DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO

Entidade Certificadora Eletrónica Raiz

SISTEMA DE CERTIFICAÇÃO ELETRÓNICA DO ESTADO (SCEE)
INFRA-ESTRUTURA DE CHAVES PÚBLICAS

24 DE ABRIL DE 2020
OID: 2.16.620.1.1.1.2.2.1.3

APROVAÇÃO E ASSINATURA

De acordo com o estipulado no ponto 1.5.1 do presente documento, aprovo o mesmo e a sua entrada em vigor com a aposição da minha assinatura.

O Diretor do Centro de Gestão da Rede Informática do Governo

TITO CARLOS SOARES VIEIRA

Digitally signed by TITO CARLOS SOARES VIEIRA
DN: c=PT, title=DIRETOR, o=Centro de Gestão da Rede Informática do Governo, cn=TITO CARLOS SOARES VIEIRA
Date: 2020.09.08 16:25:34 +01'00'

Tito Carlos Vieira

ÍNDICE

FIGURAS

TABELAS

ANEXOS

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 Eletrónica 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.

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 a SCEE compreende um Conselho Gestor que dá parecer sobre a aprovação e integração de entidades certificadoras na SCEE pronunciando-se igualmente sobre práticas e políticas de certificação, uma Entidade Certificadora Eletrónica Raiz, que constitui o primeiro nível da cadeia hierárquica de certificação, e as várias Entidades Certificadoras do Estado a esta subordinadas, bem como as Entidades Filiadas.

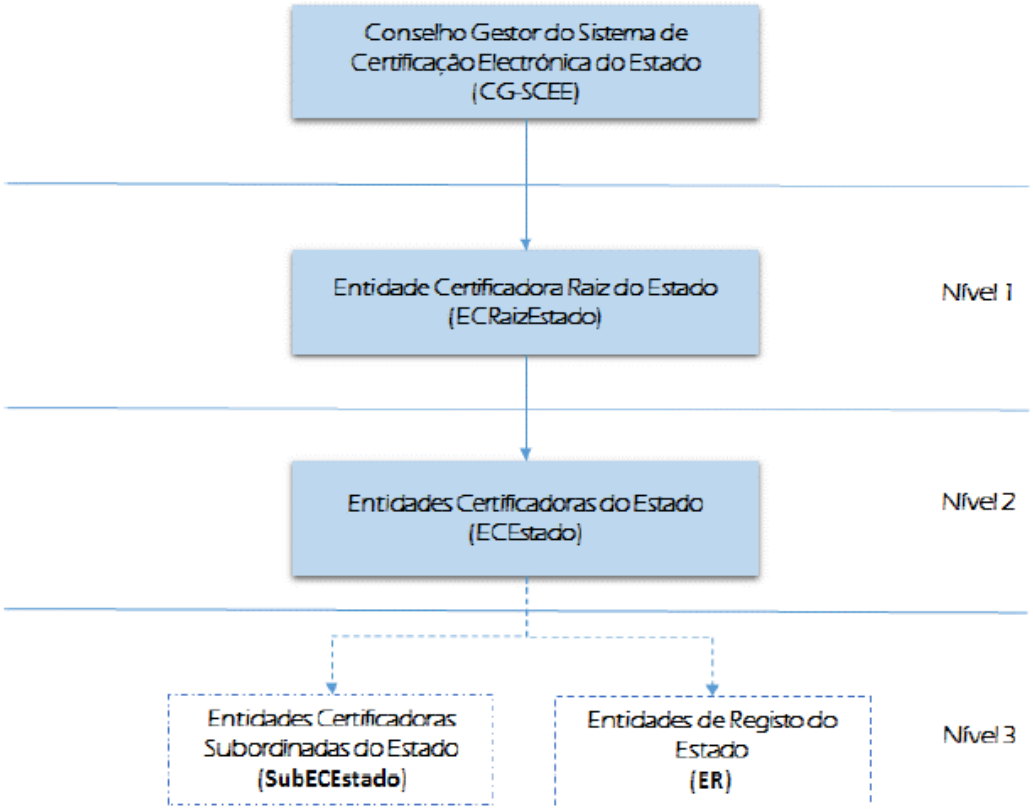

Figura 1 – Arquitetura funcional do SCEE

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 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 do Dispositivo Seguro de Criação de Assinaturas e o de Validação Cronológica.

A presente Declaração de Práticas de Certificação, adiante designada abreviadamente por DPC, descreve e regula as práticas de certificação da Entidade de Certificação Eletrónica do Estado - Entidade Certificadora Raiz – no que respeita à gestão do seu certificado autoassinado, assim como a emissão de certificados de Entidades Certificadoras do Estado.

A presente DPC dá seguimento ao estabelecido pela Política de Certificados do Sistema de Certificação Eletrónica do Estado, por isso nos capítulos em que a DPC não possa desenvolver o estabelecido na dita Política, será indicado "De acordo com a Política de Certificados do SCEE".

1.1.2 Estrutura do documento

Esta DPC assume que o leitor conhece os conceitos de Infraestrutura de Chaves Públicas, certificados e assinatura eletrónica. Caso contrário, recomenda-se ao leitor que tente obter conhecimento nos conceitos referidos anteriormente antes de continuar com a leitura do presente documento.

A presente DPC encontra-se estruturada conforme o disposto pelo grupo de trabalho PKIX do IETF (*Internet Engineering Task Force*), no seu documento de referência RFC 3647 (aprovado em novembro de 2003) "Internet X.509 *Public Key Infrastructure Certificate Policy and Certification Practices Framework*". Com o objetivo de dar um carácter uniforme ao documento e facilitar a sua leitura e análise, são incluídas todas as secções estabelecidas no RFC 3647. Quando não esteja previsto nada em alguma secção, deverá aparecer a expressão "*Não aplicável*".

Para a elaboração do seu conteúdo, foram tidos em conta os *Standards* europeus dos quais se destacam os seguintes:

- ETSI TS 101 456: *Policy Requirements for certification authorities issuing qualified certificates*

- ETSI TS 102 042: *Policy Requirements for certification authorities issuing public key certificates*

1.1.3 Hierarquia de OID

De acordo com a Política de Certificados do SCEE.

1.1.3.1 DISTRIBUIÇÃO DA ÁRVORE 2.16.620.1.1 {ID-SCEE}

De acordo com a Política de Certificados do SCEE.

1.2 IDENTIFICAÇÃO DO DOCUMENTO

O presente documento é identificado pelos dados constantes na tabela seguinte:

INFORMAÇÃO DO DOCUMENTO	
Nome do Documento	Declaração de Práticas de Certificação da Entidade de Certificação Eletrónica do Estado
Versão do Documento	Versão 3.0
Estado do Documento	Aprovado
OID	2.16.620.1.1.1.2.2.1.3
Data de Emissão	24 de abril de 2020
Validade	1 (um) ano
Localização	http://www.scee.gov.pt/rep/

1.3 PARTICIPANTES NA INFRAESTRUTURA DE CHAVES PÚBLICAS

1.3.1 Entidades Certificadoras (EC)

De acordo com a Política de Certificados do SCEE.

1.3.1.1 A ENTIDADE CERTIFICADORA RAIZ DO ESTADO (ECRAIZESTADO)

De acordo com a Política de Certificados do SCEE.

1.3.1.2 ENTIDADES CERTIFICADORAS DO ESTADO (ECESTADO)

De acordo com a Política de Certificados do SCEE.

1.3.1.3 ENTIDADES CERTIFICADORAS SUBORDINADAS (SUBECESTADO)

De acordo com a Política de Certificados do SCEE.

1.3.2 Entidades de Registo (ER)

As Entidades de Registo desenvolvem a sua atividade de acordo com o estabelecido no presente documento e pelo Conselho Gestor do SCEE.

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 deste documento, dado que se trata da DPC da ECEE – Entidade Certificadora Raiz (ECRaizEstado), os titulares dos certificados serão as pessoas coletivas, desde que sob responsabilidade humana, os quais aceitam os certificados e são responsáveis pela sua correta utilização e salvaguarda da sua chave privada. Preferencialmente, será designado como responsável pelo certificado, o representante legal da pessoa jurídica ou um dos seus representantes legais.

1.3.3 Titulares de Certificados

1.3.3.1 TITULARES

De acordo com a Política de Certificados do SCEE.

1.3.3.2 PATROCIONADOR

De acordo com a Política de Certificados do SCEE.

1.3.4 Partes Confiantes

De acordo com a Política de Certificados do SCEE.

1.3.5 Outros Participantes

1.3.5.1 O CONSELHO GESTOR DO SISTEMA DE CERTIFICAÇÃO ELETRÓNICO DO ESTADO

De acordo com a Política de Certificados do SCEE.

1.3.5.2 AUTORIDADE CREDENCIADORA

De acordo com a Política de Certificados do SCEE.

1.3.5.3 A ENTIDADE CERTIFICADORA RAIZ DO ESTADO

A ECRaizEstado é a entidade certificadora de topo da cadeia de certificação do SCEE, executora das políticas de certificados e diretrizes aprovadas pela Entidade Gestora de Políticas de Certificação. Compete a esta prestar os serviços de certificação às ECEstado 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 em detalhe, composição e seu funcionamento são definidos em documentação e legislação própria no âmbito da certificação digital.

1.3.5.4 AUTORIDADES DE VALIDAÇÃO

De acordo com a Política de Certificados do SCEE.

1.3.5.5 AUDITORES DE SEGURANÇA

De acordo com a Política de Certificados do SCEE.

1.4 UTILIZAÇÃO DO CERTIFICADO

1.4.1 Utilização adequada

Os certificados autoassinados da ECRaizEstado regulamentados pelo presente documento serão utilizados para prestar os seguintes serviços de segurança:

Tipo de certificado	Usos apropriados
Certificado autoassinado CSRS da ECRaizEstado	Assinatura de certificados, CRLs e informação do estado de certificados
Certificado autoassinado de assinatura da ECRaizEstado	Assinatura

Os certificados de autenticação de ECSubordinadas, isto é, dependentes hierarquicamente da ECRaizEstado do SCEE, são autorizadas expressamente pelo Conselho Gestor do SCEE, bem como a sua utilização.

Os certificados de ECSubordinada podem ser utilizados para prestar os seguintes serviços de segurança:

Tipo de certificado	Usos apropriados
Certificados CSRS de ECSubordinada	Assinatura de certificados, CRLs e informação de estado de certificados
Certificados de Assinatura de ECSubordinada	Assinatura
Certificados de Servidor de ECSubordinada	Autenticação do servidor e estabelecimento de comunicações mediante protocolo SSL

1.4.2 Utilização não autorizada

Qualquer uso não incluído na secção anterior fica excluído.

1.5 GESTÃO DAS POLÍTICAS

1.5.1 Entidade responsável pela gestão do documento

A gestão do presente documento é da responsabilidade da entidade que detém a gestão da ECRaizEstado.

1.5.2 Contacto

Nome	Entidade Gestora da Entidade de Certificação Eletrónica do Estado
Morada:	Av Defensores de Chaves, nº 6 – 6º 1049-063 Lisboa
Correio eletrónico:	ecee@ecee.gov.pt
Página Internet:	www.scee.gov.pt
Telefone	(+ 351) 213 923 400

1.5.3 Entidade que determina a conformidade da Declaração de Práticas de Certificação (DPC) para a Política

De acordo com a Política de Certificados do SCEE.

1.5.4 Procedimento para aprovação da Declaração de Práticas de Certificação (DPC)

A gestão e aprovação do presente documento compete ao responsável máximo da entidade que tem competência de gestão sobre a EC.

1.5.5 Definições e acrónimos

Ver Anexo B 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 para os correspondentes/destinatários, sobre os certificados e listas de revogação de certificado (LCR).

Os repositórios documentais estão disponíveis 24 horas por dia e sete dias por semana no seguinte endereço *web*: http://www.scee.gov.pt, que poderá ser acedido através de qualquer navegador de Internet utilizando o protocolo http (80) e https (443).

A LCR/LER da ECRaizEstado está disponível 24 horas por dia e sete dias por semana no seguinte endereço *web*: http://crls.ecee.gov.pt/crls/ARL.crl, que poderá ser acedido através de qualquer navegador de Internet utilizando o protocolo http (80).

O serviço de OCSP da ECRaizEstado está disponível 24 horas por dia e sete dias por semana no seguinte endereço *web*: http://ocsp.ecee.gov.pt

O acesso à informação constante do repositório público de acesso livre, é apenas disponibilizado em modo de leitura e descarga de ficheiros para equipamento local, sendo que apenas os recursos humanos com privilégios de gestão da mesma efetuam a modificação ou alteração de conteúdos.

2.2 PUBLICAÇÃO DE INFORMAÇÃO DE CERTIFICAÇÃO

No repositório está disponível a seguinte informação:

a) Uma cópia eletrónica do documento de Política de Certificados (PCert), assinado eletronicamente em http://www.scee.gov.pt/rep/;
b) Uma cópia eletrónica do presente documento, assinada eletronicamente, em http://www.scee.gov.pt/rep/;
c) Lista de Certificados de Entidades Certificadoras Revogadas (LER) em http://crls.ecee.gov.pt/crls/ARL.crl;
d) Certificado da ECEE em http://www.scee.gov.pt/rep/certificados/;
e) *Trusted List (Trusted-Service Status List)* do GNS em http://www.scee.gov.pt/rep/;
f) Outras informações em http://www.scee.gov.pt/.

São conservadas todas as versões anteriores da Declaração de Práticas de Certificação, sendo apenas disponibilizadas a quem, devidamente justificado, as solicite, não estando deste modo no repositório público de acesso livre.

2.3 PERIODICIDADE DE PUBLICAÇÃO

A informação incluída nos repositórios deverá ser disponibilizada logo que haja informação atualizada.

A publicação da LCR/LER da ECRaizEstado será publicada no repositório num prazo máximo de 24 horas desde a data da sua criação.

A DPC será publicada sempre que houver qualquer atualização à mesma, contudo, caso a esta não sofra qualquer atualização durante o período máximo de um ano, esta deverá ser na mesma publicada.

De seis em seis meses, ou sempre que exista alguma revogação de certificados, será publicada a LER.

Toda a informação considerada de suporte para a atividade de certificação da ECEE será publicada por períodos máximos de um ano.

2.4 CONTROLO DE ACESSO AOS REPOSITÓRIOS

Não existe qualquer restrição de acesso para consulta ao presente documento, à Política de Certificados e às LER.

São utilizados mecanismos e controles de acesso apropriados de forma a restringir o acesso de escrita e ou modificação das informações aí constantes, somente a pessoal autorizado.

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

3.1 ATRIBUIÇÃO DE NOMES

3.1.1 Tipos 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.

No caso dos certificados auto assinados da ECRaizEstado, o DN do emissor e do titular são os mesmos:

CN=ECRaizEstado 002

O=Sistema de Certificação Eletrónica do Estado

C=PT

3.1.2 Necessidade de nomes significativos

De acordo com a Política de Certificados do SCEE.

