DOCUMENTO DE DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO

Entidade Certificadora Electrónica Raiz

SISTEMA DE CERTIFICAÇÃO ELECTRÓNICA DO ESTADO (SCEE)

INFRA-ESTRUTURA DE CHAVES PÚBLICAS

OID: 2.16.620.1.1.1.2

Versão 1.0, 2006.07.20

ÍNDICE DO DOCUMENTO

1. INTRODUÇÃO

1.1 ENQUADRAMENTO

Decorrente da implementação em curso de vários programas públicos para a promoção das tecnologias de informação e comunicação e a introdução de novos processos de relacionamento em sociedade, entre cidadãos, empresas, organizações não governamentais e o Estado, com vista ao fortalecimento da sociedade de informação e do governo electrónico (eGovernment), foi aprovado através da Resolução do Conselho de Ministros n.º 171/2005, publicada em D.R. em 3 de Novembro de 2005, a criação da Sistema de Certificação Electrónica do Estado (SCEE) – Infra-estrutura de Chaves Públicas. Esses programas envolvem, para certos fins específicos, mecanismos de autenticação digital forte de identidades e assinaturas electrónicas que podem ser concretizados mediante a utilização das denominadas infra-estruturas de chaves públicas.

São exemplos de projectos programados ou em curso no âmbito da sociedade da informação e do governo electrónico os relativos ao cartão do cidadão, ao passaporte electrónico português, à certificação electrónica do Governo e à disponibilização de serviços da Administração Pública pela Internet que requeiram autenticação digital forte de identidades e assinaturas electrónicas e à desmaterialização dos processos intra e inter-organismos do Estado que requeiram esse tipo de autenticação.

Assim, para assegurar a unidade dos sistemas de autenticação digital forte nas relações electrónicas de pessoas singulares e colectivas com o Estado e entre entidades públicas, é necessário estabelecer uma entidade de certificação electrónica do Estado.

A arquitectura da SCEE constituirá assim uma hierarquia de confiança, que garantirá a segurança electrónica do Estado.

Para o efeito a SCEE compreenderá uma Entidade Gestora de Politicas de Certificação que aprova a integração de entidades certificadoras na SCEE pronunciando-se igualmente sobre práticas e políticas de certificação, uma Entidade Certificadora Electrónica Raiz, que constitui o primeiro nível da cadeia hierárquica de certificação, e as várias Entidades Certificadoras do Estado a esta subordinadas.

Esta entidade deve funcionar independentemente de outras infra-estruturas de chaves públicas de natureza privada ou estrangeira, mas deve permitir a interoperabilidade com as infra-estruturas 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 (UE).

Assim, é criada a Sistems de Certificação Electrónica do Estado Português – Infra-Estrutura de Chaves Públicas, adiante designada como SCEE, que opera para os organismos e funcionários da Administração Pública bem como para as pessoas

singulares e colectivas no seu relacionamento com o Estado. A SCEE estabelece uma estrutura de confiança electrónica, de forma a que os serviços disponibilizados pelas entidades certificadoras que a compõem, proporcionem nomeadamente a realização de transacções electrónicas seguras, a autenticação forte, um meio de assinar electronicamente transacções ou informações e documentos electrónicos, assegurando a sua autoria, integridade e não repúdio, e assegurando a confidencialidade das transacções ou informação.

Esta Declaração de Prácticas de Certificação (DPC) descreve e regula as práticas de certificação da Entidade de Certificação Electrónica 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.

Esta DPC da seguimento ao estabelecidos pela Política de Certificados do Sistema de Certificação Electrónica do Estado, por isso nos capítulos em que a DPC não possa desenvolver o estabelecido na dita Política, isto se indicará através do texto "De acordo com a Política de Certificados da SCEE".

Esta DPC assume que o leitor conhece os os conceitos de Infraestrutura de Chaves Públicas, certificados e assinatura electrónica; em caso contrário recomenda-se ao leitor que tente obter conhceimento nos conceitos referidos anteriomente antes de continuar com a leitura do presente documento.

