POLÍTICA DE CERTIFICADOS DO SCEE

e

Requisitos Mínimos de Segurança

19 DE JULHO DE 2016

OID: 2.16.620.1.1.1.2.1.3.0

scee@scee.gov.pt

APROVAÇÃO E ASSINATURA

De acordo com o estipulado no ponto 2.2 do presente documento e tendo sido o mesmo aprovado por unanimidade em Reunião do Conselho Gestor do SCEE, no dia 19 de julho de 2016, confirmo, com a aposição da minha assinatura, a aprovação do mesmo e a sua entrada em vigor,

A Presidente do Conselho Gestor do SCEE.

Maria Manuel de Lemos Leitão Marques

Assinado de forma digital por Maria Manuel de Lemos Leitão Marques
Dados: 2017.02.01 18:04:59 Z

Maria Manuel de Lemos Leitão Marques

Ministra da Presidência e da Modernização Administrativa

ÍNDICE

ÍNDICE DE TABELAS

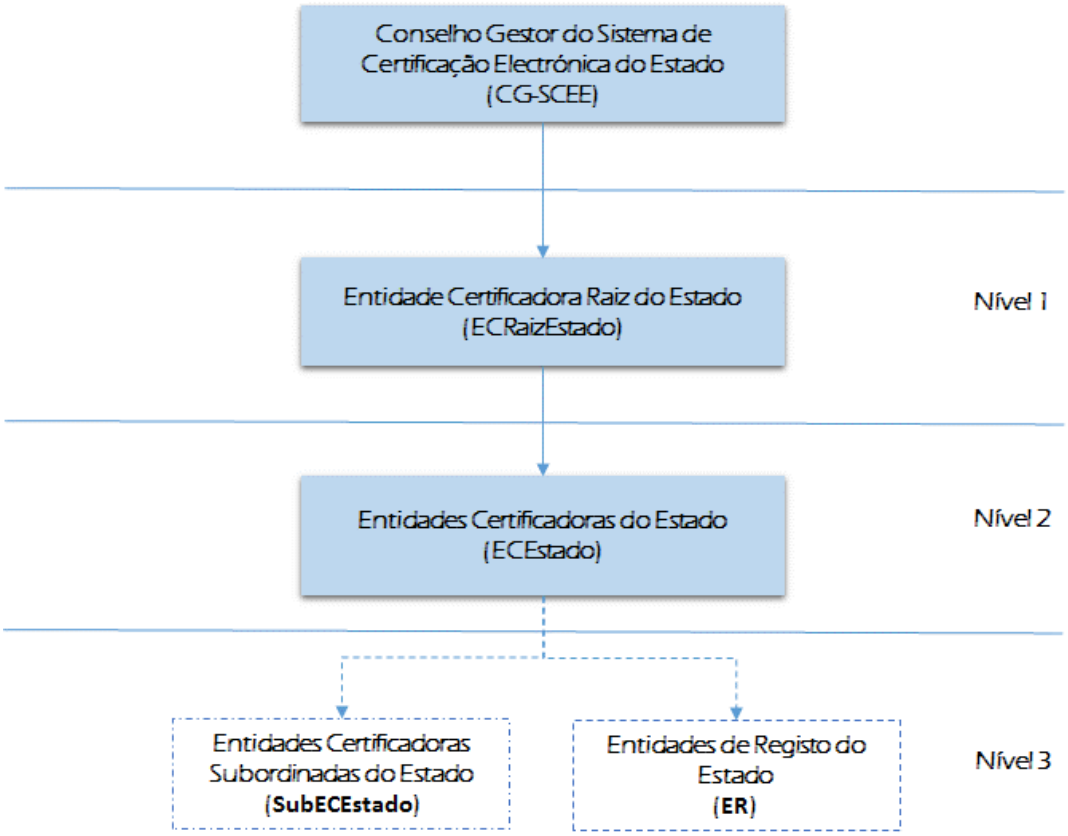
1. INTRODUÇÃO

1.1. ENQUADRAMENTO

1.1.1. ÂMBITO

No cumprimento da Resolução do Conselho de Ministros nº 171/2005, de 3 de Novembro e do Decreto-Lei n.º 116-A/2006, de 16 de Junho, procedeu-se à criação e instalação do Sistema de Certificação Electrónica do Estado (SCEE) e da Entidade de Certificação Eletrónica do Estado – Infraestrutura de Chaves Públicas (ECEE).

A arquitetura do SCEE constitui assim, uma hierarquia de confiança que garante a segurança eletrónica do Estado e a autenticação digital forte das transações eletrónicas entre os vários serviços e organismos da Administração Pública e entre o Estado e os cidadãos e as empresas.



Arquitetura funcional do SCEE

O SCEE funciona independentemente de outras infraestruturas de chaves públicas de natureza privada ou estrangeira, mas permite a interoperabilidade com as infraestruturas que satisfaçam os requisitos necessários de rigor de autenticação, através dos mecanismos técnicos adequados, e da compatibilidade em termos de políticas de certificação, nomeadamente no âmbito dos países da União Europeia.

A criação do SCEE foi efetuada, com as devidas adaptações, em conformidade com toda a legislação nacional e comunitária em vigor, nomeadamente a relativa às regras técnicas e de segurança aplicáveis às entidades certificadoras estabelecidas em Portugal na emissão de certificados qualificados.

Para o efeito o SCEE compreende:

- Um Conselho Gestor que aprova a integração ou cessação de entidades certificadoras no SCEE, pronunciando-se igualmente sobre práticas e políticas de certificação;
- Uma Entidade Certificadora Raiz do Estado (ECRaizEstado), que constitui o primeiro nível e o topo da cadeia hierárquica de certificação;
- As entidades certificadoras do Estado (ECEstado),subordinadas diretamente à entidade raiz;
- As entidades certificadoras subordinadas do Estado (SubECEstado), subordinadas diretamente ou em múltiplos níveis de uma das ECEstado;
- As entidades de registo associadas a cada uma das entidades certificadoras.

As entidades credenciadas, no âmbito SCEE, que disponibilizam certificados eletrónicos qualificados, de modo a suportar a produção de assinaturas eletrónicas qualificadas, têm de cumprir obrigatoriamente com os requisitos mínimos definidos nas disposições legais e regulamentares em vigor, disponibilizando para o efeito um conjunto de funções/serviços nucleares e opcionalmente determinados serviços suplementares.

São serviços nucleares: o Registo; Emissão; Distribuição; Estado das revogações e Gestão das revogações. Os serviços suplementares são o fornecimento de dispositivo seguro de criação de assinaturas e o de validação cronológica.

1.1.2. ESTRUTURA DO DOCUMENTO

No âmbito da presente política 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 que seja obtido um conhecimento prévio desses tópicos para uma melhor compreensão do presente documento.

Este documento segue a estrutura definida e proposta pelo standard "RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", de novembro de 2003.

De forma a facilitar a leitura e consequente análise deste documento com as práticas difundidas e recomendadas internacionalmente, optou-se por incluir todas a secções estabelecidas no índice do documento supracitado, pelo que se nada houver sobre o assunto, será incluída a expressão "nada a assinalar".

Ainda de acordo com este pressuposto foi tido em consideração as especificações e recomendações definidas nos vários documentos emanados pelo PKIX Working Group, União Europeia, legislação comunitária, legislação nacional aplicável.

1.1.3. HIERARQUIA DE OID DO SCEE

Os OID são identificadores utilizados para referenciar objetos de forma inequívoca num determinado contexto, neste caso, o SCEE, funcionando por hierarquias. Neste particular a união "ISO-ITU-T" é a responsável pela atribuição de OID para os países.

O SCEE tem como OID-Raiz = 2.16.620.1.1, com base na seguinte estrutura:

2	ISO/ITU-T jointly assigned OIDs
16	Country assignments
620	Portugal
1	Estado Português

Tabela 1 - Hierarquia superior de OID

1.1.3.1. Distribuição da árvore 2.16.620.1.1 {id-scee}

A utilização de OID derivados do OID-Raiz do SCEE, pelas entidades certificadoras e objetos no âmbito do SCEE, deverá ser efetuada em conformidade com o estipulado no Anexo E da presente política, devendo as entidades gestoras de cada uma das entidades certificadoras e de registo integradas no SCEE comunicar todos os OID's utilizados ao Centro de Gestão da Rede Informática do Governo (CEGER).

1.2. IDENTIFICAÇÃO DO DOCUMENTO

O presente documento de "Politica de Certificados do SCEE" (PCert) é identificado pelos dados constantes na tabela seguinte:

INFORMAÇÃO DO DOCUMENTO	
Versão do Documento	Versão 3.0
Estado do Documento	Aprovado
OID	2.16.620.1.1.1.2.1.3.0
Data de Emissão	19 de julho de 2015
Validade	Máximo 4 anos
Localização	http://www.scee.gov.pt/rep

Tabela 2 – Dados relativos à Politica de certificados do SCEE

1.3. PARTICIPANTES NA INFRA-ESTRUTURA DE CHAVES PÚBLICAS

1.3.1. ENTIDADES CERTIFICADORAS (EC)

São entidades que, após devida autorização da Entidade de Certificação Eletrónica do Estado (ECEE), depois da anuência do Conselho Gestor do SCEE, estão habilitadas para criar, assinar, atribuir e gerir certificados. Na prática uma EC é composta pelo conjunto de equipamentos, aplicações, pessoal e procedimentos indispensáveis para implementar os diversos serviços de certificação disponibilizados e garantir a adequada gestão do ciclo de vida dos certificados descritos neste documento.

A hierarquia de confiança da SCEE compreende a Entidade Certificadora Raiz do Estado (ECRaizEstado), as entidades certificadoras do Estado (ECEstado) e as entidades certificadoras subordinadas do Estado (SubECEstado).

Poderão ainda estabelecer-se relações hierárquicas de confiança por filiação na Entidade Certificadora Raiz do Estado de entidades de certificação públicas ou privadas que exerçam a sua atividade nos termos da legislação Nacional e Europeia em vigor.

As Entidades Certificadoras que compõem o SCEE são as previstas nos pontos 1.3.1.1 a 1.3.1.3 do presente documento.

1.3.1.1. A Entidade Certificadora Raiz do Estado (ECRaizEstado)

A ECRaizEstado é a entidade certificadora de topo da cadeia de certificação do SCEE, executora das políticas de certificados e diretrizes aprovadas pelo Conselho Gestor do SCEE. Compete a esta prestar os serviços de certificação às entidades certificadoras do Estado no nível hierárquico imediatamente inferior ao seu na cadeia de certificação, em conformidade com as normas aplicáveis às entidades certificadoras estabelecidas em Portugal na emissão de certificados digitais qualificados.

Os serviços de certificação digital disponibilizados pela ECRaizEstado englobam exclusivamente: o processo de registo das entidades certificadoras, geração de certificados e gestão do seu ciclo de vida, disseminação dos certificados, das políticas e das práticas de certificação, a gestão de revogações e disponibilização do estado/situação das mesmas.

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

O quadro seguinte apresenta os dados mais relevantes relativos aos certificados da ECRaizEstado, sendo de destacar a adoção emissão de dois certificados (pkcs1-

sha1WithRSAEncryption1 e Certificado pkcs1-sha256WithRSAEncryption) para o mesmo par de chaves.

DN	CN= ECRAIZESTADO; O=SCEE; C=PT
Certificado pkcs1-sha1WithRSAEncryption	
Número de série	42 ea 5b 0a 51 11 26 7c d8 27 74 b7 df 7f 71
Período de validade	23/6/2006 14:41:27 GMT até 23/6/2030 14:41:27
Impressão digital	39 13 85 3e 45 c4 39 a2 da 71 8c df b6 f3 e0 33 e0 4f ee 71
Certificado pkcs1-sha256WithRSAEncryption	
Número de série	14 7b c7 26 70 d6 3c d9 fa b7 72 77 e9 9c 9c
Período de validade	23/6/2006 17:43:01 GMT até 23/6/2030 14:41:27
Impressão digital	6b 87 64 3e b7 81 d4 3a 0b f9 4b b9 b6 fd b3 54 c0 cd 02 6a

Tabela 3 - Dados dos certificados da ECRaizEstado

A ECRaizEstado é a entidade certificadora de primeiro nível. A sua função é estabelecer a raiz da cadeia de confiança da infraestrutura de chaves públicas (PKI). Esta EC não emite certificados para utilizadores finais, emitindo apenas certificados para assinar as entidades certificadoras do Estado e as entidades filiadas. A ECRaizEstado assina-se a si própria, sendo ainda assinada por uma entidade

[1] O certificado pkcs1-sha1WithRSAEncryption é apenas publicado para efeitos de garantia de interoperabilidade, de modo a permitir que os sistemas e aplicações que não suportem o algoritmo pkcs1-sha256WithRSAEncryption, estejam habilitados para construir o caminho de certificação para validação de certificados e assinatura.

certificadora raiz de projeção mundial para efeitos de reconhecimento dos certificados emitidos no âmbito da SCEE.

1.3.1.2. Entidades certificadoras do Estado (ECEstado)

As ECEstado são entidades que se encontram no nível imediatamente abaixo da ECRaizEstado, sendo a sua função principal providenciar a gestão de serviços de certificação: emissão, operação, suspensão, revogação para os seus subscritores/titulares e SubECEstado que lhe estejam subordinadas. O seu certificado é assinado pela ECRaizEstado.

1.3.1.3. Entidades certificadoras subordinadas (SubECEstado)

As SubECEstado são entidades que se encontram nos níveis abaixo de uma ECEstado, tendo como função a prestação de serviços de certificação para os seus subscritores/titulares e SubECEstado que lhe estejam subordinadas. O seu certificado é assinado pela ECEstado ou SubECEstado de quem está subordinada.

As SubECEstado constituídas no âmbito do SCEE disponibilizam uma versão completa da sua Declaração de Práticas de Certificação (DPC).

1.3.2. ENTIDADES DE REGISTO (ER)

São entidades que por via do estabelecimento de acordo com uma ECEstado ou SubECEstado, estas delegam a prestação de serviços de identificação e registo de utilizadores, bem como a gestão de pedidos de revogação de certificados.

As ER desenvolvem a sua atividade de acordo com o estabelecido na DPC da EC delegante.

1.3.3. TITULARES DE CERTIFICADOS

1.3.3.1. Titulares

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

No âmbito do SCEE são considerados como titulares, aqueles cujo nome/designação 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 descrito no presente documentos, sendo consideradas as seguintes categorias de titulares:

a) Pessoa singular;

b) Pessoa coletiva;

c) Sistema ou equipamento tecnológico.

Não são considerados titulares, no âmbito deste documento, as seguintes categorias:

a) Entidades certificadoras, independentemente do nível a que se encontram;

b) Entidades de registo;

c) O pessoal das entidades certificadoras e ER, cujos certificados tem como uso exclusivo a operação dos respetivos sistemas.

1.3.3.2. Patrocinador

A emissão de certificados para pessoa coletiva, e sistema ou equipamento tecnológico (p.e: computador, firewall, router, servidor, etc.), deve ser efetuada sempre sob responsabilidade humana, sendo esta pessoa singular designada por patrocinador.

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

1.3.4. PARTES CONFIANTES

As partes confiantes ou destinatários são pessoas singulares, pessoas coletivas, ou sistemas/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 que o certificado corresponde na realidade a quem diz pertencer.

Na prática, considera-se uma parte confiante, aquela que confia no teor, validade e aplicabilidade do certificado, podendo ser titular de certificados da comunidade SCEE, ou não.

1.3.5. OUTROS PARTICIPANTES

1.3.5.1. O Conselho Gestor do Sistema de Certificação Electrónica do Estado

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.

Compete especialmente ao Conselho Gestor do SCEE:

a) Definir, de acordo com a lei e tendo em conta as normas ou especificações internacionalmente reconhecidas, a política de certificação e as práticas de certificação a observar pelas entidades certificadoras que integram o SCEE;

b) Garantir, tendo em conta a auditoria prevista na lei, que as declarações de práticas de certificação das várias entidades certificadoras do Estado, bem como da entidade certificadora raiz do Estado, estão em conformidade com a política de certificação do SCEE;

c) Propor os critérios para aprovação das entidades certificadoras que pretendam integrar o SCEE;

d) Aferir a conformidade dos procedimentos seguidos pelas entidades certificadoras do Estado com as políticas e práticas aprovadas, sem prejuízo das competências legalmente cometidas à Autoridade Credenciadora;

e) Pronunciar-se pela exclusão do SCEE das entidades certificadoras do Estado em caso de não conformidade com as políticas e práticas aprovadas, comunicando tal facto à Autoridade Credenciadora;

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

g) Representar institucionalmente o SCEE;

Compete, ainda, ao Conselho Gestor do SCEE, a promoção das atividades necessárias para o estabelecimento de acordos de interoperabilidade, com base em certificação cruzada, com outras infraestruturas de chaves públicas, de natureza privada ou pública, nacionais ou internacionais, nomeadamente:

h) Dar indicações à entidade certificadora raiz do Estado para a atribuição e a revogação de certificados emitidos com base em certificação cruzada;

i) Dar indicações à entidade certificadora raiz do Estado para a atribuição e a revogação de certificados emitidos com base em Entidades Filiadas;

j) Definir os termos e condições para o início, a suspensão ou a finalização dos procedimentos de interoperabilidade com outras infraestruturas de chaves públicas

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

1.3.5.2. Autoridade Credenciadora

De uma forma geral 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 neste documento e com o estabelecido na DPC da respetiva entidade.

Assim, consideram-se como principais atribuições as seguintes:

a) A coordenação e gestão de auditorias,

b) Validar a conformidade das DPC, face à PCert do SCEE;

c) A gestão do controlo de qualidade de todo o processo de certificação,

d) A fixação da procedimentos e documentação relativa às auditorias,

e) Gestão dos relatórios de auditoria, nomeadamente, na elaboração e receção (quando efetuados por pessoal externo);

f) A fixação de planos de medidas corretivas aplicáveis às entidades certificadoras do SCEE,

g) A fixação e acompanhamento de metas para estabelecer indicadores de qualidade, que deverá propor para aprovação do Conselho Gestor do SCEE no contexto de objetivos estratégicos previamente fixados pelo Conselho Gestor do SCEE

h) A gestão da bolsa de auditores;

i) A apresentação à ECEE de proposta de registo e de rescisão de registo de entidades certificadoras no SCEE;

j) A promoção da competência técnica dos auditores.

1.3.5.3. Autoridades de Validação

As Autoridades de Validação (AV), têm como função comprovar o estado dos certificados emitidos, através da utilização do protocolo 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 LCR.

1.3.5.4. Auditores de Segurança

O auditor de segurança é uma pessoa singular ou coletiva, de reconhecida idoneidade, experiência e qualificações comprovadas na área de sistemas de informação e de segurança de informação, devidamente credenciado pelo GNS para o efeito.

1.4. UTILIZAÇÃO DO CERTIFICADO

Os certificados emitidos no domínio do SCEE são utilizados, pelos diversos sistemas, aplicações, mecanismos e protocolos, com o objetivo de garantir os seguintes serviços de segurança:

a) Confidencialidade;

b) Integridade;

c) Autenticação;

d) Não-repúdio.

Estes serviços são obtidos com recurso à utilização de criptografia de chave pública, através da sua utilização na estrutura de confiança que o SCEE proporciona. Assim, os serviços de identificação, autenticação, integridade e não-repúdio são obtidos mediante a utilização de assinaturas digitais. A confidencialidade é garantida através dos recursos a algoritmos de cifra, quando conjugados com mecanismos de estabelecimento e distribuição de chaves.

Esta política engloba tipos e perfis de certificados, descritos sumariamente no quadro seguinte:

TIPO DE UTILIZAÇÃO	IDENTIFICADOR	OID	DESCRIÇÃO
Assinatura de Certificados e LCR	anyPolicy	2.5.29.32.0	ver Anexo A
Assinatura eletrónica	scee-assinatura	2.16.620.1.1.1.2.10	

Autenticação	scee-autenticacao	2.16.620.1.1.1.2.20	
Confidencialidade	scee-confidencialidade	2.16.620.1.1.1.2.30	

Tabela 4 – Perfis de certificados suportados pelo SCEE

1.4.1. UTILIZAÇÃO ADEQUADA

Os requisitos e regras definidos neste documento aplicam-se a todos os certificados emitidos pelas ECEstado e SubECEstado que forem constituídas como parte integrante do domínio do SCEE.

Os certificados atribuídos a pessoas, singulares e coletivas, têm como objetivos principais a sua utilização para efeitos de assinatura eletrónica, autenticação e encriptação.

Os certificados emitidos para sistemas e equipamentos tecnológicos, têm como objetivos principais a sua utilização em serviços de autenticação e autenticidade, e ainda no estabelecimento de comunicações seguras.

Os certificados emitidos para efeitos de confidencialidade, emitidos com base nas regras definidas no presente documento, podem ser utilizados com informação classificada até ao grau de RESERVADO, sobre redes públicas (p.e. Internet). A sua utilização restrita a redes privadas (proprietárias), o grau máximo de classificação da informação, deverá ser definido pela Autoridade Nacional de Segurança.

Os certificados emitidos pelo SCEE devem ser utilizados de acordo com a função e finalidade estabelecida nas Declaração de Práticas de Certificação e nas correspondentes Políticas de Certificados e de acordo com a lei em vigor.

1.4.2. UTILIZAÇÃO NÃO AUTORIZADA

Os certificados emitidos para os titulares não podem ser utilizados para desempenhar atividades como certificados de EC nem ER, consequentemente, não podem ser utilizados para assinar certificados nem LCR.

Os serviços de certificação prestados no âmbito do SCEE, não garantem o cumprimento de requisitos de alta disponibilidade e resiliência, que os qualifique para a sua utilização em serviços ou infraestruturas críticas, como as relacionadas com o funcionamento de instalações hospitalares, nucleares, controlo de tráfego aéreo, controlo de tráfego ferroviário, ou qualquer outra catividade onde uma falha possa levar à morte, lesões pessoais ou danos graves para o meio ambiente.

1.5. GESTÃO DAS POLÍTICAS

1.5.1. ENTIDADE RESPONSÁVEL PELA GESTÃO DO DOCUMENTO

A gestão do presente documento é da responsabilidade do Conselho Gestor do SCEE.

1.5.2. CONTATO

Nas DPC, devem ser incluídos, no mínimo, nome, morada, número de telefone e endereço de correio eletrónico da entidade responsável pela sua gestão.

A informação de contacto para este documento é a seguinte:

NOME	CONSELHO GESTOR DO SCEE
Morada:	Rua Professor Gomes Teixeira 350-265 Lisboa
Correio eletrónico:	scee@scee.gov.pt

Página Internet:	www.scee.gov.pt
Telefone	+ 351 213 927 600

Tabela 5 – Dados para contato

1.5.3. ENTIDADE QUE DETERMINA A CONFORMIDADE DA DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO (DPC) PARA A POLÍTICA

A Autoridade Credenciadora é o órgão competente para determinar a adequação das DPC das diversas entidades, com a presente PCert, tendo por base o processo de auditoria previsto neste documento.