3.1.3 Anonimato ou pseudónimo de titulares

Não aplicável.

3.1.4 Interpretação de formato de nomes

De acordo com a Política de Certificados do SCEE.

3.1.5 Unicidade de nomes

O conjunto de nome distinto (*distinguished name*) mais o conteúdo da extensão *KeyUsage*, deve ser único e não ambíguo. O Administrador de Segurança da ECRaizEstado é encarregue de verificar o cumprimento desta norma.

3.1.6 Reconhecimento, autenticação e funções das marcas registadas

De acordo com a Política de Certificados do SCEE, a ECRaizEstado efetuada o registo inicial de forma presencial.

3.2 VALIDAÇÃO DE IDENTIDADE NO REGISTO INICIAL

De acordo com a Política de Certificados do SCEE, a ECRaizEstado efetuada o registo inicial de forma presencial.

No presente documento estão descritos os mecanismos e procedimentos, desde o início do pedido de certificado até à atribuição do certificado digital.

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 PKIX *Certificate Management Protocol* (CMP) definido no RFC 4210 atualizado pelo RFC 6712.

No caso da chave privada da ECRaizEstado, esta é gerada no HSM que lhe está associado considerando-se método suficiente de prova.

No caso das ECSubordinadas a posse da chave privada, correspondente à chave pública para a qual solicita a geração de certificado, fica provada mediante o envio do pedido de certificação no qual se incluirá a chave pública assinada através da chave privada associada, sendo tudo isto de acordo com o CMP.

Deste modo, no caso das ECSubordinadas, o pedido de certificado e posteriormente, o certificado gerado, é entregue, presencialmente, ao representante da requerente, pelo Administrador de Segurança da ECEE.

3.2.2 Autenticação da identidade de uma pessoa coletiva

O processo de autenticação da identidade de uma pessoa coletiva utilizada pelas ECSubordinadas devem, obrigatoriamente, garantir a pessoa coletiva é quem na realidade diz ser.

As ECSubordinadas devem guardar toda a documentação utilizada para verificação da identidade do indivíduo.

O processo para autenticar os titulares de ECSubordinada é descrito no parágrafo 1.5.3, sendo a ECRaizEstado responsável por verificar a identidade dos titulares.

A ECRaizEstado verifica a identidade dos seus representantes legais, por meio legalmente reconhecido, garantindo, no caso de o pedido ser subscrito para outrem, os poderes bastantes do requerente para a referida subscrição.

Quando requerido pela pessoa coletiva a constar como titular do certificado, é subscrito pelos seus representantes legais e contém, entre outros, os seguintes elementos:

a) Denominação legal;
b) Número de pessoa coletiva, sede, objeto social, nome dos titulares dos corpos sociais e de outras pessoas com poderes para a obrigarem e número de matrícula na conservatória do registo comercial;
c) Nome completo, número do bilhete de identidade ou qualquer outro elemento que permita a identificação inequívoca das pessoas singulares que estatutária ou legalmente a representa;
d) Endereço e outras formas de contacto;
e) Indicação quanto ao uso do certificado ser ou não restrito a determinados tipos de utilização, bem como eventuais limites do valor das transações para as quais o certificado é válido;
f) Eventual referência a uma qualidade específica, em função da utilização a que o certificado estiver destinado;

g) Outras informações relativas a poderes de representação, à qualificação profissional ou a outros atributos.

No caso de o pedido de emissão ser requerido por outrem que não o titular do certificado, o mesmo, para além dos elementos referidos no número anterior, contém, consoante seja requerido por pessoa singular ou coletiva, os seguintes elementos referentes ao requerente:

a) Nome ou denominação legal;

b) Número do bilhete de identidade, data e entidade emitente, ou qualquer outro elemento que permita a identificação inequívoca, ou número de pessoa coletiva;

c) Residência ou sede;

d) Objeto social, nome dos titulares dos corpos sociais e de outras pessoas com poderes para a obrigarem e número de matrícula na conservatória do registo comercial;

e) Endereço e outras formas de contacto.

f) Declaração da pessoa singular a constar como titular do certificado de que se obriga ao cumprimento das obrigações enquanto titular.

O documento de registo do requerente é fornecido ao mesmo no momento de formalização do pedido. Neste documento constam os dados e elementos necessários.

3.2.3 Autenticação da identidade de uma pessoa singular

A autenticação das pessoas físicas participantes na geração dos certificados da ECRaizEstado e dos certificados das ECSubordinadas são regulados nos documentos adicionais que descrevem as "*Cerimónias de Geração de Chaves*".

3.2.3.1 VALIDAÇÃO DOS PODERES DE AUTORIDADE OU REPRESENTAÇÃO

As Entidades de Certificação podem autorizar entidades privadas a tomar ações em nome de outras entidades.

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.

O solicitante do certificado autoassinado da ECRaizEstado atua em nome próprio por ser membro da SCEE e responsável pela ECEE – ECRaizEstado, pelo que não é necessário definir um procedimento de comprovação das faculdades representativas.

O solicitante de certificado de ECSubordinada atua em nome próprio por ser membro daquela entidade que se pretende constituir como ECSubordinada devendo ser seu responsável.

3.2.4 Informação de subscritor/titular não verificada

De acordo com a Política de Certificados do SCEE.

3.2.5 Critérios para interoperabilidade

De acordo com a Política de Certificados do SCEE.

3.2.6 Critérios para Filiação

De acordo com a Política de Certificados do SCEE.

3.3 IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDOS DE RENOVAÇÃO DE CHAVES

3.3.1 Identificação e autenticação para renovação de chaves, de rotina

De acordo com a Política de Certificados do SCEE.

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 de o mesmo ser revogado deve seguir as regras constantes no 3.2.2 e 3.2.3 do presente documento.

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) Certificado foi emitido sem autorização na 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.

3.4 IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDO DE REVOGAÇÃO

Dado o impacto que tem a revogação de um certificado de uma EC, esta revogação deverá ser aprovada pelo Conselho Gestor do SCEE.

4. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

A geração do par de chaves da ECRaizEstado, dada a sua importância, é efetuada através de uma cerimónia completamente formalizada com presença de responsáveis e testemunhas. A realização da Cerimónia é descrita de forma detalhada no documento " Guia de Acompanhamento da Cerimónia de Geração de Chaves da Entidade Certificadora Raiz".

Em consequência, nesta Declaração de Práticas de Certificação não se vai detalhar o conteúdo respeitante ao certificado auto assinado da ECRaizEstado nos seguintes pontos:

- 4.1 Pedido do Certificado;
- 4.2 Processo de pedido de certificado;
- 4.3 Emissão de certificados;
- 4.4 Aceitação de certificado.

4.1 PEDIDO DE CERTIFICADO

4.1.1 Quem pode subscrever um pedido de certificado

O Pedido de um certificado para a ECSubordinada emoldura-se numa cerimónia de geração de chaves. Esta petição deve ser realizada por pessoa ou entidade com poder para atuar em representação da ECSubordinada.

Só podem efetuar pedidos de subscrição de um pedido de certificado, entidades públicas, ou privadas, no caso de filiação, nos termos da legislação aplicável.

A ECSubordinada deve ter sido previamente autorizada pelo Conselho Gestor do SCEE para atuar como tal, dentro da autorização é necessário identificar que pessoas podem efetuar a petição do certificado de EC.

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(s) certificado(s).

O solicitante gerará um par de chaves assimétricas a incluir no certificado. Uma vez recebidos os dados pela ECRaizEstado, esta realizará todas as verificações pertinentes sobre os dados entregues.

Se esta primeira fase de comprovação se conclui de forma satisfatória, será gerado o certificado com base na chave pública fornecida pelo solicitante. A ECRaizEstado posteriormente encarregar-se-á de fazer chegar o certificado ao solicitante por meios que garantam confidencialidade e integridade.

Na ECRaizEstado, o administrador de registo é o responsável por verificar que se cumprem as condições do pedido e ativar a emissão do certificado de acordo com os parâmetros estabelecidos pelo Administrador de Segurança.

4.2 PROCESSAMENTO DO PEDIDO DE CERTIFICADO

Os pedidos de certificado, depois de recebidos pela entidade competente (ECRaizEstado), são considerados válidos se os seguintes requisitos forem cumpridos:

- Receber e verificar toda a documentação e autorizações exigidas, nomeadamente:
  - Verificação da identidade do requisitante
  - Verificação da exatidão e integridade do pedido de certificado
- Criar e assinar o certificado;
- Disponibilizar o certificado ao titular.

São aplicados, quanto aos processos, os pontos 3.2, 4.2.1 e 4.3 do presente documento.

4.2.1 Processo para a identificação e funções de autenticação

De acordo com o estipulado na secção 3.2 deste documento.

Após aprovação do pedido pelo Conselho Gestor do SCEE, cabe, na fase operacional, ao administrador de registo proceder à identificação e autenticação, nos termos do ponto 3.2.2, do presente documento, bem como da validação de:

a) Documentação utilizada para verificação da identidade e de poderes de representação;
b) Formulário de pedido em conformidade com o presente documento;
c) PKCS#10 válido;

Será rejeitado o pedido que não cumpra o acima previsto, ou viole as disposições do presente documento.

O Pedido é formulado por via física ou digital, cada uma com o seu mecanismo de identificação.

Compete ao administrador de registo da ECEE proceder à entrega, presencial, após a emissão, do certificado solicitado mediante o registo e assinatura de documento comprovativo da entrega.

4.2.2 Aprovação ou recusa de pedidos de certificado

Compete ao administrador de registo comprovar que o processo de pedido do certificado está devidamente autorizado.

A aprovação do certificado passa pelo cumprimento dos requisitos exigidos no ponto 4.2 e 4.2.1 do presente documento. Quando tal não se verifique, a entidade competente, recusa a emissão do certificado, com recurso a um relatório fundamentado e enviado ao requerente.

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 ECRaizEstado não será responsável pelas demoras que possam surgir no período compreendido entre a solicitação de certificado, a publicação no repositório da SCEE e a entrega do certificado.

É estipulado o prazo máximo de 5 (cinco dias) dias úteis para emissão de certificado, após aprovação do pedido respetivo.

4.3 EMISSÃO DE CERTIFICADO

4.3.1 Procedimento para a emissão de certificado

A emissão de um certificado pressupõe que todos os procedimentos foram concluídos com sucesso.

Os procedimentos estabelecidos na presente secção também se aplicam no caso de renovação de certificados, já que, esta operação implica a emissão de novos certificados.

O processo é efetuado na ZAS da ECRaizEstado, seguindo o estipulado no documento "Manual de Procedimento - Assinatura de Certificado de ECSubordinada".

Cabe ao administrador de segurança da ECRaizEstado garantir que os registos e documentação do pedido e emissão ficam guardados no cofre existente na ZAS.

Quando a ECRaizEstado emite um certificado, de acordo com um pedido, efetuará as notificações que se estabeleçam no ponto 4.3.2 do presente documento.

A ECRaizEstado entregará o certificado da ECSubordinada mediante um ficheiro PKCS#7.

4.3.2 Notificação da emissão do certificado ao titular

A notificação da emissão do certificado ao titular é efetuada, de forma presencial, mediante entrega e assinatura, por ambas as partes, do documento comprovativo da emissão do certificado.

4.4 ACEITAÇÃO DO CERTIFICADO

4.4.1 Procedimentos para a aceitação de certificado

O responsável da ECSubordinada assinará de forma manuscrita ou eletrónica, o documento estabelecido para esse efeito.

4.4.2 Publicação do certificado

Os certificados da ECRaizEstado e da ECSubordinada são publicados nos respetivos repositórios.

4.4.3 Notificação da emissão de certificado a outras entidades

Não aplicável.

4.5 USO DO CERTIFICADO E PAR DE CHAVES

A ECRaizEstado apenas emite certificados a ECSubordinadas e ao seu pessoal próprio, para efeitos de operação dos seus sistemas.

As ECSubordinadas devem assegurar que a utilização da sua chave privada apenas é utilizada para assinar certificados e LCR/LER.

É ainda responsabilidade das ECSubordinadas garantir que as chaves privadas atribuídas ao seu pessoal, para efeitos de operação do sistema, são utilizadas apenas para este âmbito e finalidade.

4.5.1 Uso do certificado e da chave privada pelo titular

Os titulares de certificados utilizarão a sua chave privada apenas e só para o fim a que estas se destinam e sempre com propósitos legais. A sua utilização apenas é permitida a quem estiver designado no campo "*Subject*" do certificado.

O titular só pode utilizar a chave privada e o certificado para os usos autorizados na Política de Certificados e no presente documento, de acordo com o estabelecido nos campos '*KeyUsage*' (Uso da Chave) dos certificados. Do mesmo modo, o titular só poderá utilizar o par de chaves e o certificado depois de aceitar as condições de uso estabelecidos nos pontos 1.4.1 e 1.4.2 do presente documento e só para os fins previstos.

Depois da extinção da vigência ou a revogação do certificado o titular deverá deixar de usar a chave privada associada.

Os certificados auto assinados da ECRaizEstado podem ser utilizados para prestar os seguintes serviços:

Tipo de certificado	Usos apropriados
Certificado Auto Assinado CSRS da ECRaizEstado	Assinatura de certificados, CRLs e informação de estado de certificados

Tipo de certificado	Usos apropriados
Certificado Auto Assinado Assinatura de ECRaizEstado	Assinatura

4.5.2 Uso do certificado e da chave pública pelos correspondentes

De acordo com a Política de Certificados do SCEE.

4.6 RENOVAÇÃO DE CERTIFICADOS

Esta Prática não é suportada pela ECRaizEstado, logo em consequência não se aplicam os pontos 4.6.1 a 4.6.7 do presente documento.

4.6.1 Motivos para renovação de certificado

Não aplicável no âmbito do SCEE.

4.6.2 Quem pode submeter o pedido de renovação de certificado

Não aplicável no âmbito do SCEE.

4.6.3 Processamento do pedido de renovação de certificado

Não aplicável no âmbito do SCEE.

4.6.4 Notificação de emissão de novo certificado ao titular

Não aplicável no âmbito do SCEE.

4.6.5 Procedimentos para aceitação de certificado

Não aplicável no âmbito do SCEE.

4.6.6 Publicação de certificado após renovação

Não aplicável no âmbito do SCEE.

4.6.7 Notificação da emissão do certificado a outras entidades

Não aplicável no âmbito do SCEE.

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 na secção 4.3 deste documento.

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

Um certificado auto assinado da ECRaizEstado pode ser renovado, entre outros, pelos seguintes motivos:

a) Fim do período de validade;
b) Alteração dos dados constantes no certificado;
c) Comprometimento das chaves ou perca de fiabilidade das mesmas;
d) Alteração de formatos.

