e atualizações.
3.0	09/01/2019	Alterações ao tamanho das chaves.
4.0	Jan 2020	Atualização de referências bibliográficas.
5.0	Fev 2022	Revisão documental, inclusão entrega ao domicílio.
6.0	**Mar 2024**	**Revisão no âmbito do Novo Cartão de Cidadão**

Documentos Relacionados

Documento	Autor	Descrição
Política de Certificados da EC de Assinatura Digital Qualificada do Cartão de Cidadão (POL#23)	IRN	Descreve a Política de Certificados da EC de Assinatura Digital Qualificada do Cartão de Cidadão, identificando os perfis de certificado e LCR emitidos, assim como a resposta OCSP.
Declaração de Divulgação de Princípios da EC CC (POL#20)	IRN	Resume, de forma simples e acessível, as características descritas nas Políticas de Certificado e Declaração de Políticas de Certificação da Infraestrutura de chave pública da Entidade de Certificação do Cartão de Cidadão.
Política de Certificados da EC do Cartão de Cidadão (POL#22)	IRN	Descreve a Política de Certificados da EC do Cartão de Cidadão, identificando os perfis de certificado e LCR emitidos, assim como a resposta OCSP.

Estado do documento

Este é um documento controlado e aprovado pelo IRN.

Embora este documento possa ser impresso, a versão eletrónica assinada digitalmente pelo(s) elemento(s) do Grupo de Gestão, é a cópia controlada. Qualquer cópia impressa deste documento não é controlada.

Sendo um documento **controlado** e de **acesso público**, este documento pode ser arquivado em unidades locais ou de rede, assim como ser acedido diretamente no repositório da PKI do Cartão de Cidadão em https://pki2.cartaodecidadao.pt/.

Índice

1 Introdução

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 (e*Government*), 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 de Assinatura Digital Qualificada do Cartão de Cidadão encontra-se na hierarquia de confiança da Entidade de Certificação do Cartão de Cidadão e, 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 https://www.gns.gov.pt/media/1894/TSLPT.xml. Os certificados de assinatura emitidos por esta EC são regulados pelo Regulamento (UE) n.º 910/2014[2] (Regulamento eIDAS), no âmbito da Identificação Eletrónica.

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

1.1 Público-Alvo

Este documento deve ser lido por:

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

[1] *cf.* SCEE 2.16.620.1.1.1.2.1.5.0. 2022, Política de Certificados da SCEE e Requisitos mínimos de Segurança.
[2] 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 e que revoga a Diretiva 1999/93/CE.

1.2 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[3], de acordo também com a estrutura recomendada pelo SCEE[1] e pelos ETSI EN 319 411-1[4] e ETSI EN 319 411-2[5].

Os primeiros oito capítulos são dedicados a descrever os procedimentos e práticas mais importantes no âmbito da certificação digital da EC de Assinatura Digital Qualificada do Cartão de Cidadão. Os restantes capítulos abordam o tema das auditorias de conformidade e outras avaliações e matérias legais.

[3] IETF RFC 3647. 2003, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*.
[4] ETSI EN 319 411-1, v1.3.1, *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements*
[5] ETSI EN 319 411-2, v2.3.1, *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*

2 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 de Assinatura Digital Qualificada do Cartão de Cidadão 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. Este documento pode sofrer atualizações regulares.

Os Certificados emitidos por esta EC 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.

2.1 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 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 Entidade de Certificação de Assinatura Digital Qualificada do Cartão de Cidadão e respeita e implementa os seguintes *standards*:

- IETF RFC 3647: *Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework*;
- IETF RFC 5280: *Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile*.

Esta DPC satisfaz os requisitos impostos pela Declaração de Práticas de Certificação da SCEE[1] e pelos ETSI EN 319 411-1[4] e ETSI EN 319 411-2[5], e específica como implementar os seus procedimentos e controlos, e ainda como esta EC atinge os requisitos especificados.

2.2 Designação e Identificação do Documento

Este documento é a "Declaração de Práticas de Certificação da EC AsC". 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 indicado na tabela seguinte.

Este documento é identificado pelos dados constantes na seguinte tabela:

INFORMAÇÃO DO DOCUMENTO	
Nome	Declaração de Práticas de Certificação da EC de Assinatura Digital Qualificada do Cartão de Cidadão
Versão	6.0

INFORMAÇÃO DO DOCUMENTO	
Estado	Aprovado
OID	2.16.620.1.1.1.2.4.1.0.7
Data	Mar 2024
Validade	Até 2 (dois) anos após a sua aprovação, ou até que seja substituído por uma nova versão (o que ocorrer primeiro)
Localização	https://pki2.cartaodecidadao.pt/publico/praticas-certificacao

2.3 Participantes na Infraestrutura de Chave Pública

2.3.1 Entidades Certificadoras

Uma entidade certificadora (EC) é uma terceira parte confiável que emite certificados digitais com base na infraestrutura de chave pública (PKI), que se inserem numa hierarquia de confiança, que no âmbito do Cartão de Cidadão é o Sistema de Certificação Eletrónica do Estado (SCEE).

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

.

2.3.1.1 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 pode ser consultado em https://www.scee.gov.pt/rep/certificados/.

A informação previamente descrita consta da Política de Certificados da SCEE[1].

2.3.1.2 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 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, identificados na "Política de Certificados da EC do Cartão de Cidadão" (POL#22).

2.3.1.3 As SubECEstado

As SubECEstado encontram-se no nível imediatamente abaixo das ECEstado, tendo 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 AsC é a EC CC.

2.3.1.3.1 EC de Assinatura Digital Qualificada (EC AsC)

A EC de Assinatura Digital Qualificada (EC AsC) é responsável pela emissão dos seguintes certificados:

- Certificados digitais de assinatura qualificada, em formato X509 v3, a constar em cada Cartão de Cidadão.
- Certificados digitais para serviços:
  - Validação *on-line* OCSP.
  - Serviço de Validação Cronológica.

2.3.2 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 pelo Instituto dos Registos e do Notariado, que descentraliza estas funções através dos vários balcões de serviço (cf. referido no n.º 2 do artigo 20.º da Lei 7/2007, de 5 de fevereiro, na redação dada pela republicação na Lei n.º 61/2021), nomeadamente:

- Lojas de Cidadão e Espaços Registo,
- Serviços de Registo (Conservatórias do Registo Civil/Predial/Comercial e Cartórios Notariais de Competência Especializada),
- Balcões do Departamento de Identificação Civil, e
- Espaços Cidadão.

Na Região Autónoma da Madeira o serviço é disponibilizado através da Direção Regional da Administração da Justiça (DRAJ). Na Região Autónoma dos Açores o serviço, para além dos balcões do Instituto de Registos e Notariado, é prestado também através da Rede Integrada de Atendimento ao Cidadão (RIAC)

Relativamente aos cidadãos que se encontram no estrangeiro podem efetuar o seu pedido nos postos consulares onde já se encontra implementado o Cartão de Cidadão.

O pedido pode ainda ser efetuado através do canal online (https://eportugal.gov.pt/), (cf. Referido no n.º 3 do artigo 20.º da Lei 7/2007, de 5 de fevereiro, na redação dada pela republicação na Lei n.º 61/2021), sendo esta opção válida apenas para renovações (não permite pedidos iniciais de Cartão de Cidadão).

A entrega de Cartão de Cidadão pode ocorrer por via postal, para cidadãos portugueses de idade igual ou superior a 18 anos, residentes em território nacional, para pedidos de renovação online e presencial (cf. referido no n.º 4 do artigo 31º da Lei 7/2007, de 5 de fevereiro, na redação dada pela republicação na Lei n.º 61/2021).

2.3.3 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, 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. São emitidos certificados de Assinatura Digital Qualificada para as

seguintes categorias de titulares, nos termos do Artigo 3.° da Lei n° 7/2007 de 5 de fevereiro (alterada pela lei n.° 91/2015 de 12 de agosto e pela lei 32/2017 de 1 de junho):

- Cidadão Português;
- Cidadão Brasileiro – Com o estatuto de igualdade de direitos e deveres ao abrigo do Tratado Porto Seguro (Brasil) de 2000.

2.3.3.1 Patrocinador

Esta EC emite certificados para serviços complementares (equipamentos tecnológicos) do cartão de cidadão. Estes serviços são geridos, operados e mantidos pelas mesmas equipas de gestão, operação e manutenção da EC, sendo o grupo de Administração de Segurança responsável por garantir a correta gestão destes certificados, sempre que a sua emissão seja efetuada manualmente, sendo este grupo denominado por Patrocinador.

O patrocinador aceita o certificado e é responsável pela sua correta utilização, bem como pela proteção e salvaguarda da sua chave privada.

Os serviços complementares, para os quais são emitidos certificados por esta EC, são:

- Serviço de validação *on-line* OCSP;
- Serviço de Validação Cronológica.

2.3.4 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 AsC da hierarquia de confiança da SCEE, podendo ser titular de certificados da comunidade SCEE ou não.

2.3.5 Outros participantes

2.3.5.1 Conselho Gestor do SCEE

O Conselho Gestor do SCEE é a entidade a quem cabe pronunciar-se sobre as políticas e práticas de certificação das entidades certificadoras que integram o SCEE, conforme descrito na Política de Certificados do SCEE[1].

2.3.5.2 Autoridade Credenciadora

De uma forma geral, conforme descrito na Política de Certificados do SCEE[1], o papel da Autoridade Credenciadora, no domínio do SCEE, está relacionado com a disponibilização de serviços de 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 Política de Certificados do SCEE[1] e com o estabelecido neste documento.

2.3.5.3 Entidade Supervisora

A Entidade Supervisora é a entidade competente para a credenciação e fiscalização das entidades certificadoras, conforme Regulamento (UE) n.º 910/2014[6] (Regulamento eIDAS).

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.

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.

2.3.5.4 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*[7] (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.

2.3.5.5 Entidades externas de prestação de serviços

A Imprensa Nacional Casa da Moeda (INCM), S.A, presta serviço ao IRN, como entidade responsável pela operação e manutenção da infraestrutura de chaves públicas que suportam o Cartão de Cidadão, nomeadamente na emissão de certificados digitais, componente de validação de estado, personalização do Cartão de Cidadão. As suas responsabilidades/obrigações estão definidas através de contrato estabelecido entre as várias entidades, com objetivo de fornecimento de serviços de personalização e emissão dos certificados digitais para o cidadão, assegurando a confidencialidade, integridade e disponibilidade dos mesmos.