1.5.4. PROCEDIMENTOS PARA APROVAÇÃO DA DPC

A gestão e aprovação da DPC das ECRaizEstado, ECEstado e SubECEstado do SCEE compete ao responsável máximo da respetiva EC.

É ainda responsável pela adequação documental necessária das Entidades Certificadoras Filiadas ao SCEE.

1.5.5. DEFINIÇÕES E ACRÓNIMOS

Ver Anexo D do presente documento.

2. RESPONSABILIDADE DE PUBLICAÇÃO E REPOSITÓRIO

2.1. REPOSITÓRIOS

Um repositório é o conjunto de equipamentos (*hardware* e *software*), pessoas e procedimentos, construído com o objetivo de publicar, entre outras, informação relativa às práticas adotadas e o estado dos certificados.

Neste ponto as entidades responsáveis pelas diversas DPC devem descriminar, no mínimo:

a) Níveis de disponibilidade;

b) Os protocolos de acesso;

c) Mecanismos de segurança implementados.

2.2. PUBLICAÇÃO DE INFORMAÇÃO DE CERTIFICAÇÃO

Todos os repositórios no domínio do SCEE deverão disponibilizar, no mínimo, a seguinte informação:

a) Uma cópia eletrónica do documento PCert, assinado eletronicamente, por indivíduo devidamente autorizado e com recurso a certificado digital;

b) Uma cópia eletrónica da sua DPC, assinada eletronicamente, por individuo devidamente autorizado e com recurso a certificado digital;

c) Listas de Certificados Revogados (LCR);

d) Lista de Certificados de Entidades Certificadoras Revogadas (LER), quando aplicável;

e) Documentação de suporte em formato acessível;

f) Qualquer outra informação relevante deverá ser de igual modo publicada.

As entidades integradas no domínio do SCEE deverão conservar todas as versões anteriores da PCert do SCEE e das suas DPC, disponibilizando-as a quem o solicite, desde que justificado, ficando, no entanto, fora do repositório público de acesso livre.

Os certificados para efeitos de confidencialidade serão os únicos certificados disponibilizados com acesso livre, no entanto, apenas e quando assim esteja estabelecido na respetiva DPC.

Quando se trate dos repositórios das EC, e caso tenham sido criadas EC subordinadas ou ER, à informação referida anteriormente deve ser adicionada a mesma informação relacionada com as suas subordinadas.

Este documento pode ser consultado no sítio da internet: http://www.scee.gov.pt/rep

2.3. PERIODICIDADE DE PUBLICAÇÃO

A informação incluída nos repositórios deverá ser disponibilizada logo que existam novas versões dos documento ou, informação atualizada.

No que concerne às LCR, a sua publicação não deverá em caso algum exceder 24 horas desde a data da sua aprovação/criação até a sua publicação em repositório.

Independentemente, de haver ou não informação atualizada, devem ser considerados, como prazos mínimos, para atualização da informação os seguintes:

DOCUMENTO	PRAZOS	
Políticas de certificados do SCEE	Até quatro (4) anos	
DPC	Anualmente	
Documentação de suporte	Anualmente	
Listas de certificados revogados	ECRaizEstado	6 meses

	ECEstado	1 mês
	SubECEstado	1 semana

Tabela 6 – Prazos mínimos para renovação da informação pelas diversas entidades

2.4. CONTROLO DE ACESSO AOS REPOSITÓRIOS

No acesso à informação contida nos repositórios deverá ser garantido que esta apenas é disponibilizada, apenas e só, em modo de leitura.

Devem ser implementados mecanismos de segurança de forma a garantir que apenas pessoas autorizadas possam escrever ou modificar a informação contida nos repositórios.

A atual política não estabelece nenhum tipo de restrição de acesso para consulta da LCRs, e ultimas versões das DPC e PCert do SCEE.

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

3.1. ATRIBUIÇÃO DE NOMES

No domínio SCEE é permitida a atribuição e utilização de nomes Reais, Pseudónimos e equipamentos.

3.1.1. TIPO DE NOMES

Todos os titulares de certificados requerem um nome único (DN – *Distinguished Name*) de acordo com o *standard X.500*.

Os certificados atribuídos a cada entidade deverão conter no campo "*Subject*", um DN, para utilização como identificador único de cada entidade, de acordo com o preconizado no RFC 5280, atualizado pelo RFC 6818, pelo que:

a) Para os certificados emitidos a pessoas, o atributo descreve a organização a que o titular do certificado pertence;

b) Nos certificados atribuídos a equipamentos, é inscrito o nome da organização responsável pela sua operação (patrocinador);

c) O DN deverá ser sempre preenchido.

O campo "*Subject*" deverá ser construído seguindo o descrito na tabela seguinte, sendo obrigatória a utilização dos seguintes atributos descritos em um, ou ambos os perfis indicados:

1 – Perfil A

ATRIBUTO	CÓDIGO	REGRAS PARA PREENCHIMENTO
CountryName	C	Incluir o código "PT"

OrganizationName	O	Este campo corresponde, regra geral, ao Ministério (ou equivalente) do titular do certificado
OrganizationUnitName	OU	Neste campo deverá constar informação relativa ao organismo (ou equivalente) a que o titular do certificado pertence
CommonName	CN	É proibida a utilização de "*nicknames*"
		Os equipamentos deverão ser identificados através do modelo e número de série
		Se os equipamentos forem servidores, estes serão designados pelo FQDN (CN = "FQDN".), sendo proibida a sua designação através do endereço IP
		Nos certificados emitidos para pessoa coletiva, deverá ser incluído o nome da pessoa singular responsável pela sua utilização
		Quando se trate de nomes reais, deverá corresponder com o nome que aparece identificado no documento de Identificação
		Quando se trate de pseudónimos, o nome deverá ser antecedido da expressão "Pseudo:"

Tabela 7 – Regras para o preenchimento do DN (Perfil A)

2 – Perfil B

ATRIBUTO	CÓDIGO	REGRAS PARA PREENCHIMENTO
CountryName	C	Incluir o código "PT".

OrganizationName	O	Neste campo deverá constar informação relativa ao organismo (ou equivalente) a que o titular do certificado pertence.
CommonName	CN	É proibida a utilização de "*nicknames*"
		Os equipamentos deverão ser identificados através do modelo e número de série.
		Se os equipamentos forem servidores, estes serão designados pelo FQDN (CN = "FQDN".), sendo proibida a sua designação através do endereço IP
		Nos certificados emitidos para pessoa coletiva, deverá ser incluído o nome da pessoa singular responsável pela sua utilização
		Quando se trate de nomes reais, deverá corresponder com o nome que aparece identificado no documento de Identificação
		Quando se trate de pseudónimos, o nome deverá ser antecedido da expressão "Pseudo:"

Tabela 8 – Regras para o preenchimento do DN (Perfil B)

3.1.2. NECESSIDADE DE NOMES SIGNIFICATIVOS

Os nomes utilizados dentro da cadeia de confiança do SCEE devem identificar de forma concreta e lógica a pessoa ou objeto a quem é atribuído um certificado digital.

As EC e ER devem garantir que a relação entre o titular e a organização a que pertencem é a mesma que consta no certificado e é facilmente percetível e identificável pelos Humanos.

3.1.3. ANONIMATO OU PSEUDÓNIMO DE TITULARES

Os titulares de certificados apenas podem optar pela utilização de pseudónimos. Neste caso o atributo "*CommonName"* do campo *"subject"* deverá começar pela identificação pela palavra "pseudo:", seguida do pseudónimo do titular (CN = pseudo: "qualquer cadeia de caracteres").

As entidades responsáveis pelo processo de registo podem recusar a aceitação de pseudónimos considerados ostensivos.

Não é permitida a utilização de titulares com base no conceito de anonimato.

3.1.4. INTERPRETAÇÃO DE FORMATO DE NOMES

As regras utilizadas pelo SCEE para interpretar o formato dos nomes dos certificados que emite são as contidas na norma ISO/IEC 9594-8.

Seguir o estabelecido no RFC 5280, atualizado pelo RFC 6818, para todos os atributos *DirectoryString* dos campos *issuer* e *subject* do certificado, devem ser codificados numa *UTF8String*, com exceção dos atributos *country* e *serialnumber*, que devem estar codificados numa *PrintableString*.

3.1.5. UNICIDADE DE NOMES

Os identificadores do tipo DN deverão ser únicos para cada titular de certificado, dentro de cada EC e não podem induzir a ambiguidades.

Poderão ser utilizados caracteres adicionais ao nome original de cada entidade de forma a assegurar a unicidade do campo.

As DPC deverão descrever de forma clara os critérios que utilizam para garantir a unicidade dos nomes.

3.1.6. RECONHECIMENTO, AUTENTICAÇÃO E FUNÇÕES DAS MARCAS REGISTADAS

As entidades requisitantes de certificados devem demonstrar que têm direito à utilização do nome requisitado.

Nas DPC devem estar explícitos os procedimentos utilizados para verificação do estipulado neste ponto.

3.2. VALIDAÇÃO DE IDENTIDADE NO REGISTO INICIAL

Nas DPC devem ser descritos todos os passos necessários, desde o início do pedido de certificado até à atribuição do certificado digital ao futuro titular.

3.2.1. MÉTODO DE COMPROVAÇÃO DA POSSE DE CHAVE PRIVADA

É considerado um mecanismo aceitável como método de comprovação da posse de chave privada a utilização do *Certificate Management Protocol* (CMP) definido no RFC 4210, atualizado pelo RFC 6712.

Pode ser permitida a utilização de outros métodos, desde que o Conselho Gestor do SCEE verifique que o método proposto é no mínimo tão seguro como o descrito anteriormente.

Nas DPC deve estar descrito de forma clara o método utilizado para garantir a comprovação da posse de chave privada

3.2.2. AUTENTICAÇÃO DA IDENTIDADE DE UMA PESSOA COLETIVA

Este processo é realizado de acordo com a legislação em vigor, para a emissão de certificados qualificados.

Nas DPC deve constar um exemplar do documento que serve de base ao registo do requerente.

3.2.3. AUTENTICAÇÃO DA IDENTIDADE DE UMA PESSOA SINGULAR

Este processo é realizado de acordo com a legislação em vigor, para a emissão de certificados qualificados.

Nas DPC deve constar um exemplar do documento que serve de base ao registo do requerente.

3.2.4. INFORMAÇÃO DE SUBSCRITOR/TITULAR NÃO VERIFICADA

Toda a informação descrita nos pontos 3.2.2 e 3.2.3 deve ser obrigatoriamente verificada.

As Entidades Certificadoras e as Entidades de Registo podem autorizar entidades privadas a tomar ações em nome de outras entidades, no entanto, tais autorizações estão geralmente associadas com regras particulares das instituições.

A autenticação das autorizações é uma parte formal do pedido de registo de certificado para entidades com personalidade jurídica.

Um certificado emitido é uma confirmação de que uma entidade legal é intitulada para utilizar uma chave privada em nome de outra entidade legal.

3.2.5. CRITÉRIOS PARA INTEROPERABILIDADE

Nos processos relativos a acordos de interoperabilidade, tendo por base certificação cruzada com Infraestruturas de Chaves Públicas externas, será analisada, no mínimo, a seguinte documentação:

a) A Política de Certificados;

b) O ultimo relatório de auditoria, demonstrando a total conformidade com o estabelecido na PC e na DPC;

c) Os parâmetros respeitantes a validação técnica da certificação cruzada;

O Conselho Gestor, agirá em conformidade com o estabelecido no documento "SCEE – Regulamento para a interoperabilidade", nos casos em que seja solicitado um pedido para acordo de interoperabilidade, com base em certificação cruzada.

3.2.6. CRITÉRIOS PARA FILIAÇÃO

Nos processos relativos a acordos de filiação será, analisada, no mínimo, a seguinte documentação do requerente:

a) A Politica de Certificados;

b) O último relatório de auditoria, demonstrando a total conformidade com o estabelecido na PCert do SCEE e na DPC.

Cabe à Autoridade Credenciadora nacional a análise referida supra, devendo propor a filiação ao Conselho Gestor do SCEE, mediante envio de relatório fundamentado.

Cabe ao Conselho Gestor aprovar os pedidos para filiação de entidade certificadora no SCEE, devendo, após a mesma, serem informadas todas as entidades certificadoras que integram o SCEE.

3.3. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDOS DE RENOVAÇÃO DE CHAVES

3.3.1. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA RENOVAÇÃO DE CHAVES, DE ROTINA

A identificação e autenticação para a renovação de certificados pode realizar-se utilizado os procedimentos para a autenticação e identificação inicial, ou utilizando pedidos assinados digitalmente, mediante o certificado original que se pretende renovar, sempre que este tenha expirado e não exista pedido para a sua revogação.

3.3.2. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA RENOVAÇÃO DE CHAVES, APÓS REVOGAÇÃO

A política de identificação e autenticação para a renovação de um certificado, depois deste ser revogado deve seguir as regras constantes no 3.2.2 e 3.2.3.

A renovação não deve ser concedida, se:

a) A revogação ocorreu porque o certificado foi emitido para uma pessoa que não a que está no "*Subject* "do certificado;

b) O certificado foi emitido sem autorização da pessoa que está indicada no "*Subject*;";

c) A entidade que aprovou o titular descobre que tem razões para acreditar que a informação dada para o certificado é falsa;

As DPC devem descrever de forma clara as regras utilizadas.

3.4. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDO DE REVOGAÇÃO

As regras de identificação para os pedidos de revogação poderão ser as mesmas que para o registo inicial.

Qualquer entidade integrada no domínio do SCEE pode solicitar a revogação de um determinado certificado, havendo conhecimento ou suspeita de compromisso da chave privada do titular ou qualquer outro ato que recomende esta ação.

As DPC devem descrever de forma clara as regras utilizadas.

4. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

4.1. PEDIDO DE CERTIFICADO

4.1.1. QUEM PODE SUBSCREVER UM PEDIDO DE CERTIFICADO

As DPC devem descrever de forma clara qual a comunidade que se aceita para subscrever um pedido de certificado.

4.1.2. PROCESSO DE REGISTO E RESPONSABILIDADES

O processo de registo para pedido de um certificado, deverá ser baseado pelo menos nas seguintes etapas:

a) Estabelecimento do registo inicial do requisitante, tal como definido no ponto 3.2 “Validação de identidade no registo inicial”;

b) Obtenção por parte do requisitante, do respetivo par de chaves, por cada certificado requisitado/solicitado;

c) Assinatura por parte do requisitante de um documento onde esteja especificado os termos e condições aplicáveis à utilização do certificado.

As DPC devem descrever detalhadamente o processo de registo utilizado, nomeadamente, a documentação necessária, bem como a identificação das funções e responsabilidades dos diversos participantes no referido processo.

4.2. PROCESSAMENTO DO PEDIDO DE CERTIFICADO

Este processo é realizado de acordo com a legislação em vigor, para a emissão de certificados qualificados.

As DPC devem descrever detalhadamente todo o processo.

4.2.1. PROCESSOS PARA A IDENTIFICAÇÃO E FUNÇÕES DE AUTENTICAÇÃO

Este processo é realizado de acordo com a legislação em vigor, para a emissão de certificados qualificados.

A DPC deve indicar como e quem efetua as tarefas de identificação e autenticação, bem como os mecanismos que dispõem.

4.2.2. APROVAÇÃO OU RECUSA DE PEDIDOS DE CERTIFICADO

A aprovação do certificado passa pelo cumprimento dos requisitos mínimos exigidos no ponto 4.2. Quando tal não se verifique, a entidade competente (EC ou ER) pode recusar a emissão do certificado.

Estes procedimentos, aceitação ou recusa, serão processados de acordo com os requisitos estipulados na respetiva DPC da entidade.

As DPC devem descrever detalhadamente todo o processo.

4.2.3. PRAZO PARA PROCESSAR O PEDIDO DE CERTIFICADO

Os pedidos de certificados serão processados sem atrasos, a partir do momento em que toda a documentação exigida, esteja na posse da entidade responsável pela emissão do certificado.

A DPC estabelece o prazo máximo necessário para o processamento dos pedidos de certificados.

4.3. EMISSÃO DE CERTIFICADO

4.3.1. PROCEDIMENTOS PARA A EMISSÃO DE CERTIFICADO

Este processo é realizado de acordo com a legislação em vigor, para a emissão de certificados qualificados.

A emissão do certificado por parte de uma EC do SCEE indica que todos os procedimentos até à emissão foram concluídos com sucesso.

Os procedimentos estabelecidos no presente ponto, são também aplicados aos casos de renovação de certificados, uma vez que implica a emissão de novos certificados.

Os procedimentos adotados devem garantir que para a emissão de certificados a EC:

a) Utiliza procedimentos de geração de certificados que vincula de forma segura, o certificado com a respetiva informação de registo (incluindo a chave publica certificada);

b) Depois de emitido o certificado, as notificações são efetuadas de acordo com estabelecido no ponto 4.3.2 do presente capítulo;

c) Todos os certificados iniciam a sua vigência no momento da sua emissão, com exceção dos casos em que se indique nos próprios uma data e hora para a entrada em vigor diferente (que nunca poderá ser posterior ao dia natural da sua emissão);

d) O período de validade do certificado está sujeito à extinção antecipada, temporal ou definitiva, quando se verificarem situações para a revogação ou suspensão.

As DPC devem descrever detalhadamente todo o processo, bem como a forma utilizada para entrega do certificado ao seu titular.

4.3.2. NOTIFICAÇÃO DA EMISSÃO DO CERTIFICADO AO TITULAR

No âmbito desta política, consideram-se como formas aceitáveis de notificação da emissão do certificado ao titular por parte da respetiva EC, as que se baseiam nas seguintes formas:

a) Envio do certificado diretamente à ER requisitante (quando aplicável);

b) Envio da informação necessária para que o titular possa descarregar o certificado de um sítio *Web* ou repositório;

c) Envio da informação necessária para que a ER respetiva possa descarregar o certificado de um sítio Web ou repositório (quando aplicável);

d) De forma presencial.

Em caso algum o futuro titular pode obter previamente o certificado sem o prévio procedimento de aceitação do mesmo.

Podem ser utilizadas outras formas de notificação para além das descritas anteriormente, desde que devidamente aprovadas pelo Conselho Gestor do SCEE e descritas na respetiva DPC.

4.4. ACEITAÇÃO DO CERTIFICADO

4.4.1. PROCEDIMENTOS PARA A ACEITAÇÃO DE CERTIFICADO

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

a) O titular toma conhecimento dos seus direitos e responsabilidades;

b) O titular toma conhecimento das funcionalidades e conteúdo do certificado;

c) O titular aceita formalmente sobre a aceitação do certificado e das suas condições de utilização assinando para o efeito, de forma manuscrita ou eletronicamente, o Termo de Responsabilidade do Titular;

No termo de responsabilidade do titular, devem constar, pelo menos, os procedimentos necessários em caso de, suspensão, revogação ou renovação do certificado, bem como os termos, condições e âmbito de utilização do mesmo.

A DPC deve estabelecer os mecanismos para verificar a aceitação do certificado por parte de titular.

4.4.2. PUBLICAÇÃO DO CERTIFICADO

As entidades certificadoras, na publicação/distribuição dos certificados, devem utilizar sistemas seguros que permitam a sua conservação e disponibilização, para efeitos de verificação, assegurando que:

a) Regra geral, a EC não publica o certificado do titular;

b) O certificado é disponibilizado, integralmente, ao titular para quem foi emitido, com os constrangimentos definidos no ponto 4.4.1;

c) O certificado só é publicamente disponibilizado com o consentimento do titular;

As DPC devem descrever detalhadamente todo o processo.

4.4.3. NOTIFICAÇÃO DA EMISSÃO DE CERTIFICADO A OUTRAS ENTIDADES

A Notificação da emissão de certificado pela EC respetiva é obrigatória apenas para o requisitante/titular do certificado. Se o pedido de certificado tiver como origem com recurso aos serviços de uma ER, esta entidade deverá ser notificada igualmente.

4.5. USO DO CERTIFICADO E PAR DE CHAVES

Dentro da comunidade do SCEE, a utilização dos certificados e respetiva chave privada, pelos diversos participantes, segue os seguintes constrangimentos:

a) A ECRaizEstado apenas emite certificados apenas para a ECEstado, EC externas e ao pessoal próprio, para efeitos de operação dos seus sistemas;

b) As ECEstado emitem certificados ao pessoal próprio, para efeitos de operação dos seus sistemas e, dependendo da forma como estão organizadas, emitem

certificados para o utilizador final (titulares) ou para SubECEstado.

As EC devem assegurar que a utilização da sua chave privada apenas é utilizada para assinar certificados e LCR. É ainda responsabilidade das EC, garantir que as chaves privadas atribuídas ao seu pessoal, para efeitos de operação do sistema, são utilizadas apenas e exclusivamente para esse fim.

4.5.1. USO DO CERTIFICADO E DA CHAVE PRIVADA PELO TITULAR

Os titulares de certificados utilizam 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) A quem estiver designado no campo "*Subject*" do certificado;

b) Depois de aceitar as condições definidas nos pontos 1.4.1 e 1.4.2;

c) Enquanto este se mantiver válido.

As DPC devem descrever o tipo de certificados emitidos e sua utilização, podendo estabelecer limitações adicionais.

4.5.2. USO DO CERTIFICADO E DA CHAVE PÚBLICA PELAS PARTES CONFIANTES

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

a) Ter conhecimento, bem como o entendimento da utilização e funcionalidades proporcionadas pela criptografia de chave pública e certificados.

b) Ser responsável pela sua correta utilização;

c) Ler e entender os termos e condições descritos nas Politicas e práticas de certificação;

d) Verificar os certificados (validação de cadeias de confiança) e LCR, tendo especial atenção às suas extensões marcadas como críticas e propósito das chaves;

e) Confiar nos certificados, utilizando-os sempre que estes estejam válidos;

4.6. RENOVAÇÃO DE CERTIFICADOS

A renovação de um certificado consiste no processo em que é efetuada emissão de um novo certificado e no qual é inscrito uma nova validade. Este processo utiliza os dados anteriores do certificado, não havendo alteração das chaves ou qualquer outra informação, com exceção do período de validade do novo certificado emitido.

Este processo levanta algumas reticências uma vez que a sua utilização é caracterizada pela perda de entropia das chaves, uma vez que não são gerados novos parâmetros, mas sim utilizados os já existentes.

Esta prática não é suportada no SCEE.

4.6.1. MOTIVOS PARA RENOVAÇÃO DE CERTIFICADO

Não aplicável.

4.6.2. QUEM PODE SUBMETER O PEDIDO DE RENOVAÇÃO DE CERTIFICADO

Não aplicável.

4.6.3. PROCESSAMENTO DO PEDIDO DE RENOVAÇÃO DE CERTIFICADO

Não aplicável.