Um certificado da ECSubordinada pode ser renovado, entre outros, pelos seguintes motivos:

a) Fim do período de validade;
b) Alteração dos dados constantes no certificado;
c) Comprometimento das chaves ou perca de fiabilidade das mesmas;
d) Alteração de formatos.

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

A submissão do pedido de renovação do certificado é valida para entidades com certificados em vigor.

A renovação será solicitada respetivamente pelo responsável da ECRaizEstado e pelo responsável da ECSubordinada correspondente.

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

Os requisitos de renovação são os mesmos para a emissão inicial do certificado auto assinado da ECRaizEstado, previstos no presente documento.

Os requisitos de renovação são os mesmos para a emissão inicial do certificado de ECSubordinada, previstos no presente documento.

Em qualquer caso, a renovação de um certificado está sujeita a:

a) Que seja solicitada a devido tempo seguindo as instruções e normas que a SCEE especifica para esse efeito;
b) Que a EC não tenha tido conhecimento de nenhuma ocorrência de revogação de certificado;
c) Que o pedido de renovação de serviços de prestação se refira ao mesmo tipo de certificado emitido inicialmente.

Em todos os outros procedimentos não previstos, aplicam-se os mesmos critérios da emissão inicial.

4.7.4 Notificação da emissão de novo certificado ao titular

No caso do certificado auto assinado da ECRaizEstado não existe este procedimento.

No caso das ECSubordinadas, a forma aceitável de notificação da emissão do certificado ao titular é a presencial.

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

A receção dos certificados renovados serve como confirmação da aceitação dos mesmos. Devendo assinar-se adicionalmente um documento reconhecendo a aceitação do certificado e suas condições de uso.

Em todos os outros procedimentos não previstos, aplicam-se os mesmos critérios da emissão inicial.

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

Aplicam-se os mesmos critérios da emissão inicial.

4.7.7 Notificação da emissão de novo certificado a outras entidades

Aplicam-se os mesmos critérios da emissão inicial.

4.8 ALTERAÇÃO DE CERTIFICADO

Este processo não é suportado, devendo ser efetuado um pedido de certificado em conformidade com o disposto no ponto 4.1 do presente documento.

4.8.1 Motivos para alteração de certificado

Não aplicável no âmbito do SCEE.

4.8.2 Quem pode submeter o pedido de alteração de certificado

Não aplicável no âmbito do SCEE.

4.8.3 Processamento do pedido de alteração de certificado

Não aplicável no âmbito do SCEE.

4.8.4 Notificação da emissão de certificado alterado ao titular

Não aplicável no âmbito do SCEE.

4.8.5 Procedimentos para aceitação de certificado alterado

Não aplicável no âmbito do SCEE.

4.8.6 Publicação do certificado alterado

Não aplicável no âmbito do SCEE.

4.8.7 Notificação da emissão de certificado alterado a outras entidades

Não aplicável no âmbito do SCEE.

4.9 SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO

A revogação e suspensão dos certificados são mecanismos a utilizar no pressuposto que, por alguma causa estabelecida na PCert do SCEE ou no presente documento, se deixe de confiar nos certificados antes da finalização do período de validade originalmente previsto.

A revogação de um certificado é o ato pelo qual se torna sem efeito a validade de um certificado antes de sua data de caducidade. O efeito da revogação de um certificado é a perda de validade do mesmo, originando a cessação permanente de sua operacionalidade conforme os usos que lhe são próprios e, em consequência a revogação de um certificado desabilita o uso legítimo do mesmo por parte do titular.

Fica salvaguardado que no caso de uma suspensão, a validade do certificado pode ser recuperada.

4.9.1 Motivo para a revogação

Um certificado auto assinado da ECRaizEstado pode ser revogado por:

a) Emissão defeituosa de um certificado devido a:
   i. Não se tenha cumprido qualquer requisito fundamental para a emissão do certificado;
   ii. A convicção de que um dado fundamental relativo ao certificado pode ser falso;
   iii. Existência de um erro de escrita de dados ou outro erro de processo;
b) O par de chaves gerado pelo titular é considerado como "fraco";
c) A informação contida no certificado ou utilizada para o seu pedido é incorreta;
d) Ordem formulada do titular ou por terceiro autorizado ou a própria pessoa física solicitante em representação de pessoa jurídica;
e) Ocorrência de qualquer outra causa especificada na PCert do SCEE ou no presente documento.

Um certificado de ECSubordinada pode ser revogado por:

a) Roubo, perda, revelação, modificação, ou outro compromisso ou suspeita de compromisso da chave privada do titular;
b) Uso indevido deliberado de chaves e certificados, ou a falta de observância ou contravenção dos requerimentos operacionais contidos no presente documento ou na PCert do SCEE;
c) Fim da Atividade do SCEE;
d) Cessação da atividade de ECSubordinada ou a mesma deixar de estar subordinada;

e) Emissão defeituosa de um certificado devido a:
   i. Não se ter cumprido qualquer requisito fundamental para a emissão do certificado;
   ii. Convicção de que um dado fundamental relativo ao certificado pode ser falso;
   iii. Existência de um erro de escrita de dados ou outro erro de processo;
f) Par de chaves gerado pelo titular é considerado como "fraco";
g) A informação contida no certificado ou utilizada para o seu pedido é incorreta;
h) Ordem formulada do titular ou por terceiro autorizado ou a própria pessoa física solicitante em representação de pessoa jurídica;
i) Ocorrência de qualquer outra causa especificada na PCert do SCEE ou no presente documento;
j) Revogação do Certificado da ECRaizEstado.

4.9.2 Quem pode submeter o pedido de revogação

Está autorizado para solicitar a revogação de um certificado:

a) O titular, quando ocorra qualquer uma das circunstâncias expostas no ponto 4.9.1 do presente documento;
b) A pessoa ou organização que fez o pedido do certificado em nome de uma organização, dispositivo ou aplicação;
c) Uma terceira parte quando tenha a noção que um certificado foi utilizado com fins fraudulentos;
d) A própria EC ou ER sempre que tenha conhecimento de qualquer das circunstâncias expostas no ponto 4.9.1 do presente documento.

4.9.3 Procedimento para pedido de revogação

A solicitação de revogação deverá ser assinada eletronicamente ou de forma manuscrita, sendo que, neste último caso, se deverá identificar previamente o solicitante. A solicitação deve ser dirigida à ECEE.

Obrigatoriamente, o pedido deverá constar o seguinte:

a) Identificação do solicitante;
b) Identificar a ECRaizEstado ou a ECSubordinada para que se solicite a revogação do certificado;
c) Incluir as causas do pedido.

4.9.4 Produção de efeitos da revogação

A revogação será feita de forma imediata, após terem sido efetuados todos os procedimentos e seja verificada a validade do pedido. A partir desse momento o pedido 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 pelos correspondentes/destinatários

Antes de utilizarem um certificado, as partes confiantes têm 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)

A ECRaizEstado publica nova LCR no seu repositório quando:

a) Se proceder a qualquer revogação;
b) Em intervalos de 3 meses.

As LAR geradas pela ECRaizEstado, mesmo que não existam modificações, são geradas no prazo máximo de 3 meses.

4.9.8 Período máximo entre a emissão e a publicação da LCR

De acordo com o estipulado no ponto 4.9.7 do presente documento.

4.9.9 Disponibilidade de verificação *online* do estado / revogação de certificado

A ECEE proporciona um serviço *online* onde publica as suas LCRs/LARs para a verificação do estado dos certificados que emite. É ainda disponibilizada uma Autoridade de Validação que, mediante o protocolo OCSP, permite verificar o estado dos certificados.

Os endereços de acesso aos serviços estão referenciados no presente documento.

4.9.10 Requisitos de verificação online de revogação

De acordo com a Política de Certificados do SCEE.

4.9.11 Outras formas disponíveis para divulgação de revogação

Não aplicável.

4.9.12 Requisitos especiais em caso de comprometimento de chave privada

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

4.9.13 Motivos para suspensão

Não aplicável.

4.9.14 Quem pode submeter o pedido de suspensão

Não aplicável.

4.9.15 Procedimentos para pedido de suspensão

Não aplicável.

4.9.16 Limite do período de suspensão

Não aplicável.

4.10 SERVIÇOS SOBRE O ESTADO DO CERTIFICADO

4.10.1 Características operacionais

De acordo com a Política de Certificados do SCEE.

4.10.2 Disponibilidade de serviço

De acordo com a Política de Certificados do SCEE.

4.10.3 Características opcionais

De acordo com a Política de Certificados do SCEE.

4.11 FIM DE SUBSCRIÇÃO

A extinção da validade de um certificado acontece nos seguintes casos:

a) Revogação do certificado por qualquer das causas descritas no ponto 4.9.1 do presente documento;
b) Caducidade da vigência do certificado.

4.12 RETENÇÃO E RECUPERAÇÃO DE CHAVES (KEY ESCROW)

4.12.1 Políticas e práticas de recuperação de chaves

Não é efetuado arquivo de chaves privadas de ECRaizEstado e de ECSubordinada.

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

Não aplicável.

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 da SCEE estão definidos no documento "*Localização e Instalação das EC da SCEE – Medidas de Segurança Física*". Nesta secção apenas são descritos os aspetos mais relevantes.

5.1.1 Localização física e tipo de construção

A ECRaizEstado (ECEE) está localizada num Centro de Dados Seguro totalmente construído com paredes de alvenaria betão e tijolo e com teto e pavimento construído com materiais similares aos das paredes, não tem qualquer janela, sendo totalmente fechado. As suas portas são em aço (alma) e armações igualmente em aço, com características corta-fogo e antivandalismo e com fechaduras acionáveis eletronicamente e respetivas barras antipânico.

A Zona de Alta Segurança (ZAS) possui 4 *layers* de proteção perimétrica, de forma a controlar o acesso físico à EC. Isto inclui:

a) Uma zona de receção onde os visitantes se identificam e são reconhecidos com tal;
b) Uma zona de operações onde o acesso é restrito e é feito através da receção;
c) Uma zona de segurança, onde serão registados todos os acessos através da zona de operações;
d) Uma zona de alta segurança onde tecnologia biométrica será instalada para controlar o acesso à EC.

Este Centro de Dados está equipado com sistema de deteção de intrusões, sistema de vigilância de vídeo e sistema de monitorização 24 horas por dia.

Da mesma forma, são garantidos os mesmos níveis de construção e segurança do local primário no Centro de Dados Seguro alternativo da ECEE.

5.1.2 Acesso físico ao local

O Centro de Dados da ECRaizEstado dispõe de diversos perímetros de segurança com diferentes requisitos de segurança e autorizações. Entre os equipamentos que protegem os perímetros de segurança estão incluídos sistemas de controlo de acesso físico, sistemas de videovigilância e de gravação, sistemas de deteção de intrusões, entre outros.

Para se aceder às áreas mais protegidas é necessário primeiro obter-se autorização para aceder às áreas menos protegidas.

O acesso à zona de alta segurança, para atividades como emissão de certificados, é registado e gravado automaticamente, sendo que o acesso é feito através da conjugação de dois sistemas: biométrico e proximidade.

Os acessos à esta ZAS são sempre feitos através de sistemas de controlos de acessos, sendo que qualquer acesso considerado visita é devidamente registado no Livro de Atas onde são registados todos os acessos e qualquer tipo de atividades que ocorram nesta zona.

Da mesma forma, são garantidos os mesmos níveis de acesso físico do local primário no Centro de Dados Seguro alternativo da ECRaizEstado.

5.1.3 Energia e ar condicionado

A ZAS da ECEE dispõe de sistemas de alimentação ininterrupta com a potência suficiente para manter autonomamente a rede elétrica durante períodos de falta de corrente e para proteger os equipamentos face a flutuações elétricas que os possam danificar.

O sistema de acondicionamento ambiental é composto por vários equipamentos independentes com capacidade para manter níveis de temperatura e humidade de acordo com recomendações para operação dos sistemas informáticos.

Da mesma forma, são garantidos os mesmos níveis de energia e ar condicionado do local primário no Centro de Dados Seguro alternativo da ECEE.

5.1.4 Exposição à água

A ZAS dispõe de detetores de inundação e sistemas de alarme apropriado que ativa em caso de verificação da mesma.

Da mesma forma, são garantidos os mesmos níveis de energia e ar condicionado do local primário no Centro de Dados Seguro alternativo da ECEE.

5.1.5 Prevenção e proteção contra incêndio

O centro de dados da ECEE dispõe de sistemas automáticos de deteção e extinção de incêndios. O gás utilizado para combater o fogo é totalmente inócuo ao homem.

Os materiais da sala e portas utilizados são de material não combustível e resistentes ao fogo, sendo que no caso das portas estas têm uma resistência de pelo menos 2 horas.

Da mesma forma, são garantidos os mesmos níveis de proteção contra incêndios do local primário no Centro de Dados Seguro alternativo da ECEE.

5.1.6 Salvaguarda de suportes de armazenamento

Os suportes de informação sensível estão armazenados de forma segura em cofres de acordo com o tipo de suporte e classificação da informação, cumprindo neste caso a norma EN 1143-1 e com dupla fechadura. O acesso a estas zonas é restrito a pessoas devidamente autorizadas.

Da mesma forma, são garantidos os mesmos níveis de salvaguarda de suportes e armazenamento do local primário no Centro de Dados Seguro alternativo da ECRaizEstado.

5.1.7 Eliminação de resíduos

Toda a eliminação de suportes magnéticos, e informação em papel é realizado de forma segura, sendo utilizado para os suportes magnéticos equipamentos desmagnetizadores e para a informação em papel utilizado destruidor de papel (corte cruzado). Os periféricos criptográficos são destruídos de acordo com as recomendações dos respetivos fabricantes.

Da mesma forma, são garantidos os mesmos níveis de eliminação de resíduos do local primário no Centro de Dados Seguro alternativo da ECRaizEstado.

5.1.8 Instalação externas (alternativa) para recuperação de segurança

Todas as cópias de segurança são colocadas num local secundário que está geograficamente separado do local primário. O acesso físico ao local secundário é restrito e apenas a pessoal autorizado. O local secundário está protegido pelos mesmos níveis de segurança que o local primário.

5.2 MEDIDAS DE SEGURANÇA DOS PROCESSOS

Os sistemas de informação e os serviços da ECRaizEstado são operados de forma segura, seguindo os procedimentos estabelecidos. Por razões de segurança, a informação relativa aos controlos dos procedimentos considera-se matéria confidencial e serão apenas explicados de forma resumida.