2.4 Utilização do Certificado

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

Tipo de Certificado	Uso Apropriado
Certificado de Assinatura	Assinatura Eletrónica Qualificada
Certificado OCSP	Serviço *on-line* de Estado de Revogações dos certificados

[6] 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 e que revoga a Diretiva 1999/93/CE.
[7] *cf.* IETF RFC 6960. 2013, X.509 *Internet Public Key Infrastructure Online Certificate Status Protocol* – OCSP.

Tipo de Certificado	Uso Apropriado
Certificado de Validação Cronológica	Serviço de Validação Cronológica

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

2.4.1 Utilização adequada

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

Assim, os certificados emitidos:

- Para pessoas singulares, têm como objetivo a sua utilização em qualquer aplicação para efeitos de Assinatura digital qualificada.
- Para serviço complementares, têm como objetivo a sua utilização em serviços de autenticação e no estabelecimento de canais cifrados.

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

2.4.2 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 não poderão ser utilizados para qualquer função fora do âmbito das utilizações descritas anteriormente.

Os serviços de certificação oferecidos pela EC, 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.

2.5 Gestão das Políticas

2.5.1 Entidade responsável pela gestão do documento

A gestão desta política de certificados é da responsabilidade do Ministério da Justiça.

2.5.2 Contacto

Nome	**IRN I.P. - Departamento de Identificação Civil** **MINISTÉRIO DA JUSTIÇA**

Morada	Civil Campus de Justiça. Avenida D. João II,1.08.01, Edifício J - 4º e 5º piso. 1990-097 Lisboa
Correio eletrónico	cartaodecidadao@irn.mj.pt
Telefone	924 138 459

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

O Grupo de Trabalho de Administração de Segurança determina a conformidade e aplicação interna desta DPC (e/ou respetiva PCs) no que diz respeito a legislação e normas aplicáveis.

2.5.4 Atualização da DPC

O Grupo de Trabalho de Administração de Segurança é responsável pela atualização desta DPC garantindo que a mesma é revista pelo menos uma vez, a cada dois anos.

2.5.5 Procedimentos para Aprovação da DPC

A aprovação desta DPC (e/ou respetivas PCs) e seguintes correções (ou atualizações) é levada a cabo pelos Grupo de Gestão, após proposta elaborada pelo Grupo de Administração de Segurança. As 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.

2.6 Definições e Acrónimos

Ver Anexo A.

3 Responsabilidade de Publicação e Repositório

3.1 Repositórios

O Ministério da Justiça é responsável pelas funções de repositório da EC,), publicando, entre outras, informação relativa às práticas adotadas e ao estado dos certificados emitidos (LRC). disponível em:

- até à EC AsC 0018 - http://pki.cartaodecidadao.pt/ e
- a partir da EC AsC 0019 (inclusive) - http://pki2.cartaodecidadao.pt

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

- Disponibilidade de serviços da plataforma de 99,99%, 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: 40 pedidos/minuto;
- Número máximo de pedidos da DPC: 40 pedidos/minuto;
- Número médio de pedidos de LRC: 10 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.

3.2 Publicação de informação de certificação

O Ministério da Justiça 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.

É disponibilizada 24hx7d, a seguinte informação pública *on-line*:

- Cópia eletrónica deste DPC e Políticas de Certificados (PC) mais atuais da EC, assinada eletronicamente pelo Grupo de Gestão:
  - Declaração de Práticas de Certificação da ECdisponibilizada no URI:
    - Até à EC AsC 0018 (inclusive), o URI:

http://pki.cartaodecidadao.pt/publico/politicas/cps.html;

- Após a EC AsC 0018, o URI:

  http://pki2.cartaodecidadao.pt/publico/praticas-certificacao;

- Política de Certificados da EC de Assinatura Digital Qualificada do Cartão de Cidadão disponibilizada no URI:

  Até à EC AsC 0018 (inclusive), o URI:http://pki.cartaodecidadao.pt/publico/politicas/cp.html

  - Após a EC AsC 0018, o URI:

    http://pki2.cartaodecidadao.pt/publico/politica-certificados;

– LRC da EC AsC – URI:

- Até à EC AsC 0018 (inclusive), o URI:

  http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_assinatura_crl<ID_CA>_p<num_seq>.crl;

- Após a EC AsC 0018, o URI:

  http://pki2.cartaodecidadao.pt/entidade-certificacao-assinatura/lista-revogacao/CC_Asc<ID_CA>_partition9.crl

– Delta-LRC da EC AsC – URI:

- Até à EC AsC 0018 (inclusive), o URI:

  http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_assinatura_crl<ID_CA>_delta_p<num_seq>.crl;

- Após a EC AsC 0018, não são emitidas Delta CRLS, passando as CRL a ser emitidas numa periodicidade diária.

– Certificados da EC AsC – URI:

- Até à EC AsC 0018 (inclusive), o URI:

  http://pki.cartaodecidadao.pt/publico/certificado/cc_ec_cidadao_assinatura;

- Após a EC AsC 0018, o URI:

  http://pki2.cartaodecidadao.pt/entidade-certificacao-assinatura/certificados/CC_Asc<ID _CA>.crt

– Certificados o Serviço de Validação Cronológica:

  https://pki.cartaodecidadao.pt/publico/certificado/cc_ec_cidadao_tsa/

– Outra informação relevante – URI:
http://pki.cartaodecidadao.pt/publico/info/cc_ec_cidadao_assinatura e
http://pki2.cartaodecidadao.pt

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

3.3 Periodicidade de publicação

As atualizações a esta DPC e respetivas PCs serão publicadas imediatamente após a sua aprovação pelo Grupo de Gestão, de acordo com a secção 10.13. Será considerado como prazo máximo para revisão da informação desta DPC o prazo indicado na secção 2.2..

Os certificados da EC são publicado imediatamente após ser efetuada a respetiva análise e validação pela Entidade Supervisora.

As LRC da EC até à EC AsC 0018 (inclusive) são publicadas, no mínimo, uma vez por semana, sendo que as Delta-LRC são publicadas, no mínimo, uma vez por dia. Após a EC AsC 0018 a LRC é emitida o mínimo 1 vez por dia, não sendo emitidas Delta-LRCs.

3.4 Controlo de acesso aos repositórios

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

4 Identificação e Autenticação

4.1 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. Aos certificados de serviços complementares é atribuído o nome qualificado do domínio e/ou o âmbito da sua utilização ("Serviços do Cartão de Cidadão").

4.1.1 Tipos de nomes

O certificado da EC assim com os certificados emitidos pela por ela são identificados por um nome único (DN – *Distinguished Name*) de acordo com *standard* X.500, conforme indicado na "Política de Certificados da EC do Cartão de Cidadão" (POL#22) e na "Política de Certificados da EC de Assinatura Digital Qualificada do Cartão de Cidadão" (POL#23).

4.1.2 Necessidade de nomes significativos

A EC assegura, dentro do seu "ramo" da hierarquia de confiança do SCEE:

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

4.1.3 Anonimato ou pseudónimo de titulares

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

4.1.4 Interpretação de formato de nomes

As regras utilizadas pela EC AsC para interpretar o formato dos nomes seguem o estabelecido no RFC 5280[8], 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*.

4.1.5 Unicidade de nomes

Os identificadores do tipo DN são únicos para cada titular de certificado emitido pela EC, não induzindo em ambiguidades.

De acordo com os seus processos de emissão, a EC rejeita a emissão de certificados com o mesmo DN para titulares distintos. Quando ocorrer tal situação, é permitido a adição de

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

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.

4.1.6 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 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 de apresentar os documentos legais que demonstrem o direito à utilização do nome requisitado, sem prejuízo de, sempre que possível, serem os mesmos verificados oficiosamente por cotejo entre bases de dados/sistemas intervenientes no processo.

4.2 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" num dos locais referidos na secção 2.3.2**.**

Existem várias situações que originam procedimentos diferenciados, sendo descritas de seguida:

- No caso de ser uma primeira emissão do Cartão de Cidadão é validada a existência de Bilhete de Identidade.
    - Não havendo Bilhete de Identidade, a validação da identidade do requerente será realizada através do assento de nascimento. Neste caso, os dados biográficos surgem pré-preenchidos tendo por base de pesquisa o número do assento. Pode-se verificar, desta forma, que o requerente é quem diz ser ou, não havendo assento de nascimento informatizado, é pedido pelo serviço à conservatória competente a sua informatização, de forma a prosseguir com a validação de identidade.
    - Havendo Bilhete de Identidade, esta validação é feita pelo método "cara-a-cara", pelo funcionário do serviço, confirmando e validando através de reconhecimento facial que o requerente é quem diz ser, sem prejuízo da validação cumulativa que é sempre efetuada pelo Assento de Nascimento. Se o requerente não apresentar o Bilhete de Identidade, através do qual o funcionário possa validar a identidade do requerente, a validação poderá ser efetuada através de pesquisa baseada no nome do mesmo, sendo que os dados obtidos deverão ser validados. A forma de validação desta informação poderá ser efetuada através de um dos seguintes métodos:
        - Através de um Documento do próprio,
        - Através de um Documento de um familiar,
        - Na presença de um familiar com documento de identificação, ou
        - Com duas testemunhas presenciais que atestem que o requerente é quem diz ser.
- No caso de nova emissão de Cartão de Cidadão, motivada pelo extravio ou roubo do anterior, o funcionário do serviço valida a identidade do requerente através dos dados biométricos já registados no sistema.

Após o registo inicial, a renovação do Cartão de Cidadão (e respetiva emissão de novo certificado de Assinatura Qualificada) pode ser desencadeado pelo canal presencial, online ou de forma automática (cf. número 3 do Artigo 20º da Lei n.º 7/2007 de 5 de fevereiro, na redação dada pela republicação na Lei n.º 61/2021), conforme condições indicadas em https://eportugal.gov.pt/servicos/renovar-o-cartao-de-cidadao.

4.2.1 Método de comprovação da posse de chave privada

No caso das pessoas singulares, o par de chaves e certificado é fornecido em cartão com chip criptográfico, personalizado fisicamente para o titular. A posse da chave privada é garantida pelo processo de emissão e personalização do cartão chip, pelo Sistema de Ciclo de Vida, garantindo que:

- O par de chaves é gerado no cartão com chip criptográfico, personalizado para o titular do mesmo,
- A chave pública é enviada à EC para emissão do certificado digital correspondente, sendo este também arquivado no cartão,
- O cartão é entregue ao titular (cf. secção 5.4) ou terceiro que tenha sido previamente indicado pelo titular no pedido, bem como à pessoa que supre nos termos da lei, a incapacidade do titular (número 2 do Artigo 31.º da Lei n.º 7/2007 de 5 de fevereiro, na redação dada pela republicação na Lei n.º 61/2021).