4.6.4. NOTIFICAÇÃO DE EMISSÃO DE NOVO CERTIFICADO AO TITULAR

Não aplicável.

4.6.5. PROCEDIMENTOS PARA ACEITAÇÃO DE CERTIFICADO

Não aplicável.

4.6.6. PUBLICAÇÃO DE CERTIFICADO APÓS RENOVAÇÃO

Não aplicável.

4.6.7. NOTIFICAÇÃO DA EMISSÃO DO CERTIFICADO A OUTRAS ENTIDADES

Não aplicável.

4.7. RENOVAÇÃO DE CERTIFICADO COM GERAÇÃO DE NOVO PAR DE CHAVES

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

A emissão do certificado é feita de acordo com o estabelecido no ponto 4.3 do presente documento.

4.7.1. MOTIVOS PARA A RENOVAÇÃO DE CERTIFICADO COM GERAÇÃO DE NOVO PAR DE CHAVES

De forma geral, são considerados motivos válidos para a renovação de certificado com geração de novo par de chaves, sempre e quando que se verifique que:

a) O certificado esteja a expirar;

b) O suporte do certificado esteja expirar;

c) A informação do certificado sofra alterações.

As DPC devem descrever quais os motivos para a renovação de certificado com geração de novo par de chaves.

4.7.2. QUEM PODE SUBMETER O PEDIDO DE CERTIFICAÇÃO DE UMA NOVA CHAVE PÚBLICA

A submissão do pedido de certificação é válida para titulares com certificados em vigor.

4.7.3. PROCESSAMENTO DO PEDIDO DE RENOVAÇÃO DE CERTIFICADO COM GERAÇÃO DE NOVO PAR DE CHAVES

As DPC devem descrever os processos para os pedidos de renovação, identificando os diferentes cenários e os respetivos requisitos.

4.7.4. NOTIFICAÇÃO DA EMISSÃO DE NOVO CERTIFICADO AO TITULAR

De acordo com os critérios especificados para a emissão inicial de certificados.

4.7.5. PROCEDIMENTOS PARA ACEITAÇÃO DE UM CERTIFICADO RENOVADO COM GERAÇÃO DE NOVO PAR DE CHAVES

A receção do certificado renovado, por si só, apenas serve como confirmação da aceitação do mesmo.

As DPC devem descrever de forma clara os procedimentos adotados, no entanto, podem ser estabelecidos requisitos mais restritivos.

4.7.6. PUBLICAÇÃO DE NOVO CERTIFICADO RENOVADO COM GERAÇÃO DE NOVO PAR DE CHAVES

De acordo com os critérios especificados para a emissão inicial de certificados.

4.7.7. NOTIFICAÇÃO DA EMISSÃO DE NOVO CERTIFICADO A OUTRAS ENTIDADES

De acordo com os critérios especificados para a emissão inicial de certificados.

4.8. MODIFICAÇÃO DE CERTIFICADOS

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

Esta prática é suportada pela SCEE com restrições, nomeadamente, na informação sujeita a alterações não está contemplada a alteração da validade inicial do certificado.

Os procedimentos descritos nos seguintes parágrafos, relativos à alteração de certificados, estão sujeitas às mesmas regras definidas para os pedidos de certificado em conformidade com o disposto no ponto 4.1.

4.8.1. MOTIVOS PARA ALTERAÇÃO DE CERTIFICADO

De acordo com o ponto 4.8 da presente PCert.

4.8.2. QUEM PODE SUBMETER O PEDIDO DE ALTERAÇÃO DE CERTIFICADO

De acordo com o ponto 4.8 da presente PCert.

4.8.3. PROCESSAMENTO DO PEDIDO DE ALTERAÇÃO DE CERTIFICADO

De acordo com o ponto 4.8 da presente PCert.

4.8.4. NOTIFICAÇÃO DA EMISSÃO DE CERTIFICADO ALTERADO AO TITULAR

De acordo com o ponto 4.8 da presente PCert.

4.8.5. PROCEDIMENTOS PARA ACEITAÇÃO DE CERTIFICADO ALTERADO

De acordo com o ponto 4.8 da presente PCert.

4.8.6. PUBLICAÇÃO DO CERTIFICADO ALTERADO

De acordo com o ponto 4.8 da presente PCert.

4.8.7. NOTIFICAÇÃO DA EMISSÃO DE CERTIFICADO ALTERADO A OUTRAS ENTIDADES

De acordo com o ponto 4.8 da presente PCert.

4.9. SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO

A suspensão e revogação de certificados são mecanismos a utilizar quando por algum motivo os certificados deixam de ser fiáveis, antes do período de finalização originalmente previsto.

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

Os certificados suspensos podem recuperar a sua validade, enquanto os certificados depois de revogados não podem voltar a ser válidos, terminando deste modo o seu ciclo de vida.

4.9.1. MOTIVOS PARA A REVOGAÇÃO

Os certificados devem ser revogados, sempre que se verifiquem as seguintes situações:

a) Roubo, extravio, destruição ou deterioração do dispositivo de suporte dos certificados;

b) Incapacidade ou falecimento do titular;

c) Inexatidões nos dados fornecidos;

d) O certificado estar suspenso por um período alargado;

e) Comprometimento ou suspeita de comprometimento das chaves privada do titular;

f) Comprometimento ou suspeita de comprometimento da senha (exemplo: PIN);

g) Comprometimento ou suspeita de comprometimento das chaves privada da EC;

h) Incumprimento por parte da EC ou titular das responsabilidades prevista na DPC;

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

j) Por resolução judicial ou administrativa;

k) Por vontade do próprio.

As DPC devem estabelecer de forma detalhada as causas passíveis para revogação do certificado.

4.9.2. QUEM PODE SUBMETER O PEDIDO DE REVOGAÇÃO

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

a) O titular do certificado;

b) O responsável por um certificado emitido para produtos de tecnologia de informação;

c) Uma parte confiante, sempre que demonstre que o certificado foi utilizado com fins diferente dos previstos;

d) A EC ou ER;

e) O Conselho Gestor do SCEE;

f) A Autoridade Credenciadora.

As DPC devem descrever as entidades a quem é permitido submeter o pedido de revogação.

4.9.3. PROCEDIMENTO PARA O PEDIDO DE REVOGAÇÃO

De modo geral os procedimentos mínimos a ter em conta para um pedido de revogação serão os seguintes:

a) Qualquer pedido de revogação deve ser sempre autenticado e autorizado;

b) Todos os pedidos de revogação devem ser endereçados para a EC ou ER respetiva;

c) Os pedidos podem ser efetuados por escrito ou por um processo *online* (CMP) seguro;

d) Qualquer pedido, desde que autenticado, deve ficar registado e arquivado;

e) Sempre que um certificado for revogado, deve ficar documentado juntamente com uma descrição exaustiva do motivo da revogação, nomeadamente:

   i. data do pedido de revogação;

   ii. nome do titular do certificado (o assinante);

iii. exposição pormenorizada dos motivos para o pedido de revogação;

iv. nome e funções da pessoa que solicita a revogação;

v. informação de contacto da pessoa que solicita a revogação;

vi. assinatura da pessoa que solicita a revogação.

f) Sempre que for revogado um certificado de um titular, a revogação deve ser publicada na respetiva LCR.

As DPC devem estabelecer de forma detalhada os procedimentos utilizados para o pedido de revogação de certificados.

4.9.4. PRODUÇÃO DE EFEITOS DA REVOGAÇÃO

A revogação será efetuada de forma imediata e após terem sido efetuados todos os procedimentos, bem como seja verificado que o pedido é válido, pois o mesmo não pode ser anulado.

4.9.5. PRAZO PARA PROCESSAR O PEDIDO DE REVOGAÇÃO

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

4.9.6. REQUISITOS DE VERIFICAÇÃO DA REVOGAÇÃO PELAS PARTE CONFIANTES

Antes de utilizarem um certificado, as partes confiantes tem como responsabilidade verificar o estado de todo os certificados, através das LCR ou num servidor de verificação do estado *online*, via OCSP.

4.9.7. PERIODICIDADE DA EMISSÃO DA LISTA DE CERTIFICADOS REVOGADOS (LCR)

As EC deverão publicar uma nova LCR no repositório, sempre que haja uma revogação. Quando não existam alterações ao estado de validade dos certificados,

ou seja, se nenhuma revogação se tiver produzido as várias entidades deverão disponibilizar nova informação de revogação nos seguintes limites máximos:

a) Para as EC que emitam certificados de utilizador final, as LCR serão disponibilizadas a cada 24 Horas;

b) Para as EC que não emitam certificados de utilizador final, as LCR serão disponibilizadas a cada 6 meses;

As DPC devem estabelecer de forma detalhada a periodicidade utilizada para emissão das LCR.

4.9.8. PERÍODO MÁXIMO ENTRE A EMISSÃO E A PUBLICAÇÃO DA LCR

Conforme o descrito no ponto 4.9.7.

4.9.9. DISPONIBILIDADE DE VERIFICAÇÃO ONLINE DO ESTADO / REVOGAÇÃO DE CERTIFICADO

As DPC deverão estabelecer se dispõem, e em que condições, de serviços de validação do estado dos certificados de forma *online* (OCSP).

4.9.10. REQUISITOS DE VERIFICAÇÃO ONLINE DE REVOGAÇÃO

No caso de serem utilizadas as AV, as partes confiantes deverão dispor de *software* capaz de operar o protocolo OCSP, de forma a obter a informação sobre o estado do certificado.

4.9.11. OUTRAS FORMAS DISPONÍVEIS PARA DIVULGAÇÃO DE REVOGAÇÃO

Não estabelecido.

4.9.12. REQUISITOS ESPECIAIS EM CASO DE COMPROMETIMENTO DE CHAVE PRIVADA

Apenas quando se trate do comprometimento da chave privada. Neste caso deverão ser adotados os procedimentos descritos no ponto 5.7.3 do presente documento.

4.9.13. MOTIVOS PARA SUSPENSÃO

As DPC deverão definir os motivos e identificar as causas em que se aplica a suspensão do certificado em detrimento da revogação.

4.9.14. QUEM PODE SUBMETER O PEDIDO DE SUSPENSÃO

A estabelecer na DPC.

4.9.15. PROCEDIMENTOS PARA PEDIDO DE SUSPENSÃO

A estabelecer na DPC.

4.9.16. LIMITE DO PERÍODO DE SUSPENSÃO

A estabelecer na DPC.

4.10. SERVIÇOS SOBRE O ESTADO DO CERTIFICADO

4.10.1. CARACTERÍSTICAS OPERACIONAIS

Caso seja adotado algum serviço para além das LCR, será um serviço de validação *online*, com implementação do protocolo OCSP, de acordo com o estipulado no RFC 6960.

4.10.2. DISPONIBILIDADE DE SERVIÇO

Salvo causa justificada, a disponibilidade do serviço será contínua (24 horas, todos os dias do ano).

4.10.3. CARACTERÍSTICAS OPCIONAIS

Para usufruir do serviço de validação *online*, as partes confiantes deverão dispor de um cliente OCSP que cumpra o RFC 6960.

4.11. FIM DE SUBSCRIÇÃO

O fim da operacionalidade de um certificado acontece quando se verificarem uma das seguintes situações previstas na RFC 3647.

As DPC devem estabelecer de forma detalhada os procedimentos a adotar.

4.12. RETENÇÃO E RECUPERAÇÃO DE CHAVES (*KEY ESCROW*)

4.12.1. POLÍTICAS E PRÁTICAS DE RECUPERAÇÃO DE CHAVES

Apenas é autorizada a retenção de chaves, nos seguintes casos:

a) Chaves privadas das EC;

b) Chaves para efeitos de confidencialidade.

Em ambos os casos apenas é permitido a realização desta operação, no mínimo por duas pessoas.

As políticas e práticas de recuperação fazem parte integral da DPC da entidade.

4.12.2. POLÍTICAS E PRÁTICAS DE ENCAPSULAMENTO E RECUPERAÇÃO DE CHAVES DE SESSÃO.

Não estipulado.

5. MEDIDAS DE SEGURANÇA FÍSICA, DE GESTÃO E OPERACIONAIS

5.1. MEDIDAS DE SEGURANÇA FÍSICA

Todos os aspetos relacionados com as medidas de segurança física exigidas às instalações onde operam as EC do SCEE estão definidas em norma própria da Autoridade Credenciadora, nomeadamente, no GNS/NT-D-02.

5.1.1. LOCALIZAÇÃO FÍSICA E TIPO DE CONSTRUÇÃO

Conforme descrito no ponto 5.1.

As DPC devem materializar as medidas adotadas.

5.1.2. ACESSO FÍSICO AO LOCAL

Conforme descrito no ponto 5.1.

As DPC devem materializar as medidas adotadas.

5.1.3. ENERGIA E AR CONDICIONADO

Conforme descrito no ponto 5.1.

As DPC devem materializar as medidas adotadas.

5.1.4. EXPOSIÇÃO À ÁGUA

Conforme descrito no ponto 5.1.

As DPC devem materializar as medidas adotadas.

5.1.5. PREVENÇÃO E PROTECÇÃO CONTRA INCÊNDIO

Conforme descrito no ponto 5.1.

As DPC devem materializar as medidas adotadas.

5.1.6. SALVAGUARDA DE SUPORTES DE ARMAZENAMENTO

Os suportes de informação sensível deverão ser armazenados, de forma segura, em cofres e de acordo com o tipo de suporte e classificação da informação. O acesso a estas zonas deve ser restrito a pessoas devidamente autorizadas.

5.1.7. ELIMINAÇÃO DE RESÍDUOS

A eliminação de suportes magnéticos, óticos e informação em papel, deve ser realizada de forma segura, seguindo os procedimentos estabelecidos para este fim, recorrendo a processos de desmagnetização, de esterilização e de destruição ou triturando em função do tipo de suporte a tratar.

Periféricos criptográficos devem ser destruídos de acordo com as recomendações dos respetivos fabricantes.

5.1.8. INSTALAÇÕES EXTERNAS (ALTERNATIVA) PARA RECUPERAÇÃO DE SEGURANÇA

Todas as cópias de segurança (e.g., base de dados, programas, *file system*,) devem ser colocadas em *site* remoto que será geograficamente separado do site primário.

As condições de segurança do *site* remoto deverão ser idênticas ou superiores ao estipulado para o local primário.

O acesso é restrito apenas ao pessoal autorizado.

5.2. MEDIDAS DE SEGURANÇA DOS PROCESSOS

Os sistemas de informação e os serviços disponibilizados pelas várias EC que integram o SCEE devem ser operados de forma controlada.

5.2.1. FUNÇÕES DE CONFIANÇA

As funções de confiança a estabelecer deverão estar em conformidade com os requisitos definidos na legislação nacional para a emissão de certificados qualificados.

Nas funções de confiança está incluído todo o pessoal com acesso aos sistemas de certificação das EC e que na prática podem materialmente afetar:

a) Manipulação de informações de subscritor e validação de informação de emissão de Certificado;

b) Funções do ciclo de vida dos certificados;

c) Configuração e manutenção dos sistemas de certificação.

No âmbito da sua estrutura organizativa são consideradas funções de confiança as descritas a seguir, estando divididas e diferenciadas pela natureza da sua catividade, quer se trate das *software* para certificação digital, quer se trate das funções relacionadas com o dispositivo seguro para criação de assinaturas. A cada uma delas são cometidas as seguintes responsabilidades consoante o âmbito.

5.2.1.1. *Software* para certificação digital

a) Administrador de Segurança (AdmSeg), responsáveis segurança global dos sistemas, nomeadamente, pela gestão e implementação das regras e práticas de segurança;

b) Administrador de registo (AdmReg), responsáveis pela aprovação da emissão, suspensão e revogação de certificados de titulares;

c) Administrador de Sistemas (AdmSist), responsáveis pela instalação, configuração e manutenção dos sistemas, no entanto, com acesso controlado às configurações relacionadas com a segurança;

d) Operador de Sistemas (OpSist), responsáveis pela operação de rotina dos sistemas, estando autorizados a realizar as cópias de segurança e sua recuperação;

e) Auditor de Sistemas (AuditorS), responsáveis pela análise da catividade do sistema, estão autorizados a ver e monitorizar os arquivos de catividade dos sistemas.

As DPC devem descrever em detalhe as responsabilidades inerentes a cada função.

5.2.1.2. Dispositivo seguro para criação de assinaturas

a) Administradores do HSM (AdmHSM), responsáveis pela segurança das chaves;

b) Operadores do HSM (OpHSM), autorizados a utilizarem as chaves.

As DPC devem descrever em detalhe as responsabilidades inerentes a cada função.

5.2.2. NÚMERO DE PESSOAS EXIGIDAS POR TAREFA

As seguintes tarefas/ações/atividade requerem o mínimo a presença 2 pessoas em simultâneo:

a) Qualquer acesso à ZAS;

b) Geração das chaves da EC;

c) Configuração dos perfis para o desempenho das funções de confiança;

d) Manutenção e atualização dos sistemas dos sistemas;

e) Recuperação de chaves para efeitos de confidencialidade;

f) Recuperação das chaves da EC.

As DPC devem descrever em detalhe a metodologia e o número de pessoas por tarefa adotada.

5.2.3. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA CADA FUNÇÃO

Todos os utilizadores autorizados devem identificar-se, preferencialmente, através de certificados digitais emitidos pela própria EC.

No caso dos HSM são empregues as técnicas de segredo partilhado.

As DPC devem descrever em detalhe os mecanismos adotados.

5.2.4. FUNÇÕES QUE REQUEREM SEPARAÇÃO DE RESPONSABILIDADES

De acordo com o descrito no quadro seguinte:

	AdmSeg	AdmReg	AdmSist	OpSist	AuditorS	AdmHSM *	opHSM *
AdmSeg			×		×		
AdmReg					×		
AdmSist	×				×		
OpSist							
AuditorS	×	×	×			×	×
AdmHSM *					×		
OpHSM. *					×		

NOTAS

× – As funções assinaladas são incompatíveis;

*– Estas funções não são obrigatoriamente requeridas pela legislação, nem necessárias a todas as entidades certificadoras, podendo no entanto ser necessárias em casos específicos.

Tabela 9 – Incompatibilidade entre funções

5.3. MEDIDAS DE SEGURANÇA DE PESSOAL

As DPC devem descrever em detalhe os requisitos adotados nas diversas secções, no entanto, a EC deve garantir que o pessoal com funções de confiança cumpre os seguintes requisitos mínimos:

a) Nomeado formalmente para a função;

b) Ter recebido formação e treino adequado para o desempenho da respetiva função;

c) Garantir que o funcionário (p.e: contrato, estatuto próprio, etc.), não revela informação sensível sobre a EC ou dados de identificação dos titulares;

d) Garantir que o funcionário, (p.e: contrato, estatuto próprio, etc.), conhece os termos e condições para o desempenho da respetiva função;

e) Garantir que o funcionário não desempenha funções que possam causar conflito com as suas responsabilidades nas atividades da EC.

5.3.1. REQUISITOS RELATIVOS ÀS QUALIFICAÇÕES, EXPERIÊNCIA, ANTECEDENTES E CREDENCIAÇÃO

O pessoal que desempenha funções nas EC deve possuir suficientes qualificações para o desempenho da função.

5.3.2. PROCEDIMENTOS 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 credenciação vária tendo em conta a função de confiança e o tipo de EC onde se desenvolvem as atividades.

O grau de credenciação mínimo de segurança[2] exigido está descrito no quadro seguinte:

	ECRAIZESTADO	ECESTADO	SUBECESTADO	ERESTADO
AdmSeg	Confidencial	Confidencial	Confidencial	Confidencial
AdmReg	Confidencial	Confidencial	Confidencial	Confidencial
AdmSist	Confidencial	Confidencial	Confidencial	Confidencial
OpSist	Confidencial	Confidencial	Confidencial	Confidencial
AuditorS	Confidencial	Confidencial	Confidencial	Confidencial
AdmHSM	Confidencial	Confidencial	Confidencial	Confidencial
OpHSM.	Confidencial	Confidencial	Confidencial	Confidencial

Tabela 10 – Credenciação de segurança

5.3.3. REQUISITOS DE FORMAÇÃO E TREINO

Os elementos com cargos que desempenhem atividades nas várias EC devem estar sujeitos a um plano de formação e treino, englobando os seguintes tópicos:

a) Certificação digital e Infraestruturas de Chave Publica;

b) Conceitos gerais sobre segurança da informação;

c) Formação específica para o seu posto;

d) Funcionamento do *software* e/ou *hardware* usado pela EC;

e) Política de Certificados e Declaração de Práticas de Certificação;

f) Recuperação face a desastres;

g) Procedimentos de continuidade da atividade;

h) Aspetos legais básicos relativos à prestação de serviços de certificação.

[2] Resolução do Conselho de Ministros n.º 50/88 (SEGNAC 1), Capitulo 4

5.3.4. FREQUÊNCIA E REQUISITOS PARA ACÇÕES DE RECICLAGEM

Sempre que existe qualquer alteração tecnológica, introdução de novas ferramentas ou modificação de procedimentos, dever levar-se a cabo a adequada formação para todo o pessoal afeto às EC.

Sempre que sejam levadas a cabo alterações nas Politicas de Certificação ou Declaração de Práticas de Certificação devem ser realizadas sessões formativas aos elementos das EC.

5.3.5. FREQUÊNCIA E SEQUÊNCIA DA ROTAÇÃO DE FUNÇÕES

Não é definido nenhum plano de rotação na atribuição de tarefas ao pessoal das EC, contudo, sempre que alguma EC o faça, deve materializar de forma clara a forma como esta rotação é realizada.

5.3.6. SANÇÕES PARA ACÇÕES NÃO AUTORIZADAS

No caso da realização de ações não autorizadas respeitantes às EC, devem ser tomadas as medidas disciplinares adequadas.

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.

Se for realizada alguma infração, a EC suspenderá o acesso a todos os sistemas de EC, de forma imediata, às pessoas envolvidas com o conhecimento destes.

Adicionalmente, em função da gravidade da infração cometida, devem aplicar-se as sanções previstas na lei geral da função pública, das organizações ou entidades em causa.

5.3.7. CONTRATAÇÃO DE PESSOAL

O pessoal contratado para exercer cargos relacionados com funções de confiança de qualquer parte da EC ou ER, está sujeito aos mesmos critérios que um funcionário dos quadros da própria organização e é credenciado de acordo com o especificado no ponto 5.3.2 do presente documento.

5.3.8. DOCUMENTAÇÃO FORNECIDA AO PESSOAL

Ao pessoal com cargos nas várias EC deve ser disponibilizado, no mínimo, os seguintes documentos:

a) Política de Certificados;

b) Declaração de Práticas de Certificação;

c) Documento com a descrição das responsabilidades, obrigações e tarefas para a respetiva função;

d) Documentação técnica sobre o *software* e *hardware* da EC.