A presente DPS 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 obejctivo de dar um caracter uniforme ao documento e facilitar a sua leitura e análise, são incluidas todas as secções estabelecidas no RFC 3647. Quando não esteja previsto nada em alguma secção, deverá aparecer a frase "Não aplicado".

Para a eleboração 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

1.2 IDENTIFICAÇÃO DO DOCUMENTO

Em virtude dos vários projectos em curso e tendo conta a diversidade e especificidade de cada um dos mesmos, as várias politicas de certificados são identificadas por um Object Identifier (OID), que traduz a sua aplicabilidade ção na atribuição de certificados digitais por cada uma das Entidade Certificadoras do Estado. Os diversos OIDs, estão de acordo com as especificações definidas na Estrutura de OID da SCEE (http://www.scee.gov.pt/).

Este documento de Politica de Certificação é identificado pelos dados constantes na seguinte tabela:

INFORMAÇÃO DO DOCUMENTO	
Nome do Documento	Declaração de Práticas de Certificação da Entidade de Certificação Electrónica do Estado
Versão do Documento	Versão 0.1
Estado do Documento	Em aprovação
OID	2.16.620.1.1.1.2.1.1.0
Data de Emissão	24 de Maio de 2006
Válidade	Não aplicável
Localização	http://www.scee.gov.pt/dpcert

1.3 PARTICIPANTES NA INFRA-ESTRUTURA DE CHAVES PÚBLICAS

1.3.1 Entidades Certificadoras (EC)

São entidades que, após devida autorização da Entidade Gestora de Politicas de Certificação (EGPC), estão habilitadas para criar, assinar, atribuir e gerir certificados digitais. Na prática uma EC é composta pelo conjunto de equipamentos, aplicações, pessoal e procedimentos que são indispensáveis para implementar os diversos serviços de certificação disponibilizados e garantir a adequada gestão do ciclo de vida dos certificados descritos nesta politica de certificação.

A hierarquia de confiança da SCEE compreende a Entidade de Certificação Electrónica do Estado (ECRaizEstado), as Entidades Certificadoras do Estado (ECEstado) e Entidades Certificadoras Subordinadas (subECEstado).

As Entidades Certificadoras que compõem a SCEE são:

- A ECRaizEstado, como Entidade de Certificação de primeiro nível. A sua função é estabelecer a raiz da cadeia de confiança da infra-estrutura de chaves públicas (PKI). Esta EC não emite certificados para utilizadores finais, emitindo apenas certificados para assinar as Entidades Certificadoras do Estado. A ECRaizEstado assina-se a si própria.

Subject	CN= ECRaizEstado, O=SCEE, C=PT
Certificado pkcs1-sha1WithRSAEncryption (*)	
Número de série	42 ea 5b 0a 51 11 26 7c d8 27 74 b7 df 7f 71
Periodo de validade	De sexta-feira, 23 de Junho de 2006 13:41:27 Até domingo, 23 de Junho de 2030 13:41:27
Marca Digital (SHA-1)	39 13 85 3e 45 c4 39 a2 da 71 8c df b6 f3 e0 33 e0 4f ee 71

Huella Digital (MD5)	15 5e f5 11 7a a2 c1 15 0e 92 7e 66 fe 3b 84 c3
Certificado pkcs1-sha256WithRSAEncryption	
Número de série	14 7b c7 26 70 d6 3c d9 fa b7 72 77 e9 9c 9c
Periodo de validade	sexta-feira, 23 de Junho de 2006 17:43:01 domingo, 23 de Junho de 2030 14:41:27
Marca Digital (SHA-1)	6b 87 64 3e b7 81 d4 3a 0b f9 4b b9 b6 fd b3 54 c0 cd 02 6a