5.2.1 Funções de confiança

As pessoas de confiança incluem todos os empregados, contratados ou colaboradores que têm acesso à sala de operações criptográficas da ECRaizEstado e que podem materialmente afetar:

a) Validação de informação de emissão de Certificado;
b) Aceitação, rejeição, pedido de revogação, de renovação ou outro processo de emissão de Certificado;
c) Emissão, revogação de Certificados;
d) Manipulação de informações de Subscritor ou pedidos.

As funções de confiança incluem:

a) Administrador de Sistemas;
b) Operador de Sistemas;
c) Administrador de Segurança;
d) Administrador de Registo;
e) Auditor de Sistemas;
f) Administradores de HSM (Módulo Segurança por Hardware);
g) Operadores de HSM (Módulo Segurança por Hardware).

5.2.1.1 ADMINISTRADOR DE SISTEMAS

É a pessoa responsável pela:

a) Instalação e configuração de sistemas operativos de produtos de *software;*

b) Manutenção e atualização dos produtos instalados;
c) Garantia da prestação do serviço com o adequado nível de qualidades e fiabilidade em função do grau de criticidade do mesmo;
d) Colaboração com os auditores em tudo aquilo que lhe for solicitado;
e) Manter o inventário dos equipamentos e servidores que compõem o núcleo da plataforma de certificação digital.

5.2.1.2 OPERADOR DE SISTEMAS

É a pessoa responsável pela:

a) Operação regular dos sistemas;
b) Correta execução da política de cópias de segurança e em particular de as manter atualizadas.

Esta função na ECEE é acumulada pelo Administrador de Sistemas.

5.2.1.3 ADMINISTRADOR DE SEGURANÇA

Responsável pela gestão e implementação das regras e práticas de segurança.

Responsável por fazer cumprir as políticas de segurança da SCEE e encarregue de qualquer aspeto relativo à segurança (física, das aplicações, da rede, entre outras).

É encarregue da gestão dos sistemas de proteção perimétrica.

É responsável por resolver todos os incidentes de segurança e eliminar todas as vulnerabilidades detetadas.

É responsável pela gestão e controle dos sistemas de segurança física da sala de operações da EC e de todos os controles de acesso, dos sistemas de acondicionamento ambiental e de alimentação elétrica.

É responsável por explicar todos os mecanismos de segurança aos funcionários que devam conhecê-los e de consciencializá-los para as questões de segurança levando-os a fazer cumprir as normas e políticas de segurança estabelecidas.

É responsável por estabelecer os calendários para a execução de análise de vulnerabilidades, testes, e treino, bem como dos planos de continuidade de serviço e auditoria dos sistemas de informação.

Colabora com os Auditores em tudo aquilo que lhe for solicitado.

5.2.1.4 ADMINISTRADOR DE REGISTO

Responsável pela aprovação da emissão, suspensão e revogação de certificados digitais.

Colabora com os Auditores em tudo aquilo que lhe for solicitado.

5.2.1.5 AUDITOR DE SISTEMAS

Corresponde a um perfil de auditor interno, sem prejuízo de existir pessoal externo responsável pelas auditorias.

O auditor está encarregue de:

a) Verificar da existência de toda a documentação necessária e devidamente numerada;
b) Verificar a coerência da documentação e dos procedimentos;
c) Verificar os procedimentos de incidentes e eventos;
d) Verificar e analisar a proteção dos sistemas (exposição a vulnerabilidades, registos de acesso, utilizadores, etc.);
e) Verificar a existência e funcionamento dos alarmes e elementos de segurança física;
f) Verificar a adequação com a legislação em vigor;
g) Verificar o conhecimento dos procedimentos por parte do pessoal implicado;
h) Deve comprovar todos os aspetos reconhecidos na política de segurança, políticas de cópias de segurança, práticas de certificação, políticas de certificação, entre outros.

5.2.1.6 ADMINISTRADORES DE HSM (MODULO DE SEGURANÇA EM HARDWARE)

Define-se um conjunto de 4 Administradores para o HSM da ECRaizEstado, cada um com um cartão criptográfico de controlo de acesso às suas funções. Para a realização das operações que requeiram um papel de administrador é necessário introduzir no leitor do HSM um total de 2 cartões dos 4 atribuídos. Os Administradores de HSM são responsáveis por realizar as seguintes operações:

a) Recuperação da funcionalidade do *hardware* criptográfico em caso de falha de um HSM;
b) Recuperação de chaves em caso de terem sido apagadas acidentalmente;
c) Substituição de um conjunto de cartões de administrador. Esta operação só é necessária ser realizada se se deseja ampliar ou reduzir o número de cartões de administrador;
d) Substituição de um conjunto de cartões de operador. Esta operação só é necessária se se deseja ampliar ou reduzir o número de cartões de operador ou substituir algum cartão deteriorado;
e) Ampliação do número de HSM integrados na infraestrutura;
f) Dado que se opera em modo FIPS140-2 Nível 3, autorização para a geração de conjuntos de cartões de operador e chaves. Esta operação só se requere durante a cerimónia de geração de chaves para a EC.

5.2.1.7 OPERADORES DE HSM

Define-se um conjunto de 5 operadores para a ECRaizEstado, cada um com um cartão criptográfico de controlo de acesso à sua função. Para a utilização das chaves protegidas por um conjunto de cartões de operador é necessário introduzi-lo num leitor do HSM dois cartões de operador. Os Operadores de HSM estão encarregues de realizar as seguintes operações:

a) Ativação de chaves para sua utilização. Isto significa que cada vez que se inicie a EC, é necessário a inserção dos cartões de operadores associados às chaves;
b) Autorização para a geração de chaves da aplicação. Esta operação só é requerida durante a cerimónia de geração de chaves para a EC;

c) Arranque do interface de configuração da EC e do resto das entidades que formam a PKI.

As operações realizadas pelos operadores são mais frequentes que as realizadas pelos administradores, tendo de intervir cada vez que seja necessário voltar a configurar a EC ou voltar a arrancar um dos processos envolvidos na ECRaizEstado.

5.2.2 Número de pessoas exigidas por tarefa

A ECEE deverá garantir que nenhum acesso individual pode ser feito à sala das operações da EC. Qualquer acesso a estas instalações deverá ser sempre feito no mínimo por duas pessoas.

Do mesmo modo será sempre requerido um acesso multiutilizador para a geração de chaves nas ECs.

A atribuição de funções faz com que seja sempre requerido a participação de um mínimo de duas pessoas para todas as atividades relacionadas com o ciclo de vida das chaves das ECs.

5.2.3 Identificação e autenticação para cada função

Os administradores e Operadores de HSM são identificados e autenticados nos HSM através de técnicas de segredo partilhado com cartões criptográficos específicos do HSM.

Os restantes dos utilizadores da ECRaizEstado são identificados mediante certificados eletrónicos emitidos pela própria infraestrutura da ECRaizEstado e são autenticados através de cartões criptográficos.

A autenticação complementa-se com as correspondentes autorizações para aceder a determinados recursos de informação dos sistemas da ECRaizEstado.

5.2.4 Funções que requerem separação de responsabilidades

Entre as funções, estabelecem-se as seguintes incompatibilidades, de forma que um utilizador não possa ter duas funções marcados como "*incompatíveis*":

- Incompatibilidade entre a função de auditor (i.e., auditor de sistema) e qualquer outra função;
- Incompatibilidade entre as funções administrativas (Administrador de segurança, administrador de sistema e administrador de registo).

5.3 MEDIDAS DE SEGURANÇA PESSOAL

5.3.1 Requisitos relativos às qualificações, experiência, antecedentes e credenciação

Todo o pessoal que desempenhe funções na ECRaizEstado tem as qualificações e experiência na prestação de serviços de certificação.

Todo o pessoal cumpre os requisitos de segurança da organização.

Os elementos possuem:

- Conhecimentos e formação sobre certificação digital;
- Formação básica sobre segurança em sistemas de informação;
- Formação específica para o seu posto.

5.3.2 Procedimentos de verificação de antecedentes

Mediante credenciação, pela Autoridade Nacional de Segurança, dos elementos que desempenham funções na ECRaizEstado.

5.3.3 Requisitos de formação e treino

Os elementos que vão operar a Entidade Certificadora deverão estar sujeitos a um plano de formação para o correto desempenho das suas funções.

Este plano incluiu os seguintes aspetos:

- Formação nos aspetos legais básicos relativos à prestação de serviços de certificação;
- Formação em segurança dos sistemas de informação;
- Serviços disponibilizados pela Entidade Certificadora;
- Conceitos básicos sobre PKI;
- Declaração de Práticas de Certificação e Políticas de Certificação;
- Gestão de ocorrências.

5.3.4 Frequência e requisitos para ações de reciclagem

Sempre que exista qualquer alteração tecnológica, introdução de novas ferramentas ou modificação de procedimentos, será levada a cabo a adequada formação para todo o pessoal afeto à Entidade Certificadora

Sempre que sejam levadas a cabo alterações nas Políticas de Certificação ou Declaração de Práticas de Certificação serão realizadas sessões formativas aos elementos da Entidade Certificadora.

5.3.5 Frequência e sequência da rotação de funções

Não é definido nenhum plano de rotação na atribuição de tarefas ao pessoal da Entidade Certificadora.

5.3.6 Sanções para ações não autorizadas

No caso da realização de ações não autorizadas respeitantes às Entidades Certificadoras, 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 por negligência.

Se for realizada alguma infração, a Autoridade Certificadora suspenderá o acesso a todos os sistemas, 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.

5.3.7 Requisitos para a contratação de pessoal

Todo o pessoal da Entidade Certificadora Raiz está sujeito ao dever de sigilo mediante a assinatura de um termo de confidencialidade relativo às funções que desempenha. Este acordo descreve as suas tarefas de acordo com o presente documento e a Políticas de Segurança da Informação.

A Entidade Certificadora tem como requisito na contratação de pessoal, a Credenciação dos mesmos pela Autoridade Nacional de Segurança.

5.3.8 Documentação fornecida ao pessoal

A todo o pessoal que constitui uma Entidade Certificadora, são disponibilizados os seguintes documentos:

- Declaração de Práticas de Certificação;
- Política de Segurança;
- Organigrama e funções do pessoal.

É ainda disponibilizada de forma idêntica toda e qualquer documentação técnica necessária ao desempenho das funções em causa.

5.4 PROCEDIMENTOS DE AUDITORIA DE SEGURANÇA

5.4.1 Tipo de eventos registados

A Entidade Certificadora Raiz registará todos os eventos relacionados com:

- Tentativas de sucesso ou fracasso da alteração dos parâmetros de segurança do sistema operativo;
- Arranque e paragem de aplicações;
- Tentativas de sucesso ou fracasso de início e fim da sessão;
- Tentativas de sucesso ou fracasso de criar, modificar, apagar contas do sistema;
- Tentativas de sucesso ou fracasso de solicitar, gerar, assinar, emitir ou revogar chaves e certificados;
- Tentativas de sucesso ou fracasso de gerar ou emitir LCRs;
- Tentativas de sucesso ou fracasso de criar, modificar ou apagar informação dos titulares dos certificados;
- Tentativas de sucesso ou fracasso de acesso às instalações por parte de pessoal autorizado ou não;
- Cópias de segurança, recuperação ou arquivo dos dados;
- Alterações ou atualizações de *software* e *hardware*;
- Manutenção do sistema;

- Mudança de pessoal;
- A cerimónia de geração de chaves e as bases de dados de gestão de chaves;

As operações dividem-se em eventos, pelo que se guarda informação sobre um ou mais eventos para cada operação relevante. Os eventos registados possuem, como mínimo, a seguinte informação:

Categoria: Indica a importância do evento.

- Informativo: Os eventos desta categoria contêm informação sobre operações realizadas com êxito;
- Marca: cada vez que começa e termina uma sessão de administração, regista-se um evento desta categoria;
- Advertência: indica que se detetou um acontecimento não habitual durante uma operação, mas não provocou uma falha na operação;
- Erro: indica falha duma operação devido a um erro;
- Erro Fatal: indica que ocorreu uma circunstância excecional durante uma operação.

Data: Data e hora em que ocorreu o evento.

Autor: Nome único da Entidade que gerou o evento.

Função: Tipo de Entidade que gerou o evento.

Tipo evento: Identifica o tipo do evento, distinguindo, entre outros, os eventos criptográficos, de interface de utilizador, de Livraria.

Módulo: Identifica o módulo que gerou o evento. Os módulos possíveis são:

- EC;
- ER;
- Repositório de informação;
- Livrarias de controlo de armazenamento de informação.

Descrição: Representação textual do evento. Para alguns eventos, a descrição vem seguida duma lista de parâmetros cujos valores variam dependendo dos dados sobre os quais se executou a operação. Alguns exemplos dos parâmetros que se incluem para a descrição do evento "*Certificado gerado*" são: o número de serie, o nome único do titular do certificado emitido e o perfil de certificação que se aplicou.

5.4.2 Frequência da auditoria de registos

Os registos são analisados seguindo procedimentos manuais e automáticos quando seja necessário, deste modo define-se um nível de auditorias de controlo e dos eventos com uma frequência trimestral.

5.4.3 Período de retenção dos registos de auditoria

A informação gerada pelos registos de auditoria é mantida acessível até que seja arquivada. Uma vez arquivados os registos de auditoria são conservados pelo menos durante 20 anos.

5.4.4 Proteção dos registos de auditoria

Os eventos registados estão protegidos mediante técnicas criptográficas, de forma que nada, salvo as próprias aplicações de visualização de eventos, com seu devido controlo de acessos, possa aceder a eles.

As cópias de segurança e seus registos são armazenados num local resistente ao fogo, dentro das instalações seguras das ECRaizEstado.

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

5.4.5 Procedimentos para a cópia de segurança dos registos

De acordo com o manual de procedimentos relativo à cópia de segurança e restauro.

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 da Entidade Certificadora e pelo pessoal que as opera.

O Sistema de Informação de auditoria da PKI é uma combinação de processos automáticos e manuais executados pelas aplicações da PKI. Todos os registos de auditoria são armazenados nos sistemas internos da ECRaizEstado.

Todos os elementos significativos existentes na ECRaizEstado são acumulados numa base de dados. Os procedimentos de controlo de segurança empregues baseiam-se na tecnologia de construção empregue nas bases de dados.

As características deste sistema são as seguintes:

- Permite verificar a integridade da base de dados, deteta uma possível manipulação fraudulenta dos dados.
- Assegurar o não repúdio por parte dos autores das operações realizadas sobre os dados. Isto consegue-se através das assinaturas eletrónicas.
- Guarda um registo histórico de atualização dos dados, armazena versões sucessivas de cada registo resultante de diferentes operações realizadas sobre ele. Isto permite guardar um registo das operações realizadas e evita que se percam assinaturas eletrónicas realizadas anteriormente por outros utilizadores quando se atualizam os dados.