5.4. PROCEDIMENTOS DE AUDITORIA DE SEGURANÇA

5.4.1. TIPO DE EVENTOS REGISTADOS

As EC devem registar, entre outros, os eventos especificado no documento CWA 14167-1, sendo obrigatório o registo dos seguintes:

a) Ligar e desligar os servidores;

b) Tentativas com sucesso ou fracassadas de alteração dos parâmetros de segurança do sistema operativo;

c) Tentativas com sucesso ou fracassadas de criar, modificar, apagar contas do sistema;

d) Ligar e desligar as aplicações e sistemas utilizados para a catividade de certificação;

e) Tentativas com sucesso ou fracassadas de início e fim de sessão;

f) Tentativas com sucesso ou fracassadas das operações relativas ao pedido, emissão, renovação, modificação e revogação chaves e certificados;

g) Tentativas com sucesso ou fracassadas de gerar ou emitir LCR;

h) Tentativas com sucesso ou fracassadas de criar, modificar ou apagar informação dos titulares dos certificados;

i) Tentativas com sucesso ou fracassadas de acesso às ZAS da EC;

j) Cópias de segurança, recuperação ou arquivo dos dados;

k) Alterações ou atualizações de *software* e *hardware*;

l) Manutenção do sistema;

m) Mudança de pessoal.

O registo dos eventos, efetuado com recurso a meios automáticos e/ou manuais, devem conter, pelo menos, a data e hora do evento, bem como a identificação da entidade causadora do evento.

Os eventos registados devem ser especificados na respetiva DPC.

5.4.2. FREQUÊNCIA DA AUDITORIA DE REGISTOS

A auditoria dos registos deve ser realizada com uma frequência mínima de 3 meses, no caso de a EC ser do tipo *offline* e semanal, se a EC for do tipo *online*. Todos os eventos significativos devem ficar registados num relatório sumário de análise de eventos. Cada EC deve declarar na sua DPC a frequência com que auditoria de registos é implementada e quais os tipos de eventos considerados como significativos e que justificam a sua inclusão no Relatório Sumário de Análise de Eventos (RSAE).

5.4.3. PERÍODO DE RETENÇÃO DOS REGISTOS DE AUDITORIA

As EC deverão guardar os registos de auditoria nos sistemas por um período mínimo de 12 meses. Depois de arquivados, os registos de auditoria devem ser conservados por um período mínimo de 20 anos.

Nas DPC deve ser especificado quais os períodos adotados para a retenção dos registos de auditoria.

5.4.4. PROTECÇÃO DOS REGISTOS DE AUDITORIA

Os registos de auditoria devem estar protegidos contra acessos não autorizados, alteração e destruição.

Por regra, os registos eletrónicos devem estar protegidos com recurso a técnicas criptográficas, para que ninguém, com exceção das próprias aplicações de visualização de registos, com o controlo de acessos adequado, possa aceder aos mesmos.

Os registos manuais devem ser armazenados em local, que cumpra os requisitos definidos anteriormente, dentro das instalações seguras das EC.

A destruição de um arquivo de auditoria só pode ser levado a cabo com a autorização do Administrador de Sistema, Administrador de Segurança e Auditor de Sistemas. Esta destruição só pode proceder-se por recomendação escrita de qualquer dos três elementos.

Os registos de auditoria são considerados informação sensível como especificado no ponto 9.4 do presente documento.

5.4.5. PROCEDIMENTOS PARA A CÓPIA DE SEGURANÇA DOS REGISTOS

Devem ser realizadas cópias de segurança dos registos de auditoria bem como dos RSAE.

As DPC devem descrever os mecanismos adotados para efetuar as cópias de segurança dos registos e RSAE.

5.4.6. SISTEMA DE RECOLHA DE DADOS DE AUDITORIA (INTERNO/EXTERNO)

O sistema de recolha dos dados de auditoria deve ser uma combinação de processos automáticos e manuais executados pelos sistemas operativos, pelas aplicações das EC e pelo pessoal que as opera.

As DPC devem descrever de forma clara o procedimento para este sistema.

5.4.7. NOTIFICAÇÃO DE AGENTES CAUSADORES DE EVENTOS

Não está contemplada qualquer notificação. As DPC, caso implementem notificações, devem descrever o método e as pessoas/sistemas alvo de notificação.

5.4.8. AVALIAÇÃO DE VULNERABILIDADES

Não havendo alterações significativas no ambiente global da EC deve ser efetuada pelo menos uma vez por ano uma avaliação das vulnerabilidades.

O resultado da análise deve ser reportado ao responsável da EC para rever e aprovar, caso se justifique, um plano de implementação e correção das vulnerabilidades detetadas.

5.5. ARQUIVO DE REGISTOS

5.5.1. TIPO DE DADOS ARQUIVADOS

As EC devem arquivar, no mínimo, os seguintes tipos de dados:

a) Os registos de auditoria especificados no ponto 5.4 do presente documento;

b) As cópias de segurança dos sistemas que compõem a infraestrutura da EC;

c) Documentação relativa ao ciclo de vida dos certificados.

d) Chaves para efeitos de confidencialidade (quando aplicável);

e) Contratos estabelecidos entre a EC e outras entidades.

Nas DPC devem estar especificados o tipo de dados sujeitos a arquivos.

5.5.2. PERÍODO DE RETENÇÃO EM ARQUIVO

Os dados sujeitos a arquivo são retidos por um período mínimo de 20 anos.

5.5.3. PROTECÇÃO DOS ARQUIVOS

De acordo com o disposto no ponto 5.4.4 do presente documento.

5.5.4. PROCEDIMENTOS PARA AS CÓPIAS DE SEGURANÇA DO ARQUIVO

De acordo com o disposto no ponto 5.4.5 do presente documento.

5.5.5. REQUISITOS PARA VALIDAÇÃO CRONOLÓGICA DOS REGISTOS

Os registos arquivados são certificados por assinatura eletrónica qualificada com validação cronológica que liga criptograficamente os dados com os valores de tempo.

Assim, os sistemas de informação utilizados pelas EC devem garantir o registo da data e hora do momento, tendo por base uma fonte de tempo segura.

Os sistemas da EC devem estar sincronizados entre si e as fontes de tempo utilizadas, devem-se calibrar automaticamente, devendo ser utilizada com referência a fonte de tempo do Observatório Astronómico de Lisboa (http://www.oal.ul.pt).

5.5.6. SISTEMA DE RECOLHA DE DADOS DE ARQUIVO (INTERNO/EXTERNO)

De acordo com o disposto no ponto 5.4.6 do presente documento.

5.5.7. PROCEDIMENTOS DE RECUPERAÇÃO E VERIFICAÇÃO DE INFORMAÇÃO ARQUIVADA

Só o pessoal devidamente autorizado deve ter acesso aos arquivos.

As EC devem verificar a integridade da informação arquivada a cada 12 meses, de forma a garantir que os mesmos se encontram em bom estado e que podem ser recuperados.

As EC devem garantir a capacidade para realizar verificações de integridade dos arquivos eletrónicos na altura da sua criação. No caso de erros ou comportamentos imprevistos, deve ser criado um evento de segurança e ser criado novo arquivo para o efeito.

As DPC devem descrever de forma clara os mecanismos utilizados.

5.6. RENOVAÇÃO DE CHAVES

Apenas os titulares de certificados válidos podem requerer a renovação do respetivo par de chaves.

As DPC devem descrever de forma clara os processos utilizados para a renovação de certificado com geração de novo par de chaves (*re-key*), bem como os prazos mínimos exigidos para iniciar o processo de renovação.

5.7. RECUPERAÇÃO EM CASO DE DESASTRE OU COMPROMETIMENTO

As DPC de cada EC deverão indicar, no caso de indisponibilidade das instalações da Entidade Certificadora, qual o tempo máximo para esta indisponibilidade antes de ser ativado o Plano de Continuidade de Serviço da respetiva EC.

O Plano de Continuidade deverá garantir que os serviços indicados como críticos pela sua necessidade de disponibilidade estão disponíveis no Local Alternativo, devendo a DPC indicar o tempo máximo para ativação dos serviços.

5.7.1. PROCEDIMENTOS EM CASO DE INCIDENTE OU COMPROMETIMENTO

As EC devem estabelecer procedimentos de contingência para as EC e ER subordinadas, estabelecendo as etapas necessárias, de modo a dar continuidade à sua catividade em caso de incidentes, nomeadamente, corrupção ou perda dos dados, *software* e equipamentos.

Se as EC subcontratarem alguns serviços, as EC garantem que os requisitos anteriores são acautelados e estabelece, obrigatoriamente, um contrato escrito com as provisões necessárias.

As DPC devem descrever os procedimentos adotados.

5.7.2. CORRUPÇÃO DOS RECURSOS INFORMÁTICOS, DO *SOFTWARE* E/OU DOS DADOS

Se os recursos de *hardware, software* e/ou dados estão alterados ou há suspeita de terem sido alterados as EC devem suspender os serviços até ao restabelecimento das condições seguras com a inclusão de novos componentes de eficácia credível. A ECEE deve ser notificada no prazo máximo de 24 horas.

As DPC devem descrever de forma clara os procedimentos adotados.

5.7.3. PROCEDIMENTOS EM CASO DE COMPROMETIMENTO DA CHAVE PRIVADA DA ENTIDADE

No caso de comprometimento da chave privada de uma entidade, deverá proceder-se à sua revogação imediata e informar deste facto todo o resto das entidades que compõem o SCEE dependentes ou não da Entidade afetada.

Os certificados assinados por entidades dependentes da comprometida, no período compreendido entre o compromisso da chave e a revogação do certificado, deverão por sua vez ser revogados.

No caso de comprometimento da chave de uma EC, o seu certificado é revogado e deve ser gerada nova chave. Dependendo do tipo de EC em causa deverão ser adotados, no mínimo, os requisitos definidos no quadro seguinte:

ECRAIZESTADO	ECESTADO OU SUBECESTADO
- Revoga o seu certificado; - Emite nova LER; - Gera nova chave; - Dissemina novo certificado.	- Gera um pedido de revogação (CMP); - Gera nova chave; - Efetua pedido de certificado (PKCS#10); - Recebe o novo certificado; - Dissemina novo certificado.
NOTIFICA:	**NOTIFICA:**
- Tutela Politica da ECEE; - Conselho Gestor do SCEE; - Outras EC com quem tenha certificação cruzada; - EC subordinadas.	- ECEE; - Conselho Gestor do SCEE; - EC subordinadas e ER; - Todos os titulares.

Tabela 11 – Procedimentos em caso de comprometimento de chaves

As DPC devem descrever de forma clara os procedimentos adotados.

5.7.4. CAPACIDADE DE CONTINUIDADE DA ACTIVIDADE EM CASO DE DESASTRE

As EC devem obrigatoriamente dispor de um plano de continuidade da atividade, onde estão descritos todos os procedimentos a acionar em caso de desastre onde haja perda ou corrupção de dados, *software* e equipamentos.

O Plano de Continuidade deverá garantir que os serviços indicados como críticos pela sua necessidade de disponibilidade estão disponíveis no Local Alternativo, devendo a DPC indicar o tempo máximo para ativação dos serviços.

Nas DPC deverá ser indicado, em caso de indisponibilidade das instalações da EC, o tempo máximo de inatividade antes de ser ativado o respetivo Plano de Continuidade da Atividade.

5.8. PROCEDIMENTOS EM CASO DE EXTINÇÃO DE EC OU ER

Em caso de cessação de atividade como prestador de serviços de Certificação, a EC deverá, com uma antecedência mínima de três meses, proceder às seguintes ações:

a) Informar o Conselho Gestor do SCEE;

b) Informar a Entidade de Certificação Eletrónica do Estado;

c) Informar todos os titulares de certificados;

d) Informar as EC com quem tenha efetuado acordos de certificação cruzada (caso existam);

e) Revogar todos os certificados e de certificados cruzados (caso existam);

f) Efetuar uma notificação final aos titulares 2 (dois) dias antes da cessação formal da atividade;

g) Garantir a transferência (para retenção por outra organização) de toda a informação relativa à atividade da EC, nomeadamente, chave da EC, certificados, documentação em arquivos (interno ou externo), repositórios e arquivos de registo de eventos.

Os arquivos devem ficar sob retenção de acordo com o estipulado no ponto 5.5.2 do presente documento.

Em caso de alterações do organismo/estrutura responsável de gestão da atividade da EC, esta deve informar de tal facto às entidades listadas nas alíneas anteriores.

As DPC devem descrever de forma clara os procedimentos adotados.

6. MEDIDAS DE SEGURANÇA TÉCNICA

6.1. GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES

A geração dos pares de chaves dos vários participantes nesta Infraestrutura de chaves públicas é processada de acordo com os requisitos e algoritmos definidos nesta política.

6.1.1. GERAÇÃO DO PAR DE CHAVES

A hierarquia do SCEE prevê a existência de participantes em três níveis.

No primeiro nível, encontra-se a ECRaizEstado, que funciona obrigatoriamente em modo *offline*, em que o respetivo par de chaves é gerado num módulo criptográfico, de acordo com requisitos definidos no ponto 6.2.1 do presente documento, e o certificado desta entidade é autoassinado.

No segundo nível, encontra-se as ECEstado, em que o seu funcionamento pode ser efetuado em modo *offline* ou em modo *online* (devendo nestes casos obedecer aos requisitos descrito adiante no ponto 6.7 do presente documento). O respetivo par de chaves é gerado, obrigatoriamente, num módulo criptográfico com o nível de proteção adequada, que corresponde aos requisitos definidos no ponto 6.2.1 do presente documento. O certificado desta entidade é assinado pela ECRaizEstado.

Às entidade de terceiro nível aplicam-se os mesmos requisitos que às entidade de segundo nível.

A geração do par de chaves para o titular é efetuada de acordo com as seguintes condições:

6.1.1.1. Chaves para efeitos de Assinatura Digital e Autenticação

O processo de geração das chaves é, obrigatoriamente, efetuado diretamente num módulo criptográfico em *hardware* (p.e. *smartcard*), sob o único controlo do titular, não podendo ser feita qualquer cópia da mesma.

O módulo criptográfico, tem obrigatoriamente, um nível de proteção de acordo com o especificado no ponto 6.2.1 do presente documento. Estes certificados são assinados pela EC respetiva.

As DPC devem descrever de forma clara e em pormenor os procedimentos adotados.

6.1.1.2. Chaves para efeitos de Confidencialidade

O processo de geração das chaves é, obrigatoriamente, efetuado diretamente num módulo criptográfico em *hardware* (p.e. *smartcard*). O módulo criptográfico, tem obrigatoriamente, um nível de proteção de acordo com o especificado no ponto 6.2.1 do presente documento. Estes certificados são assinados pela EC respetiva.

As DPC devem descrever de forma clara e em pormenor os procedimentos adotados, em particular se são efetuadas cópias de segurança, como é feita a sua retenção e a sua recuperação, caso seja necessário.

6.1.2. ENTREGA DA CHAVE PRIVADA AO TITULAR

6.1.2.1. Chaves para efeitos de Assinatura Digital e Autenticação

A forma de entrega dos módulos criptográficos, que contem as chaves, devem ser descritas na respetiva DPC. No entanto, é obrigatório que a forma de entrega do módulo criptográfico e a forma de entrega do PIN de acesso a este não seja entrega em simultâneo.

6.1.2.2. Chaves para efeitos de Confidencialidade

As DPC devem descrever de forma clara e em pormenor os procedimentos adotados para entrega da chave privada e certificado ao seu titular.

6.1.3. ENTREGA DA CHAVE PÚBLICA AO EMISSOR DO CERTIFICADO

Nos casos em que a entidade emissora do certificado não gera diretamente o par de chaves, a sua entrega à EC emissora do certificado deve ser efetuada através de um pedido de certificado (PKCS#10), através de uma transação *online* (de acordo com o especificado no RFC 4210, atualizado pelo RFC 6712) ou por outro método igualmente seguro desde que aprovado pelo Conselho Gestor do SCEE.

Os métodos utilizados devem estar descritos nas respetivas DPC.

6.1.4. ENTREGA DA CHAVE PÚBLICA DA EC ÀS PARTES CONFIANTES

A entrega da chave pública da EC é efetuada pela disponibilização do seu certificado (p.e. no sítio "*Web*").

Os formatos a disponibilizar podem ser em codificação DER (binário ou base64) ou no formato PKCS#7 (binário ou base64), com ou sem cadeia de certificação, dependendo dos requisitos estabelecidos na respetiva DPC. Outros formatos, para além dos descritos anteriormente, requerem autorização do Conselho Gestor do SCEE.

As DPC devem descrever os métodos utilizados na entrega da chave da EC, bem como os formatos disponibilizados.

6.1.5. DIMENSÃO DAS CHAVES

No que respeita à dimensão das chaves, os vários participantes devem obedecer aos comprimentos mínimos de chaves:

a) ECRaizEstado: RSA 4096 bit;

b) ECEstado: RSA 2048 bit;

c) SubECEstado: RSA 2048 bit;

d) Titulares: RSA 2048 bit.

6.1.6. GERAÇÃO DOS PARÂMETROS DA CHAVE PÚBLICA E VERIFICAÇÃO DA QUALIDADE

A geração dos parâmetros da chave pública e verificação da qualidade deverá ter sempre por base a norma que define o algoritmo. Em termos exemplificativos, para o caso do algoritmo RSA, deverá ser feita de acordo com o estipulado no PKCS#1 e RFC 5280 atualizado pelo RFC 6818.

As chaves das EC devem ser geradas com base na utilização de processos aleatórios ou pseudoaleatórios descritos, respetivamente, na ISO 9564-1 e ISO 11568-5.

6.1.7. FINS A QUE SE DESTINAM AS CHAVES (CAMPO "KEY USAGE" X.509V3)

O campo "*keyUsage*" dos certificados deve ser utilizado de acordo com o recomendado no RFC 5280, atualizado pelo RFC 6818.

CAMPO "KEYUSAGE" DO CERTIFICADO	BIT ACTIVO
digitalSignature	0
nonRepudiation (contentcommitment)	1
keyEncipherment	2
dataEncipherment	3
keyAgreement	4
keyCertSign	5
cRLSign	6
encipherOnly	7

decipherOnly	8

Tabela 12 – Definição dos campos "Keyusage" dos Certificados SCEE

6.1.7.1. Chaves para efeitos de Assinatura Digital

De acordo com a legislação em vigor, para a emissão de certificados qualificados.

6.1.7.2. Chaves para efeitos de Autenticação

Este tipo de chaves é utilizado, primordialmente, para a assinatura digital de *e-mail*, autenticação em sistemas, etc.

Na prática, estas chaves irão dar suporte às atividades que requerem o uso estendido das chaves.

Deve ser ativado o bit "*digitalSignature*", da extensão "*KeyUsage*" do certificado.

6.1.7.3. Chaves para efeitos de Confidencialidade

Este tipo de chaves é utilizado, primordialmente, para a troca e estabelecimento de chaves de sessão e processamento da informação cifrada, devendo terem consideração que neste tipo de chaves pelo menos um dos seguintes atributos deverá estar presente nos certificados: *keyEncipherment* e/ou *keyAgreement*.

Não é permitida a presença de outros atributos nos certificados emitidos com este fim.

6.1.8. OUTRA UTILIZAÇÃO PARA AS CHAVES

Podem ser atribuídas, adicionalmente, outro tipo de utilização das chaves, para além da utilização base descrita anteriormente.

A utilização alargada das chaves apenas é permitida para certificados de titulares (pessoas, organizações ou equipamentos).

A extensão "*extKeyUsage*" pode incluir, os seguintes tipos de utilização:

a) Server Authentication;

b) Client Authentication;

c) CodeSigning;

d) Email Protection ;

e) TimeStamping;

f) OCSPSigning;

g) Smart Card Logon.

6.2. PROTECÇÃO DA CHAVE PRIVADA E CARACTERÍSTICAS DO MÓDULO CRIPTOGRÁFICO

Quando for requerida a utilização de módulos criptográficos para proteção das chaves privadas, os participantes desta infraestrutura deverão empregar dispositivos devidamente avaliados e certificados por organismo e esquema de avaliação adequado para o efeito. O nível de avaliação de segurança requerido, para os dispositivos, varia em função do nível de proteção requerido e do nível hierárquico que o participante ocupa dentro da infraestrutura.

6.2.1. NORMAS E MEDIDAS DE SEGURANÇA DO MÓDULO CRIPTOGRÁFICO

Aos módulos criptográficos utilizados pela ECRaizEstado, ECEstado ou SubECEstado, nomeadamente para as operações que dizem respeito à geração, armazenamento e assinatura, é requerida a conformidade e respetiva certificação em pelo menos uma das seguintes normas (ou critérios reconhecidos como equivalentes):

a) FIPS PUB 140-2 com nível 3 ou superior;

b) CWA 14167-2;

c) ISO/IEC 15408 em EAL 4 ou superior.

Quando está em causa uma EREstado, os requisitos expressos anteriormente, referem-se às chaves do sistema /administrador da mesma.

Aos titulares de certificados, é requerida a utilização de módulos criptográficos certificados segundo o padrão ISO/IEC 15408 EAL4+ com suporte às normas PKCS#11 e CSP.

6.2.2. CONTROLO MULTI-PESSOAL (N DE M) PARA A CHAVE PRIVADA

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

Todas as operações deverão ser efetuadas com um mínimo de 2 pessoas (com funções qualificadas dentro da entidade) por tarefa, sendo empregues nas diversas funções, pelo menos 2 pessoas (N=2), entre o conjunto total de pessoas com funções atribuídas dentro da entidade (M=staff).

As DPC deverão descrever de forma precisa o número de pessoal empregue por tarefa.

6.2.3. RETENÇÃO DA CHAVE PRIVADA (KEY ESCROW)

Não é autorizada a retenção de chaves privadas para efeitos de assinatura digital.

Está autorizada a retenção de chaves privadas para efeitos de confidencialidade. Nos procedimentos para recuperação deste tipo de chaves, é requerido controlo multi-pessoal.

As DPC deverão descrever de forma precisa os mecanismos utilizados.

6.2.4. CÓPIA DE SEGURANÇA DA CHAVE PRIVADA

As chaves privadas dos titulares, para efeitos de assinatura digital, não são alvo de qualquer cópia de segurança.

As chaves privadas das Entidades Certificadoras do SCEE deverão ser alvo, obrigatoriamente, de pelo menos uma cópia de segurança, a realizar pela própria entidade. As cópias de segurança deverão ter o mesmo nível de segurança que a chave original.

6.2.5. ARQUIVO DA CHAVE PRIVADA

Todas as chaves que tenham sido alvo de cópias de segurança, deverão ser arquivadas de acordo com o estabelecido no ponto 5.5.2 do presente documento.

6.2.6. TRANSFERÊNCIA DA CHAVE PRIVADA PARA/DO MÓDULO CRIPTOGRÁFICO

No caso das chaves com utilização para efeitos de assinatura digital a transferência de e para o módulo criptográfico não se aplica, uma vez que são geradas dentro deste.