(*) Além do certificado com algoritmo de assinatura sha256withRsaEncryption será emitirá, para o mesmo par de chaves, um certificado assinado com sha1. Este será distribuido por razões de interoperabilidade para facilitar todos aqueles sistemas e aplicações que não suportem este algoritmo, construir a cadeia de confiança nos processos de validação de certificados e assinatura, dando-se um prazo até 31 Dezembro de 2007 para realizar as adaptações que sejam necessárias. A partir dessa data a DPC será revista para indicar de forma expressa que dito certificado não pode ser utilizado

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

- As subECEstado, são entidades que se encontram no nível imediatamente abaixo das EC, tendo como função a prestação de serviços de certificação para o utilizador final. O seu certificado é assinado pela respectiva ECEstado

As Entidades Certificadoras constituídas no âmbito da SCEE, deverão disponibilizar uma versão completa da sua Declaração de Práticas de Certificação (DPC).

1.3.2 Entidades de Registo (ER)

As Entidades de Registo desenvolvem a sua actividade de acordo com o estabelecido na DPC da respectiva EC e pelo Conselho Gestor do SCEE

1.3.3 Titulares de Certificados

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

No âmbito deste documento, dado que se trata da DPC da ECEE – Entidade Certificadora Raiz, os titulares dos certificados serão as pessoas colectivas, desde que sob responsabilidade humana, o qual aceita o certificado e é responsavel pela sua correcta utilização e salvagurada da sua chave privada. Preferencialemnte, será designado como responsavel pelo certificado, o representante legal da pessoa jurídica ou um dos seus representantes legais

Definitivamente, os titulares serão os responsáveis da própria EC Raiz (autocertificado) e das EC Subordindas

1.3.4 Partes confiantes

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

1.3.5 Outros participantes

1.3.5.1 A ENTIDADE GESTORA DE POLÍTICAS DE CERTIFICAÇÃO

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

1.3.5.2 A ENTIDADE CERTIFICADORA RAIZ DO ESTADO

A Entidade Certificadora Raíz do Estado é a entidade certificadora de topo da cadeia de certificação da SCEE, executora das políticas de certificados e directrizes aprovadas pela Entidade Gestora de Políticas de Certificação. Compete a esta prestar os serviços de certificação às Entidades Certificadoras do Estado no nível hierárquico imediatamente inferior ao seu na cadeia de certificação em conformidade com as normas aplicáveis às entidades certificadoras estabelecidas em Portugal na emissão de certificados digitais qualificados.

Os serviços de certificação digital disponibilizados pela Entidade de Certificação Raiz do Estado englobam exclusivamente: o processo de registo das entidades certificadoras, geração de certificados e gestão do seu ciclo de vida, disseminação dos certificados, das politicas e das praticas 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 (D-L nº 116-A/2006).

1.3.5.3 AUTORIDADE CREDENCIADORA

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

1.3.5.4 AUTORIDADES DE VALIDAÇÃO

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

1.4 UTILIZAÇÃO DO CERTIFICADO

1.4.1 Utilização adequada

Os certificado autoassinados da EC Raiz regulamentados por esta DPC serão utilizados para prestar os siguintes serviços de segurança:

Tipo de certificado	Usos apropiados
Certificado autoassinado CSRS da EC Raíz	Assinatura de certificados, CRLs e informação de estado de certificados
Certificado autoassinado de assinatura da EC Raíz	Assinatura

Os certificados de autenticação de EC Subordinadas, isto é, dependentes hierarquicamente da EC Raíz de SCEE, que sejam autorizadas expresamente pelo Conselho Gestor do SCEE a utiliza-los.

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

Tipo de certificado	Usos apropiados
Certificados CSRS de EC Subordinada	Assinatura de certificados, CRLs e informação de estado de certificados
Certificados de Assinatura de EC Subordinada	Assinatura
Certificados de Servidor de EC Subordinada	Autenticação do servidor e establecimento de comunicações mediante protocolo SSL

1.4.2 Utilização não autorizada

Qualquer uso não incluido na secção anterior fica excluido.

1.5 GESTÃO DAS POLÍTICAS

1.5.1 Entidade responsável pela Gestão do documento

A gestão deste Declaração de Práticas de Certificação é da responsabilidade da ECEE.