No caso dos pedidos online e de forma automática na renovação do Cartão de Cidadão (e respetiva emissão de novo certificado de Assinatura Qualificada), previstos em https://eportugal.gov.pt/servicos/renovar-o-cartao-de-cidadao, a entrega é sempre presencial (não é aplicável a entrega a terceiro), conforme número 4 do Artigo 31.º da Lei n.º 7/2007 de 5 de fevereiro, na redação dada pela republicação na Lei n.º 61/2021.

No caso dos certificados para serviços complementares, quando emitidos manualmente, a prova da posse da chave privada será garantida através da presença física do patrocinador (ver 2.3.3.1), que apresentará o pedido de certificado no formato PKCS#10, cf. secção 4.2.2.

4.2.2 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.

No âmbito desta, a autenticação da identidade de pessoa coletiva apenas é efetuada para certificados emitidos para serviços complementares.

4.2.2.1 Certificado de serviço complementar (equipamento tecnológico)

Para os certificados de serviços complementares, que sejam emitidos manualmente, é guardada informação sobre o certificado emitido e as pessoas envolvidas no processo de emissão e submissão dos mesmos nos respetivos serviços, executado em intervenção planeada e registada em Livro de presenças próprio para o efeito. Apenas elementos devidamente autorizados têm acesso aos sistemas e serviços para realizar ações de emissão e submissão de certificados nos mesmos, assim como garantir a correta gestão e manutenção.

4.2.3 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 pelo Sistema de Ciclo de Vida.

No âmbito dos processos "Pedido Inicial e Renovação" do IRN, o Sistema de Ciclo de Vida suporta as atividades relacionadas com a recolha e validação de dados biográficos e biométricos do cidadão, de modo a registar o pedido para emissão do Cartão de Cidadão (e respetivos certificados digitais). 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, quer pelo funcionário, quer pelo Cidadão.

Os métodos de validação de identidade são descritos na secção 4.2.

4.2.4 Informação de subscritor/titular não verificada

Toda a informação descrita nos pontos 4.2.2 e 4.2.3 é verificada.

4.2.5 Validação de Autoridade

A intervenção dos representantes legais do titular, no pedido de emissão de certificado de Assinatura Qualificada, deriva do Quadro Normativo Vigente relativo à Representação Legal dos Incapazes. No entanto, todos os dados apresentados relativos ao pedido do Cartão de Cidadão, serão os do titular do documento de identificação cuja emissão está a ser requerida.

4.2.6 Critérios para interoperabilidade

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

4.3 Identificação e autenticação para pedidos de renovação de chaves

Não são efetuadas renovações de chaves, são geradas novas chaves que darão origem a novo certificado, utilizando-se os procedimentos para a autenticação e identificação inicial.

4.4 Identificação e autenticação para pedido de revogação

O processo de identificação e autenticação para pedido de revogação de certificado de pessoa singular, é efetuado pelo Sistema de Ciclo de Vida e pelo Portal https://eportugal.gov.pt/, segundo o disposto no Artigo 33.º da Lei n.º 7/2007 de 5 de fevereiro (alterada pela lei n.º 91/2015 de 12 de agosto, pela lei 32/2017 de 1 de junho e pela lei 61/2021 de 19 de agosto).

O pedido poderá ser efetuado de três formas[9]:

[9] Poderá consultar informação mais detalhada e atualizada em https://eportugal.gov.pt/pt/servicos/cancelar-o-cartao-de-cidadao.

1) Presencial, onde é verificada a identidade do titular tal como descrito na secção 4.2;
2) Telefone, neste caso, terá de ser utilizado pelo titular o código de cancelamento, presente na carta PIN que lhe foi enviado aquando da emissão do Cartão de Cidadão e que se encontra à sua responsabilidade, ou
3) *Online*, através do *site* https://eportugal.gov.pt/, sendo que neste caso a utilização deste canal, depende:
    a) De autenticação com Chave Móvel Digital e introdução do número do documento ou do código de cancelamento constante da Carta PIN enviada ao cidadão; ou,
    b) De introdução do número de cartão de cidadão em simultâneo com código de cancelamento constante da Carta PIN enviada ao cidadão.
        i. Neste caso, a conclusão do pedido depende de confirmação pelo titular, após receção de *short message service* (SMS) ou de mensagem de correio eletrónico, enviadas para os contactos fornecidos pelo requerente, no âmbito de pedido relativo ao Cartão de Cidadão.

O pedido relativo a menor que ainda não tenha completado 16 anos de idade, a interdito ou a inabilitado por anomalia psíquica, é efetuado por quem, nos termos da lei, exerce as responsabilidades parentais, a tutela ou a curatela. Nestas situações, a autenticação é sempre efetuada através de Cartão de Cidadão ou de Chave Móvel Digital, estando o cancelamento dependente da introdução do número do cartão de cidadão e do código de cancelamento constante da Carta PIN do cartão a cancelar.

O site https://eportugal.gov.pt/ garante:

a) A recolha dos dados de identificação do interessado e dos representantes legais;
b) A apresentação do pedido de cancelamento, o motivo pelo qual pretende o cancelamento, o número do documento e a introdução do código de cancelamento;
c) A recolha de endereço eletrónico ou de número de telemóvel que permita o contacto entre os serviços competentes e os interessados ou os seus representantes legais;
d) A certificação da data e da hora em que o pedido foi apresentado;
e) A comunicação eletrónica da conclusão com sucesso do pedido, que é efetuada para o contacto fornecido pelo cidadão, nos termos da alínea c).

No âmbito do processo "Cancelamentos", o sistema de Ciclo de Vida (no canal presencial, telefone e *online*) e o site https://eportugal.gov.pt/ (no canal *online*) suportam as atividades relacionadas com o registo dos pedidos de cancelamento de determinado Cartão de Cidadão, devido a motivos relacionados com roubo, extravio, morte, entre outros, comunicando essa informação à EC AsC.

Salienta-se a necessidade de definir que o termo "Cancelamento" do Cartão de Cidadão é utilizado quando este é dado como inutilizado, sendo se possível, remetido aos serviços apropriados, para destruição. Da mesma forma, salienta-se que o termo "Cancelamento" de Certificado, que no âmbito do Cartão de Cidadão só poderá ser efetuado ao Certificado de Assinatura Digital Qualificada, será utilizado quando este certificado é revogado, sendo que o Cartão de Cidadão continua válido.

O pedido de revogação de certificado emitido para serviço complementar tem um formulário próprio 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;
- Informação das atividades a efetuar pela EC subordinada para revogar todos os certificados emitidos pela mesma, no caso de revogação de certificado de EC subordinada.

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

- Patrocinador;
- o Grupo de Gestão da PKI do Cartão de Cidadão;
- Parte confiante, sempre que demonstre que o certificado foi utilizado com fins diferentes dos previstos.

5 Requisitos Operacionais do Ciclo de Vida do Certificado

5.1 Pedido de Certificado

5.1.1 Quem pode subscrever um pedido de certificado

O Sistema de Ciclo de Vida é a única entidade que pode aceitar pedidos de certificados de pessoa singular referidos na secção 2.3.3., despoletados através dos canais e serviços identificados em 2.3.2.

Relativamente a certificados de Serviço complementar, o patrocinador é a única entidade que pode subscrever estes pedidos de certificados desde que sejam utilizados no âmbito do Cartão de Cidadão e sempre que sejam emitidos manualmente.

5.1.2 Processo de registo e responsabilidades

O processo de registo de certificado de pessoa singular é da responsabilidade do Sistema de Ciclo de Vida.

Os pedidos de certificados, quando chegam à EC, 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 4.2.

Ao titular do Cartão de Cidadão, é entregue o seu Cartão de Cidadão com os certificados de Assinatura Digital Qualificada e de Autenticação no estado inativo, sendo que a ativação do Certificado de Assinatura Digital Qualificada é opcional, podendo ser efetuada mediante consentimento expresso do titular (num dos locais referidos na secção 152.3.2), conforme descrito na secção 5.4.1.1.

Faz prova de posse da chave privada e certificado de Assinatura Digital Qualificada, a entrega do Cartão de Cidadão ao seu titular, conforme descrito na secção 4.2.1.

No comprovativo do pedido de emissão do Cartão de Cidadão é fornecido ao titular, informação sobre a utilização do certificado de Assinatura Digital Qualificada. No ato da entrega, quando presencial (num dos locais referidos na secção 2.3.2), esta informação é novamente fornecida, verbalmente, pelo funcionário do serviço ao titular, sendo que este é questionado se pretende ativar o Certificado de Assinatura Digital Qualificada e, em caso afirmativo, a sua utilização ficará da sua responsabilidade.

No caso de certificado para serviços complementares e de este ser emitido manualmente, o processo de registo é constituído pelos seguintes passos, a serem efetuados pelo patrocinador requerente:

- Geração do par de chaves (chave pública e privada);
- Geração do PKCS#10 correspondente;
- Geração do *hash* (SHA-256[10]) do PKCS#10 e registo em formulário de intervenção

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

- Emissão do certificado em intervenção própria para o efeito, efetuada pelos elementos autorizados dos Grupos de trabalho da PKI do Cartão de Cidadão;
- Submissão do certificado no serviço complementar respetivo pelos elementos autorizados dos Grupos de trabalho da PKI do Cartão de Cidadão;

5.2 Processamento do pedido de certificado

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

- Receção e verificação de toda a documentação e autorizações exigidas;
- Verificação da identidade do requisitante;
- Verificação da exatidão e integridade do pedido de certificado.

As secções 4.2, 5.2.1 e 5.3 descrevem detalhadamente todo o processo.

5.2.1 Processos para a identificação e funções de autenticação

5.2.1.1 Certificado de pessoa singular

O Sistema de Ciclo de Vida é responsável por todos os processos para a identificação e funções de autenticação, de acordo com as secções 4.2.

5.2.1.2 Certificado de serviço complementar

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

- Formulário de pedido de emissão corretamente preenchido;
- PKCS#10 válido.

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" que dará seguimento à submissão do certificado junto dos elementos autorizados e com permissão de acesso aos serviços complementares.

5.2.2 Aprovação ou recusa de pedidos de certificado

O pedido de certificado de pessoa singular enviado pelo Sistema de Ciclo de Vida é sempre considerado válido.

A aprovação de certificado de serviço complementar, emitido manualmente, passa pelo cumprimento dos requisitos exigidos nas secções 5.2 e 5.2.1. Quando tal não se verifique, é recusada a emissão do certificado.