A seguinte lista é um resumo dos possíveis perigos a que uma base de dados pode estar exposta e que podem detetar-se com as provas de integridade:

- Inserção ou alteração fraudulenta de um registo de sessão;
- Supressão fraudulenta de sessões intermedias;
- Inserção, alteração ou supressão fraudulenta de um registo histórico;

- Inserção, alteração ou supressão fraudulenta do registo de uma tabela de consultas.

5.4.7 Notificação da causa do evento

Não é necessária qualquer notificação quando um evento é auditado.

5.4.8 Avaliação de vulnerabilidades

É realizada, pelo menos, uma análise anual às vulnerabilidades e segurança perimétrica.

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

5.5 ARQUIVO DE REGISTOS

5.5.1 Tipo de dados arquivados

- Os registos de auditoria especificados no ponto 5.4 do presente documento;
- Os suportes de Backups dos servidores que compõem a infraestrutura da EC;
- Documentação relativa ao ciclo de vida dos certificados:
    - Contrato/acordo de certificação;
    - Cópia da documentação de identificação facultada pelo requerente do certificado;
    - Identidade do operador que emitiu o certificado;
    - Data da última identificação direta do titular.
- Acordos de confidencialidade;
- Autorizações de acesso aos sistemas de informação.

5.5.2 Período de retenção em arquivo

Toda a informação e documentação relativa ao ciclo de vida dos certificados emitidos pela Entidade Certificadora Raiz é conservada por um período de 20 anos.

5.5.3 Proteção dos arquivos

O Acesso aos arquivos é restrito a pessoal autorizado.

Os eventos relativos aos certificados emitidos pela ECRaizEstado estão protegidos criptograficamente para garantir a deteção de manipulação dos seus conteúdos.

5.5.4 Procedimentos para as cópias de segurança do arquivo

São realizadas cópias de segurança dos ficheiros que compõem os arquivos a reter.

Uma cópia é guardada num cofre antifogo dentro da Sala Segura da ECRaizEstado. Uma outra cópia é realizada de forma cifrada e armazenada num cofre antifogo no local Seguro Alternativo.

5.5.5 Requisitos para validação cronológica dos registos

Os sistemas de informação de ECRaizEstado garantem o registo de tempo nos quais se realizam. O instante de tempo dos sistemas provém de uma fonte segura que constata a data e hora. Os servidores do sistema da ECRaizEstado estão sincronizados em data e hora.

Relativamente às fontes de tempo utilizadas, baseadas no protocolo NTP (*Network Time Protocol*), são usadas diferentes fontes, utilizando como referência as do Observatório astronómico de Lisboa.

5.5.6 Sistema de recolha de dados de arquivo (interno/externo)

O sistema de arquivo é interno à ECRaizEstado.

5.5.7 Procedimentos de recuperação e verificação de informação arquivada

Só o pessoal devidamente autorizado tem acesso aos arquivos físicos de suporte (medias) e arquivo informático para levar a cabo ações de verificação de integridade e outras.

São realizadas, de forma automática, verificações de integridade dos arquivos eletrónicos (cópias de segurança) na altura da sua criação, devendo criar-se um incidente e realizar-se novo arquivo no caso de erros ou comportamentos imprevistos.

5.6 TROCA DE CHAVES

Os procedimentos para proporcionar uma nova chave pública para os utilizadores / operadores de uma EC devem ser especificados na Política de Certificado correspondente a cada tipo de Certificado.

5.7 RECUPERAÇÃO EM CASO DE DESASTRE OU COMPROMETIMENTO

O Plano de Continuidade da ECRaizEstado é ativado em caso de uma indisponibilidade máxima de 24 horas, estando preparada para a emissão de LAR antes das 12 horas seguintes.

5.7.1 Procedimentos em caso de incidente ou comprometimento

No caso de ser afetada a segurança dos dados de verificação de assinatura da ECRaizEstado, esta deverá informar a todos os titulares de seus certificados e terceiras partes conhecidas que todos os certificados e listas de revogação assinados com estes dados já não são válidos. Logo que possível proceder-se-á ao restabelecimento do serviço.

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

Se os recursos de *hardware*, *software* e ou os dados forem alterados ou existe a suspeita de terem sido alterados, serão parados os serviços da ECRaizEstado até ao

restabelecimento das condições seguras com a inclusão de novos componentes de eficácia credível.

De forma paralela, serão realizadas auditorias para identificar as causas da alteração e assegurar que não voltam a existir.

Em caso de afetar certificados emitidos, são notificados os titulares dos mesmos e proceder-se-á à sua retificação.

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, informados os seus subscritores, e devidamente retificados.

5.7.4 Capacidade de continuidade da atividade em caso de desastre

Conforme o previsto no documento referente ao plano de contingência e continuidade de serviço.

5.8 PROCEDIMENTOS EM CASO DE EXTINÇÃO DE EC OU ER

As causas que podem conduzir à extinção da atividade de Entidade de Certificação são:

- Compromisso da chave privada da EC;
- Decisão política.

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

- Informar todos os titulares de certificados e extinguir a vigência dos mesmos revogando-os;
- Informar todas as terceiras partes com as quais tenha formado acordos de certificação;
- Comunicar ao Conselho Gestor do SCEE;
- Remeter ao Membro do Governo que tutela a ECRaizEstado toda a informação relativa aos certificados eletrónicos revogados, para que este os tome com sua custódia.

6. MEDIDAS DE SEGURANÇA TÉCNICAS

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 da SCEE prevê a existência de participantes, excluindo os subscritores/titulares, em três níveis.

No primeiro nível encontra-se a Entidade Certificadora de Raiz do Estado, que funciona obrigatoriamente em modo *off-line*, e em que o respetivo par de chaves é gerado num módulo criptográfico, de acordo com requisitos definidos no ponto "6.2.1". O certificado desta entidade é autoassinado.

As chaves para os certificados auto assinados da ECRaizEstado emitidos pela ECRaizEstado são geradas em módulos de *hardware* criptográficos com validação FIPS 140-2 Nível 3 que têm instalados nos seus respetivos sistemas.

As chaves para os certificados da ECSubordinada emitidos pela ECRaizEstado são geradas em módulos de *hardware* criptográfico com validação FIPS 140-2 Nível 3 que têm instalado nos seus respetivos sistemas.

6.1.2 Entrega da chave privada ao titular

Não se procede a entrega da chave privada do certificado auto assinado da ECRaizEstado e do certificado da ECSubordinada ao titular, estando a mesma armazenada no HSM.

6.1.3 Entrega da chave pública ao emissor do certificado

No caso do certificado auto assinado da ECRaizEstado não se procede a entrega.

A entrega do par das chaves à ECRaizEstado deve ser efetuada através de um pedido de certificado, segundo o formato descrito no PKCS#10, através de uma transação *online* de acordo com ou especificado no RFC4210 atualizado pelo RFC6712 (*PKI Certificate Management Protocols*).

6.1.4 Entrega da chave pública da EC aos correspondentes/destinatários

A chave pública da ECRaizEstado está incluída no certificado da EC. O certificado da ECRaizEstado deve ser obtido do repositório especificado no presente documento onde fica a disposição dos titulares de certificados e os terceiros aceitantes para realizar qualquer tipo de comprovação.

6.1.5 Dimensão das chaves

A dimensão das chaves dos vários participantes deve obedecer aos seguintes comprimentos mínimos:

- Nível 1 (ECRaizEstado): RSA 4096 bit;
- Nível 2 (ECSubordinada): 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 dos mesmos, 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.

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 recomendado no RFC 5280, atualizado pelo RFC 6818.

A chave definida pela política, e, por conseguinte, o certificado associado, será utilizado para a verificação da identidade da ECRaizEstado.

Para tal efeito, nos campos '*Key Usage*' e '*Extended Key Usage* do certificado são incluídos os seguintes usos:

Tipo certificado	Key Usage	Extended Key Usage
Certificado auto assinado CSRS da ECRaizEstado	keyCertSign CRLSign	Não aplicável
Certificado auto assinado de Assinatura da ECRaizEstado.	digitalSignature nonRepudiation keyAgreement	clientAuth emailProtection
Certificado de OCSP Responder	digitalSignature nonRepudiation	OCSPSigning

A chave definida na política e por conseguinte no certificado associado é utilizada para a verificação da entidade das ECSubordinadas.

Para esse efeito nos campos '*Key Usage*' e '*Extended Key Usage'* do certificado são incluídas as seguintes utilizações:

Tipo certificado	Key Usage	Extended Key Usage
Certificados CSRS de ECSubordinada.	keyCertSign CRLSign	Não Aplicável
Certificados de Assinatura de ECSubordinada.	digitalSignature nonRepudiation keyAgreement	clientAuth emailProtection

Tipo certificado	Key Usage	Extended Key Usage
Certificados de Servidor de ECSubordinada.	digitalSignature nonRepudiation keyEncipherment keyAgreement	serverAuth

6.2 PROTEÇÃO DA CHAVE PRIVADA E CARACTERÍSTICAS DO MÓDULO CRIPTOGRÁFICO

6.2.1 Normas e medidas de segurança do módulo criptográfico

Os módulos utilizados para a criação das chaves utilizadas pela ECRaizEstado cumprem os requisitos estabelecidos num perfil de proteção de dispositivo seguro de assinatura eletrónica de Entidade de Certificação normalizada, de acordo com ITSEC, *Common Criteria* ou FIPS 140-1 Nível 3 ou nível superior de segurança.

Os sistemas de *hardware* e *software* que se empregam estão conforme às normas CWA 14167-1 e CWA 14167-2.

A implementação de cada uma das Autoridades de Certificação, levando em conta que se utiliza um Módulo Criptográfico de Segurança (HSM), comporta as seguintes tarefas:

a) Iniciação do estado do módulo HSM;
b) Criação dos cartões de administração e de operador;
c) Geração das chaves da EC.

6.2.2 Controlo multi-pessoal (N de M) para a chave privada

Todas as operações são efetuadas com um mínimo de dois elementos em funções qualificadas dentro da entidade e em tarefa distinta.

Na prática, são empregues nas diversas funções, pelo menos dois elementos (N=2), entre o conjunto total de pessoas com funções atribuídas dentro da entidade (M=staff).

A chave privada da ECRaizEstado encontra-se na posse de mais que um elemento. Esta é ativada mediante a inicialização do *software* da EC por meio de uma combinação de operadores da EC, administradores do *HSM* e utilizadores de Sistema Operativo. Este é o único método de ativação da chave privada.

6.2.3 Retenção da chave privada (key escrow)

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

6.2.4 Cópia de segurança da chave privada

As chaves privadas de ECRaizEstado dispõem de uma cópia de segurança realizada pela própria entidade. As cópias de segurança têm 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, são arquivadas por um período mínimo de 20 anos após expiração da sua validade.

6.2.6 Transferência da chave privada para/do módulo criptográfico

A transferência da chave privada das ECRaizEstado só se pode efetuar entre módulos criptográficos (HSM) e requer a intervenção de um mínimo de dois administradores de HSM, operadores do HSM, um Administrador de Sistemas, ficando com a custódia do material criptográfico.

6.2.7 Armazenamento da chave privada no módulo criptográfico

As chaves privadas são geradas no módulo criptográfico no momento da criação de cada uma das Entidades Certificadoras que fazem uso de ditos módulos.

6.2.8 Processo para ativação da chave privada

A chave privada deverá ser ativada quando o sistema/aplicação da ECRaizEstado é ligado ("*startup process*"). Esta ativação só deverá ser efetivada quando previamente tiver sido feita a autenticação no módulo criptográfico pelos operadores indicados para o efeito.

Tal como se estipula no ponto 6.2.2 Controlo multi-pessoal (N de M) para a chave privada, a chave privada da ECRaizEstado é ativada mediante a inicialização do *software* e pela combinação mínima de operadores de HSM. Este é o único método de ativação da referida chave privada.

6.2.9 Processo para desativação da chave privada

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

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.

Ao nível do controlo multi-pessoal é aplicado o ponto 6.2.2 do presente documento.

6.2.10 Processo para destruição da chave privada

A destruição deve sempre ser precedida por uma revogação do certificado associado à chave, mesmo que esta esteja em vigor.

As várias chaves privadas devem ser destruídas sempre que deixarem de ser necessárias.

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

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

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

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

6.2.11 Avaliação/nível do módulo criptográfico

Descrito no ponto 6.2.1 do presente documento.

6.3 OUTROS ASPETOS DA GESTÃO DO PAR DE CHAVES

6.3.1 Arquivo da chave pública

As Entidades Certificadoras 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 o 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.

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

[VALIDADE DOS CERTIFICADOS] – [PERÍODO DE RENOVAÇÃO]					
ECRaizEstado	ECEstado	subECEstado	Outras Entidades PKI	Titulares	
				Hardware	Software
[24] – [12]	[12] – [6]	[6] – [3]	[3] – [3]	[6] – [6]	[1] – [1]

Tabela 3 – Definição dos Períodos de Validade dos Certificados

Os períodos de utilização das chaves são os determinados pela duração do certificado e uma vez passado, não é possível a utilização do mesmo.

A caducidade produzirá automaticamente a invalidação dos Certificados, originando a cessação permanente de sua operacionalidade conforme os usos que lhe são próprios e, em consequência, da prestação dos serviços de certificação em causa.

6.4 DADOS DE ATIVAÇÃO

6.4.1 Geração e instalação dos dados de ativação

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

A ECRaizEstado utiliza dispositivos/mecanismos criptográficos, do tipo *smartcard*, para suporte às atividades, nomeadamente no seu funcionamento.

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

Para a instauração de uma Entidade de Certificação do domínio do SCEE são criados cartões criptográficos, que servirão para atividades de funcionamento e recuperação. As EC operam com vários tipos de funções, cada uma com os seus correspondentes cartões criptográficos, onde se armazenam os dados de ativação.

Para a ativação das chaves da EC é necessária a intervenção dos administradores do HSM que têm capacidade para colocar em estado operativo o HSM, e dos operadores do HSM que têm o conhecimento do PIN ou palavra de acesso do mesmo para ativação das chaves privadas.

6.4.2 Proteção dos dados de ativação

Só o pessoal autorizado, neste caso os Operadores e Administradores das EC correspondentes, possui os cartões criptográficos com capacidade de ativação das chaves e conhecem as respetivas palavras passe para aceder aos dados de ativação.

No caso dos códigos das chaves associadas aos certificados pessoais, só o titular conhece o código a chave pessoal de acesso ou PIN, sendo, portanto, o único responsável da proteção dos dados de ativação e dos seus códigos ativação das suas chaves privadas.

6.4.3 Outros aspetos dos dados de ativação

Não aplicável.

6.5 MEDIDAS DE SEGURANÇA INFORMÁTICA

Os dados referentes a esta secção são considerados como informação confidencial, devendo apenas ser cedida a quem se reconheça a necessidade de os conhecer, sendo exemplo as auditorias externas, internas e inspeções.