1.5.2 Contacto

NOME	ENTIDADE GESTORA DE ENTIIDADE DE CERTIFICAÇÂO ELECTRÓNICA DO ESTADO
Morada:	Rua Almeida Brandão nº 7 1200-602 Lisboa
Correio electrónico:	ecee@ecee.gov.pt
Página Internet:	www.scee.gov.pt
Telefone	+ 351 213 923 410
Fax:	+351 213 923 499

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

O Conselho Gestor do Sistema de Certificação Electrónico do Estado é o órgão competente para determinar a adequação das DPC das diversas entidades, com a Política de Certificados definida neste documento.

1.5.4 Procedimentos para aprovação da DPC

A entidade Gestora da ECEE é a Autoridade encarregada da aprovação da presente DPC.

Este entidade é também competente para aprovar as modificações desta DPC.

1.6 DEFINIÇÕES E ACRÓNIMOS

1.6.1 Definições

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

1.6.2 Acrónimos

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

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 objectivo de publicar, entre outras, informação para os correspondentes/destinatários, sobre os certificados e listas de revogação de certificado.

Os repositórios 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 utilizado o protocolo http (80) e https (443).

Não são implementados mecanismos de segurança para acesso ao conteúdo público constante nos repositórios.

É indicado o endereço do repositório da DPC, dos certificados da EC Raiz e EC subordindas e CRL da EC Raiz.

2.2 PUBLICAÇÃO DE INFORMAÇÃO DE CERTIFICAÇÃO

Nos repositorios da ECEE está disponível a seguintes infofmação:

a) Uma cópia electrónica do documento de Politica de Certificados (PCert), assinado electronicamente, por indivíduo devidamente autorizado e com certificado digital atribuído para o efeito;

b) Uma cópia electrónica desta DPC, assinada electronicamente, pelo administrador de segurança com certificado digital atribuído para o efeito;

c) Listas de Certificados Revogados (LCR)

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

e) Formulário para pedido de certificado;

f) Formulário para pedido revogação;

g) As LCR;

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.

A Entidade Certificadora Raiz publica toda a informação requerida na Política de Certificados.

2.3 PERIODICIDADE DE PUBLICAÇÃO

A informação incluída nos repositórios deverá ser disponibilizadas logo que haja informação actualizada.

A publicação da CRL da EC Raiz será publicada no repositório num prazo máximo de 24 horas desde a data da sua aprovação.

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

De três em três meses ou sempre que exista alguma revogação de certificados serão publicado as listas de certificados revogados.

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

2.4 CONTROLO DE ACESSO AOS REPOSITÓRIOS

Não existe qualquer restrição de acesso para consulta a esta DPC aos certificados emitidos e às listas de certificados revogados (CRL).

São utilizados mecanismos e controles de acesso apropriados de forma a restringir ao 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 Tipo de nomes

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

Os certificados atribuídos a cada entidade deverão conter no campo "Subject", um DN, para utilização como identificador único de cada entidade, de acordo com o preconizado no RFC 3280.

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

CN=ECRaizEstado

O=SCEE-ICP

C=PT

3.1.2 Necessidade de nomes significativos

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

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

3.1.3 Anonimato ou pseudónimo de titulares

Não aplicavel

3.1.4 Interpretação de formato de nomes

As regras utilizadas pela SCEE para interpretar o formato dos nomes dos certificados que emite são as contidas na norma ISO 9595.

Seguir o estabelecido no RFC 3280, para certificados emitidos a partir de 31 de Dezembro de 2003, todos os atributos *DirectoryString* dos campos *issuer* e *subject* do certificado, devem ser codificados numa *UTF8String*, com excepção dos atributos *country* e *serialnumber*, que devem estar codificados numa *PrintableString*

3.1.5 Unicidade de nomes

O conjunto de nome distinto (distinguished name) mais o conteúdo da extensão *KeyUsage* deve ser único e não ambiguo. O Administrador de Segurança da EC Raiz é encarregado de verificar o cumprimento desta norma.