5.2.3 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 serviço complementar.

5.3 Emissão de Certificado

5.3.1 Procedimentos para a emissão de certificado

5.3.1.1 Certificado de pessoa singular

A emissão do certificado é efetuada como resposta ao pedido do Sistema de Ciclo de Vida.

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

Os procedimentos estabelecidos neste ponto são também aplicados aos casos de renovação de certificados, uma vez que implica a emissão de novos certificados.

A EC 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.

Na componente da PKI, emissão de certificados digitais, são gerados os pares de chaves e emitidos novos certificados pela EC associando assim cada chave pública ao cidadão. Os certificados são enviados ao sistema de personalização cumprindo a norma PKCS#10, onde é personalizado um novo Cartão de Cidadão.

Quando a EC emite um certificado, efetuará as notificações que se estabelecem no ponto 5.3.2.

Os certificados são emitidos no estado inativo, para garantia de que apenas o seu titular tem poderes para os ativar, iniciando a sua vigência apenas nesse momento (ativação, cf. indicado na secção 5.4.1.1).

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.

5.3.1.2 Certificado de serviço complementar

O certificado de serviço complementar pode ser emitido automaticamente ou manualmente, sempre que não se possa garantir o processo automático.

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

- O patrocinador;
- Dois (2) 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 Grupos de Trabalho e pelo patrocinador.

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

- Identificação e autenticação de todas as pessoas presentes na intervenção, garantindo que o patrocinador e os membros dos Grupos de Trabalho estão autorizados para os atos a praticar;

- O patrocinador disponibiliza o ficheiro de pedido de certificado ao Grupo de Trabalho de Operação EC;
- Os membros do Grupo de Operação da EC efetuam o procedimento de acesso ao EC e emitem o certificado (correspondente ao PKCS#10 fornecido pelo patrocinador) em formato PEM;
- Os membros do Grupo de Trabalho da EC arquivam o certificado em formato PEM o qual é entregue ao patrocinar;
- Após a emissão do certificado e sua validação pelo patrocinador, o mesmo é submetido no serviço complementar, pelos elementos do Grupo de Trabalho de Operação supervisionados pelo patrocinador.

O certificado emitido inicia a sua vigência no momento da sua emissão, mas ficará em plena produção assim que submetido no serviço complementar.

5.3.2 Notificação da emissão do certificado ao titular

O Sistema de Ciclo de Vida é responsável por notificar o titular do certificado pela emissão do certificado de Assinatura Digital Qualificada, considerando-se notificado da emissão do mesmo, com a receção da carta PIN associada ao Cartão de Cidadão.

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

5.4 Aceitação do Certificado

5.4.1 Procedimentos para a aceitação de certificado

5.4.1.1 Certificado de pessoa singular

No âmbito do processo de "Entrega", o sistema de Ciclo de Vida suporta as atividades associadas à identificação do Cartão de Cidadão a entregar, à sua leitura, à sua ativação e dos respetivos certificados digitais e ao registo da entrega em perfeitas condições ao Cidadão. Prevê também as funcionalidades de suporte à ocorrência de erros nas diversas atividades associadas à entrega, de modo a suportar os procedimentos a realizar em cada situação, quer pelo funcionário, quer pelo Cidadão, comunicando com outros sistemas como a EC que emitiu o certificado.

A **aceitação** do Certificado de Assinatura Digital Qualificada é concretizada com a entrega do Cartão de Cidadão ao seu titular[11], conforme artigo 31.º da Lei n.º 7/2007 de 5 de fevereiro, na redação dada pela republicação na Lei n.º 61/2021.

A **ativação** do Certificado de Assinatura Digital Qualificada é facultativa11, podendo ser efetuada pelo titular desde que com idade igual ou superior a 16 anos e não se encontrando sujeito às medidas de acompanhamento previstas no Código Civil (cf. número 3 do Artigo 18.º da Lei n.º 7/2007 de 5 de fevereiro, na redação dada pela republicação na Lei n.º 61/2021), nos locais identificados na secção 2.3.2, com recurso à verificação dos dados biométricos (cf. números 2 e 4 do Artigo 18.º e número 2 do Artigo 31.º da Lei n.º 7/2007 de 5 de fevereiro, na redação dada pela republicação na Lei n.º 61/2021).

[11] Poderá consultar informação mais detalhada e atualizada em https://eportugal.gov.pt/servicos/renovar-o-cartao-de-cidadao.

5.4.1.2 Certificado de serviço complementar

Sempre que o certificado é emitido manualmente, este considera-se aceite após a submissão do certificado no sistema complementar, supervisionado pelo patrocinador, de acordo com intervenção de emissão (conforme secção 5.3.1).

5.4.2 Publicação do certificado

A EC não publica os certificados emitidos para o cidadão, estes são disponibilizados integralmente aos titulares do cartão de cidadão. Publica, apenas o certificado emitido para o Serviço de validação Cronológica, no site da PKI referenciado na secção 3.1, os restantes certificados emitido são disponibilizados e ao patrocinador, com os constrangimentos definidos na secção 5.4.1.

5.4.3 Notificação da emissão de certificado a outras entidades

Nada a assinalar.

5.5 Uso do certificado e par de chaves

5.5.1 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;
- Após a sua aceitação e ativação, conforme definido na secção 5.4.1;
- De acordo com as condições definidas nas secções 2.4.1 e 2.4.2;
- Desde que no âmbito do Cartão de Cidadão e,
- Enquanto o certificado se mantiver válido e não estiver na LRC da EC AsC.

Adicionalmente:

- O certificado de assinatura digital qualificada atribuído a pessoa singular tem como objetivo a sua utilização em qualquer aplicação para efeitos de assinatura digital qualificada, de acordo com Regulamento (UE) nº 910/2014[6], em que a chave privada se encontra num dispositivo criptográfico QSCD;
- Os certificados de emitidos para serviços complementares:
    - certificado de Validação *on-line* OCSP, tem como objetivo a sua utilização em servidores OCSP[7];
    - certificado de Validação Cronológica, tem como objetivo a sua utilização em servidores de validação cronológica[12].

[12] *cf.* IETF RFC 3161. 2001, *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*.

5.5.2 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.

A aceitação do certificado é da responsabilidade exclusiva da parte confiante.

5.6 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.

5.7 Renovação de certificado com geração de novo par de chaves

Na renovação de chaves do certificado (*certificate re-key*) é gerado um novo par de chaves e submetido o pedido para emissão de novo certificado à Entidade Certificadora 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 e está associado ao processo de Renovação do Cartão de Cidadão nos termos do Artigo 26.º da Lei n.º 7/2007 de 5 de fevereiro (na redação dada pela republicação na Lei n.º 61/2021).

A renovação de certificado com geração de novo par de chaves é feita de acordo com o estabelecido na secção 5.3.

5.7.1 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 está a expirar;
b) O suporte do certificado está a expirar;
c) O suporte do certificado apresenta-se em mau estado de conservação ou de funcionamento;
d) A informação do certificado sofreu alterações;
e) Sempre que tenha havido necessidade de revogação do certificado anterior.

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

Tal como na secção 5.1.1.

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

Tal como na secção 5.1.2 e 5.2.

5.7.4 Notificação da emissão de novo certificado ao titular

Tal como na secção 5.3.2.

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

Tal como na secção 5.4.1.

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

Tal como na secção 5.4.2.

5.7.7 Notificação da emissão de certificado renovado a outras entidades

Tal como na secção 5.4.3.

5.8 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 por esta EC.

5.9 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 recuperar a sua validade, enquanto os certificados suspensos podem voltar ao estado Ativo.

5.9.1 Motivos para revogação (cancelamento)

Para qualquer certificado emitido por esta EC, podem ser causas para a sua revogação:

a) Comprometimento ou suspeita de comprometimento da chave privada desta EC ou de outra EC no "caminho" até à ECRaizEstado ou do serviço complementar;

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

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

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

e) Sempre que existam 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;

h) Inexatidões graves nos dados fornecidos;

i) Pedido do titular ou pessoa legalmente habilitada.

j) No caso do Certificado de pessoa singular, este apenas assume o estado de revogado quando houver Cancelamento do Cartão de Cidadão, conforme Artigo 18.º e Artigo 33.º da Lei n.º 7/2007 de 5 de fevereiro (na redação dada pela republicação na Lei n.º 61/2021).

k) No caso de certificado para serviço complementar, quando este equipamento deixa de ser utilizado no âmbito do Cartão de Cidadão;

5.9.2 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 5.9.1, os seguintes:

a) No caso de certificado para pessoa singular será o titular, ou pessoa legalmente habilitada conforme definido no Artigo 33.º da Lei n.º 7/2007 de 5 de fevereiro (na redação dada pela republicação na Lei n.º 61/2021).

b) No caso de Certificado de serviço complementar este pode ser revogado a pedido de um dos seguintes elementos:

- O patrocinador do certificado;
- O Grupo de Gestão da EC;
- Uma parte confiante, sempre que demonstre que o certificado foi utilizado com fins diferente dos previstos.

Esta EC guarda toda a documentação utilizada para verificação da identidade e autenticidade da entidade que efetua o pedido de revogação de certificados de serviço complementar.

5.9.3 Procedimento para o pedido de revogação

5.9.3.1 Certificado de pessoa singular

No âmbito do processo "Cancelamentos", o sistema de Ciclo de Vida (no canal presencial, telefone e *online*) e o site https://eportugal.gov.pt/ (no canal *online*) suportam as atividades relacionadas com o registo dos pedidos de cancelamento de determinado Cartão de Cidadão, devido a motivos relacionados com roubo, extravio, morte, entre outros, comunicando essa informação a esta EC.

Quando é efetuado um pedido de Cancelamento de Cartão de Cidadão, todos os certificados associados a este serão revogados e o Cartão de Cidadão é, se possível, destruído.

A forma de pedido de revogação poderá ser consultada na secção 4.4.

5.9.3.2 Certificado de serviço complementar

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

- Os pedidos de revogação de certificados de serviços complementares, emitidos por esta EC, devem ser endereçados à Entidade identificada na secção 2.5.1, por escrito ou por mensagem eletrónica assinada digitalmente**;**
- Identificação e autenticação da entidade que efetua o pedido de revogação, conforme secção 5.4;
- Registo e arquivo do pedido de revogação;
- Análise do pedido de revogação pelo Grupo de Trabalho de Administração de Segurança da EC
- Mediante o parecer do Grupo de trabalho de Administração de Segurança, o Grupo de trabalho de Gestão decide a aprovação ou recusa do pedido de revogação do certificado;
- Sempre que se decida pela revogação, esta é publicada na LRC da EC emissora do certificado.