A ECRaizEstado tem estabelecidos os controlos necessários referentes à segurança da informação, de acordo com a Política de Certificados e os *standards* aplicáveis.

6.6 REQUISITOS TÉCNICOS ESPECÍFICOS

Os dados referentes a esta secção são considerados como informação confidencial, devendo apenas ser cedida a quem se reconheça a necessidade de os conhecer.

De modo geral, a ECRaizEstado segue as boas práticas estabelecidas na norma ISO 17799:2005 *Code of practice for information security management*.

6.6.1 Avaliação/nível de segurança

Os vários sistemas e produtos em produção na ECRaizEstado 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 15408 ou perfil equivalente.

6.7 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 da ECRaizEstado, apenas são fornecidos à Autoridade Credenciadora, ou terceira pessoa mandata para tal.

A ECRaizEstado implementa um conjunto de medidas de segurança consideradas adequadas, em resultado da arquitetura escolhida e dos riscos avaliados.

6.7.1 Medidas de desenvolvimento dos sistemas

Os requisitos de segurança são exigíveis, desde seu início, tanto na aquisição de sistemas informáticos como no desenvolvimento dos mesmos já que possam ter algum impacto sobre a segurança da SCEE.

É realizada uma análise de requisitos de segurança durante as fases de *design* e especificação de requisitos de qualquer componente utilizado nas aplicações que constituem cada um dos sistemas da ECRaizEstado, para garantir que os mesmos são seguros.

Utilizam-se procedimentos de controlo de mudanças para as novas versões, atualizações e correções de emergência dos ditos componentes.

A infraestrutura da ECRaizEstado é dotada de ambiente de desenvolvimento e produção claramente diferenciados e independentes.

6.7.2 Medidas para a gestão da segurança

A ECEE mantém um inventário de todos os ativos de:

a) Equipamentos físicos;
b) Sistemas lógicos;
c) Pessoal.

Os mesmos são classificados de acordo com a sua necessidade de proteção e os riscos a que possam estar expostos. Assim é feita uma análise de risco para que se consiga efetuar uma eficaz gestão do risco.

As configurações dos sistemas são auditadas de forma periódica, aferindo-se as necessidades e a sua capacidade.

6.7.3 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, devendo ser instalados pelo pessoal com funções de confiança, com adequada formação para o efeito, e seguindo os procedimentos definidos para o efeito.

A atualização e manutenção dos produtos e sistemas que compõem o sistema e ambiente da ECRaizEstado são efetuados de acordo com as recomendações dos respetivos fabricantes e são sempre realizadas por pessoal com funções de confiança da ECRaizEstado.

Em casos excecionais, podem estar presentes entidades terceiras, desde que devidamente autorizadas para o efeito.

6.8 MEDIDAS DE SEGURANÇA DE REDE

Não aplicável.

6.9 VALIDAÇÃO CRONOLÓGICA (TIME-STAMPING)

Não aplicável.

7. PERFIS DE CERTIFICADO, CRL 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.

7.1.1 Número(s) de versão

Neste campo os certificados deverão conter o valor 2 (dois), 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 (PKIX certificate and CRL profile).

7.1.2.1 AUTORITYKEYIDENTIFIER

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).

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. Esta extensão especifica o fim a que o certificado se destina.

Especificado na secção 6.1.7 "Fins a que se destinam as chaves (campo "*key usage*" X.509v3)", deste documento.

7.1.2.4 CERTIFICATEPOLICIES

Extensão obrigatória e não critica. Esta extensão lista as Políticas de Certificados que dão suporte e regem o ambiente em que se processou a emissão do certificado. Deve ser incluído o OID das Políticas de Certificados e o *link* para a respetiva Declaração de Práticas de Certificação.

7.1.2.5 BASICCONSTRAINTS

É uma extensão obrigatória e crítica para Certificados de EC, é opcional para certificados de titular Esta extensão indica se o certificado é um certificado de EC, em que 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 ("True"), ou o processo de verificação do certificado falha.

De seguida, identificam-se os perfis dos quatro tipos de certificados auto assinados que emite a ECEE da ECRaizEstado.

Certificado auto assinado de CSRS ECRaizEstado		
CAMPO	**CONTEÚDO**	**CRÍTICA para extensões**
Campos de X509v1		
1. Version	V3	
2. Serial Number	Aleatório	
3. Signature Algorithm	Sha256withRsaEncryption	
4. Issuer Distinguished Name	CN=ECRaizEstado 002 O=Sistema de Certificação Eletrónica do Estado C=PT	
5. Validity	24 anos.	
6. Subject	CN=ECRaizEstado 002 O=Sistema de Certificação Eletrónica do Estado C=PT	
7. Subject Public Key Info	Algoritmo: RSA Tamanho da Chave: 4096	
Campos de X509v2		
1. issuerUniqueIdentifier	Não utilizado	
2. subjectUniqueIdentifier	Não utilizado	
Extensões de X509v3		
1. Subject Key Identifier	Derivada de utilizar a função de hash SHA-1 sobre a chave pública do *subject*.	Não
2. Authority Key Identifier	Não aplicável	Não
3. KeyUsage		Sim
Digital Signature	0	
Non Repudiation	0	
Key Encipherment	0	
Data Encipherment	0	
Key Agreement	0	
Key Certificate Signature	1	
CRL Signature	1	
4. extKeyUsage	Não utilizado	
5. privateKeyUsagePeriod	Não utilizado	
6. Certificate Policies		Não
Policy Identifier	*2.5.29.32.0 (Any Policy)*	

Certificado auto assinado de CSRS ECRaizEstado		
CAMPO	**CONTEÚDO**	**CRÍTICA para extensões**
URL CPS	http://www.scee.gov.pt/rep	
Notice Reference	Não utilizado	
7.Policy Mappings	Não utilizado	
8. Subject Alternate Names	Não utilizado	
9. Issuer Alternate Names	Não utilizado	
10. Subject Directory Attributes	Não utilizado	
11. Basic Constraints		Sim
Subject Type	CA	
Path Length Constraint	none	
12. Policy Constraints	Não utilizado	Não
13. CRLDistributionPoints	Não utilizado	
14. Auth. Information Access	Não aplicável	
15.netscapeCertType	Não aplicável	
16. netscapeRevocationURL	Não aplicável	
17. netscapeCAPolicyURL	Não aplicável	
18. netscapeComment	Não aplicável	

Certificado Auto Assinado de Assinatura da ECRaizEstado		
CAMPO	**CONTEÚDO**	**CRÍTICA para extensões**
Campos de X509v1		
1. Version	V3	
2. Serial Number	Aleatorio	
3. Signature Algorithm	Sha256withRsaEncryption	
4. Issuer Distinguished Name	CN=ECRaizEstado 002 O=Sistema de Certificação Eletrónica do Estado C=PT	
5. Validity	24 anos.	
6. Subject	CN=ECRaizEstado 002 O=Sistema de Certificação Eletrónica do Estado C=PT	
7. Subject Public Key Info	Algoritmo: RSA Tamanho da Chave: 4096	
Campos de X509v2		
1. issuerUniqueIdentifier	Não será utilizado	
2. subjectUniqueIdentifier	Não será utilizado	
Extensões de X509v3		
1. Subject Key Identifier	Derivada de utilizar a função de hash SHA-1 sobre a chave pública do subject.	Não
2. Authority Key Identifier	Derivada de utilizar a função de hash SHA-1 sobre a chave pública da EC emissora.	Não
3. KeyUsage		Sim

Certificado Auto Assinado de Assinatura da ECRaizEstado		
CAMPO	**CONTEÚDO**	**CRÍTICA para extensões**
Digital Signature	1	
Non Repudiation	1	
Key Encipherment	0	
Data Encipherment	0	
Key Agreement	1	
Key Certificate Signature	0	
CRL Signature	0	
4. extKeyUsage	clientAuth, emailProtection	
5. privateKeyUsagePeriod	Não utilizado	
6. Certificate Policies		Não
Policy Identifier	*2.5.29.32.0*	
URL CPS	http://www.scee.gov.pt/rep	
Notice Reference	Não será utilizado	
7.Policy Mappings	Não será utilizado	
8. Subject Alternate Names	Não será utilizado	
9. Issuer Alternate Names	Não será utilizado	
10. Subject Directory Attributes	Não será utilizado	
11. Basic Constraints		Sim
Subject Type	CA	
Path Length Constraint	none	
12. CRLDistributionPoints	Não será utilizado	Não
13. CRLDistributionPoints	Não será utilizado	Não
14. Auth. Information Access	Não será utilizado	
15.netscapeCertType	SSL_Client, SMIME_Client	Não
16. netscapeRevocationURL	Não será utilizado	
17. netscapeCAPolicyURL	Não será utilizado	
18. netscapeComment	Não será utilizado	

De seguida discriminam-se os perfis dos quatro tipos de certificados de ECSubordinada que a ECRaizEstado emite

Certificado CSRS de ECSubordinada		
CAMPO	**CONTEÚDO**	**CRÍTICA para extensões**
Campos de X509v1		
1. Version	V3	
2. Serial Number	Aleatório	
3. Signature Algorithm	Sha256withRsaEncryption	

4. Issuer Distinguished Name	CN=ECRaizEstado 002 O=Sistema de Certificação Eletrónica do Estado C=PT	
5. Validity	12 anos.	
6. Subject	CN=<OBJECTO> OU=ECEstado O=Sistema de Certificação Eletrónica do Estado C=PT	
7. Subject Public Key Info	Algoritmo: RSA Tamanho da Chave: 4096	
Campos de X509v2		
1. issuerUniqueIdentifier	Não utilizado	
2. subjectUniqueIdentifier	Não utilizado	
Extensões de X509v3		
1. Subject Key Identifier	Função hash SHA-1 sobre a chave pública do subject (ECSubordinada).	Não
2. Authority Key Identifier	Função de hash SHA-1 sobre a chave pública da EC emissora (ECRaizEstado). NÃO SE INCLUI a identificação do certificado da EC emissora (neste caso, DN da ECRaizEstado, número de série da AC Raiz).	Não
3. KeyUsage		Sim
Digital Signature	0	
Non Repudiation	0	
Key Encipherment	0	
Data Encipherment	0	
Key Agreement	0	
Key Certificate Signature	1	
CRL Signature	1	
4. extKeyUsage	Não aplicável	
5. privateKeyUsagePeriod	Não utilizado	
6. Certificate Policies		Não
Policy Identifier	*2.5.29.32.0*	
URL CPS	http://www.scee.gov.pt/rep	
Notice Reference	Não utilizado	
7.Policy Mappings	Não utilizado	
8. Subject Alternate Names	Não utilizado	
9. Issuer Alternate Names	Não utilizado	
10. Subject Directory Attributes	Não utilizado	
11. Basic Constraints		Sim
Subject Type	CA	
Path Length Constraint	none	
12. Policy Constraints		
13. CRLDistributionPoints	(1) HTTP: http://crls.ecee.gov.pt/crls/ARL-002.crl	Não
14. Auth. Information Access	OCSP: http://ocsp.ecee.gov.pt Certification Authority Issuers: http://trust.ecee.gov.pt/ecraiz002.crt	
15.netscapeCertType	Não aplicável	Não

16. netscapeRevocationURL	Não aplicável	
17. netscapeCAPolicyURL	Não aplicável	
18. netscapeComment	Não aplicável	

Certificado de Assinatura de ECSubordinada		
CAMPO	**CONTEÚDO**	**CRÍTICA para extensões**
Campos de X509v1		
1. Version	V3	
2. Serial Number	Aleatório	
3. Signature Algorithm	Sha256withRsaEncryption	
4. Issuer Distinguished Name	CN=ECRaizEstado 002 O=Sistema de Certificação Eletrónica do Estado C=PT	
5. Validity	12 anos.	
6. Subject	CN=<OBJECTO> OU=ECEstado O=Sistema de Certificação Eletrónica do Estado C=PT	
7. Subject Public Key Info	Algoritmo: RSA Tamanho da chave: 4096	
Campos de X509v2		
1. issuerUniqueIdentifier	Não utilizado	
2. subjectUniqueIdentifier	Não utilizado	
Extensões de X509v3		
1. Subject Key Identifier	Derivada de utilizar a função de hash SHA-1 sobre a chave pública do sujeito.	Não
2. Authority Key Identifier	Derivada de utilizar a função de hash SHA-1 sobre a chave pública da EC emissora.	Não
3. KeyUsage		Sim
Digital Signature	1	
Non Repudiation	1	
Key Encipherment	0	
Data Encipherment	0	
Key Agreement	1	
Key Certificate Signature	0	
CRL Signature	0	
4. extKeyUsage	clientAuth, emailProtection	
5. privateKeyUsagePeriod	Não utilizado	
6. Certificate Policies		Não
Policy Identifier	*2.5.29.32.0 (AnyPolicy)*	
URL CPS	http://www.scee.gov.pt/rep	
Notice Reference	Não utilizado	

Certificado de Assinatura de ECSubordinada		
CAMPO	**CONTEÚDO**	**CRÍTICA para extensões**
7.Policy Mappings	Não utilizado	
8. Subject Alternate Names	Não utilizado	
9. Issuer Alternate Names	Não utilizado	
10. Subject Directory Attributes	Não utilizado	
11. Basic Constraints		Sim
Subject Type	CA	
Path Length Constraint	none	
12. Policy Constraints	Não utilizado	
13. CRLDistributionPoints	(1) HTTP: http://crls.ecee.gov.pt/crls/ARL-002.crl	Não
14. Auth. Information Access	OCSP: http://ocsp.ecee.gov.pt	
15. netscapeCertType	Não aplicável	
16. netscapeRevocationURL	Não aplicável	
17. netscapeCAPolicyURL	Não aplicável	
18. netscapeComment	Não aplicável	

Certificado de Servidor		
CAMPO	**CONTEÚDO**	**CRÍTICA para extensões**
Campos de X509v1		
1. Version	V3	
2. Serial Number	Aleatório	
3. Signature Algorithm	Sha256withRsaEncryption	
4. Issuer Distinguished Name	CN=ECRaizEstado 002 O=Sistema de Certificação Eletrónica do Estado C=PT	
5. Validity	3 anos.	
6. Subject	CN=<OBJECTO>, OU=ECEstado, O=Sistema de Certificação Eletrónica do Estado L=<Localidade>, S=Portugal, C=PT	
7. Subject Public Key Info	Algoritmo: RSA Tamanho da chave: 4096	
Campos de X509v2		
1. issuerUniqueIdentifier	Não utilizado	
2. subjectUniqueIdentifier	Não utilizado	
Extensões de X509v3		
1. Subject Key Identifier	Derivada de utilizar a função de hash SHA-1 sobre a chave pública do sujeito.	Não
2. Authority Key Identifier	Derivada de utilizar a função de hash SHA-1 sobre a chave pública da EC emissora.	Não