3.1.6 Reconhecimento, autenticação e funções das marcas registadas

De acordo com a legislação a entidade Certificado Raiz do Estado é denomindada ECEE

3.2 VALIDAÇÃO DE IDENTIDADE NO REGISTO INICIAL

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 2510.

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

No caso das EC Subordninadas 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 todo isto de acordo com o CMP.

3.2.2 Autenticação da identidade de uma pessoa colectiva

O processo de autenticação da identidade de uma pessoa colectiva utilizados pelas EC ou ER deve obrigatoriamente garantir a pessoa colectiva é quem na realidade diz ser.

As EC ou ER, devem guardar toda a documentação utilizada para verificação da identidade do indivíduo.

El proceso para autenticar a los titulares de EC Subordinadas se describe en el apartado 1.5.3, siendo la EGPC el órgano responsable de verificar la identidad de dichos titulares.

A ECCE, 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.

Entre outras, considera-se como documentação mínima exigível, a documentação onde conste todos os dados necessários para a criação e emissão do certificado digital, destacando-se, os seguintes elementos:

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

- Denominação legal;
- Número de pessoa colectiva, sede, objecto social, nome dos titulares dos corpos sociais e de outras pessoas com poderes para a obrigarem e número de matrícula na conservatória do registo comercial;
- Nome completo, número do bilhete de identidade ou qualquer outro elemento que permita a identificação inequívoca das pessoas singulares que estatutária ou legalmente a representam;
- Endereço e outras formas de contacto;
- Indicação quanto ao uso do certificado ser ou não restrito a determinados tipos de utilização, bem como eventuais limites do valor das transacções para as quais o certificado é válido;
- Eventual referência a uma qualidade específica, em função da utilização a que o certificado estiver destinado;
- 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 colectiva, os seguintes elementos referentes ao requerente:

- Nome ou denominação legal;
- Número do bilhete de identidade, data e entidade emitente, ou qualquer outro elemento que permita a identificação inequívoca, ou número de pessoa colectiva;
- Residência ou sede;

- Objecto 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;
- Endereço e outras formas de contacto.
- Declaração da pessoa singular a constar como titular do certificado de que se obriga ao cumprimento das obrigações enquanto titular.

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

3.2.3 Autenticação da identidade de uma pessoa singular

A autenticação das pessoas físicas participantes na geração dos certificados da AC Raiz e dos certificados das EC subordinadas são regulados nos documentos adicionais que descrevem as "Cerimónias de Geração de Chaves".

3.2.4 Informação de subscritor/titular não verificada

Toda a informação estabelecida nas pontos 3.2.3 e 3.2.4 ha de ser cumprida.

3.2.5 Validação dos poderes de autoridade ou representação

As Entidades de Certificação e as Entidades de Registo podem autorizar entidades privadas a tomar acções 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 júridica.

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 EC Raiz actúa em nome próprio por ser membro da SCEE e responsavel pela ECEE – EC Raiz, pelo que não é necessário definir um procedimento de comprovação das faculdades representativas.

O solicitante de certifiado de EC Subordinada actúa am nome próprio por ser membro daquela entidade que se preytende constituir como EC Subordinada devendo ser seu responsavel.

3.2.6 Critérios para interoperabilidade

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

3.3 IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDOS DE RENOVAÇÃO DE CHAVES

3.3.1 Identificação e autenticação para renovação de chaves, de rotina

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

3.3.2 Identificação e autenticação para renovação de chaves, após revogação

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

A renovação não deve ser concedida se:

- A revogação ocorreu porque o certificado foi emitido para uma pessoa que não a que está no Subject do certificado;
- certificado foi emido sem autorização na pessoa que está indicada no Subject;
- 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

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

A política de autenticação aceitará pedidos de revogação assinados digitalmente pelo titular do certificado.

Qualquer entidade que componha a SCEE, pode solicitar a revogação de um determinado certificado, se tiverem conhecimento ou suspeita de compromisso da chave privada do titular ou qualquer outro acto que recomende esta acção.