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.

5.9.4 Produção de efeitos da revogação

A revogação será feita de forma imediata. Após terem sido efetuados todos os procedimentos de validação, efetuada a revogação e emitida a LRC esta é efetivada e irreversível.

5.9.5 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.

5.9.6 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).

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

A partir da EC AsC 0018, é disponibiliza diariamente uma nova LRC.

Até à EC AsC 0018 (inclusive) é emitida diariamente uma Delta-LRC e emitida uma nova LRC a cada 7 dias.

5.9.8 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.

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

Esta EC dispõe de serviços de validação OCSP[7] do estado dos certificados de forma *on-line*. Esse serviço poderá ser acedido em:

- para certificados emitidos por EC's até à AsC 0018 (inclusive):

  http://ocsp.asc.cartaodecidadao.pt/publico/ocsp,

- para certificados emitidos por EC's posteriores à EC AsC 0018:

  http://ocsp.asc.pki2.cartaodecidadao.pt/ocsp

O período máximo entre a revogação e a disponibilização através do serviço de validação OCSP não ultrapassa os 30 minutos.

5.9.10 Requisitos de verificação on-line de revogação

As partes confiantes deverão dispor de *software* capaz de operar o protocolo OCSP[7], de forma a obter a informação sobre o estado do certificado.

5.9.11 Outras formas disponíveis para divulgação de revogação

Não aplicável.

5.9.12 Requisitos especiais em caso de comprometimento de chave privada

Quando se trate do comprometimento da chave privada de uma EC deverão ser adotados os procedimentos descritos na secção 6.7.3.

5.9.13 Motivos para suspensão

Esta EC só suspende certificados emitidos para titulares de um cartão de cidadão, esta prática não se aplica a certificados emitidos para serviços complementares.

O Sistema de Ciclo de Vida é responsável pelo registo do motivo da suspensão.

Os certificados emitidos para titulares de cartão de cidadão são emitidos suspensos, sendo ativados a pedido do titular e através do Sistema de Ciclo de Vida.

Os certificados ativos de um Cartão de Cidadão, apenas são suspensos quando o cartão é encontrado perdido e posteriormente entregue em qualquer um dos balcões presenciais do serviço, definidos na secção 2.3.2, que o regista como "cartão encontrado", desencadeando o envio de uma mensagem ao titular pelo Sistema de Ciclo de Vida, notificando-o desta situação.

5.9.14 Quem pode submeter o pedido de suspensão

O pedido à EC,de suspensão, só é aceite quando submetido pelo Sistema de Ciclo de Vida.

5.9.15 Procedimentos para pedido de suspensão

É desencadeada uma mensagem via Sistema de Ciclo de Vida para a EC logo que o cartão assuma o estado de "cartão encontrado", procedendo-se à mudança de estado dos certificados para suspensos.

5.9.16 Limite do período de suspensão

Após a suspensão dos certificados, estes permanecem no estado suspenso no máximo 30 dias sendo que, durante este prazo, se o titular não proceder ao levantamento do Cartão de Cidadão, os certificados serão revogados.

5.10 Serviços sobre o estado do certificado

5.10.1 Caraterísticas operacionais

O estado dos certificados emitidos está disponível publicamente através das LRC e adicionalmente no serviço OCSP.

5.10.2 Disponibilidade do serviço

O Serviço sobre o estado do certificado está disponível 24 horas por dia, 7 dias por semana, salvo em situações de manutenção em que a informação será disponibilizada nos sites públicos da pki, referenciados na secção 3.1.

5.10.3 Caraterísticas opcionais

Não aplicável.

5.11 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.

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

Esta EC só efetua a retenção da sua chave privada.

5.12.1 Políticas e práticas de recuperação de chaves

A chave privada da EC 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.

A intervenção de cópia de segurança utiliza um HSM com autenticação de dois fatores, em que várias pessoas, cada uma delas possuindo um token de autenticação físico, 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 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 pode ser recuperada no caso de mau funcionamento da chave original. A intervenção de recuperação da chave utiliza os mesmos mecanismos de autenticação de dois fatores e com múltiplas pessoas, que foram utilizados na intervenção de cópia de segurança.

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

Não aplicável.

6 Medidas de segurança física, de gestão e operacionais

Existem várias regras e políticas implementadas, 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.

6.1 Medidas de segurança física

6.1.1 Localização física e tipo de construção

As instalações da EC 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 são realizadas numa sala numa zona de alta segurança, 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 seguintes condições de segurança são garantidas no ambiente da EC:

- Perímetros de segurança claramente definidos;
- Configuração da área que impede 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.

6.1.2 Acesso físico ao local

Os sistemas da EC estão protegidos por um mínimo de 4 níveis de segurança física hierárquicos de acordo com a NT D-02[13], garantindo-se que o acesso a um nível de segurança mais elevado

[13] GNS/NT D-02 – https://www.gns.gov.pt/docs/nt-d-02.pdf

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. Acessos físicos são automaticamente registados e gravados em circuito fechado de TV para efeitos de auditorias.

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, incluindo autenticação biométrica, na área mais restrita.

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.

6.1.3 Energia e ar condicionado

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

- 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.

6.1.4 Exposição à água

As zonas de alta segurança têm instalados detetores de inundação, para minimizar o impacto de inundações nos sistemas da EC.

6.1.5 Prevenção e proteção contra incêndio

O ambiente seguro da EC 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.

6.1.6 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, a 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 de 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).

6.1.7 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 deverão ser devidamente limpos de modo a não ser possível recuperar nenhuma informação (através de formatações seguras, ou destruição física dos equipamentos).

6.1.8 Instalações externas (alternativa) para recuperação de segurança

São guardadas em ambiente seguro em instalações externas, cópias de segurança, 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).

6.2 Medida de segurança dos processos

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

- Dados os requisitos de segurança inerentes ao seu funcionamento, 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;

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.

6.2.1 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.

Estão estabelecidos papéis de confiança, agrupados em categorias (que correspondem a 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.

6.2.1.1 Grupo de Trabalho de Administração de Sistemas

A função do Grupo de Trabalho de Administração de Sistemas é instalar, configurar e manter os sistemas informáticos, tendo acesso controlado a informação relativa à segurança.

6.2.1.2 Grupo de Trabalho de Operação de Sistemas

A função do Grupo de Trabalho de Operação de Sistemas é operar diariamente os sistemas informáticos, assim como as tarefas de rotina essenciais ao bom funcionamento e operacionalidade da EC.

6.2.1.3 Grupo de Trabalho de Administração de Segurança

A função do Grupo de Trabalho de Administração de Segurança é gerir e implementar as regras, políticas e práticas de segurança, tendo acesso a toda a informação relativa à segurança. Adicionalmente, propõem todos os documentos da EC, assegurando que se encontram atualizados, e garantem que toda a informação indispensável ao funcionamento e auditoria da EC se encontra disponível (para elementos devidamente autorizados) ao longo do tempo.

6.2.1.4 Grupo de Trabalho de Auditoria de Sistemas

A função do Grupo de Trabalho de Auditoria de Sistemas é efetuar a auditoria interna a todas as ações relevantes e necessárias para assegurar a correta operacionalidade da EC. Estão autorizados a aceder aos arquivos e logs da EC, com o objetivo de auditar as operações, de acordo com a política de segurança, assim como aos logs de acessos físicos a fim de identificar potenciais tentativas de intrusão. Compete-lhes também monitorizar o cumprimento das políticas e regras emanadas pelo Grupo de Administração de Segurança.

6.2.1.5 Grupo de Trabalho de Custódia

A função do Grupo de Trabalho de Custódia é efetuar a gestão, guarda e disponibilidade (nas situações previstas) dos artefactos sensíveis (*e.g.,* palavras-passe não pessoais) e artefactos físicos (e.g., *tokens*), no Ambiente de Custódia, que podem ser levantados pelos membros de outros grupos, de acordo com as regras definidas pelo Grupo de Trabalho de Administração de Segurança.

6.2.1.6 Grupo de Trabalho de Manutenção de Sistemas de Suporte

A função deste Grupo de Trabalho é garantir o bom funcionamento dos sistemas de suporte da sala segura da EC, nomeadamente acompanhar e realizar as atividades de manutenção dos sistemas de suporte assim como intervir em caso de verificada alguma anomalia nos referidos sistemas.

6.2.1.7 Grupo de Trabalho de Gestão

A função do Grupo de Trabalho de Gestão é a gestão da EC, que inclui a nomeação dos membros dos restantes grupos.

6.2.1.8 Grupo de Trabalho de Registo

A função do Grupo de Trabalho de Registo é a verificação da identidade e de atributos específicos (se aplicável) do titular que efetua o pedido do certificado.

6.2.1.9 Grupo de Trabalho de Revogação

A função do Grupo de Trabalho de Revogação é operar a mudança no estado dos certificados de utilizador final.

6.2.1.10 Grupo de Trabalho de Personalização

A função do Grupo de Trabalho de Personalização é operar os equipamentos e ferramentas que colocam o par de chaves e certificados do titular em *token* ou *hardware* criptográfico.

6.2.2 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.

6.2.3 Funções que requerem separação de responsabilidades

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

	Administração de Sistemas	Operação de Sistemas	Administração de Segurança	Auditoria de Sistemas	Custódia	Gestão	Registo	Revogação	Personalização
Administração de Sistemas			X	X	X	X	X	X	X
Operação de Sistemas			X	X	X	X			X
Administração de Segurança	X	X		X	X	X			X
Auditoria de Sistemas	X	X	X		X	X	X	X	X
Custódia	X	X	X	X		X	X	X	X
Gestão	X	X	X	X	X		X	X	X
Registo	X			X	X	X			X
Revogação	X			X	X	X			X
Personalização	X	X	X	X	X	X	X	X	

6.3 Medidas de Segurança de Pessoal

6.3.1 Requisitos relativos às qualificações, experiência, antecedentes e credenciação

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

- Ter sido nomeado formalmente, pelo Grupo de Gestão, para a função a desempenhar;
- Apresentar provas de antecedentes, qualificações e experiência necessárias para a realização das tarefas inerentes à função;
- Ter grau de credenciação de segurança conforme documento de políticas do SCEE[1];
- 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 desempenha funções que possam causar conflito com as suas responsabilidades nas atividades da EC.

6.3.2 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.

6.3.3 Requisitos de formação e treino

Os elementos dos Grupos de Trabalho deverão ter formação de base ou demonstrada experiência em segurança, administração e operação de sistemas, para poderem integrar os grupos de trabalho.