Assim esta situação não é aplicável para as chaves das EC, nem para as chaves de titulares, quando utilizadas para efeitos de assinatura digital.

No caso das chaves com utilização para efeitos de confidencialidade, se estas não forem geradas dentro do módulo criptográfico, a forma de a transferir deverá ser efetuada de acordo com o descrito no RFC 4210, atualizado pelo RFC 6712.

6.2.7. ARMAZENAMENTO DA CHAVE PRIVADA NO MÓDULO CRIPTOGRÁFICO

As chaves das EC são geradas e guardadas em módulo criptográfico de acordo com o especificado no ponto 6.2.1 do presente documento.

6.2.8. PROCESSO PARA ACTIVAÇÃO DA CHAVE PRIVADA

A chave privada deverá ser ativada quando o sistema quando o sistema/aplicação da EC é ligado ("*startup process*"). Esta ativação só deverá ser efetivada quando

previamente tiver sido feita a autenticação no módulo criptográfico pelos indivíduos indicados para o efeito.

O mecanismo de autenticação mínimo exigido é a autenticação por PIN/ palavra-chave. O número máximo de tentativas de autenticação permitidas não deve ser superior a 5 tentativas.

As DPC deverão descrever o procedimento utilizado para ativação da chave privada, bem como a identificação e interação das pessoas com o sistema/aplicação/módulo criptográfico durante o processo.

6.2.9. PROCESSO PARA DESACTIVAÇÃO DA CHAVE PRIVADA

A chave privada deverá ser desativada quando o sistema quando o sistema/aplicação da EC é desligado ("*shutdown process*"). Esta desativação só deverá ser efetivada quando previamente tiver sido encerrada a sessão com o módulo criptográfico.

Neste processo, antes de finalizado, deve ser garantido que todas as chaves são eliminadas da memória do módulo criptográfico. Qualquer espaço em disco, onde a chave tenha sido eventualmente armazenada, deve ser reescrito.

As DPC deverão descrever o procedimento utilizado para desativação da chave privada, bem como a identificação e interação das pessoas com o sistema/aplicação/módulo criptográfico durante o processo.

6.2.10. PROCESSO PARA DESTRUIÇÃO DA CHAVE PRIVADA

As várias chaves privadas devem ser destruídas sempre que deixarem de ser necessárias. De forma geral, esta catividade deve ser precedida sempre pela revogação do certificado, no caso de estar em vigor.

Para além do descrito no ponto anterior (6.2.9), as respetivas cópias de segurança devem também ser alvo de destruição.

A destruição das chaves privadas podem passar por processos diversos, consoante se enquadrem nos casos descritos a seguir:

a) **Sem formatação do módulo criptográfico**: Nas situações renovação de chaves (de rotina), a destruição da chave privada antiga é efetuada reescrevendo a nova chave privada do titular.

b) **Com formatação do módulo criptográfico**: Nas situações em a chave privada deixou de poder ser utilizada, nomeadamente, após expiração ou revogação do certificado.

c) **Destruição física**: Sempre que existam modulo criptográficos personalizados, nomeadamente, cartões inteligentes (*smartcards*) com fotografia. Antes da sua destruição física, devem ser previamente formatados.

Todos os procedimentos relativos à destruição das chaves privadas, bem como a gestão do ciclo de vida dos módulos criptográficos personalizados devem estar descritos na respetiva DPC

6.2.11. AVALIAÇÃO/NÍVEL DO MÓDULO CRIPTOGRÁFICO

Descrito no ponto 6.2.1 do presente documento.

6.3. OUTROS ASPECTOS DA GESTÃO DO PAR DE CHAVES

6.3.1. ARQUIVO DA CHAVE PÚBLICA

As EC devem efetuar o arquivo das suas chaves e das chaves por si emitidas (para efeitos de assinatura digital), permanecendo armazenadas após a expiração dos certificados correspondentes, de acordo com os requisitos definidos no ponto 5.5 do presente documento, para verificação de assinaturas geradas durante seu prazo de validade.

6.3.2. PERÍODOS DE VALIDADE DO CERTIFICADO E DAS CHAVES

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

Neste sentido a tabela seguinte apresenta a validade máxima dos diversos tipos de certificados e período em que os mesmos devem ser renovados. Os valores estão expressos em anos.

ECRaizEstado	ECEstado	SubECEstado	Outras Entidades PKI (1)	Titulares	
				HW	SW
4096				Certificados qualificados	
	2048	2048	2048	2048	2048
	12	6	3	6	3
	6	3	3	6	3
24				Certificados não qualificados	
	2048	2048	2048	2048	2048
	12	12	3	10	3
	2	2	3	10	3
12				Todos os certificados	
	4096	4096	N/A	3072 (2) (3)	3072 (2)
	12	12		10	3
	2	2		10	3

Tabela 13 – Definição dos Períodos Máximos de Validade dos Certificados

Legenda:

Tamanho das chaves RSA (bits)
Validade dos certificados (anos)
Período de renovação (anos)

Notas:

(1) EREstado, Serviços de Validação Cronológica e Serviços de Validação Online do Estado de Certificados.

(2) Para as chaves a 3.072 bits deverá ser aplicada a Suite RSASSA-PSS com mgf1SHA-256 Identifier [ETSI TS 102 176-1 V2.1.1 (2011-07)].

(3) É autorizada a emissão de chaves a 2.048 bits, exclusivamente no âmbito do cartão de cidadão, até ao máximo de doze meses após a publicação da lei que altere o prazo de validade do cartão de cidadão para até 10 anos.

6.4. DADOS DE ATIVAÇÃO

6.4.1. GERAÇÃO E INSTALAÇÃO DOS DADOS DE ATIVAÇÃO

Os dados de ativação devem ser gerados de forma a serem únicos e imprevisíveis. Os dados de ativação conjugados com outro tipo de controlo de acessos devem ter um adequado nível de robustez para as chaves e dados a proteger.

A entrada de uma EC no domínio do SCEE requer a existência de dispositivos/mecanismos criptográficos para suporte às atividades das EC, nomeadamente, no seu funcionamento e na sua recuperação.

A atividade das EC é efetuada com base em funções diferenciadas, cada uma com o correspondente dispositivo onde se encontram os respetivos dados de ativação.

6.4.2. PROTECÇÃO DOS DADOS DE ATIVAÇÃO

Apenas o pessoal autorizado tem em posse os dispositivos seguros e respetivo segrego (p.e. PIN) dos dados de ativação das EC.

No caso de chaves associadas a certificados de titulares, apenas o próprio conhece o respetivo segredo para ativação, sendo este o único e exclusivo responsável pela proteção e guarda dos dados de ativação das suas chaves.

6.4.3. OUTROS ASPETOS DOS DADOS DE ACTIVAÇÃO

Não estipulado.

6.5. MEDIDAS DE SEGURANÇA DE INFORMAÇÃO

Os dados relativos a esta seção são considerados sensíveis, sendo apenas disponibilizados a quem tiver necessidade de conhecer. No domínio do SCEE, apenas são fornecidos à ECEE, ao Conselho Gestor do SCEE e a Autoridade Credenciadora.

Cada EC deve implementar o conjunto de medidas de segurança consideradas adequadas, em resultado da arquitetura escolhida e dos riscos avaliados.

No desenvolvimento da sua atividade, cada EC implementa um sistema de gestão de segurança da informação baseado na Norma ISO/IEC 27001, fornecendo à Autoridade Credenciadora a documentação comprovativa, nomeadamente:

a) Da realização de uma avaliação exaustiva dos riscos que identifique o âmbito de aplicação do sistema e assinale o impacto na atividade em caso de violação da garantia da informação;

b) Da identificação das ameaças e vulnerabilidades e da produção de um documento de avaliação de riscos onde se enumerem igualmente contramedidas para evitar tais ameaças, e as medidas corretivas a tomar caso a ameaça se concretize, bem como a apresentação de uma lista hierarquizada de melhorias a introduzir;

c) Da identificação dos riscos residuais por escrito;

d) Cada EC seleciona os controlos de segurança adequados com base na análise de riscos prevista no número anterior, e na norma ISO/IEC 27002.

As DPC devem conter uma descrição das medidas de segurança implementadas, sem colocar em causa a segurança dos sistemas por eventual excesso de divulgação de informação.

6.5.1. REQUISITOS TÉCNICOS ESPECÍFICOS

De forma geral os sistemas que compõe a EC devem proporcionar, desde que aplicável, no mínimo, as seguintes capacidades/funcionalidades:

a) As descritas no ponto 5, do documento "CWA 14167-1", ou documento equivalente;

b) Mecanismo para recuperação dos sistemas e chaves de EC;

c) Dispositivos de proteção de fronteira, nomeadamente, *firewall, IDS/IPS*.

Os requisitos definidos anteriormente, devem ser alcançados pela conjunção dos diversos sistemas que compõem os sistemas seguros da EC (p.e. sistema operativo, *software*, HSM, medidas de segurança física, entre outras.).

Outros tipos de *software* (p.e. antivírus,), só deve ser instalado se for verificado que:

a) Não interfere com as configurações previamente definidas pelos fabricantes/organismos de avaliação;

b) Se demonstrar que proporciona um acréscimo no nível de segurança.

De modo general as EC devem seguir as boas práticas estabelecidas na norma ISO 17799:2005.

6.5.2. AVALIAÇÃO/NÍVEL DE SEGURANÇA

Os vários sistemas e produtos empregues pelas EC, no domínio do SCEE, são fiáveis e protegidos contra modificações. Os produtos e sistemas referidos, são avaliados, estando em conformidade com os requisitos definidos na especificação técnica CWA 14167-1 e/ou com a norma ISO/IEC 15408 ou perfil equivalente.

6.6. CICLO DE VIDA DAS MEDIDAS TÉCNICAS DE SEGURANÇA

Os dados relativos a esta secção são considerados sensíveis, sendo apenas disponibilizados a quem tiver necessidade de conhecer. No domínio do SCEE, apenas são fornecidos à ECEE, ao Conselho Gestor do SCEE e à Autoridade Credenciadora.

Cada EC deve implementar o conjunto de medidas de segurança consideradas adequadas, em resultado da arquitetura escolhida e dos riscos avaliados.

As DPC devem conter uma descrição das medidas de segurança implementadas, sem colocar em causa a segurança dos sistemas por eventual excesso de divulgação de informação.

6.6.1. MEDIDAS DE DESENVOLVIMENTO DO SISTEMA

São exigidos requisitos de segurança desde o início, na aquisição dos sistemas informáticos, como na instalação e implementação dos mesmos, visto que têm impacto sobre a segurança do SCEE.

Serão realizadas análises dos requisitos de segurança durante as fases de desenho e especificação de requisitos de qualquer componente utilizado nas aplicações que constituem cada um dos sistemas do SCEE, para garantir que os sistemas são seguros.

Utilizam-se procedimentos de verificação de alteração de versões, atualizações e instalação de *patches* ou *fixes* dos ditos componentes.

A infraestrutura das EC deve estar dotada de ambientes de desenvolvimento e pré-produção segregados dos ambientes de produção.

6.6.2. MEDIDAS PARA A GESTÃO DA SEGURANÇA

A EC deve manter atualizado um inventário com todos os ativos (equipamento, dados e pessoal), sendo classificados de acordo com a sua importância e necessidades de proteção, tendo em conta o normal funcionamento da atividade da EC. Esta classificação deve estar coerente com a análise de riscos inicial.

De modo geral as EC devem regular a sua atividade pela adoção dos seguintes princípios:

a) Os produtos e sistemas da EC devem únicos e exclusivamente ser utilizados para as atividades de certificação;

b) A configuração dos produtos e sistemas da EC, tal como a sua manutenção devem ser sempre documentadas;

c) Nos sistemas das EC apenas deve ser instalado aplicações e componentes indispensáveis para o seu funcionamento;

d) Devem estar previstos mecanismo para deteção de eventuais modificações na sua configuração;

e) Devem ser adotadas medidas adequadas para a prevenção de *software*

malicioso carregado através dos equipamentos das ER;

f) Depois de instalado, os sistemas e produtos da EC devem efetuar verificações da sua integridade, de forma periódica, nunca ultrapassando, o período de 30 dias entre verificações.

A DPC deve descrever a medidas adotadas, com um detalhe que não coloque em causa a segurança do sistema.

6.6.3. CICLO DE VIDA DAS MEDIDAS DE SEGURANÇA

As operações de atualização e manutenção dos produtos e sistemas das EC devem seguir o mesmo controlo que o equipamento original, sendo que o mesmo deve ser instalado pelo pessoal com funções de confiança, com adequada formação para o efeito e seguindo os procedimentos definidos para o efeito.

Nas DPC devem estar descritos os procedimentos a seguir para a atualização e manutenção dos produtos e sistemas que compõe o sistema da EC.

6.7. MEDIDAS DE SEGURANÇA DA REDE

Os sistemas da EC que se encontrem a funcionar em modo *online* devem estar protegidos de eventuais ataques em virtude de estarem interligados, direta ou indiretamente, a redes externas. Esta proteção deve ser garantida com o recurso a equipamentos de proteção de fronteira, nomeadamente, um *Firewall,* configurado de forma a permitir apenas a utilização de protocolos e comandos necessários para o correto funcionamento do sistema da EC responsável pela emissão dos certificados.

A DPC deve descrever a medidas de segurança de rede adotadas, com um detalhe que não coloque em causa a segurança do sistema.

6.8. VALIDAÇÃO CRONOLÓGICA (TIME-STAMPING)

De acordo com a legislação nacional em vigor.

7. PERFIS DE CERTIFICADO, LCR E OCSP

7.1. PERFIL DO CERTIFICADO

A emissão de certificados é feita segundo o perfil de Certificados ITU-T X.509 versão 3, de acordo, com as recomendações definidas no RFC 5280, atualizado pelo RFC 6818, RFC 3739, ETSI TS 101 862 e ETSI 102 280.

Os certificados emitidos pelas EC, no domínio do SCEE, devem incluir:

CAMPO	DESCRIÇÃO
serialNumber	Número inteiro que indica o número de série do certificado;
signature	OID do algoritmo utilizado pela EC para assinar o certificado;
issuer	Um X.500 DN da EC que emite o certificado
validity	O período de tempo em que o certificado é considerado válido.
	Nos certificados até 2049: representado num "UTC Time "(YYMMDDHHMMSSZ).
	Nos certificados após 2049: representado num "generalized time" (YYYYMMDDHHMMSSZ).
subject	Um X.500 DN a quem é atribuído o certificado
subjectPublicKeyInfo	OID do algoritmo e uma cópia da chave pública do certificado

Tabela 14 – Campos básicos do certificado

7.1.1. NÚMERO DE VERSÃO

Neste campo os certificados deverão conter o valor 3 (três), de forma a identificar a utilização de certificados ITU-T X.509 versão 3.

7.1.2. EXTENSÕES DO CERTIFICADO

Todos os sistemas das várias entidades deverão processar corretamente todas as extensões identificadas no RFC 5280, atualizado pelo RFC 6818.

7.1.2.1. authorityKeyIdentifier

Extensão obrigatória e não critica. Esta extensão é utilizada para verificar a assinatura do certificado, possibilitando que as várias chaves utilizadas pelas EC na assinatura dos certificados, sejam facilmente diferenciadas. O valor do "*keyIdentifier*" deve derivar da chave pública da EC (normalmente um *hash* da chave pública que consta no campo "*subjectPublicKeyInfo*" do certificado da EC que o emitiu).

Nos certificados auto assinados não é utilizado.

7.1.2.2. subjectKeyIdentifier

Extensão obrigatória e não critica. Esta extensão é utilizada para identificar de forma inequívoca a chave pública do certificado. Possibilita que várias chaves sejam utilizadas pelo mesmo *"subject"* e que sejam facilmente diferenciadas. O valor utilizado é normalmente um *hash* da chave pública que consta no campo do certificado "subjectPublicKeyInfo".

7.1.2.3. KeyUsage

Extensão obrigatória e crítica. Especificado no ponto 6.1.7 do presente documento.

7.1.2.4. CertificatePolicies

Extensão obrigatória e não critica. Esta extensão lista as Politicas de Certificados que dão suporte e regem o ambiente em que se processou a emissão do certificado. Deve ser incluído o OID da Politica de Certificado e o URL da DPC.

7.1.2.5. BasicConstraints:

É uma extensão obrigatória e crítica para Certificados de EC, é opcional para certificados de titular. Se o certificado é um certificado de EC, o valor "cA", deverá estar ativo (cA=True).

Em termos práticos, se num certificado o campo "*keyUsage*" estiver presente o valor "*keyCertSign*", então no *BasicConstraints*, o valor do campo "cA", deverá ser estar ativo, ou o processo de verificação do certificado falha.

7.1.2.6. Authority Information Access

A extensão "*Authority Information Access*" é introduzida nos vários perfis de certificados definidos no âmbito do SCEE, de forma a permitir futuras implementações para verificação via OSCP, sem que para isso haja necessidade de futuras alterações nesta infraestrutura de chaves públicas

Esta extensão poderá igualmente conter a identificação da localização do certificado da EC.

7.1.3. IDENTIFICADORES DE ALGORITMO

ALGORITMO	OID
Sha1WithRSAEncryption	1.2.840.113549.1.1.5
Sha256withRSAEncryption	1.2.840.113549.1.1.11
RSASSA-PSS	1.2.840.113549.1.1.10
RsaEncryption	1.2.840.113549.1.1.1

Tabela 15 – Identificadores OID de Algoritmos

7.1.4. FORMATOS DE NOME

Os certificados emitidos para cada entidade do SCEE, são referenciados através de um DN, a aplicar nos campos "*issuer*" e "*subject*" do certificado.

O DN deverá ser representado através de uma *X.501 UTF8String*.

7.1.5. RESTRIÇÕES DE NOME

Os nomes incluídos nos certificados estão restritos à utilização de DN, únicos e sem ambiguidades.

O atributo "C" (*countryName*) é codificado de acordo com a ISO 3166-1-alpha-2 "*code elements*", numa *PrintableString*.

7.1.6. OBJECTO IDENTIFICADOR DA POLÍTICA DE CERTIFICADO

Todos os certificados emitidos pelas Entidades Certificadoras do SCEE devem garantir a inclusão do OID da Politica de Certificados.

7.1.7. UTILIZAÇÃO DA EXTENSÃO DE RESTRIÇÃO DE POLÍTICAS

Não estabelecido.

7.1.8. SINTAXE E SEMÂNTICA DOS QUALIFICADORES DE POLÍTICAS

Nos certificados emitidos, as Entidades Certificadoras devem incluir no campo *policyQualifiers* da extensão "*CertificatePolicies*" o URL da sua DPC.

Nas DPC poderão ser estabelecidos a utilização do '*Policy Qualifier*', o campo '*Notice Reference*'. O '*Notice Reference*' é uma nota de texto que aparece no monitor, quando se procede a verificação do certificado.

7.1.9. SEMÂNTICA DE PROCESSAMENTO DA EXTENSÃO DE POLÍTICA DE CERTIFICADOS CRÍTICOS

Tendo em consideração as recomendações introduzidas pelo RFC 5280, atualizado pelo RFC 6818, quanto à utilização desta extensão, os certificados das EC do SCEE devem incluir no OID o valor 2.5.29.32.0.

Esta opção tem como objetivo não limitar, em termos futuros, o conjunto de políticas a emitir sob o domínio de certificação do SCEE.

Nos certificados para titulares serão incluídos os OID respetivo, tendo em conta a sua aplicação.

Esta extensão é marcada como não critica para evitar possíveis problemas de interoperabilidade.

7.2. PERFIL DA LCR

Cada EC do SCEE, na emissão de uma LCR, deve obrigatoriamente incluir:

CAMPO	DESCRIÇÃO
signature	OID do algoritmo utilizado pela EC para assinar o certificado; o algoritmo e respetivo OID
issuer	Um X.500 DN da EC que emite o certificado o X.500 DN da EC que gerou a LCR;
thisUpdate	A indicação de quando a LCR foi gerada
nextUpdate	A indicação de quando será gerada nova LCR
revokedCertificates	Deverá ser introduzida a sequência de dados correspondentes aos campos *userCertificate*, *revocationDate* e *crlEntryExtensions*, de forma a fornecer informação do estado dos certificados no que diz respeito, respetivamente, ao número de série do certificado revogado, a data em que foi revogado e o motivo da sua revogação

Tabela 16 – Campos básicos do certificado

Adicionalmente, as diversas aplicações e sistemas utilizados pelos participantes que integram o SCEE, devem garantir, entre outras que:

a) A verificação da assinatura constante na LCR, através da chave pública constante no certificado da EC que emite a LCR;

b) Verificar a cadeia de certificação do certificado da EC;

c) Verificar que é utilizada a versão 2;

d) No momento da verificação a data está enquadrada de acordo com os valores indicados nos campos da LCR "*thisUpdate*" e "*nextUpdate*";

e) A LCR que está a ser verificada, no seu campo "CRLNumber", o valor indicado é superior ao valor constante no mesmo campo da LCR já existente;

f) Que a entidade que emite a LCR é a mesma que emitiu o certificado;

7.2.1. NÚMERODA VERSÃO

A LCR emitida pelas EC, deve implementar versão 2 padrão ITU X.509, de acordo com o RFC 5280, atualizado pelo RFC 6818.

7.2.2. EXTENSÕES DA LCR E DAS SUAS ENTRADAS

O SCEE define como extensões de LCR obrigatórias, mas não criticas, as seguintes:

a) *CRLNumber*, implementado de acordo com as recomendações do RFC 5280, atualizado pelo RFC 6818;

b) *AuthorityKeyIdentifier*: contem um identificador da chave pública da EC que assinou a LCR.

7.3. PERFIL DO OCSP

Se o serviço de OCSP for implementado, os certificados de *OCSPResponder*, devem estar em concordância com as seguintes normas:

a) RFC 5280, atualizado pelo RFC 6818;

b) ITU-T X.509 (2005);

c) RFC 6960.

E tendo em conta os seguintes constrangimentos:

a) O período de validade não deve ser superior a 6 meses.

b) No certificado de OCSP será incluída a extensão "*id-pkix-ocsp-nocheck*".

No entanto, de futuro, não deve ser excluída a possibilidade de inclusão da extensão AIA, fornecendo informação sobre os mecanismos adicionais para comprovação da validade dos certificados.

7.3.1. NÚMERO DA VERSÃO

Os certificados de OCSP *Responder* utilizam a norma X.509 versão 3 (X.509 v3).

7.3.2. EXTENSÕES DO OCSP

Os certificados de OCSP *Responder* emitidos por uma EC no domínio do SCEE incluirão o DN da entidade emissora e do titular, nos campos "issuer name" e "subject name", respetivamente.