Certificado de Servidor		
CAMPO	**CONTEÚDO**	**CRÍTICA para extensões**
3. KeyUsage		Sim
Digital Signature	1	
Non Repudiation	0	
Key Encipherment	1	
Data Encipherment	0	
Key Agreement	0	
Key Certificate Signature	0	
CRL Signature	0	
4. extKeyUsage	ServerAuth (1.3.6.1.5.5.7.3.1)	
5. privateKeyUsagePeriod	Não utilizado	
6. Certificate Policies		
Policy Identifier	*2.5.29.32.0 (AnyPolicy)*	
URL CPS	http://www.scee.gov.pt/rep	
Notice Reference	Não utilizado	
7.Policy Mappings	Não utilizado	
8. Subject Alternate Names	DNS Name=<nome do servidor>	
9. Issuer Alternate Names	Não utilizado	
10. Subject Directory Attributes	Não utilizado	
11. Basic Constraints		
Subject Type	Não utilizado	
Path Length Constraint	Não utilizado	
12. Policy Constraints	Não utilizado	
13. CRLDistributionPoints	(1) HTTP: http://crls.ecee.gov.pt/crls/ARL-002.crl	
14. Auth. Information Access	OCSP: http://ocsp.ecee.gov.pt	
15. netscapeCertType	Não aplicável	
16. netscapeRevocationURL	Não aplicável	
17. netscapeCAPolicyURL	Não aplicável	
18. netscapeComment	Não aplicável	

Certificado de OCSP Responder		
CAMPO	**CONTEÚDO**	**CRÍTICA para extensões**
Campos de X509v1		
1. Version	V3	
2. Serial Number	Aleatório	
3. Signature Algorithm	Sha256withRsaEncryption	
4. Issuer Distinguished Name	CN=ECRaizEstado O=Sistema de Certificação Eletrónica do Estado C=PT	

Certificado de OCSP Responder		
CAMPO	**CONTEÚDO**	**CRÍTICA para extensões**
5. Validity	6 meses.	
6. Subject	CN=VA-ECEE, OU=ECEstado, O=Sistema de Certificação Eletrónica do Estado C=PT	
7. Subject Public Key Info	Algoritmo: RSA Tamanho da chave: 4096	
Campos de X509v2		
1. issuerUniqueIdentifier	Não utilizado	
2. subjectUniqueIdentifier	Não utilizado	
Extensões de X509v3		
1. Subject Key Identifier	Derivada de utilizar a função de hash SHA-1 sobre a chave pública do sujeito.	
2. Authority Key Identifier	Derivada de utilizar a função de hash SHA-1 sobre a chave pública da EC emissora.	
3. KeyUsage		Sim
Digital Signature	1	
Non Repudiation	1	
Key Encipherment	0	
Data Encipherment	0	
Key Agreement	0	
Key Certificate Signature	0	
CRL Signature	0	
4. extKeyUsage	OCSP Signing (1.3.6.1.5.5.7.3.9)	Sim
5. privateKeyUsagePeriod	Não utilizado	
6. Certificate Policies		Não
Policy Identifier	*2.5.29.32.0 (AnyPolicy)*	
URL CPS	http://www.scee.gov.pt/rep	
Notice Reference	Não utilizado	
7.Policy Mappings	Não utilizado	
8. Subject Alternate Names	Não utilizado	
9. Issuer Alternate Names	Não utilizado	
10. Subject Directory Attributes	Não utilizado	
11. Basic Constraints		Não
Subject Type	End Entity	
Path Length Constraint	None	
12. Policy Constraints	Não utilizado	
13. CRLDistributionPoints	Não utilizado	
14. Auth. Information Access	Não utilizado	
15. netscapeCertType	Não aplicável	
16. netscapeRevocationURL	Não aplicável	
17. netscapeCAPolicyURL	Não aplicável	

Certificado de OCSP Responder		
CAMPO	**CONTEÚDO**	**CRÍTICA para extensões**
18. netscapeComment	Não aplicável	
19. OCSP No Revocation Check	Ativo	

7.1.3 Identificadores de algoritmo

Algoritmo	OID
Sha1WithRSAEncryption	1.2.840.113549.1.1.5
Sha256WithRSAEncryption	1.2.840.113549.1.1.11
rsaEncryption	1.2.840.113549.1.1.4

Tabela 4 – Identificadores OiD de Algoritmos

7.1.4 Formatos de nome

Os Certificados emitidos para cada entidade do SCEE são referenciados através de um identificador único (DN) no formato X.500, a aplicar nos campos "*issuer*" e "*subject*" do certificado.

Os DNs deverão ser representados através de uma X.501 UTF8String.

7.1.5 Restrições de nome

Os nomes contidos nos certificados são restringidos a '*Distinguished Names*' X.500. O atributo "C" (*countryName*) é codificado de acordo a "*ISO 3166-1-alpha-2 code elements*", em *PrintableString*.

No caso dos certificados autoassinados da ECRaizEstado o DN do emissor e do titular são os mesmos:

CN=ECRaizEstado 002

O=Sistema de Certificação Eletrónica do Estado

C=PT

No caso dos certificados das ECSubordinadas o DN do titular é:

CN=<Nome da ECSuborndinada>

OU=ECEstado

O=Sistema de Certificação Eletrónica do Estado

C=PT

No CN tem de se identificar o nome de ECSubordinada respetiva e no campo O deve constar o nome da organização responsável.

7.1.6 Objeto identificador da política de certificado

Com o objetivo de não limitar o conjunto de políticas para as cadeias de certificação na qual se incluem os certificados da ECRaizEstado e da ECSubordinada utiliza-se a política especial '*anyPolicy*' com um valor de 2.5.29.32.0.

7.1.7 Utilização da extensão de restrição de políticas

Não aplicável.

7.1.8 Sintaxe e semântica dos qualificadores de políticas

Nos certificados emitidos, a ECRaizEstado inclui no campo "*policyQualifiers*" da extensão "*Certificate Policies*", o URL da DPC.

7.1.9 Semântica de processamento da extensão de política de certificados críticos

Tendo em consideração as recomendações introduzidas no 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 respetivos, tendo em conta a sua aplicação.

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

7.2 PERFIL DA LCR

7.2.1 Número (s) da versão

As LCRs emitidas pelas EC, implementam a versão 2 padrão ITU X.509, de acordo com o RFC 5280, atualizado pelo RFC 6818 (*Certificate and CRL Profile*).

7.2.2 Extensões da LCR e das suas entradas

A ECRaizEstado define como extensões de LCR obrigatórias, não críticas, as seguintes:

- *CRLNumber*, implementado de acordo com as recomendações do RFC 5280, atualizado pelo RFC 6818;
- *AuthorityKeyIdentifier*: deve conter o hash (SHA-1) da chave pública da EC que assinou a LCR.

CAMPO	CONTEÚDO	CRÍTICA para extensões
Version	2	
Signature		
AlgorithmIdentifier		
Algorithm	Sha256withRsaEncryption	
Parameters		
IssuerName		
ThisUpdate	Data de emissão	
validityPeriod	6 meses	
NextUpdate	6 meses	
revokedCertificates		
Usercertificate	Não	
CertificateSerialNumber	Sim	
RevocationDate	Sim	
crlEntryExtension		
reasonCode		Não
CRLReason		
Unspecified	1	
KeyCompromise	1	
CACompromise	1	
affiliationChanged	1	
superseded	1	
cessationOfOperation	1	
certificateHold	1	
removeFromCRL	0	
certificateissuer	CN=ECRaizEstado O= Sistema de Certificação Eletrónica do Estado C=PT	Sim
crlExtensions		
authorityKeyIdentifier	Derivada de utilizar a função hash sha-1 sobre a chave pública da EC emissora	Não
issuerAltName		Não
crlNumber	Sequencial	Não
issuingDistributionPoint	(1) HTTP: http://crls.ecee.gov.pt/crls/ARL-002.crl	Não
onlyContainsUserCerts	0	
onlyContainsCACerts	1	
IndirectCRL	0	
DeltaCRLIndicator	Não utilizado	Sim
BaseCRLNmber	Este valor será igual ao do CRLNumber	

7.3 PERFIL DO OCSP

O serviço de OCSP disponibilizado pela ECRaizEstado está implementado para que os certificados de OCSPResponder estejam 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*".

7.3.1 Número(s) da versão

Os certificados de OCSP responder disponibilizados pela ECRaizEstado utilizam e estão em conformidade com a norma X.509 versão 3 (X.509 v3).

7.3.2 Extensões do OCSP

Os certificados de OCSP Responder emitidos pela ECRaizEstado incluem 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.

8. AUDITORIA E OUTRAS AVALIAÇÕES DE CONFORMIDADE

8.1 FREQUÊNCIA OU MOTIVO DA AUDITORIA

De acordo com o descrito no ponto 8 da PCert do SCEE, 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.

Anualmente será efetuada uma auditoria interna à ECRaizEstado de acordo com o Plano de Auditorias do SCEE. Com isto garante-se a adequação do seu funcionamento e operação com as estipulações do presente documento.

Sem prejuízo do anterior, o SCEE realizará auditorias internas baseando-se no seu próprio critério e em qualquer altura.

Entre as auditorias a realizar inclui-se uma auditoria a cada dois anos de cumprimento da legislação de proteção de dados pessoais.

8.2 IDENTIDADE E QUALIFICAÇÕES DO AUDITOR

A identidade e qualificação do auditor são determinadas de acordo com o estabelecido na Política de Certificados do SCEE.

8.3 RELAÇÃO ENTRE O AUDITOR E A ENTIDADE CERTIFICADORA

A relação entre o auditor e a ECRaizEstado será feita de acordo com o estabelecido na Política de Certificados do SCEE.

.

8.4 ÂMBITO DA AUDITORIA

A auditoria de segurança é efetuada com base nos requisitos mínimos definidos neste documento.

As auditorias determinam a conformidade dos serviços da ECRaizEstado com a PCert do SCEE e o presente documento.

Devem, igualmente, 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) Contratos;

g) Política de Privacidade.

As auditorias podem ser completas ou parciais, incidir sobre qualquer outro tipo de documentos / procedimentos, tendo em consideração os critérios definidos no CWA 14172-2.

Em particular, para o caso da ECRaizEstado, a auditoria deverá incidir também sobre as cerimónias de geração de chaves, tanto do certificado autoassinado da ECRaizEstado como dos certificados das ECSubordinadas que se venham a gerar.

8.5 PROCEDIMENTOS APÓS UMA AUDITORIA COM RESULTADO DEFICIENTE

As auditorias com resultado deficiente são tratadas de acordo com o estabelecido na PCert do SCEE.

8.6 COMUNICAÇÃO DE RESULTADOS

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

Comunicação de resultados	Auditor	ECEE	Autoridade Credenciadora
RPI	No final da auditoria		
RAF	2 Semanas		
RCI		1 Semana	
Decisão sobre irregularidades			1 Semana

Tabela 5 – Prazos de comunicação dos resultados de Auditoria

O Auditor comunicará os resultados da auditoria à Direção da ECRaizEstado como entidade máxima responsável.

9. OUTRAS SITUAÇÕES E ASSUNTOS LEGAIS

9.1 TAXAS

9.1.1 Taxas por emissão ou renovação de certificados

O acesso aos certificados de ECRaizEstado, dado a sua natureza pública, é livre e gratuito não podendo haver deste modo qualquer taxa aplicada.

9.1.2 Taxas para acesso a certificados

O acesso aos certificados de ECRaizEstado, dado a sua natureza pública, é livre e gratuito não podendo haver deste modo qualquer taxa aplicada.

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

Não se aplicará nenhuma taxa por este serviço de informação sobre a DPC nem por nenhum outro serviço adicional que se tenha conhecimento no momento da redação do presente documento.

9.1.5 Política de reembolso

Não Aplicável.

9.2 RESPONSABILIDADE FINANCEIRA

9.2.1 Seguro de cobertura

Não Aplicável.

9.2.2 Outros recursos

Não aplicável.

9.2.3 Seguro ou garantia de cobertura para utilizadores

Não aplicável.

9.3 CONFIDENCIALIDADE DA INFORMAÇÃO PROCESSADA

9.3.1 Âmbito da confidencialidade da informação

De acordo com a Política de Certificados do SCEE.

9.3.2 Informação não protegida pela confidencialidade

De acordo com a Política de Certificados do SCEE.

9.3.3 Responsabilidade de proteção da confidencialidade da informação

Todo o pessoal de administração, operação e supervisão da ECRaizEstado mantêm o segredo profissional sobre a informação que conheçam devido ao desempenho das suas funções. Esta obrigação é estendida tanto ao pessoal próprio como ao pessoal externo que colabora no âmbito das obrigações contratuais estabelecidas.

O pessoal do CEGER afeto a funções na ECRaizEstado está credenciado, a título individual, pelo Gabinete Nacional de Segurança, marca nacional no grau secreto.

Os auditores externos à ECRaizEstado prestam serviços no âmbito da supervisão desta EC, são os constantes da lista do Gabinete Nacional de Segurança com credenciação para esta função.

As entidades terceiras, no âmbito dos contratos celebrados, estão obrigadas a assinatura de um acordo de confidencialidade e medidas de segurança, sendo o mesmo aplicável aos seus colaboradores.

9.4 PRIVACIDADE DOS DADOS PESSOAIS

Não aplicável.

9.4.1 Medidas para garantia da privacidade

Não aplicável.

9.4.2 Informação privada

Não aplicável.

9.4.3 Informação não protegida pela privacidade

Não aplicável.

9.4.4 Responsabilidade de proteção da informação privada (dados pessoais)

Não aplicável.

9.4.5 Notificação e consentimento para utilização de informação privada

Não aplicável.

9.4.6 Divulgação resultante de processo judicial ou administrativo

Não aplicável.

9.4.7 Outras circunstâncias para revelação de informação

Não aplicável.

9.5 DIREITOS DE PROPRIEDADE INTELECTUAL

De acordo com a Política de Certificados do SCEE.

9.6 REPRESENTAÇÕES E GARANTIAS

9.6.1 Representação das EC e garantias

De acordo com a Política de Certificados do SCEE.

9.6.2 Representação das ER e garantias

De acordo com a Política de Certificados do SCEE.

9.6.3 Representação e garantias do titular

De acordo com a Política de Certificados do SCEE.

9.6.4 Representação dos correspondentes (Relying party) e garantias

De acordo com a Política de Certificados do SCEE.

9.6.5 Representação e garantias de outros participantes

De acordo com a Política de Certificados do SCEE.

9.7 RENÚNCIA DE GARANTIAS

De acordo com a Política de Certificados do SCEE.

9.8 LIMITAÇÕES ÀS OBRIGAÇÕES

De acordo com a Política de Certificados do SCEE.