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

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

6.3.4 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 se verifiquem alterações processuais de gestão da EC;
- Sempre que são introduzidas alterações nas Políticas de Certificação ou Declaração de Práticas de Certificação são realizadas sessões de reciclagem aos elementos das EC.

6.3.5 Frequência e sequência da rotação de funções

Nada a assinalar.

6.3.6 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 do Ministério da Justiça e das leis de segurança nacional, a todos os indivíduos que realizem ações não autorizadas ou que façam uso não autorizado dos sistemas.

6.3.7 Requisitos para prestadores de serviços

Consultores ou prestadores de serviços independentes têm permissão de acesso à zona de alta segurança desde que, estejam devidamente autorizados, pelo Grupo de Administração de Segurança e 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.

6.3.8 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.

6.4 Procedimentos de auditoria de segurança

6.4.1 Tipo de eventos registados

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

- Eventos com obrigatoriedade de registo, identificados na Política de Certificados do SCEE[1];
- 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 intervenção 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.

6.4.2 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.

6.4.3 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 6.5.

6.4.4 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 poderá ser levada a cabo, após o período legal em que têm de ser retidos, na presença de, no mínimo dois elementos dos Grupos de Trabalho. Estes só podem ser destruídos com autorização expressa do Grupo de Administração de Segurança.

6.4.5 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.

6.4.6 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 e pelo pessoal que as opera. Todos os registos de auditoria são armazenados nos sistemas internos da EC.

6.4.7 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.

6.4.8 Avaliação de vulnerabilidades

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

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

O Grupo de Administração de Segurança analisa o relatório dos testes, delineia um plano de ação para implementação e correção das vulnerabilidades detetadas.

Caso se verifique alguma das seguintes situações, deverá o plano ser aprovado pelo Grupo de Gestão:

- ➔ Se houver Riscos Altos ou Muito altos sobre a infraestrutura, na implementação das ações corretivas, e/ou
- ➔ Caso esse plano careça de investimento.

Caso contrário, o Grupo de Administração de Segurança dará seguimento ao cumprimento do plano pelas equipas intervenientes.

6.5 Arquivo de registos

6.5.1 Tipo de dados arquivados

Todos os dados auditáveis são arquivados (conforme indicado na secção 6.4.1), 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 6.4.1 desta DPC;
- As cópias de segurança dos sistemas que compõem a infraestrutura da EC;
- Toda a documentação relativa ao ciclo de vida dos certificados, designadamente:
  - Comprovativos de segunda via de Cartas PIN;
  - Cancelamentos de Cartão de Cidadão;
  - Todos os Cartões de Cidadão que não foram levantados;
  - Procedimentos de emissão e revogação de certificados de serviço;
  - Procedimentos de emissão e receção dos certificados de serviço;

- 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

6.5.2 Período de retenção em arquivo

Os dados sujeitos a arquivo são retidos, pelo período definido pela legislação nacional (cf. alínea f) do Artigo 13.º do Decreto-Lei n.º 12/2021 de 9 de fevereiro).

6.5.3 Proteção dos arquivos

O arquivo é protegido para 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 dispositivo de armazenamento 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.

6.5.4 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.

6.5.5 Requisitos para validação cronológica dos registos

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

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

Os sistemas de recolha de dados de arquivo são internos.

6.5.7 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, e em caso de erros ou comportamentos imprevistos, realiza-se novo arquivo.

6.6 Renovação de chaves

Nada a assinalar.

6.7 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.

6.7.1 Procedimentos em caso de incidente ou comprometimento

As cópias de segurança das chaves privadas da EC (geradas e mantidas de acordo com a secção 7.2.4) e dos registos arquivados (secção 6.5.1) são guardados em ambientes seguros externos e disponíveis em caso de desastre. No caso de comprometimento da chave privada da EC AsC, esta deverá tomar as seguintes ações, até 24h após deteção de comprometimento:

- Proceder à sua revogação imediata;
- Revogar todos os certificados por ela emitidos;
- Informar todos os titulares dos seus certificados e terceiras partes conhecidas;
- Informar o Conselho Gestor do SCEE.

6.7.2 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 suspenderá os seus serviços e notificará o Conselho Gestor do SCEE e a Entidade Supervisora. 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, até 24h após deteção de comprometimento.

6.7.3 Procedimentos em caso de comprometimento da chave privada da entidade

No caso da chave privada da EC ser comprometida ou exista suspeita do seu comprometimento, devem ser tomadas medidas apropriadas de resposta ao incidente. As respostas a esse incidente, devem ser dadas até 24h após deteção de comprometimento, podendo incluir:

- Notificação da Entidade Supervisora;
- Revogação do certificado da EC e de todos os certificados emitidos no seu "ramo" de hierarquia de confiança;
- Notificação do Conselho Gestor do SCEE e todos os titulares de certificados emitidos no "ramo" da hierarquia de confiança da EC;
- Geração de novo par de chaves para a EC, e pedido de novo certificado à EC CC;
- Emissão de todos os certificados no "ramo" da hierarquia de confiança da EC, que forem solicitados.

6.7.4 Capacidade de continuidade da atividade em caso de desastre

Existem disponíveis recursos de computação, *software*, cópias de segurança e registos arquivados nas suas instalações secundárias de segurança, necessários para restabelecer ou recuperar as operações essenciais: alteração de estado dos certificados emitidos e a publicação de lista de certificados revogados atualizada, a realizar com base em procedimentos definidos a executar após um desastre natural ou outro.

6.8 Procedimentos em caso de extinção de EC ou ER

Em caso de cessação de atividade, como prestador de serviços de Certificação, a EC deve, atempadamente, com uma antecedência mínima de três meses, proceder às ações descritas na secção 10.10.

7 Medidas de Segurança Técnicas

Esta secção define as medidas de segurança implementadas para a EC 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 criptográficas, assim como dados de ativação, estejam sempre protegidos e sejam apenas acedidos por pessoas devidamente autorizadas.

7.1 Geração e instalação do par de chaves

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

7.1.1 Geração do par de chaves

Esta EC funciona em modo on-line. A geração das suas chaves criptográficas é feita por um Grupo de Trabalho, composto por elementos autorizados, numa intervenção planeada e auditada de acordo com procedimentos escritos das operações a realizar. Estas intervenções ficam registadas, datadas e assinadas pelos elementos dos Grupo de Trabalho envolvidos.

O *hardware* criptográfico, usado para a geração de chaves da EC, 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 através de *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 do titular do Cartão de Carão de Cidadão, é efetuada em hardware criptográfico que cumpre os requisitos definidos na secção 7.2.1. O par de chaves é transmitido de modo seguro ao chip do Cartão de Cidadão, no momento da sua personalização.

7.1.2 Entrega da chave privada ao titular

A entrega da chave privada, associada aos certificados emitidos para o cidadão é efetuada no Cartão de Cidadão, cujo chip contém um dispositivo criptográfico SSCD (I, cf. número 1 do artigo 51.º do regulamento eIDAS[6]) ou QESCD (*Qualified Electronic Signature Creation Device*, cf. Artigo 29.º do regulamento eIDAS[6]).

7.1.3 Entrega da chave pública ao emissor do certificado

A chave pública é entregue à EC para a emissão do certificado, de acordo com os procedimentos indicados na secção 5.3.1.

7.1.4 Entrega da chave pública da EC às partes confiantes

A chave pública da EC é disponibilizada através do seu certificado, assinado pela EC do Estado, conforme secção 3.2.

7.1.5 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:

- A partir da EC AsC 0019 (inclusive) as chaves utilizadas são de 384 bits ECC
- As geradas anteriormente são 4096 bits RSA.

7.1.6 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/pseudoaleatórios descritos no ANSI X9.17 (Anexo C), de acordo com o estipulado no PKCS#1.

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

7.2 O campo "*keyUsage*" dos certificados emitidos por esta EC estão descritos na POL#23. 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. Está implementada uma combinação de controlos físicos, lógicos e procedimentais, devidamente documentados, de forma a assegurar confidencialidade e integridade das chaves privadas da EC.

7.2.1 Normas e medidas de segurança do módulo criptográfico

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

- Segurança Física (Certificações de Segurança)
  - *Common Criteria* EAL 4+ (AVA_VAN.5),
  - FIPS 140-2, nível 3,
  - FIPS 186-4,
  - NIST SP800-131A,
  - Certificação OCSI para uso como QsigCD e QSealCD.
- Certificações Regulamentares

    - *UL, CSA, CE*
    - *FCC, VCCI, CE*
    - *RoHS, WEEE*
- Papéis
    - Autenticação de dois fatores
- Geração de números aleatórios
    - DRBG (*Deterministic Random Bit Generator*) com certificação FIPS 140-2 (SP 800-90 modo CTR)
- Troca de chaves e chave de cifra assimétrica
    - RSA (2048-8192)
    - DSA (2048-3072)
    - Diffie-Hellman
    - Curvas elípticas (ECDSA, ECDH, ECIES)
- Assinatura Digital
    - RSA (512-4096)
    - PKCS#1 v1.5
- Algoritmos de chave simétrica
    - AES
- Algoritmos de Hash
    - SHA-2 (256-512)

7.2.2 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.

Está implementado 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 são divididos em várias partes, 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 guardada no módulo criptográfico em *hardware*. São necessárias, no mínimo, duas (n) partes para a ativação da chave privada da EC.

7.2.3 Retenção da chave privada (*key escrow*)

A retenção da chave privada da EC é explicada em detalhe na secção 5.12.

7.2.4 Cópia de segurança da chave privada

A chave privada da EC tem pelo menos uma cópia de segurança, com o mesmo nível de segurança que a chave original, conforme secção 5.12.

Não são efetuadas cópias das chaves privadas dos certificados para o cidadão incluídos no chip do Cartão de Cidadão.

7.2.5 Arquivo da chave privada

As chaves privadas da EC, alvo de cópias de segurança, são arquivadas conforme identificado na secção 5.12.

7.2.6 Transferência da chave privada para/do módulo criptográfico

As chaves privadas da EC não são extraíveis a partir do *hardware* criptográfico.

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

7.2.7 As chaves privadas do cidadão, para os quais são emitidos certificados de assinatura, são transferidas do Hardware criptográfico onde são geradas, diretamente para o Chip (hardware criptográfico) de forma a garantir o transporte das chaves entre módulos numa transmissão cifrada.Armazenamento da chave privada no módulo criptográfico

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

7.2.8 Processo para ativação da chave privada

A EC é uma EC *on-line*, cuja chave privada é ativada quando o sistema da EC é ligado. Esta ativação é efetivada através da autenticação no módulo criptográfico pelos indivíduos autorizados para o efeito, sendo obrigatória a utilização de autenticação de dois fatores, em que várias pessoas (membros dos grupos de trabalho), cada uma delas possuindo um token de autenticação, são obrigadas a autenticar-se antes que seja possível efetuar a ativação.