Os campos e extensões utilizadas nos certificados de *OCSP Responder* são:

a) Version;

b) serialNumber;

c) subject;

d) issuer;

e) signingAlgorithms;

f) validityPeriod;

g) extKeyUsage;

h) subjectKeyIdentifier;

i) authorityKeyIdentifier issuerAndSerialPresent;

j) KeyUsage, marcada como crítica;

k) BasicConstraint, marcada como crítica;

l) CertificatePolicies;

m) OCSPNocheck;

n) AIA.

8. AUDITORIA E AVALIAÇÕES DE CONFORMIDADE

Todas as EC integradas na hierarquia do SCEE devem, obrigatoriamente, construir as suas DPC em conformidade com os requisitos mínimos definidos neste documento.

São alvo de auditoria, todas as entidades que, direta ou indiretamente, exerçam atividade de certificação nos termos do definido nesta política, como são o caso da ECRaizEstado, das ECEstado e das SubECEstado, EREstado e EC filiada, caso existam.

A Autoridade Credenciadora é o organismo responsável pela condução das auditorias de conformidade, podendo, de acordo com a lei, recorrer a pessoal externo qualificado e credenciado, para o efeito.

8.1. FREQUÊNCIA OU MOTIVO DA AUDITORIA

De acordo com o descrito no ponto 8, as diversas entidades são alvo de auditoria nas seguintes situações:

a) No processo de integração no SCEE;

b) Anualmente;

c) A qualquer momento, sem aviso prévio.

As EC do Estado devem declarar na DPC a frequência das auditorias, sendo que estas devem ser realizadas pelo menos uma vez por ano, de forma a garantir a adequação do funcionamento e operação, de acordo com a DPC.

Podem ser levadas a cabo outras auditorias técnicas e de segurança segundo o estabelecido nas DPC.

Cada EC deverá efetuar com uma regularidade a explicitar, auditorias de cumprimento de legislação e de proteção de dados pessoais.

8.2. IDENTIDADE E QUALIFICAÇÕES DO AUDITOR

O auditor é uma pessoa ou organização, de reconhecida idoneidade, com experiência e qualificações comprovadas na área da segurança da informação e dos sistemas de informação, infraestruturas de chaves pública, familiarizado com as aplicações e programas de certificação digital e na execução de auditorias de segurança credenciado pelo Gabinete Nacional de Segurança.

Cabe a cada EC do SCEE, de acordo com a lei e os regulamentos da Autoridade Credenciadora, selecionar o auditor com base na lista de auditores credenciados pelo Gabinete Nacional de Segurança.

8.3. RELAÇÃO ENTRE O AUDITOR E A ENTIDADE CERTIFICADORA

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

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

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

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

8.4. ÂMBITO DA AUDITORIA

A auditoria de segurança é efetuada com base nos requisitos mínimos definidos neste documento e na DPC da entidade que irá ser alvo da auditoria.

As auditorias determinam a conformidade dos serviços das EC do Estado com estas Políticas de Certificados e com as Declarações de Práticas. Também devem determinar a adequação referente aos seguintes documentos:

a) Política de Segurança;

b) Segurança Física;

c) Avaliação Tecnológica;

d) Gestão dos serviços da EC;

e) Seleção de Pessoal;

f) DPC e PC (em vigor);

g) Contratos;

h) Política de Privacidade.

As auditorias podem ser completas ou parciais e incidir sobre qualquer outro tipo de documentos/procedimentos.

8.5. PROCEDIMENTOS APÓS UMA AUDITORIA COM RESULTADO DEFICIENTE

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

a) Documenta todas as deficiências encontradas durante a auditoria;

b) No final do processo de auditoria, reúne-se com os responsáveis da entidade submetida a auditoria e apresenta de forma resumida um relatório de primeiras impressões (RPI);

c) Elabora o relatório da auditoria. O relatório de acordo com as regras e boas práticas estabelecidas pela Autoridade Credenciadora;

d) Submete o relatório de auditoria à Autoridade Credenciadora;

e) Depois de apreciado pela Autoridade Credenciadora, é remetida uma cópia do relatório de auditoria final (RAF), para a entidade auditada;

f) A entidade submetida a auditoria enviará um relatório de correção de

irregularidades (RCI), para a Autoridade Credenciadora, no qual deve estar descrito quais as ações, metodologia e tempo necessário para corrigir as irregularidades encontradas;

g) A Autoridade Credenciadora depois de analisar o RCI, toma uma das três seguintes opções, consoante o nível de gravidade/severidade das irregularidades:

   i. Aceitam os termos, permitindo que a atividade seja desenvolvida até à próxima auditoria;

   ii. Permite que a entidade continue em atividade por um período máximo de 60 dias até à correção das irregularidades antes da revogação;

   iii. Revogação imediata da atividade da entidade.

8.6. COMUNICAÇÃO DE RESULTADOS

Os resultados devem ser comunicados de acordos com os prazos estabelecidos no quadro seguinte:

COMUNICAÇÃO DE RESULTADOS	AUDITOR	ENTIDADE	AUTORIDADE CREDENCIADORA
RPI	No final da auditoria		
RAF	2 semanas		
RCI		1 semana	
Decisão sobre irregularidades			4 semanas

Tabela 17 – Prazos de comunicação dos resultados de Auditoria

9. OUTRAS SITUAÇÕES E ASSUNTOS LEGAIS

9.1. TAXAS

9.1.1. TAXAS POR EMISSÃO OU RENOVAÇÃO DE CERTIFICADOS

As taxas de emissão ou renovação de certificados se existirem, devem estar detalhadas na DPC, tendo em conta a necessidade de instrumento legal de habilitação para a sua cobrança.

9.1.2. TAXAS PARA ACESSO A CERTIFICADO

De forma geral, a natureza pública de que se reveste o SCEE, o acesso será tendencialmente gratuito, no entanto, a EC deve descrever a sua aplicabilidade na sua DPC.

9.1.3. TAXAS PARA ACESSO A INFORMAÇÃO DO ESTADO CERTIFICADO OU DE REVOGAÇÃO

O acesso a informação sobre o estado ou revogação dos certificados é livre e gratuita não se podendo aplicar nenhuma taxa.

9.1.4. TAXAS PARA OUTROS SERVIÇOS

De forma geral, a natureza pública de que se reveste o SCEE, o acesso será tendencialmente gratuito, no entanto, a EC deve descrever a sua aplicabilidade na sua DPC.

9.1.5. POLÍTICA DE REEMBOLSO

Nos casos em que a DPC especifique alguma taxa aplicável à prestação de serviços de certificação ou revogação para determinado tipo de certificados, é obrigatório que esse documento especifique a política de reembolso.

9.2. RESPONSABILIDADE FINANCEIRA

9.2.1. SEGURO DE COBERTURA

As Entidade Certificadoras do Estado devem respeitar a legislação em vigor no que se concerne aos seguros de cobertura de responsabilidade civil, devendo identificar na respetiva DPC o montante e a cobertura.

9.2.2. OUTROS RECURSOS

Como as Entidades Certificadoras do SCEE pertencem ao Estado Português, não estão sujeitas aos riscos inerentes às Entidade Certificadoras Privadas.

9.2.3. SEGURO OU GARANTIA DE COBERTURA PARA UTILIZADORES

Existindo seguro de ou garantia de cobertura para utilizadores, as EC devem especifica-los na DPC.

9.3. CONFIDENCIALIDADE DA INFORMAÇÃO PROCESSADA

O pedido de inclusão no certificado de dados pessoais da pessoa singular a constar como seu titular terá de ser expressamente autorizado pela própria.

9.3.1. ÂMBITO DA CONFIDENCIALIDADE DA INFORMAÇÃO

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

a) As chaves privadas das Entidades que compõem o SCEE;

b) As chaves privadas dos titulares do SCEE;

c) Toda a informação relativa aos parâmetros de segurança, controlo e procedimentos de auditoria;

d) Toda a informação de carácter pessoal proporcionada às EC durante o processo de registo dos subscritores de certificados, salvo se houver autorização explícita para a sua divulgação;

e) Planos de continuidade de negócio e recuperação;

f) Registos de transações, incluindo os registos completos e os registos de auditoria das transações.

9.3.2. INFORMAÇÃO FORA DO ÂMBITO DA CONFIDENCIALIDADE DA INFORMAÇÃO

Considera-se informação de acesso público:

a) Política de Certificados;

b) Declaração de Práticas de Certificação;

c) Os certificados, para efeitos de confidencialidade, desde que declarado na respetiva DPC;

d) LCR e LER;

e) Toda a informação classificada como “pública”;

As Entidades Certificadoras devem permitir o acesso a informação não confidencial, sem prejuízo do que se venha a estabelecer nas DPC, no domínio dos controles de segurança necessários para proteger a autenticidade e integridade da mesma.

9.3.3. RESPONSABILIDADE DE PROTECÇÃO DA CONFIDENCIALIDADE DA INFORMAÇÃO

Deve ser declarado na DPC a responsabilidade de proteção da confidencialidade da informação.

9.4. PRIVACIDADE DOS DADOS PESSOAIS

As Entidades Certificadoras devem ter uma Política de Privacidade nos seus repositórios, onde se declara o cumprimento das disposições estabelecidas na legislação de proteção de dados pessoais, tendo em consideração que:

a) As EC só podem coligir dados pessoais necessários ao exercício das suas atividades e obtê-los diretamente das pessoas interessadas na titularidade dos dados de criação e verificação de assinatura e respetivos certificados, ou de terceiros junto dos quais aquelas pessoas autorizem a sua coleta;

b) Os dados pessoais coligidos pela EC não poderão ser utilizados para outra finalidade que não seja a de certificação, salvo se outro uso for consentido expressamente por lei ou pela pessoa interessada;

c) As EC respeitarão as normas legais vigentes sobre a proteção, tratamento e circulação dos dados pessoais e sobre a proteção da privacidade no sector das telecomunicações.

9.4.1. MEDIDAS PARA GARANTIA DA PRIVACIDADE

No cumprimento do estabelecido pela lei sobre assinaturas eletrónicas, informação de carácter pessoal disponibilizada às EC do Estado pelos titulares de certificados, deve ser tratada de acordo com a lei de proteção de dados pessoais.

Desta forma cada DPC deve declarar a existência de um ficheiro de dados utilizadores de assinaturas eletrónicas, indicando a responsabilidade do mesmo e a autorização da Comissão Nacional de Proteção de Dados (CNPD).

9.4.2. INFORMAÇÃO PRIVADA

A informação pessoal que não incluída nos certificados, bem como o mecanismo de comprovação do estado dos certificados, devem ser considerados informação de carácter privado. Em qualquer caso são exemplos de informação considerada privada:

a) Pedidos de certificados, aprovados ou negados assim como toda a informação pessoal obtida para a emissão e manutenção de certificados;

b) Chaves privadas geradas e/ou armazenadas pelas EC do SCEE;

c) Os dados pessoais a que se refere a Lei n.º 67/98, de 26 de outubro;

Em nenhum caso as EC do Estado poderão incluir nos certificados que emitem, os dados que se faz referência no artigo 7º da Lei n.º 67/98., de 26 de outubro.

9.4.3. INFORMAÇÃO NÃO PROTEGIDA PELA PRIVACIDADE

Esta informação é referente à informação pessoal que se inclui no certificado e no mecanismo de comprovação do estado dos mesmos, de acordo com o ponto 3.1 do presente documento.

Esta informação, proporcionada aquando do pedido de certificado é incluída nos certificados.

Esta informação não tem carácter privado / reservado, sendo deste modo pública caso seja consentido pelo titular.

Em todo o caso, não é considerada confidencial a seguinte informação:

a) O período de validade do certificado assim como a data de emissão do certificado e a data de caducidade;

b) O número de série do certificado;

c) Os diferentes estados e situações do certificado e a data do início de cada um deles;

d) As LCR e OCSP, assim como o resto das informações de estado de revogação;

e) A informação contida no Repositório das EC.

9.4.4. RESPONSABILIDADE DE PROTECÇÃO DA INFORMAÇÃO PRIVADA

As EC devem garantir o cumprimento das suas obrigações, como previsto no presente documento.

9.4.5. NOTIFICAÇÃO E CONSENTIMENTO PARA UTILIZAÇÃO DE INFORMAÇÃO PRIVADA

Para a prestação de serviço, as EC deverão obter o consentimento dos titulares dos dados necessários para a prestação do serviço de certificação.

Considera-se obtido o consentimento por parte do titular a oposição da assinatura do TRT.

9.4.6. DIVULGAÇÃO RESULTANTE DE PROCESSO JUDICIAL OU ADMINISTRATIVO

As EC só poderão fornecer dados e informações consideradas, no âmbito desta política, como informação privada, nos pressupostos em que estes são requeridos pela autoridade pública competente no âmbito da lei.

Em concreto, as EC estão obrigadas a revelar a identidade dos assinantes quando lhes for solicitado pelos órgãos judiciais, no exercício das funções que lhe sejam atribuídas.

9.4.7. OUTRAS CIRCUNSTÂNCIAS PARA REVELAÇÃO DE INFORMAÇÃO

As EC devem incluir na sua política de privacidade prevista no ponto 9.4 do presente documento, regras para permitir a divulgação de informação dos titulares das chaves, diretamente ao próprio ou a terceiros.

9.5. DIREITOS DE PROPRIEDADE INTELECTUAL

Todos os direitos de propriedade intelectual, incluindo os que se referem a certificados e LCR emitidos, OID, DPC, PC e PCert, bem como qualquer outro documento, propriedade das EC pertencem à respetiva EC.

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

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

9.6. REPRESENTAÇÕES E GARANTIAS

9.6.1. REPRESENTAÇÃO E GARANTIAS DAS ENTIDADES CERTIFICADORAS

As Entidade Certificadoras do SCEE estão obrigadas a:

a) Realizar as suas operações de acordo com esta Política;

b) Declarar de forma clara todas as suas Práticas de Certificação no documento apropriado – DPC;

c) Proteger as suas chaves privadas;

d) Emitir certificados de acordo com o *standard* X.509;

e) Emitir certificados que estejam conformes com a informação conhecida no momento de sua emissão e livres de erros de *input* de dados;

f) Garantir a confidencialidade no processo da geração dos dados da criação da assinatura e a sua entrega por um procedimento seguro ao titular;

g) Utilizar sistemas e produtos fiáveis que estejam protegidos contra toda a alteração e que garantam a segurança técnica e criptográfica dos processos de certificação;

h) Utilizar sistemas fiáveis para armazenar certificados reconhecidos, que permitam comprovar a sua autenticidade e impedir pessoas não autorizadas altere os dados;

i) Arquivar sem alteração os certificados emitidos;

j) Garantir que podem determinar, com precisão da data e hora, em que emitiu, ou revogou, ou suspendeu um certificado;

k) Empregar pessoal com qualificações, conhecimentos e experiência necessárias para a prestação de serviços de certificação;

l) Revogar os certificados nos termos da Ponto *Suspensão e Revogação de Certificados* do presente documento e publicar os certificados revogados na LCR do repositório da respetiva EC, com a frequência estipulada no ponto 4.9.7 do presente documento;

m) Publicar a sua DPC e as Políticas de Certificado aplicáveis no seu repositório garantindo o acesso às versões atuais assim como as versões anteriores;

n) 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;

o) Colaborar com as auditorias externas, para validar a renovação das suas próprias chaves;

p) Operar de acordo com a legislação aplicável;

q) Proteger, em caso de existirem, as chaves que estejam sobre sua custódia;

r) Garantir a disponibilidade da LCR de acordo com as disposições do ponto 4.9.7 do presente documento, bem como a disponibilidade do serviço de OCSP, caso o tenha implementado;

s) Em caso de cessar a sua atividade, a EC deverá comunicar com uma antecedência mínima de dois meses a todos os titulares dos certificados emitidos assim como à ECEE;

t) Cumprir com as especificações contidas na norma sobre Proteção de Dados

Pessoais;

u) Conservar toda a informação e documentação relativa a um certificado reconhecido e as Declarações de Práticas de Certificação vigentes em cada momento e durante quinze anos desde o momento da emissão;

v) Disponibilizar os certificados da sua EC e da ECRaizEstado.

9.6.2. REPRESENTAÇÃO E GARANTIAS DAS ENTIDADES DE REGISTO

As entidade que operam ER integradas na hierarquia do SCEE, estão obrigadas a:

a) Realizar suas operações de acordo com esta Politica de Certificados;

b) Realizar suas operações de acordo com as DPC da sua EC;

c) Comprovar, rigorosamente, a identidade das pessoas as quais se concede o certificado digital por eles tratado, pelo que requer a presença física da pessoa;

d) Não armazenar nem copiar os dados de criação de assinatura da pessoa a quem tenham prestado os seus serviços;

e) Informar, antes da emissão de um certificado, a pessoa que solicite seus serviços, das obrigações que assume, bem com deve guardar os dados de criação de assinatura e que procedimentos devem seguir para comunicar a perca ou utilização indevida dos dados ou dispositivos de criação ou verificação da assinatura, do seu preço, e das condições precisas para a utilização do certificado bem como das suas limitações de uso;

f) Validar e enviar, de forma segura, à EC a que está subordinada a ER, um pedido de certificação devidamente complementada com a informação fornecida pelo titular e assinada digitalmente e receber os certificados emitidos de acordo com esse pedido;

g) Armazenar de forma segura até ao momento do envio, tanto a documentação fornecida pelo titular como a gerada pela própria ER durante o processo de registo ou revogação;

h) Formalizar o contrato de Certificação com o titular segundo o estabelecido na

DPC;

i) Solicitar a revogação de um certificado quando tenha conhecimento ou suspeita de compromisso de uma chave privada;

j) Autenticar os pedidos dos utilizadores finais para a renovação ou revogação de seus certificados, gerar pedidos de renovação ou revogação assinados digitalmente e enviados a sua EC;

k) Em caso de aprovação de um pedido de certificação, notificar o titular a emissão do certificado e a forma de obtê-lo;

l) Em caso de negação de um pedido de certificação, notificar o titular desta recusa e o motivo da mesma;

m) Tratando-se de certificados pessoais, deve utilizar ferramentas de pedido e envio na presença da pessoa;

n) Manter sobre controlo restrito as ferramentas de tramitação de certificados digitais e notificar a sua EC, de qualquer mal funcionamento ou outra eventualidade que possa fugir ao comportamento normal;

o) Enviar uma cópia assinada do contracto de certificação e dos seus pedidos de revogação à EC;

p) Receber e tratar todos os pedido de revogação presenciais que receba, de forma imediata, depois de ter levar a cabo a respetiva identificação baseada no DN de quem solicita;

q) Colaborar nos vários aspetos da operação, auditoria ou controlo da ER, se tal lhe for solicitado pela EC;

r) Obrigada a confidencialidade durante e posteriormente, à prestação de serviços como Entidade de Registo, no que diz respeito à informação recebida da EC.

9.6.3. REPRESENTAÇÃO E GARANTIAS DOS TITULARES

É obrigação dos titulares dos certificados emitidos:

a) Limitar e adequar a utilização dos certificados, de acordo com as utilizações previstas na DPC;

b) Tomar todos os cuidados e medidas necessárias para garantir a posse da sua chave privada;

c) Solicitar de imediato a revogação de um certificado, em caso de ter conhecimento ou suspeita de compromisso da chave privada correspondente à chave pública contida no certificado. Os moldes em que pode fazer este pedido devem estar especificados na DPC, de acordo com o ponto 4.9.3 do presente documento;

d) 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;

e) Submeter à ER a informação que considerem exata e completa, com relação aos dados que estas solicitem para realizar o processo de registo. Deve informar a EC de qualquer modificação desta informação;

f) 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, de EC.

9.6.4. REPRESENTAÇÃO E GARANTIAS DAS PARTES CONFIANTES

É obrigação das partes que confiem nos certificados emitidos pelas EC do SCEE:

a) Limitar a fiabilidade dos certificados às utilizações permitidas para os mesmos em conformidade com o expresso na DPC correspondente;

b) Verificar a validade dos certificados no momento de realizar qualquer operação baseada nos mesmos;

c) Assumir a responsabilidade na correta verificação das assinaturas digitais;

d) Assumir a responsabilidade na comprovação da validade, revogação ou suspensão dos certificados em que confia;

e) Ter pleno conhecimento das garantias e responsabilidades aplicáveis na aceitação e uso de certificados em que confia e aceitar sujeitar-se às mesmas;

f) 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 da internet.

9.6.5. REPRESENTAÇÃO E GARANTIAS DE OUTROS PARTICIPANTES

Caso existam outros participantes as DPC devem declara-las nesta secção.

9.7. RENÚNCIA DE GARANTIAS

As EC do Estado podem recusar todas as garantias de serviço que não se encontrem vinculadas nas obrigações estabelecidas.

9.8. LIMITAÇÕES ÀS OBRIGAÇÕES

De acordo com a legislação em vigor.

9.9. INDEMNIZAÇÕES

De acordo com a legislação em vigor.

9.10. TERMO E CESSAÇÃO DA ATIVIDADE

9.10.1. TERMO

Esta PCert entra em vigor desde o momento de sua publicação no repositório de SCEE e após aprovação, nos termos do presente documento.

Esta PCert estará em vigor enquanto não for revogada expressamente pela emissão de uma nova versão, nos termos do presente documento, ou pela renovação das chaves da AC Raiz, momento em que, obrigatoriamente, se redigira uma nova versão.

9.10.2. SUBSTITUIÇÃO E REVOGAÇÃO DA PCERT

Esta PCert será substituída por uma nova versão, com independência da transcendência das mudanças efetuadas na mesma, de modo que será sempre de aplicação na sua totalidade.

Quando a PCert ficar revogada será retirada do repositório público, garantindo-se contudo que será conservada durante 20 anos.

9.10.3. CONSEQUÊNCIAS DA CESSAÇÃO DA ACTIVIDADE

As obrigações e restrições que estabelece esta PCert, em referência a auditorias, informação confidencial, obrigações e responsabilidades do SCEE, nascidas sob sua vigência, subsistirão após sua substituição ou revogação, por uma nova versão, em tudo o que não se oponha a esta.

9.11. NOTIFICAÇÃO INDIVIDUAL E COMUNICAÇÃO AOS PARTICIPANTES

Sem prejuízo do estabelecido no capítulo 4, do presente documento, sobre requisitos operacionais para o ciclo de vida dos certificados, os titulares de Certificados poderão comunicar com o SCEE, na qualidade de entidade que tem atribuídas as competências da infraestrutura de chave pública, através de mensagem eletrónica ou por escrito através de correio postal dirigido a qualquer das direções contidas no ponto 1.5 do presente documento.

No sítio da internet www.scee.gov.pt são disponibilizados outros mecanismos de contacto com a entidade competente.

As comunicações eletrónicas produzirão os seus efeitos assim que as receba o destinatário ao qual são dirigidas.

9.12. ALTERAÇÕES

9.12.1. PROCEDIMENTO PARA ALTERAÇÕES

Compete ao Conselho Gestor do SCEE realizar e aprovar mudanças sobre esta PCert. Os dados de contato do Conselho Gestor encontram-se no ponto 1.5 do presente documento.