9.9 INDEMNIZAÇÕES

De acordo com a Política de Certificados do SCEE.

9.10 TERMO E CESSAÇÃO DA ATIVIDADE

9.10.1 Termo

O presente documento estará em vigor enquanto não for revogada expressamente pela emissão de uma nova versão ou pela renovação das chaves da ECRaizEstado, momento em que obrigatoriamente se redigirá uma nova versão.

9.10.2 Substituição e revogação da DPC

O presente documento será substituído 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 versão do presente documento ficar revogada será retirada do repositório público, garantindo-se, contudo, que será conservada durante 20 anos.

9.10.3 Consequências da conclusão da atividade e sobrevivência

As obrigações e restrições que são estabelecidas no presente documento, em referência a auditorias, informação confidencial, obrigações e responsabilidades da ECRaizEstado, 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, relativo aos requisitos operacionais para o ciclo de vida dos certificados, os representantes das entidades titulares dos certificados poderão comunicar com a ECEE, na qualidade de entidade que tem atribuídas as competências da raiz do Estado, através de mensagem eletrónica ou, por escrito, através de correio postal, conforme previsto no ponto 1.5.2 do presente documento.

9.12 ALTERAÇÕES

9.12.1 Procedimento para alterações

Compete ao Diretor do CEGER, na qualidade de dirigente máximo da entidade que detém atribuições de gestão da ECRaizEstado, realizar e aprovar alterações ao presente documento.

9.12.2 Prazo e mecanismo de notificação

No caso em que a entidade competente pela gestão da ECRaizEstado julgue que as mudanças à especificação podem afetar à aceitabilidade dos certificados para propósitos específicos, comunicar-se-á às entidades titulares dos certificados, que se efetuou uma mudança e que devem consultar a nova versão no repositório estabelecido no presente documento.

9.12.3 Motivos para mudar de OID

De acordo com a Política de Certificados do SCEE.

9.13 DISPOSIÇÕES PARA RESOLUÇÃO DE CONFLITOS

Para a resolução de qualquer conflito que possa surgir com relação ao presente documento, 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 à ECRaizEstado está disponível em https://www.scee.gov.pt/legislacao/

9.15 CONFORMIDADE COM A LEGISLAÇÃO EM VIGOR

É responsabilidade da entidade a quem compete a gestão da ECRaizEstado zelar pelo cumprimento da legislação aplicável reconhecida no ponto anterior.

9.16 PROVIDÊNCIAS VÁRIAS

9.16.1 Acordo completo

Todas as terceiras partes confiantes assumem na sua totalidade o conteúdo da última versão do presente documento.

9.16.2 Independência

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

A situação anterior é valida, apenas e só nos casos em que tais estipulações não sejam consideradas essenciais. É responsabilidade da entidade a quem compete a gestão da ECRaizEstado 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

Nada a assinalar.

A. ANEXO – NORMALIZAÇÃO TÉCNICA

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:	Juho 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)
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
SO27001	Nome:	ISO/IEC 27001:2005
	Versão:	—
	Tipo:	Recommendation
	Data:	outubro de 2005
	Organismo:	International Telecommunications Union
	Descrição:	formation technology-Security techniques-Information security management systems-Requirements
ISO27002	Nome:	ISO/IEC 27002:2005
	Versão:	—
	Tipo:	Recommendation
	Data:	junho de 2005
	Organismo:	International Telecommunications Union
	Descrição:	Information technology – Security techniques – Code of practice for information security management
ISO17799	Nome:	ISO/IEC 17799:2005
	Versão:	Atualiza a ISO/IEC 17799:2000
	Tipo:	International Standard
	Data:	junho de 2005

	Organismo:	International Organization for Standardization e International Electrotechnical Commission
	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
ISO9594	Nome:	ISO/IEC 9594-8
	Versão:	4ª correção
	Tipo:	International Standard
	Data:	
	Organismo:	International Organization for Standardization e International Electrotechnical Commission
	Descrição:	Public-key and Attribute Certificate framework

ISO9595	Nome:	ISO/IEC 9595:1998
	Versão:	4ª correção
	Tipo:	International Standard
	Data:	outubro de 1998
	Organismo:	International Organization for Standardization e International Electrotechnical Commission
	Descrição:	Information technology - Open Systems Interconnection - Common management information Service definition"
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
ISO9564-2	Nome:	ISO 9564-2
	Versão:	Atualiza a versão de 1991
	Tipo:	International Draft
	Data:	janeiro de 2005
	Organismo:	International Organization for Standardization
	Descrição:	Banking – Personal Identification Number management and security – Part 2: Approved algorithms for PIN encipherment
ISO9564-3	Nome:	ISO 9564-3
	Versão:	
	Tipo:	International Draft
	Data:	novembro de 2003
	Organismo:	International Organization for Standardization
	Descrição:	Banking – Personal Identification Number management and security – Part 3: Requirements for offline PIN handling in ATM and POS 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
ISO 11568-1	Nome:	ISO 11568-1
	Versão:	
	Tipo:	International Standard
	Data:	2005
	Organismo:	International Organization for Standardization
	Descrição:	Banking – Key management (retail) - Part 1: Principles
ISO 11568-2	Nome:	ISO 11568-2
	Versão:	
	Tipo:	International Standard
	Data:	2005
	Organismo:	International Organization for Standardization
	Descrição:	Banking – Key management (retail) – Part 2: Symmetric ciphers, their key management and life cycle
ISO 11568-4	Nome:	ISO 11568-4
	Versão:	
	Tipo:	International Standard
	Data:	1998
	Organismo:	International Organization for Standardization
	Descrição:	Banking – Key management (retail) – Part 4: Key management techniques using public key cryptosystems
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
ETSI102176-1	Nome:	ETSI TS 102 176- 1
	Versão:	V1.2.1
	Tipo:	
	Data:	julho de 2005
	Organismo:	Electronic Signatures and Infrastructures (ESI);
	Descrição:	Part 1 - Algorithms and Parameters for Secure Electronic Signatures;
ETSI102176-2	Nome:	ETSI TS 102 176- 2
	Versão:	V1.2.1
	Tipo:	
	Data:	julho de 2005
	Organismo:	Electronic Signatures and Infrastructures (ESI);
	Descrição:	Part 2: Secure channel protocols and algorithms for signature creation devices
ETSI102158	Nome:	ETSI TS 102 158
	Versão:	V1.1.1
	Tipo:	
	Data:	outubro de 2003
	Organismo:	Electronic Signatures and Infrastructures (ESI);
	Descrição:	Policy requirements for Certification Service Providers issuing attribute certificates usable with Qualified certificates
ETSI102042	Nome:	ETSI TS 102 042
	Versão:	1.2.2
	Tipo:	Technical Specification
	Data:	junho de 2005
	Organismo:	ESI - Electronic Signatures and Infrastructures
	Descrição:	Policy Requirements for certification authorities issuing public key certificates

ETSI102023	Nome:	ETSI TS 102 023
	Versão:	V1.2.1
	Tipo:	Technical Specification
	Data:	janeiro de 2003
	Organismo:	Electronic Signatures and Infrastructures (ESI);
	Descrição:	Policy requirements for time-stamping authorities
ETSI101903	Nome:	ETSI TS 101 903
	Versão:	V1.3.2
	Tipo:	Technical Specification
	Data:	março de 2006
	Organismo:	Electronic Signatures and Infrastructures (ESI);
	Descrição:	XML Advanced Electronic Signatures (XAdES)
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
ETSI101861	Nome:	ETSI TS 101 861
	Versão:	V1.3.1
	Tipo:	Technical Specification
	Data:	janeiro de 2006
	Organismo:	Electronic Signatures and Infrastructures (ESI);
	Descrição:	Time stamping profile
ETSI101733	Nome:	ETSI TS 101 733
	Versão:	V1.6.3
	Tipo:	Technical Specification
	Data:	setembro de 2005
	Organismo:	Electronic Signatures and Infrastructures (ESI);
	Descrição:	CMS Advanced Electronic Signatures (CAdES)
ETSI101456	Nome:	ETSI TS 101 456
	Versão:	V1.4.1

	Tipo:	Technical Specification
	Data:	janeiro de 2006
	Organismo:	Electronic Signatures and Infrastructures (ESI);
	Descrição:	Policy requirements for certification authorities issuing qualified certificates
CWA15264-3	Nome:	
	Versão:	
	Tipo:	abril 2005
	Data:	
	Organismo:	
	Descrição:	User Requirements for a European interoperable eID system within a smart card infrastructure
CWA15264-2	Nome:	
	Versão:	
	Tipo:	
	Data:	april 2005
	Organismo:	
	Descrição:	Best Practice Manual for card scheme operators exploiting a multi-application card scheme incorporating interoperable IAS services
CWA15264-1	Nome:	
	Versão:	
	Tipo:	
	Data:	abril 2005
	Organismo:	
	Descrição:	Architecture for a European interoperable eID system within a smart card infrastructure
CWA14890-2	Nome:	CWA 14890-2
	Versão:	
	Tipo:	
	Data:	
	Organismo:	
	Descrição:	Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional Services

CWA14890-1	Nome:	CWA 14890-1
	Versão:	
	Tipo:	
	Data:	
	Organismo:	
	Descrição:	Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic requirements
CWA14365-2	Nome:	CWA 14365-2
	Versão:	
	Tipo:	CEN Workshop Agreement
	Data:	
	Organismo:	European Committee for Standardization
	Descrição:	Guide on the Use of Electronic Signatures - Part 2: Protection Profile for Software Signature Creation Devices
CWA14365-1	Nome:	CWA 14365-1
	Versão:	
	Tipo:	CEN Workshop Agreement
	Data:	
	Organismo:	European Committee for Standardization
	Descrição:	Guide on the Use of Electronic Signatures - Part 1: Legal and Technical Aspects
CWA14355	Nome:	CWA 14355
	Versão:	
	Tipo:	CEN Workshop Agreement
	Data:	março de 2004
	Organismo:	European Committee for Standardization
	Descrição:	Guidelines for the implementation of Secure Signature-Creation Devices
CWA14172-8	Nome:	CWA 14172-8
	Versão:	
	Tipo:	CEN Workshop Agreement
	Data:	março 2004
	Organismo:	European Committee for Standardization

	Descrição:	EESSI Conformity Assessment Guidance - Part 8: Time-stamping Authority services and processes
CWA14172-7	Nome:	CWA 14172-7
	Versão:	
	Tipo:	CEN Workshop Agreement
	Data:	
	Organismo:	European Committee for Standardization
	Descrição:	EESSI Conformity Assessment Guidance - Part 7: Cryptographic modules used by Certification Service Providers for signing operations and key generation services
CWA14172-6	Nome:	CWA 14172-6
	Versão:	
	Tipo:	CEN Workshop Agreement
	Data:	
	Organismo:	European Committee for Standardization
	Descrição:	EESSI Conformity Assessment Guidance - Part 6: Signature-creation device supporting signatures other than qualified
CWA14172-5	Nome:	CWA 14172-5
	Versão:	
	Tipo:	CEN Workshop Agreement
	Data:	
	Organismo:	European Committee for Standardization
	Descrição:	EESSI Conformity Assessment Guidance - Part 5: Secure signature-creation devices
CWA14172-4	Nome:	CWA 14172-4
	Versão:	
	Tipo:	CEN Workshop Agreement
	Data:	
	Organismo:	European Committee for Standardization
	Descrição:	EESSI Conformity Assessment Guidance - Part 4: Signature-creation applications and general guidelines for electronic signature verification
CWA14172-3	Nome:	CWA 14172-3
	Versão:	
	Tipo:	CEN Workshop Agreement

	Data:	
	Organismo:	European Committee for Standardization
	Descrição:	EESSI Conformity Assessment Guidance - Part 3: Trustworthy systems managing certificates for electronic signatures
CWA14172-2	Nome:	CWA 14172-2
	Versão:	
	Tipo:	CEN Workshop Agreement
	Data:	
	Organismo:	European Committee for Standardization
	Descrição:	EESSI Conformity Assessment Guidance - Part 2: Certification Authority services and processes
CWA14172-1	Nome:	CWA 14172-1
	Versão:	
	Tipo:	CEN Workshop Agreement
	Data:	
	Organismo:	European Committee for Standardization
	Descrição:	EESSI Conformity Assessment Guidance - Part 1: General introduction
CWA14171	Nome:	CWA 14171
	Versão:	
	Tipo:	CEN Workshop Agreement
	Data:	maio de 2004
	Organismo:	European Committee for Standardization
	Descrição:	General guidelines for electronic signature verification
CWA14170	Nome:	CWA 14170
	Versão:	
	Tipo:	CEN Workshop Agreement
	Data:	maio de 2004
	Organismo:	European Committee for Standardization
	Descrição:	Security requirements for signature creation applications
CWA14169	Nome:	CWA 14169
	Versão:	
	Tipo:	CEN Workshop Agreement
	Data:	março de 2004
	Organismo:	European Committee for Standardization

	Descrição:	Secure signature-creation devices "EAL 4+"
CWA14167-4	Nome:	CWA 14167-4
	Versão:	
	Tipo:	CEN Workshop Agreement
	Data:	
	Organismo:	European Committee for Standardization
	Descrição:	Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 4: Cryptographic module for CSP signing operations - Protection profile - CMCSO PP
CWA14167-3	Nome:	CWA 14167-3
	Versão:	
	Tipo:	CEN Workshop Agreement
	Data:	
	Organismo:	European Committee for Standardization
	Descrição:	Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 3: Cryptographic module for CSP key generation services - Protection profile (CMCKG-PP)
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
CCMB3	Nome:	CCMB-2005-08-003
	Versão:	V 2.3

	Tipo:	
	Data:	agosto de 2005
	Organismo:	
	Descrição:	Common Criteria for Information Technology Security Evaluation Part 3: Security assurance
CCMB2	Nome:	CCMB-2005-08-002
	Versão:	V 2.3
	Tipo:	
	Data:	agosto de 2005
	Organismo:	
	Descrição:	Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements
CCMB1	Nome:	CCMB-2005-08-001
	Versão:	V 2.3
	Tipo:	
	Data:	agosto de 2005
	Organismo:	
	Descrição:	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model
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

B. 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:

B.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

B.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: a) Identifica de forma unívoca o titular como autor do documento; b) A sua aposição ao documento depende apenas da vontade do titular; c) É criada com meios que o titular pode manter sob seu controlo exclusivo; d) A sua conexão com o documento permite detetar toda e qualquer alteração superveniente do conteúdo deste.
Assinatura eletrónica qualificada	Assinatura digital ou outra modalidade de assinatura eletrónica avançada que satisfaça exigências de segurança idênticas às da assinatura digital baseadas num certificado qualificado e criadas através de um dispositivo seguro de criação de assinatura.
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: a) 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; b) 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; c) 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; d) 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	*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.

FIM DE DOCUMENTO