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

7.2.9 Processo para desativação da chave privada

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

Para a desativação das chaves privadas da EC é necessária, no mínimo, a intervenção de dois elementos dos Grupos de Trabalho, autorizados. Uma vez desativada, esta permanecerá inativa até que o processo de ativação seja executado.

7.2.10 Processo para destruição da chave privada

As chaves privadas da EC (incluindo as cópias de segurança) são apagadas/destruídas num procedimento devidamente identificado e auditado, no máximo 90 dias após 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.

7.2.11 Avaliação/nível do módulo criptográfico

Descrito na secção 7.2.1.

7.3 Outros aspetos da gestão do par de chaves

7.3.1 Arquivo da chave pública

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

7.3.2 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 desta EC tem a validade de 12 anos, sendo renovado antes de atingir os dois anos de validade, uma vez que os certificados emitidos para cidadãos que tenham completado 25 anos de idade, têm 10 anos e 1 mês de validade.
- O certificado de pessoa singular tem uma validade máxima de 10 anos e 1 mês, para certificados emitidos para cidadãos que tenham completado 25 de idade, podendo ser inferior no caso de cidadãos que não tenham completado essa idade e cidadãos brasileiros portadores do Estatuto de Igualdade de Direitos e Deveres - Tratado de Porto Seguro do ano 2000, com Título de Residência, casos onde a validade poderá ser igual ou inferior a 5 anos;
- Os certificados de serviço complementar para o serviço OCSP têm uma validade de 5 anos e 2 meses;
- O certificado de serviço complementar para a entidade de Validação Cronológica é emitido com uma validade de 6 anos e 6 meses, sendo a chave usada no 1º ano de validade, procedendo-se à geração de novo certificado com novo par de chaves.

7.4 Dados de ativação

7.4.1 Geração e instalação dos dados de ativação

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

7.4.2 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 são guardadas, de forma cifrada, em *token* criptográfico.

7.4.3 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.

7.5 Medidas de segurança informáticas

7.5.1 Requisitos técnicos específicos

O acesso aos servidores da EC é restrito aos membros dos Grupos de Trabalho. A EC 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 para serviços complementares).

A EC 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.

7.5.2 Avaliação/nível de segurança

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

O módulo criptográfico em Hardware da EC, satisfaz os requisitos descritos na secção 7.2.1.

7.6 Ciclo de vida das medidas técnicas de segurança

7.6.1 Medidas de desenvolvimento do sistema

As aplicações são desenvolvidas e implementadas de acordo com regras de desenvolvimento de sistemas e de gestão de mudanças devidamente definidas.

É fornecida metodologia auditável que permite verificar que o *software* da EC 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.

7.6.2 Medidas para a gestão da segurança

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

7.6.3 Ciclo de vida das medidas de segurança

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

7.7 Medidas de Segurança da rede

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

7.8 Validação cronológica

Certificados, LRCs 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 uma fonte de tempo confiável externa, sendo escolhida 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).

A sincronização de toda a infraestrutura da EC 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.

8 Perfis de Certificado, CRL e OCSP

8.1 Perfil de Certificado

O perfil dos certificados emitidos pela EC deve ser consultado na "Política de Certificados da EC de Assinatura Digital Qualificada do Cartão de Cidadão" (POL#23).

8.2 Perfil da lista de revogação de certificados

O perfil da lista de revogação de certificados da EC deve ser consultado na "Política de Certificados da EC de Assinatura Digital Qualificada do Cartão de Cidadão" (POL#23).

8.3 Perfil de resposta OCSP

O perfil de resposta OCSP da EC deve ser consultado na "Política de Certificados da EC de Assinatura Digital Qualificada do Cartão de Cidadão" (POL#23).

9 Auditoria e Avaliações de Conformidade

É efetuada, pelo Grupo de Trabalho da EC, uma inspeção regular de conformidade a esta DPC e a outras regras, procedimentos, intervenções e processos.

A auditoria de avaliação de conformidade, no contexto do regulamento (EU) nº 910/2014, é efetuado por um Organismo de Avaliação de Conformidade, devidamente credenciado.

Para além de auditorias de conformidade, poderão ser efetuadas outras fiscalizações e investigações para aferir a conformidade da EC com a legislação nacional aplicável e o regulamento (EU) 910/2014[6]. A execução destas auditorias, fiscalizações e investigações poderá ser delegada a uma entidade externa de auditoria.

9.1 Frequência ou motivo da auditoria

As auditorias de avaliação de conformidade são realizadas regularmente de acordo com o definido pelo regulamento (EU) nº 910/2014[6] e pela Política de Certificados do SCEE[1], caso não exista outra diretiva emitida pelo Conselho Gestor do SCEE ou pela Entidade Supervisora. A EC precisa de provar, com a auditoria e relatório de segurança, que a avaliação dos riscos foi assegurada, tendo sido identificadas e implementadas todas as medidas necessárias para a segurança de informação.

9.2 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.

Para auditoria no contexto da Política de Certificados do SCEE[1], o auditor é credenciado pelo Gabinete Nacional de Segurança.

Para auditoria no contexto do regulamento (EU) nº 910/2014[6], o Organismo Nacional de Acreditação (IPAC) é responsável pela acreditação dos auditores (denominados de Organismos de Avaliação de Conformidade) estando estes capacitados para efetuar as avaliações de conformidade, resultando dessa avaliação um Relatório de Conformidade (CAR) que é disponibilizado à Entidade Supervisora, para avaliar a continuidade de disponibilização de serviços de confiança.

9.3 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 garantida a 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 este poderá aceder a dados pessoais dos titulares dos certificados emitidos pela EC e dos elementos os Grupos de Trabalho da EC.

9.4 Âmbito da auditoria

A auditoria pode ser efetuada no contexto da Política de Certificados do SCEE[1] ou do regulamento (EU) nº 910/2014[6], encontrando-se o seu âmbito descrito nesses documentos.

9.5 Procedimentos após uma auditoria com resultado deficiente

Os procedimentos após uma auditoria com resultado deficiente encontram-se descritos na Política de Certificados do SCEE[1] (para auditoria no contexto dessa política) e no regulamento (EU) nº 910/2014[6] (para auditoria no contexto desse regulamento).

9.6 Comunicação de resultados

Os resultados são comunicados conforme descrito na Política de Certificados do SCEE[1] (para auditoria no contexto dessa política) e no regulamento (EU) nº 910/2014[6] (para auditoria no contexto desse regulamento).

10 Outras Situações e Assuntos Legais

Esta secção aborda aspetos de negócio e assuntos legais.

10.1 Taxas

10.1.1 Taxas por emissão ou renovação de certificados

A Lei n.º 7/2007 de 5 de fevereiro, que criou o cartão de cidadão determina nos seus artigos 34.º, n.os 1 e 2, e 61.º-A, n.º 9, que as taxas devidas pela prestação dos serviços associados ao cartão de cidadão e pela emissão do cartão de cidadão provisório, bem como as situações de redução, isenção ou gratuitidade daquelas, são definidas por portaria do membro do Governo responsável pela área da justiça. No caso, a Portaria 291/2017, de 28 de setembro, regula a matéria atinente às taxas devidas pela prestação do serviço público do cartão de cidadão, bem como as situações de redução, isenção e gratuitidade.

10.1.2 Taxas para acesso a certificado

Nada a assinalar.

10.1.3 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.

10.1.4 Taxas para outros serviços

Nada a assinalar.

10.1.5 Política de reembolso

Nada a assinalar.

10.2 Responsabilidade financeira

10.2.1 Seguro de cobertura

Nada a assinalar.

10.2.2 Outros recursos

Nada a assinalar.

10.2.3 Seguro ou garantia de cobertura para utilizadores

Nada a assinalar.

10.3 Confidencialidade da informação processada

10.3.1 Âmbito da confidencialidade da informação

Considera-se Informação Confidencial, aquela que não poderá ser divulgada a terceiros, nomeadamente:

- Dados do cidadão que não estejam incluídos no certificado emitido pela EC;
- As chaves privadas das EC;
- Toda a informação relativa a parâmetros de segurança, controlo e procedimentos de auditoria;
- Toda a informação de carácter pessoal proporcionada à EC, durante o processo de registo dos subscritores de certificados, salvo se houver autorização explícita para a sua divulgação;
- Registos de transações, incluindo os registos completos e os registos de auditoria das transações;
- Documentos da EC que não forem classificados como "público", assim como artefactos operacionais, conceitos técnicos, organizacionais, financeiros e comerciais. Esta informação é confiada aos recursos humanos dos Grupos de Trabalho da EC (seguindo o princípio do menor privilégio) com a condição de não serem usados ou divulgados para além do âmbito dos seus deveres nos termos estabelecidos, sem autorização prévia e explícita do Prestador de serviços de Confiança.

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

10.3.3 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 do Prestador de serviços de Confiança.

10.4 Privacidade dos dados pessoais

10.4.1 Medidas para garantia da privacidade

O Sistema de Ciclo de Vida é responsável pela implementação das medidas que garantem a privacidade dos dados pessoais, que estão de acordo com a Política de Certificados do SCEE[1], regulamento (EU) nº 910/2014[6] e com a legislação em vigor.

10.4.2 Informação privada

De acordo com a Política de Certificados do SCEE[1] e com o regulamento (EU) nº 910/2014[6].

10.4.3 Informação não protegida pela privacidade

De acordo com a Política de Certificados do SCEE[1] e com o regulamento (EU) nº 910/2014[6].

10.4.4 Responsabilidade de proteção da informação privada

De acordo com a Política de Certificados do SCEE[1] e com o regulamento (EU) nº 910/2014[6].

10.4.5 Notificação e consentimento para utilização de informação privada

De acordo com a Política de Certificados do SCEE[1] e com o regulamento (EU) nº 910/2014[6].

10.4.6 Divulgação resultante de processo judicial ou administrativo

De acordo com a Política de Certificados do SCEE[1] e com o regulamento (EU) nº 910/2014[6].

10.4.7 Outras circunstâncias para revelação de informação

Nada a assinalar.

10.5 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, pertencem ao Ministério da Justiça.

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.