9.12.2. PRAZO E MECANISMO DE NOTIFICAÇÃO

No caso em que o Conselho Gestor do SCEE julgue que as mudanças à especificação podem afetar à 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 PCert no repositório estabelecido. O mecanismo de comunicação será o sitio da internet http://www.scee.gov.pt.

9.12.3. MOTIVOS PARA MUDAR DE OID

Nos casos em que, a julgamento do Conselho Gestor do SCEE, as mudanças das especificações não afetem à aceitação dos certificados proceder-se-á ao aumento do número menor de versão do documento e o último número de Identificador de objeto (OID) que o representa, mantendo o número maior da versão do documento, assim como o resto de seu OID associado. Não se considera necessário comunicar este tipo de modificações aos utilizadores dos certificados.

No caso em que o Conselho Gestor do SCEE julgue que as mudanças à especificação podem afetar à aceitabilidade dos certificados para propósitos específicos proceder-se-á ao aumento do número maior de versão do documento e colocado

a zero o número menor da mesma. Também se modificarão os dois últimos números do Identificador de objeto (OID) que o representa. Este tipo de modificações comunicar-se-á aos utilizadores dos certificados segundo o estabelecido no ponto 9.12.2 do presente documento.

9.13. DISPOSIÇÕES PARA RESOLUÇÃO DE CONFLITOS

Todas reclamações, entre utilizadores e as EC do SCEE, deverão ser comunicadas pela parte em disputa ao Conselho Gestor do SCEE, com o fim de tentar resolvê-lo entre as partes.

Para a resolução de qualquer conflito que possa surgir com relação a esta PCert, as partes, com renúncia a qualquer outro foro que pudesse corresponder-lhes, submetem-se à jurisdição de contencioso administrativo.

9.14. LEGISLAÇÃO APLICÁVEL

A legislação aplicável ao SCEE está disponível no sitio da internet www.scee.gov.pt,

Todas as EC do SCEE devem nos seus sítios da internet terem disponíveis a legislação aplicável à sua atividade de certificação eletrónica, devendo a mesma estar atualizada.

9.15. CONFORMIDADE COM A LEGISLAÇÃO EM VIGOR

É responsabilidade do Conselho Gestor do SCEE zelar pelo cumprimento da legislação aplicável listada nos termos do ponto 9.14 do presente documento.

9.16. PROVIDÊNCIAS VÁRIAS

9.16.1. ACORDO COMPLETO

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

9.16.2. INDEPENDÊNCIA

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

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

9.16.3. SEVERIDADE

Não estipulado.

9.16.4. EXECUÇÕES (TAXAS DE ADVOGADOS E DESISTÊNCIA DE DIREITOS)

Não estipulado.

9.16.5. FORÇA MAIOR

Não estipulado.

9.17. OUTRAS PROVIDÊNCIAS

Não estipulado.

A. ANEXO – PERFIL DOS CERTIFICADOS

A.1. PERFIL DE CERTIFICADO DE ECRAIZESTADO

DESIGNAÇÃO (RFC 5280, ATUALIZADO PELO RFC 6818)	PERFIL	OBSERVAÇÕES
Basic Certificate Fields		
Certificate Fields		
4.1.1.1 tbsCertificate	Sim	
4.1.1.2 signatureAlgorithm	Sim	Sha256withRsaEncryption
4.1.1.3 signatureValue	Sim	
TBSCertificate		
4.1.2.1 Version	Sim	Versão 3
4.1.2.2 Serial number	Sim	Inteiro aleatório
4.1.2.3 Signature	Sim	
4.1.2.4 Issuer	Sim	CN=ECRaizEstado; O=SCEE; C=PT
4.1.2.5 Validity	Sim	24 Anos, com renovação a cada 12 anos
4.1.2.6 Subject	Sim	CN=ECRaizEstado; O=SCEE; C=PT
4.1.2.7 Subject Public Key Info	Sim	RSAEncrytion, com dimensão de 4096 bit
4.1.2.8 Unique Identifiers	Não	
4.1.2.9 Extensions	Sim	
Standard Extensions		
4.2.1.1 Authority Key Identifier	Não	
4.2.1.2 Subject Key Identifier	Sim	KeyIdentifier=Hash (SubjectPublicKey do certificado)

4.2.1.3 Key Usage	Crítica	bit(s) ativo(s): KeyCertSign; cRLSign
4.2.1.4 Private Key Usage Period	Não	
4.2.1.5 Certificate Policies	Sim	policyIdentifier=“AnyPolicy” com o OID: 2.5.29.32.0 e cPSuri=http://www.scee.gov.pt
4.2.1.6 Policy Mappings	Não	
4.2.1.7 Subject Alternative Name	Não	
4.2.1.8 Issuer Alternative Name	Não	
4.2.1.9 Subject Directory Attributes	Não	
4.2.1.10 Basic Constraints	Crítica	cA=True e PathLenConstraint=0
4.2.1.11 Name Constraints	Não	
4.2.1.12 Policy Constraints	Não	
4.2.1.13 Extended Key Usage	Não	
4.2.1.14 CRL Distribution Points	Não	
4.2.1.15 Inhibit Any-Policy	Não	
4.2.1.16 Freshest CRL	Não	
Internet Certificate Extensions		
4.2.2.1 Authority Information Access	Não	

4.2.2.2 Subject Information Access	Não	

A.2. PERFIL DE CERTIFICADO DE ECESTADO

DESIGNAÇÃO (RFC 5280, ATUALIZADO PELO RFC 6818)	PERFIL	OBSERVAÇÕES
Basic Certificate Fields		
Certificate Fields		
4.1.1.1 tbsCertificate	Sim	
4.1.1.2 signatureAlgorithm	Sim	Sha256withRsaEncryption
4.1.1.3 signatureValue	Sim	
TBSCertificate		
4.1.2.1 Version	Sim	Versão 3
4.1.2.2 Serial number	Sim	Inteiro aleatório
4.1.2.3 Signature	Sim	
4.1.2.4 Issuer	Sim	CN=ECRaizEstado; O=SCEE; C=PT
4.1.2.5 Validity	Sim	12 Anos, com renovação a cada 6 anos ou 2 anos
4.1.2.6 Subject	Sim	CN=[...]; OU= ECEstado; O=SCEE; C=PT
4.1.2.7 Subject Public Key Info	Sim	RSAEncrytion, com dimensão mínima de 2048 bit
4.1.2.8 Unique Identifiers	Sim	
4.1.2.9 Extensions	Sim	

Standard Extensions		
4.2.1.1 Authority Key Identifier	Sim	KeyIdentifier=Hash (SubjectPublicKey do certificado do Issuer)
4.2.1.2 Subject Key Identifier	Sim	KeyIdentifier=Hash (SubjectPublicKey do certificado)
4.2.1.3 Key Usage	CRÍTICA	bit(s) ativo(s): KeyCertSign; cRLSign
4.2.1.4 Private Key Usage Period	Não	
4.2.1.5 Certificate Policies	Sim	policyIdentifier="AnyPolicy" com o OID: 2.5.29.32.0 e cPSuri=[...]
4.2.1.6 Policy Mappings	Não	
4.2.1.7 Subject Alternative Name	Não	
4.2.1.8 Issuer Alternative Name	Não	
4.2.1.9 Subject Directory Attributes	Não	
4.2.1.10 Basic Constraints	Crítica	cA=True e PathLenConstraint=[...]
4.2.1.11 Name Constraints	Não	
4.2.1.12 Policy Constraints	Não	
4.2.1.13 Extended Key Usage	Não	
4.2.1.14 CRL Distribution Points	Sim	"distributionPoint"= [Inserir a localização do(s) repositório(s) onde podem ser descarregada(s) as LRC]

		(1) HTTP – http://crls.ecee.gov.pt/crls/ARL.crl (2) [a DPC descreverá a existência ou não de outros pontos]
4.2.1.15 Inhibit Any-Policy	Não	
4.2.1.16 Freshest CRL	Não	
Internet Certificate Extensions		
4.2.2.1 Authority Information Access	Opcional	accessMethod ::={1.3.6.1.5.5.7.48.1} – "id-ad-ocsp" accessLocation ::= {Introduzir a localização do OCSP responder}
4.2.2.2 Subject Information Access	NÃO	

A.3. PERFIL DE CERTIFICADO DE ASSINATURA DIGITAL

Perfil A

DESIGNAÇÃO (RFC 5280, ATUALIZADO PELO RFC 6818)	PERFIL	OBSERVAÇÕES
Basic Certificate Fields		
Certificate Fields		
4.1.1.1 tbsCertificate	Sim	
4.1.1.2 signatureAlgorithm	Sim	Sha256withRsaEncryption RSASSA-PSS com mgf1SHA-256
4.1.1.3 signatureValue	Sim	
TBSCertificate		
4.1.2.1 Version	Sim	Versão 3
4.1.2.2 Serial number	Sim	Inteiro aleatório
4.1.2.3 Signature	Sim	
4.1.2.4 Issuer	Sim	CN=[...]; OU= ECEstado; O=SCEE; C=PT
4.1.2.5 Validity	Sim	Até 10 Anos
4.1.2.6 Subject	Sim	CN=[nome]; OU=[organismo]; O=[ministério]; C=PT
4.1.2.7 Subject Public Key Info	Sim	RSAEncrytion, com dimensão mínima de 2048 bit
4.1.2.8 Unique Identifiers	Não	

4.1.2.9 Extensions	Sim	
Standard Extensions		
4.2.1.1 Authority Key Identifier	Sim	KeyIdentifier=Hash (SubjectPublicKey do certificado do Issuer)
4.2.1.2 Subject Key Identifier	Sim	KeyIdentifier=Hash (SubjectPublicKey do certificado)
4.2.1.3 Key Usage	Crítica	bit(s) ativo(s): nonRepudiation (contentCommitment)
4.2.1.4 Private Key Usage Period	Não	
4.2.1.5 Certificate Policies	Sim	policyIdentifier= scee-assinatura, com o OID: [2.16.620.1.1.1.2.10] ; cPSuri=[...]; userNotice="O certificado emitido segundo esta política é equivalente a um certificado digital qualificado, nos termos, do definido na Legislação Portuguesa, aplicável para o efeito"
4.2.1.6 Policy Mappings	Não	
4.2.1.7 Subject Alternative Name	Opção	
4.2.1.8 Issuer Alternative Name	Não	
4.2.1.9 Subject Directory Attributes	Não	
4.2.1.10 Basic Constraints	Crítica	cA=False

4.2.1.11 Name Constraints	Não	
4.2.1.12 Policy Constraints	Não	
4.2.1.13 Extended Key Usage	Opção	
4.2.1.14 CRL Distribution Points	Sim	"distributionPoint"= [Inserir a localização do(s) repositório(s) onde podem ser descarregada(s) as LRC] (1) HTTP - http://crls.ecee.gov.pt/crls/ARL.crl (2) [a DPC descreverá a existência ou não de outros pontos]
4.2.1.15 Inhibit Any-Policy	Não	
4.2.1.16 Freshest CRL	Não	
Internet Certificate Extensions		
4.2.2.1 Authority Information Access	Opcional	accessMethod ::={1.3.6.1.5.5.7.48.1} - "id-ad-ocsp" accessLocation ::= { Introduzir a localização do OCSP responder }
4.2.2.2 Subject Information Access	Não	

Perfil B

DESIGNAÇÃO (RFC 5280, ATUALIZADO PELO RFC 6818)	PERFIL	OBSERVAÇÕES
Basic Certificate Fields		
Certificate Fields		
4.1.1.1 tbsCertificate	Sim	
4.1.1.2 signatureAlgorithm	Sim	Sha256withRsaEncryption RSASSA-PSS com mgf1SHA-256
4.1.1.3 signatureValue	Sim	
TBSCertificate		
4.1.2.1 Version	Sim	Versão 3
4.1.2.2 Serial number	Sim	Inteiro aleatório
4.1.2.3 Signature	Sim	
4.1.2.4 Issuer	Sim	CN=[...]; OU= ECEstado; O=SCEE; C=PT
4.1.2.5 Validity	Sim	Até 10 Anos
4.1.2.6 Subject	Sim	CN=[nome]; O=[organismo]; C=PT
4.1.2.7 Subject Public Key Info	Sim	RSAEncrytion, com dimensão mínima de 2048 bit
4.1.2.8 Unique Identifiers	Não	
4.1.2.9 Extensions	Sim	
Standard Extensions		
4.2.1.1 Authority Key Identifier	Sim	KeyIdentifier=Hash (SubjectPublicKey do certificado do Issuer)

4.2.1.2 Subject Key Identifier	Sim	KeyIdentifier=Hash (SubjectPublicKey do certificado)
4.2.1.3 Key Usage	Crítica	bit(s) ativo(s): nonRepudiation (contentCommitment)
4.2.1.4 Private Key Usage Period	Não	
4.2.1.5 Certificate Policies	Sim	policyIdentifier= scee-assinatura, com o OID: [2.16.620.1.1.1.2.10] ; cPSuri=[...]; userNotice="O certificado emitido segundo esta política é equivalente a um certificado digital qualificado, nos termos, do definido na Legislação Portuguesa, aplicável para o efeito"
4.2.1.6 Policy Mappings	Não	
4.2.1.7 Subject Alternative Name	Opção	
4.2.1.8 Issuer Alternative Name	Não	
4.2.1.9 Subject Directory Attributes	Não	
4.2.1.10 Basic Constraints	Crítica	cA=False
4.2.1.11 Name Constraints	Não	
4.2.1.12 Policy Constraints	Não	
4.2.1.13 Extended Key Usage	Opção	

4.2.1.14 CRL Distribution Points	Sim	"distributionPoint"= [Inserir a localização do(s) repositório(s) onde podem ser descarregada(s) as LRC] (1) HTTP - http://crls.ecee.gov.pt/crls/ARL.crl (2) [a DPC descreverá a existência ou não de outros pontos]
4.2.1.15 Inhibit Any-Policy	Não	
4.2.1.16 Freshest CRL	Não	
Internet Certificate Extensions		
4.2.2.1 Authority Information Access	Opcional	accessMethod ::={1.3.6.1.5.5.7.48.1} - "id-ad-ocsp" accessLocation ::= { Introduzir a localização do OCSP responder }
4.2.2.2 Subject Information Access	Não	

A.4. PERFIL DE CERTIFICADO DE AUTENTICAÇÃO

Perfil A

DESIGNAÇÃO (RFC 5280, ATUALIZADO PELO RFC 6818)	PERFIL	OBSERVAÇÕES
Basic Certificate Fields		
Certificate Fields		
4.1.1.1 tbsCertificate	Sim	
4.1.1.2 signatureAlgorithm	Sim	Sha256withRsaEncryption RSASSA-PSS com mgf1SHA-256
4.1.1.3 signatureValue	Sim	
TBSCertificate		
4.1.2.1 Version	Sim	Versão 3
4.1.2.2 Serial number	Sim	Inteiro aleatório
4.1.2.3 Signature	Sim	
4.1.2.4 Issuer	Sim	CN=[...]; OU= ECEstado; O=SCEE; C=PT
4.1.2.5 Validity	Sim	Até 10 Anos
4.1.2.6 Subject	Sim	CN=[nome];OU=[organismo];O=[ministério]; C=PT
4.1.2.7 Subject Public Key Info	Sim	RSAEncrytion, com dimensão mínima de 2048 bit
4.1.2.8 Unique Identifiers	Não	
4.1.2.9 Extensions	Sim	
Standard Extensions		
4.2.1.1 Authority Key Identifier	Não	KeyIdentifier=Hash (SubjectPublicKey do certificado do Issuer)

4.2.1.2 Subject Key Identifier	Sim	KeyIdentifier=Hash (SubjectPublicKey do certificado)
4.2.1.3 Key Usage	Crítica	bit(s) ativo(s): digitalSignature e/ou keyAgreement
4.2.1.4 Private Key Usage Period	Não	
4.2.1.5 Certificate Policies	Sim	policyIdentifier= scee-autenticacao, com o OID: [2.16.620.1.1.1.2.20] ; cPSuri=[...] ; userNotice=[...]
4.2.1.6 Policy Mappings	Não	
4.2.1.7 Subject Alternative Name	Não	
4.2.1.8 Issuer Alternative Name	Não	
4.2.1.9 Subject Directory Attributes	Não	
4.2.1.10 Basic Constraints	Crítica	cA=False
4.2.1.11 Name Constraints	Não	
4.2.1.12 Policy Constraints	Não	
4.2.1.13 Extended Key Usage	Opcional	

4.2.1.14 CRL Distribution Points	Sim	"distributionPoint"= [Inserir a localização do(s) repositório(s) onde podem ser descarregada(s) as LRC] (1) HTTP - http://crls.ecee.gov.pt/crls/ARL.crl (2) [a DPC descreverá a existência ou não de outros pontos]
4.2.1.15 Inhibit Any-Policy	Não	
4.2.1.16 Freshest CRL	Não	
Internet Certificate Extensions		
4.2.2.1 Authority Information Access	Opcional	accessMethod ::={1.3.6.1.5.5.7.48.1} - "id-ad-ocsp" accessLocation ::= { Introduzir a localização do OCSP responder }
4.2.2.2 Subject Information Access	Não	

Perfil B

DESIGNAÇÃO (RFC5280, ATUALIZADO PELO RFC 6818)	PERFIL	OBSERVAÇÕES
Basic Certificate Fields		
Certificate Fields		
4.1.1.1 tbsCertificate	Sim	
4.1.1.2 signatureAlgorithm	Sim	
4.1.1.3 signatureValue	Sim	Sha256withRsaEncryption RSASSA-PSS com mgf1SHA-256
TBSCertificate		
4.1.2.1 Version	Sim	Versão 3
4.1.2.2 Serial number	Sim	Inteiro aleatório
4.1.2.3 Signature	Sim	
4.1.2.4 Issuer	Sim	CN=[...]; OU= ECEstado; O=SCEE; C=PT
4.1.2.5 Validity	Sim	Até 10 Anos
4.1.2.6 Subject	Sim	CN=[nome];O=[organismo]; C=PT
4.1.2.7 Subject Public Key Info	Sim	RSAEncrytion, com dimensão mínima de 2048 bit
4.1.2.8 Unique Identifiers	Não	
4.1.2.9 Extensions	Sim	
Standard Extensions		
4.2.1.1 Authority Key Identifier	Não	KeyIdentifier=Hash (SubjectPublicKey do certificado do Issuer)

4.2.1.2 Subject Key Identifier	Sim	KeyIdentifier=Hash (SubjectPublicKey do certificado)
4.2.1.3 Key Usage	Crítica	bit(s) ativo(s): digitalSignature e/ou keyAgreement
4.2.1.4 Private Key Usage Period	Não	
4.2.1.5 Certificate Policies	Sim	policyIdentifier= scee-autenticacao, com o OID: [2.16.620.1.1.1.2.20] ; cPSuri=[...] ; userNotice=[...]
4.2.1.6 Policy Mappings	Não	
4.2.1.7 Subject Alternative Name	Não	
4.2.1.8 Issuer Alternative Name	Não	
4.2.1.9 Subject Directory Attributes	Não	
4.2.1.10 Basic Constraints	Crítica	cA=False
4.2.1.11 Name Constraints	Não	
4.2.1.12 Policy Constraints	Não	
4.2.1.13 Extended Key Usage	Opcional	

4.2.1.14 CRL Distribution Points	Sim	"distributionPoint"= [Inserir a localização do(s) repositório(s) onde podem ser descarregada(s) as LRC] (1) HTTP - http://crls.ecee.gov.pt/crls/ARL.crl (2) [a DPC descreverá a existência ou não de outros pontos]
4.2.1.15 Inhibit Any-Policy	Não	
4.2.1.16 Freshest CRL	Não	
Internet Certificate Extensions		
4.2.2.1 Authority Information Access	Opcional	accessMethod ::={1.3.6.1.5.5.7.48.1} - "id-ad-ocsp" accessLocation ::= { Introduzir a localização do OCSP responder }
4.2.2.2 Subject Information Access	Não	

A.5. PERFIL DE CERTIFICADO DE CONFIDENCIALIDADE

Perfil A

DESIGNAÇÃO (RFC 5280, ATUALIZADO PELO RFC 6818)	PERFIL	OBSERVAÇÕES
Basic Certificate Fields		
Certificate Fields		
4.1.1.1 tbsCertificate	Sim	
4.1.1.2 signatureAlgorithm	Sim	Sha256withRsaEncryption RSASSA-PSS com mgf1SHA-256
4.1.1.3 signatureValue	Sim	
TBSCertificate		
4.1.2.1 Version	Sim	Versão 3
4.1.2.2 Serial number	Sim	Inteiro aleatório
4.1.2.3 Signature	Sim	
4.1.2.4 Issuer	Sim	CN=[...]; OU= ECEstado; O=SCEE; C=PT
4.1.2.5 Validity	Sim	Até 10 Anos
4.1.2.6 Subject	Sim	CN=[nome];OU=[organismo];O=[ministério]; C=PT
4.1.2.7 Subject Public Key Info	Sim	RSAEncrytion, com dimensão mínima de 2048 bit
4.1.2.8 Unique Identifiers	Não	

4.1.2.9 Extensions	Sim	
Standard Extensions		
4.2.1.1 Authority Key Identifier	Não	KeyIdentifier=Hash (SubjectPublicKey do certificado do Issuer)
4.2.1.2 Subject Key Identifier	Sim	KeyIdentifier=Hash (SubjectPublicKey do certificado)
4.2.1.3 Key Usage	Crítica	bit(s) ativo(s): keyEncipherment e/ou Dataencipherment
4.2.1.4 Private Key Usage Period	Não	
4.2.1.5 Certificate Policies	Sim	policyIdentifier=scee-confidencialidade, com o OID: 2.16.620.1.1.1.2.30 ; cPSuri=[...] ; userNotice=[...]
4.2.1.6 Policy Mappings	Não	
4.2.1.7 Subject Alternative Name	Não	
4.2.1.8 Issuer Alternative Name	Não	
4.2.1.9 Subject Directory Attributes	Não	
4.2.1.10 Basic Constraints	Crítica	cA=False
4.2.1.11 Name Constraints	Não	
4.2.1.12 Policy Constraints	Não	
4.2.1.13 Extended Key Usage	Opcional	

4.2.1.14 CRL Distribution Points	Sim	"distributionPoint"= [Inserir a localização do(s) repositório(s) onde podem ser descarregada(s) as LRC]
4.2.1.15 Inhibit Any-Policy	Não	
4.2.1.16 Freshest CRL	Não	
Internet Certificate Extensions		
4.2.2.1 Authority Information Access	Opcional	accessMethod ::={1.3.6.1.5.5.7.48.1} - "id-ad-ocsp" accessLocation ::= { Introduzir a localização do OCSP responder }
4.2.2.2 Subject Information Access	Não	

Perfil B

DESIGNAÇÃO (RFC 5280, ATUALIZADO PELO RFC 6818)	PERFIL	OBSERVAÇÕES
Basic Certificate Fields		
Certificate Fields		
4.1.1.1 tbsCertificate	Sim	
4.1.1.2 signatureAlgorithm	Sim	Sha256withRsaEncryption RSASSA-PSS com mgf1SHA-256
4.1.1.3 signatureValue	Sim	
TBSCertificate		
4.1.2.1 Version	Sim	Versão 3

4.1.2.2 Serial number	Sim	Inteiro aleatório
4.1.2.3 Signature	Sim	
4.1.2.4 Issuer	Sim	CN=[...]; OU= ECEstado; O=SCEE; C=PT
4.1.2.5 Validity	Sim	Até 10 Anos
4.1.2.6 Subject	Sim	CN=[nome];O=[organismo; C=PT
4.1.2.7 Subject Public Key Info	Sim	RSAEncrytion, com dimensão mínima de 2048 bit
4.1.2.8 Unique Identifiers	Não	
4.1.2.9 Extensions	Sim	
Standard Extensions		
4.2.1.1 Authority Key Identifier	Não	KeyIdentifier=Hash (SubjectPublicKey do certificado do Issuer)
4.2.1.2 Subject Key Identifier	Sim	KeyIdentifier=Hash (SubjectPublicKey do certificado)
4.2.1.3 Key Usage	Crítica	bit(s) ativo(s): keyEncipherment e/ou Dataencipherment
4.2.1.4 Private Key Usage Period	Não	
4.2.1.5 Certificate Policies	Sim	policyIdentifier=scee-confidencialidade, com o OID: 2.16.620.1.1.1.2.30 ; cPSuri=[...] ; userNotice=[...]
4.2.1.6 Policy Mappings	Não	
4.2.1.7 Subject Alternative Name	Não	

4.2.1.8 Issuer Alternative Name	Não	
4.2.1.9 Subject Directory Attributes	Não	
4.2.1.10 Basic Constraints	Crítica	cA=False
4.2.1.11 Name Constraints	Não	
4.2.1.12 Policy Constraints	Não	
4.2.1.13 Extended Key Usage	Opcional	
4.2.1.14 CRL Distribution Points	Sim	"distributionPoint"= [Inserir a localização do(s) repositório(s) onde podem ser descarregada(s) as LRC]
4.2.1.15 Inhibit Any-Policy	Não	
4.2.1.16 Freshest CRL	Não	
Internet Certificate Extensions		
4.2.2.1 Authority Information Access	Opcional	accessMethod ::={1.3.6.1.5.5.7.48.1} - "id-ad-ocsp" accessLocation ::= { Introduzir a localização do OCSP responder }
4.2.2.2 Subject Information Access	Não	

B. ANEXO – PERFIL DAS LCR

DESIGNAÇÃO (RFC 5280, ATUALIZADO PELO RFC 6818)	PERFIL	OBSERVAÇÕES
CertificateList Fields		
5.1.1.1 tbsCertList		
5.1.1.2 signatureAlgorithm	Sim	
5.1.1.3 signatureValue	Sim	
tbsCertList		
5.1.2.1 Version	Sim	
5.1.2.2 Signature	Sim	
5.1.2.3 Issuer Name	Sim	
5.1.2.4 This Update	Sim	
5.1.2.5 Next Update	Sim	
5.1.2.6 Revoked Certificates	Sim	
5.1.2.7 Extensions	Sim	
CRL Extensions		
5.2.1 Authority Key Identifier	Sim	
5.2.2 Issuer Alternative Name	Não	

5.2.3 CRL Number	Sim	
5.2.4 Delta CRL Indicator	Não	
5.2.5 Issuing Distribution Point	Não	
5.2.6 Freshest CRL	Não	
CRL Entry Extensions		
5.3.1 Reason Code	Sim	
5.3.2 Hold Instruction Code	Não	
5.3.3 Invalidity Date	Não	
5.3.4 Certificate Issuer	Não	

C. ANEXO – NORMALIZAÇÃO TÉCNICA

X.501	**Nome:**	ITU-T RECOMMENDATION X.501 (10/12) | ISO/IEC 9594-2:2001
	Versão:	-----
	Tipo:	Recommendation
	Data:	Novembro de 2012
	Organismo:	International Telecommunications Union
	Descrição:	Information technology – Open Systems Interconnection – The Directory: Models
X.509	**Nome:**	ITU-T Recommendation X.509 (10/12) | ISO/IEC 9594-8
	Versão:	-----
	Tipo:	Recommendation
	Data:	Novembro de 2012
	Organismo:	International Telecommunications Union
	Descrição:	Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks
RFC3647	**Nome:**	RFC 3647
	Versão:	Torna obsoleto o RFC 2527
	Tipo:	Request For Comments
	Data:	Novembro de 2003
	Organismo:	Internet Engineering Task Force – PKIX Working Group
	Descrição:	Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework

RFC3739	**Nome:**	RFC 3739
	Versão:	
	Tipo:	Request For Comments
	Data:	Março de 2013
	Organismo:	Internet Engineering Task Force – PKIX Working Group
	Descrição:	Internet X.509 Public Key Infrastructure: Qualified Certificates Profile
RFC 5280	**Nome:**	RFC 5280
	Versão:	Torna obsoleto o RFC 3280 e é atualizado pelo RFC 6818
	Tipo:	Request For Comments
	Data:	Março de 2013
	Organismo:	Internet Engineering Task Force – PKIX Working Group
	Descrição:	Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL).
RFC6960	**Nome:**	RFC 6960
	Versão:	Torna obsoleto o RFC 2560
	Tipo:	Request For Comments
	Data:	Junho de 2013
	Organismo:	Internet Engineering Task Force – PKIX Working Group
	Descrição:	X.509 Internet Public Key Infrastructure – Online Certificate Status Protocol – OCSP
RFC4210	**Nome:**	RFC 4210
	Versão:	Torna obsoleto o RFC 2510 e é atualizado pelo RFC 6712
	Tipo:	Request For Comments
	Data:	Fevereiro de 2013

	Organismo:	Internet Engineering Task Force - PKIX Working Group
	Descrição:	Internet X.509 Public Key Infrastructure - Certificate Management Protocols (CMP)
ISO27001	**Nome:**	ISO/IEC 27001:2013
	Versão:	-----
	Tipo:	Recommendation
	Data:	Outubro de 2013
	Organismo:	International Telecommunications Union
	Descrição:	formation technology-Security techniques-Information security management systems-Requirements
ISO27002	**Nome:**	ISO/IEC 27002:2013
	Versão:	-----
	Tipo:	Recommendation
	Data:	Junho de 2013
	Organismo:	International Telecommunications Union
	Descrição:	Information technology -- Security techniques -- Code of practice for information security management
ISO15408-1	**Nome:**	ISO/IEC 15408-1:2009
	Versão:	---
	Tipo:	International Standard
	Data:	Dezembro 2009
	Organismo:	International Organization for Standardization) e International Electrotechnical Commission
	Descrição:	Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model

ISO15408-2	**Nome:**	ISO/IEC 15408-2:2008
	Versão:	---
	Tipo:	International Standard
	Data:	Agosto de 2008
	Organismo:	International Organization for Standardization) e International Electrotechnical Commission
	Descrição:	Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements
ISO15408-3	**Nome:**	ISO/IEC 15408-1:2005
	Versão:	---
	Tipo:	International Standard
	Data:	Agosto de 2008
	Organismo:	International Organization for Standardization) e International Electrotechnical Commission
	Descrição:	model Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements
ISO9564-1	**Nome:**	ISO 9564-1:2011
	Versão:	----
	Tipo:	International Draft
	Data:	Maio de 2002
	Organismo:	International Organization for Standardization
	Descrição:	Financial services -- Personal Identification Number (PIN) management and security -- Part 1: Basic principles and requirements for PINs in card-based systems
ISO3166-1	**Nome:**	ISO 3166-1:2013

	Versão:	-----
	Tipo:	International Draft
	Data:	Novembro 2013
	Organismo:	International Organization for Standardization
	Descrição:	Codes for the representation of names of countries and their subdivisions -- Part 1: Country codes
ISO11568-5	**Nome:**	ISO 11568-5:2007
	Versão:	-----
	Tipo:	International Standard
	Data:	Janeiro de 2007
	Organismo:	International Organization for Standardization
	Descrição:	Banking -- Key management (retail) -- Part 4: Asymmetric cryptosystems -- Key management and life cycle
FIPS140-2	**Nome:**	FIPS PUB 140-2
	Versão:	Atualiza o FIPS PUB 140-1 de Janeiro de 1994
	Tipo:	Federal Information Processing Standards Publication
	Data:	Março 2002
	Organismo:	US National Institute of Standards and Technology
	Descrição:	"Security Requirements For Cryptographic Modules".
ETSI102280	**Nome:**	ETSI TS 102 280
	Versão:	V1.1.1
	Tipo:	
	Data:	Março de 2004
	Organismo:	
	Descrição:	X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons

ETSI101862	**Nome:**	ETSI TS 101 862
	Versão:	V1.3.3
	Tipo:	Technical Specification
	Data:	Janeiro de 2006
	Organismo:	Electronic Signatures and Infrastructures (ESI);
	Descrição:	Qualified Certificate profile
ETSI102176	**Nome:**	ETSI TS 102 176-1
	Versão:	V2.1.1
	Tipo:	Technical Specification
	Data:	Julho de 2011
	Organismo:	Electronic Signatures and Infrastructures (ESI);
	Descrição:	Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures Part 1: Hash functions and asymmetric algorithms
CWA14167-2	**Nome:**	CWA 14167-2
	Versão:	
	Tipo:	CEN Workshop Agreement
	Data:	Março de 2012
	Organismo:	
	Descrição:	European Committee for Standardization Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 2: Cryptographic Module for CSP signing operations with backup – Protection profile (CMCSOB-PP)
CWA14167-1	**Nome:**	CWA 14167-1
	Versão:	

	Tipo:	CEN Workshop Agreement
	Data:	
	Organismo:	European Committee for Standardization
	Descrição:	Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1: System Security Requirements
CCMB1	**Nome:**	CCMB-2012-09-001
	Versão:	Versão 3.1 Rev. 4
	Tipo:	
	Data:	Setembro de 2012
	Organismo:	
	Descrição:	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model
CCMB2	**Nome:**	CCMB-2012-09-002
	Versão:	Versão 3.1 Rev. 4
	Tipo:	
	Data:	Setembro de 2012
	Organismo:	
	Descrição:	Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements
CCMB3	**Nome:**	CCMB-2012-09-003
	Versão:	Versão 3.1 Rev. 4
	Tipo:	
	Data:	Setembro de 2012
	Organismo:	
	Descrição:	

		Common Criteria for Information Technology Security Evaluation Part 3: Security assurance
GNS/NT-D-02	**Nome:**	GNS/NT-D-02
	Versão:	-----
	Tipo:	Requisitos
	Data:	Setembro de 2008
	Organismo:	Gabinete Nacional de Segurança
	Descrição:	Requisitos Mínimos de Segurança Física de Instalações de Entidades Certificadoras
GNS/NT-D-03	**Nome:**	GNS/NT-D-03
	Versão:	-----
	Tipo:	Requisitos
	Data:	Novembro de 2009
	Organismo:	Gabinete Nacional de Segurança
	Descrição:	Requisitos para entidades Certificadoras que emitem Certificados Qualificados

D. ANEXO – DEFINIÇÕES E ACRÓNIMOS

Com o objetivo de conhecer os conceitos que são utilizados no presente documento e nas diferentes Declarações de Práticas de Certificação deve entender-se:

D.1. ACRÓNIMOS

AdmHSM	Administradores do HSM
AdmReg	Administrador de registo
AdmSeg	Administrador de Segurança
AdmSist	Administrador de Sistemas
AuditorS	Auditor de Sistemas
AV	Autoridades de Validação
C	Country
CEN	Comité Européen de Normalisation
CMP	Certificate Management Protocols
CMP	Certificate Management Protocol
CN	Common Name
CSP	Cryptographic Service Provider Microsoft
CWA	CEN Workshop Agreement
DN	Distinguished Name
DPC	Declaração de Práticas de Certificação

EC	Entidade Certificadora
SCEE	Sistema de Certificação Eletrónica do Estado
ECEstado	Entidade Certificadora do Estado
ECRaizEstado	Entidade Certificadora de Raiz do Estado
ER	Entidade de registo
EREstado	Entidade de Registo do Estado
ETSI	European Telecommunications Standard Institute
FIPS	Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
HSM	Hardware Security Module.
ICP	Infraestrutura de Chave Pública
IDS/IPS	Intrusion Detection System / Intrusion Prevention System
IETF	Internet Engineering Task Force
LCR	Lista de Certificados Revogados
LDAP	Lightweight Directory Access Protocol
LER	Lista de Entidades Revogadas
O	Organization
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OpHSM	Operadores do HSM

OpSist	Operador de Sistemas
OU	Organizacional Unit
P1	Perfil de Certificado de ECRaizEstado;
P2	Perfil de Certificado de ECEstado;
P3	Perfil de Certificado de Assinatura Digital;
P4	Perfil de Certificado de Autenticação;
P5	Perfil de Certificado de Confidencialidade;
P6	Perfil de Certificado de Time Stamping;
P7	Perfil de Certificado de OCSP.
PC	Política de Certificado
PCert	Política de Certificados do SCEE
PED	PIN Entry Device
PKCS	Public-Key Cryptography Standards
PKCS#1	RSA Cryptography Standard
PKCS#10	Certification Request Syntax Standard
PKCS#11	Cryptographic Token Interface Standard
PKCS#7	Cryptographic Message Syntax Standard
RAF	Relatório de auditoria final
RCI	Relatório de correção de irregularidades
RFC	Request For Comments

RPI	Relatório de primeiras impressões
RSA	Algoritmo criptográfico (Rivest | Shamir | Adleman)
RSAE	Relatório Sumário de Análise de Eventos
SubECEstado	Entidade Certificadora Subordinada duma ECEstado
TCP/IP	Transmission Control Protocol/Internet Protocol
TRT	Termo de Responsabilidade do Titular
OID	Identificador de Objecto
URL	Unified Resource Locator

D.2. 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 avançada	Assinatura eletrónica que preenche os seguintes requisitos: i) Identifica de forma unívoca o titular como autor do documento; ii) A sua aposição ao documento depende apenas da vontade do titular; iii) É criada com meios que o titular pode manter sob seu controlo exclusivo; iv) 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;

Assinatura eletrónica	É o 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.
Autoridade Credenciadora	Entidade competente para a credenciação e fiscalização das entidades certificadoras;
C	Atributo do DN de um objeto dentro da estrutura de diretório X.500.
Certificado	Estrutura de dados assinado eletronicamente por um prestador de serviços de certificação e que vincula ao titular os dados de validação de assinatura que confirma a sua identidade.
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;
Chave	Sequência de símbolos
CN	Atributo do DN de um objeto dentro da estrutura de diretório X.500.
Credenciação	Ato pelo qual é reconhecido a uma entidade que o solicite e que exerça a catividade de entidade certificadora o preenchimento

	dos requisitos definidos no presente diploma para os efeitos nele previstos;
Dados de Ativação	Dados privados, diferentes das chaves, exigidos para o acesso aos módulos criptográficos.
Dados de criação de assinatura	São dados únicos, como códigos ou chaves criptográficas privadas que o titular utiliza para gerar a sua assinatura eletrónica.
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	São dados como códigos ou chaves criptográficas públicas, que se utilizam para verificar a assinatura eletrónica.
Dados de verificação de assinatura	Conjunto de dados, como chaves públicas, utilizado para verificar uma assinatura eletrónica;
Declaração de Práticas de Certificação	Documento onde são especificados ao pormenor a forma como Prestador de Serviços de Certificação realiza as atividades relacionadas com a gestão do ciclo de vida do certificado
Diretório de Certificados:	Repositório de informação que segue o standard X500
Dispositivo de criação de assinatura	Suporte lógico ou dispositivo de equipamento utilizado para possibilitar o tratamento dos dados de criação de assinatura;
Dispositivo seguro de criação de assinatura	Dispositivo de criação de assinatura que assegure, através de meios técnicos e processuais adequados, que:

	i) Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura só possam ocorrer uma única vez e que a confidencialidade desses dados se encontre assegurada; ii) Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura não possam, com um grau razoável de segurança, ser deduzidos de outros dados e que a assinatura esteja protegida contra falsificações realizadas através das tecnologias disponíveis; iii) Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura possam ser eficazmente protegidos pelo titular contra a utilização ilegítima por terceiros; iv) Os dados que careçam de assinatura não sejam modificados e possam ser apresentados ao titular antes do processo de assinatura;
DN	Identificação unívoca de uma entrada dentro da estrutura de diretório X.500.
Documento Eletrónico	Conjunto de dados lógicos armazenados em suporte suscetível de poder ser lido por equipamentos eletrónicos de processamento de dados.
Endereço eletrónico	Identificação de um equipamento informático adequado para receber e arquivar documentos eletrónicos.
Entidade certificadora	Entidade ou pessoa singular ou coletiva que cria ou fornece meios para a criação e verificação das assinaturas, emite os certificados, assegura a respetiva publicidade e presta outros serviços relativos a assinaturas eletrónicas;

Entidade Filiada	Entidade certificadora pública ou privada que, após o processo administrativo e de segurança para a filiação, é aprovada pelo Conselho Gestor do SCEE formalmente como EC filiada ao SCEE.
Entidade de Registo	Entidade ou pessoa singular ou coletiva designada pelas Entidades Certificadoras para realizar atividades de comprovação da identidade dos subscritores ou titulares e consequente registo, bem como a gestão de pedidos de revogação de certificados.
Função hash	É uma operação que se realiza sobre um conjunto de dados de qualquer tamanho de forma que o resultado obtido é outro conjunto de dados de tamanho fixo independente do tamanho original e que tem a propriedade de estar associado univocamente aos dados inicias e garantir que é impossível obter mensagens distintas que gerem o mesmo resultado ao aplicar esta função.
Hash ou impressão digital	Resultado de tamanho fixo que se obtém após a aplicação de uma função hash a uma mensagem e que cumpre a requisito de estar associado univocamente aos dados iniciais.
HSM	Módulo de segurança criptográfico empregue para armazenar chaves e realizar operações criptográficas de modo seguro.
Infraestrutura de Chave Pública	Estrutura de *hardware*, software, pessoas, processos e políticas que usa a tecnologia de assinatura digital para dar a terceiros de confiança uma associação verificável entre a componente pública de um par de chaves assimétrico e um assinante específico.
LCR	Lista de certificados revogados que é criada e assinada pela EC que emitiu os certificados. Um certificado é introduzido na lista quando é revogado (por exemplo, por suspeita de

	comprometimento da chave). Em determinadas circunstâncias, a EC pode dividir uma LCR num conjunto de LCR mais pequenas.
LER	Lista de certificados de outras CA revogados. Uma LER é equivalente a uma LCR para os certificados cruzados com outras CA.
Módulo Criptográfico Hardware	Módulo de *hardware* utilizado para realizar funções criptográficos e armazenar chaves em modo seguro.
Número de série de Certificado	Valor inteiro e único que está associado inequivocamente com um certificado emitido pelo SCEE.
O	Atributo do DN de um objeto dentro da estrutura de diretório X.500.
OCSP	Protocolo que permite a comprovação do estado do certificado no momento em que o mesmo é utilizado.
OCSP Responder	Servidor que responde segundo o protocolo OCSP aos pedidos OCSP com o estado do certificado.
OID	O identificador alfanumérico/numérico único registado em conformidade com a norma de registo ISO, para fazer referência a um objeto específico ou a uma classe de objetos específica.
OU	Atributo do DN de um objeto dentro da estrutura de diretório X.500.
Pedido OCSP	Pedido de consulta de estado de um certificado a um OCSP Responder.
PIN	Personal Identification Number
PIN	Número específico apenas conhecido pela pessoa que tem de aceder a um recurso que se encontra protegido por este mecanismo.

PKCS	Conjunto de standard desenvolvido pela RSA Labs aceite internacionalmente para definição da sintaxe a utilizar com a criptografia de chave pública.
PKIX	Grupo de trabalho do IETF constituído para desenvolver as especificações relacionadas com PKI e Internet.
Time Stamping	Constatação da data e hora de um documento eletrónico mediante processos criptográficos, para datar os documentos de forma objetiva.
SHA	Desenvolvido pelo NIST e revisto em 1994 (SHA-1). Este algoritmo consiste em transformar mensagens de menos de 264 bits e gerar um resumo de 160 bits de comprimento. A probabilidade de encontrar duas mensagens distintas que produzam o mesmo resumo é praticamente nula, por esse motivo utiliza-se para assegurar a integridade dos documentos durante o processe de assinatura eletrónica.
SmartCard	Cartão criptográfico utilizado pelo titular para armazenar chaves privadas de assinatura e ou cifra. Os smartcards são considerados dispositivos seguros de criação de assinatura e de acordo com a lei permitem a geração de assinaturas eletrónicas qualificadas.
Titular	Pessoa singular ou coletiva identificada num certificado como a detentora de um dispositivo de criação de assinatura;
Validação cronológica	Declaração de entidade certificadora que atesta a data e hora da criação, expedição ou receção de um documento eletrónico;
X.500	Standard desenvolvido pelo ITU que define as recomendações de um diretório. Corresponde ao standard ISO 9594-1

X.509	Standard desenvolvido pelo ITU que define o formato eletrónico dos certificados eletrónicos.
Zona de Alta Segurança	Área de acesso controlado através de um ponto de entrada e limitada a pessoal autorizado devidamente credenciado e a visitantes devidamente acompanhados. As zonas de alta segurança devem estar encerradas em todo o seu perímetro e ser vigiadas 24 horas por dia, 7 dias por semana, por pessoal de segurança, por outro pessoal ou por meios eletrónicos.

E. ANEXO – HIERARQUIA DE OID DO SCEE

CONSTRUÇÃO DO OID					DESCRIÇÃO
0					Testes/experimental
1					Objetos Relacionados com a PKI do SCEE {id-pki-scee }
1	1				Objetos relacionados com a identificação de entidades
1	1	1			ECRaizEstado
1	1	1	m		M-ésimo processo de renovação
1	1	2			Entidades Certificadoras do Estado (ECEstado)
1	1	2	n		ECEstado n
1	1	2	n	m	SubECEstado
1	1	3			Entidade de Registo do Estado (EREstado)

1	1	3	n		EREstado n
1	1	3	n	m	Processo de renovação m-ésimo
1	1	100			Outros objetos relacionados com a identificação de entidades da comunidade SCEE-ICP.
1	2				Objetos relacionados com Politicas de Certificados
1	2	1			SCEE Politicas de Certificado
1	2	1	V	v	Política de Certificados do SCEE (Versão V.v)
1	2	10			Política de Certificado para Assinatura Digital
1	2	20			Política de Certificado para Autenticação
1	2	30			Política de Certificado para Confidencialidade

FIM DE DOCUMENTO