10.6 Representações e garantias

10.6.1 Representação e garantias das entidades certificadoras

A EC 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 pode determinar com precisão a 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 5.9.7;
- Publicar a sua DPC e as Políticas de Certificado aplicáveis no seu repositório garantindo o acesso às versões atuais assim como a 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 5.9.7;
- 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 ao CG e Entidade Supervisora;
- 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 o prazo legal e,

- Disponibilizar os certificados da EC AsC.

10.6.2 Representação e garantias das Entidades de Registo

De acordo com a Política de Certificados do SCEE[1] e com o regulamento (EU) nº 910/2014[6].

10.6.3 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 5.9.3;
- 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.

10.6.4 Representação e garantias das partes confiantes

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

- Limitar a fiabilidade dos certificados às utilizações permitidas para os mesmos em conformidade com o expresso nesta DPC e na Política 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 a EC publique no seu sítio *Web*, conforme seção 4.4.

10.6.5 Representação e garantias de outros participantes

Nada a assinalar.

10.7 Renúncia de garantias

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

10.8 Limitações às obrigações

A EC AsC:

- 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.
- 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.
- 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 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
- 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.
- 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.
- 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
- não assume qualquer responsabilidade no caso de perca ou prejuízo:
    i. Dos serviços que prestam, em caso de guerra, desastres naturais ou qualquer outro caso de força maior;
    ii. Ocasionados pelo uso dos certificados quando excedam os limites estabelecidos pelos mesmo na Política de Certificados e correspondente DPC:
    iii. Ocasionado pelo uso indevido ou fraudulento dos certificados ou LRC emitidos pela EC.

10.9 Indemnizações

De acordo com a legislação em vigor.

10.10 Termo e cessação da atividade

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

10.10.1 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 ou são partes confiantes na EC.

Desta forma o IRN deverá informar de forma imediata:

- Entidade supervisora;
- Conselho Gestor do SCEE;
- Grupo de Gestão da EC CC;
- Cidadão para quem tenham sido emitidos certificados e que ainda se encontrem válidos à data da decisão de cessação de atividade;
- Outras partes confiantes.

A notificação inclui, no mínimo, a seguinte informação:

- Entidade supervisora 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.

10.10.2 Cessação de Relações contratuais

Serão cessadas as relações contratuais com todas as entidades terceiras que, de alguma forma, intervenham nas atividades inerentes à EC AsC.

10.10.3 Revogação dos certificados

Todos os certificados emitidos no âmbito da EC, 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 serviços complementares, que ainda se encontrem válidos;
2. Emissão e disponibilização pública das Listas de Certificados Revogados da EC;
3. Destruição das Chaves Privadas da EC;
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 legalmente exigido.

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

10.11 Prazo e Terminação

10.11.1 Prazo

Esta DPC torna-se efetiva assim que seja aprovada pelo Grupo de Gestão e apenas é eliminada ou alterada por sua ordem e/ou do Conselho Gestor.

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

10.11.2 Terminação

Esta DPC cessa a sua vigência quando for substituída pela publicação de uma nova versão no repositório da EC CC.

10.11.3 Efeito da Terminação e Sobrevivência

As obrigações e restrições estabelecidas nesta DPC, relativamente a auditorias, informação confidencial, arquivo de registos, obrigações e responsabilidades, criadas sob a sua vigência, subsistirão após a sua substituição por uma nova versão em tudo o que não se oponha a esta.

10.12 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 sítios web do Instituto dos Registos e Notariado e do Portal do Cidadão.

10.13 Alterações

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

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

10.13.1 Procedimento para alterações

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

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

O Grupo de Administração de Segurança 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 para revisão, aos elementos que considerar necessários dentro do âmbito da EC para permitir o seu escrutínio. Contando a partir da data de disponibilização, as várias partes têm 10 dias úteis para submeter os seus comentários. Quando esse período terminar, o Grupo de Administração de Segurança tem mais 5 dias úteis para analisar todos os comentários recebidos e, se relevante, incorporá-los no documento. O documento é de seguida analisado e aprovado pelo Grupo de Gestão. Depois da sua aprovação, o Grupo de Administração de Segurança é responsável pela sua publicação no repositório público do cartão de cidadão, tornando-se as alterações finais e efetivas.

10.13.1.1 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 de Administração de Segurança tem 30 dias úteis para submeter para aprovação pelo Grupo de Trabalho de Gestão, uma nova versão do(s) documento(s) substituto(s).

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 (EU) nº 910/2014[6] ou, caso exista, pelo período indicado pela Entidade Supervisora.

10.13.2 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, da forma identificada na secção 10.11.

Essa notificação será publicitada no site do TSP, o IRN.

10.13.3 Motivos para mudar de OID

O Grupo de Administração de Segurança 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.

No caso em que o Grupo de Administração de Segurança julgue que as alterações à especificação podem afetar à aceitabilidade dos certificados para propósitos específicos proceder-se-á à modificação dos 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 10.11.

10.14 Disposições para resolução de conflitos

Todas reclamações entre utilizadores e EC AsC deverão ser comunicadas pela parte em disputa ao Prestador de serviços de confiança (TSP), no caso ao IRN, com o fim de tentar resolvê-lo entre as mesmas partes.

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

10.15 Legislação aplicável

É aplicável à atividade inerente da EC as políticas da SCEE[1], a legislação nacional, o Regulamento (EU) nº 910/2014[6] e standards internacionais indicados nas Referências Bibliográficas, deste documento.

Relativamente à proteção de dados pessoais é aplicável o:

- Regulamento Geral sobre a Proteção de Dados – Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho da União Europeia, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE;
- Lei n.º 58/2019 de 8 de agosto: Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

10.16 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 do Grupo de Administração de Segurança e do Grupo de Gestão do Cartão de Cidadão zelar pelo cumprimento da legislação aplicável listada na secção 10.15.

10.17 Providências várias

10.17.1 Acordo completo

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

10.17.2 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 válida, apenas e só nos casos em que tais estipulações não sejam consideradas essenciais. É responsabilidade do Conselho Gestor e da Entidade Supervisora, ou em falta destes, do Grupo de Gestão da EC, a avaliação da essencialidade das mesmas.

10.17.3 Severidade

Nada a assinalar.

10.17.4 Execuções (taxas de advogados e desistência de direitos)

Nada a assinalar.

10.17.5 Força Maior

Nada a assinalar.

10.18 Outras providências

Nada a assinalar.

Referências Bibliográficas

- Lei n.º 19-A/2024, de 7 de fevereiro. Alteração às Leis 7/2007, de 5 de fevereiro, que cria o cartão de cidadão e rege a sua emissão e utilização, 37/2014, de 26 de junho, que estabelece um sistema alternativo e voluntário de autenticação dos cidadãos nos portais e sítios na Internet da Administração Pública denominado Chave Móvel Digital, e 13/99, de 22 de março, que estabelece o novo regime jurídico do recenseamento eleitoral, e ao Decreto-Lei n.º 135/99, de 22 de abril, que define os princípios gerais de ação a que devem obedecer os serviços e organismos da Administração Pública na sua atuação face ao cidadão;
- SCEE 2 OID: 2.16.620.1.1.1.2.1.5.0 de 2022, Política de Certificados da SCEE e Requisitos mínimos de Segurança.
- Regulamento (UE) 1157/2019 visa reforçar a segurança dos bilhetes de identidade dos cidadãos e dos títulos de residência emitidos aos cidadãos da União e seus familiares.
- Regulamento nº 910/2014 de 23 de julho de 2014 do Parlamento Europeu e do Conselho, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE;
- Decreto-Lei nº12/2021, de 9 de fevereiro;
- Decreto Regulamentar n.º 25/2004, de 15 de julho.
- Lei n.º 7/2007, de 5 de fevereiro (na redação dada pela republicação na Lei n.º 61/2021, de 19 de agosto).
- 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 Directory: Authentication Framework.
- NIST FIPS PUB 180-2. 2002, Secure Hash Standard, U. S. Department of Commerce, Technology Administration, National Institute of Standards and Technology
- 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).*
- ETSI EN 319 401 v2.3.1 – Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- ETSI EN 319 411-1 v1.3.1 – *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements*.
- ETSI EN 319 411-2, v2.3.1, *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 v1.4.4 – *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures*.

- Regulamento Geral sobre a Proteção de Dados – Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho da União Europeia, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE.
- Lei n.º 58/2019 de 8 de agosto: Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

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*
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, conforme regulamento (UE) n.º 910/2014[6].
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 de assinatura eletrónica, que seja emitido por um prestador de serviços de confiança e satisfaça os requisitos estabelecidos no anexo I, III ou IV do Regulamento (UE) Nº 910/2014[6].
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 regulamento (UE) n.º 910/2014[6] 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 criar assinaturas eletrónicas.
Dispositivo Seguro de Criação de Assinatura	Dispositivo de criação de assinatura que cumpra os requisitos estabelecidos no anexo II do regulamento (UE) n.º 910/2014[6].
Dispositivo Qualificado de Criação de Assinaturas Eletrónicas	O mesmo que "Dispositivo Seguro de Criação 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.
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 assinatura eletrónica, que confia na mesma.
Prestador de serviços de confiança	Pessoa singular ou coletiva que preste um ou mais do que um serviço de confiança (cf. regulamento (UE) n.º 910/2014[6]) quer como prestador qualificado quer como prestador não qualificado de serviços de confiança.
Prestador qualificado de serviços de confiança	Prestador de serviços de confiança que preste um ou mais do que um serviço de confiança qualificado e ao qual é concedido o estatuto de qualificado pela entidade supervisora.
Revogação de Certificado	Ato de invalidar definitivamente o certificado. Após revogado, o certificado, não voltará a ficar ativo.
Selo 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.
Sistema de Ciclo de Vida	Sistema que gere todos os fluxos de mensagem inerentes ao processo de emissão, substituição e cancelamento do Cartão de Cidadão. O Sistema do Ciclo de Vida é uma das componentes intervenientes na estrutura global de suporte à operação do Cartão de Cidadão, sendo responsável pela execução, gestão e controlo dos principais processos administrativos relacionados com o Cartão. Implementado pelo Ministério da Justiça permitindo o controlo de todo o processo, desde o pedido nos balcões do serviço, até à sua entrega, contemplando os atos inerentes à emissão, substituição e cancelamento do Cartão.
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

Aprovado pelo Grupo de Gestão.

Assinado por: **DIOGO DE CAMPOS MONTEIRO BRÁS**
Num. de Identificação: 10295504
Data: 2024.03.01 13:42:21+00'00'

Assinado por: **RICARDO JOÃO CORREIA VIEIRA**
Num. de Identificação: 13004962
Data: 2024.05.06 15:14:02+01'00'