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 EC Raiz, dada a sua importância, é efectuada através de uma cerimónia completamente formalizada com presença de responsaveis 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 EC Raiz 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 EC Subordinada emuldura-se numa cerimónia de geração de chaves. Esta petição deve ser realizada por:

A pessoa ou entidade com poder para actuar em representação da EC Subordinada.

A EC Subordinada deve ter sido previam,ente autorizada pela ECEE para actuar como tal, dentro da autorização será identificará que pessoas podem efectuar a petição do certificado de EC

O pedido do certificado não implica a sua obtenção, se o solicitante não cumpre os requistos estabelecidos na DPC e Pcert para certificado de EC subordinada. A ECEE poderá pedir ao solicitante documentação adicional que considere oportuna.

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:

- Estabelecimento do registo inicial do requisitante, tal como definido no ponto 3.2 "Validação de identidade no registo inicial";
- Obtenção por parte do requisitante, do respectivo par de chaves, por cada certificado requisitado/solicitado;
- 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 recebisdos dos dados pela ECEE, está 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 EC Raiz posteriormente encarregar-se-a de fazer chegar o certificado ao solicitante por meios que garantam confidencialidade e integridade.

Na EC Raiz, o administrador de registo é o responsável por verificar que se cumprem as condições do pedido e activar 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 (EC Raiz), são considerados válidos se os seguintes requisitos forem cumpridos:

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

4.2.1 Processos para a identificação e funções de autenticação

De acordo com o estipulado na secção 3.2 deste documento.

O Pedido pode chegar por duas vias, cada uma com o seu mecanismos de identificação:

- Solicitação assinada electronicamente: o administrador de registo verifica a validade da assinatura e que o assinante está capacitado para realizar o pedido.
- Solicitação assinada em papel: o administrador de registo verifica a assinatura manuscrita e em caso de não conhecer o solicitante é requirida a sua documentação identificativa.

4.2.2 Aprovação ou recusa de pedidos de certificado

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

As solicitações devem ser aprovada previamente pela ECEE ao tratar-se de certificados de EC, devendo o administrador de registo comprovar que dispõe da dita autorização.

A EC Raiz pode negar-se a emitir um certificadode qualquer solicitante baseando-se exclusivamente nos seus próprios critérios, sem que isso implique contrair responsabilidade alguma pelas conseqüências que possam derivar-se de tal negativa.

4.2.3 Prazo para processar o pedido de certificado

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

A EC Raiz não será responsável das demoras que possam surgir no período compreendido entre a solicitação de certifiado, a publicação no repositorio de SCEE e a entrega do certificado. Na medida do possível a AC Raiz processrá as petições em menos de 24 horas, sempre que se tenham cumprido todos os requisitos estabelecidos neste documento

4.3 EMISSÃO DE CERTIFICADO

4.3.1 Procedimentos para a emissão de certificado

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

Os procesimentos estabelecidos nesta secção também se aplicam no caso de renovação de certificados, já que esta implica a emissão de novos certificados.

Na emissão dos certificados da AC:

- Utiliza um procedimento de geração de certificados que vincula de forma segura o certificado com a informação de registo, incluindo a chave pública certificada.
- Protege a confidencialidade e integridade dos dados de registro

Quando uma EC emita um certificado de acordo com um pedido, efectuará as notificações que se estabeleçam no ponto 4.3.2 do presente capitulo.

Todos os certificados iniciam a sua vigência no momento da sua emissão, salvo que se indique no mesmo uma data ou hora posterior à sua entrada em vigor. O periodo de vigência está sujeito a uma possivel extinção antecipada, temporal ou definitiva, quando se expliquem as causas que motivem a revogação do certificado.

A EC Raiz entregará o certificado de EC Subordainada mediante um ficheiro PKCS#7.

4.3.2 Notificação da emissão do certificado ao titular

O solicitante conhecerá a emissão do certificado de AC subordinada através de correio electrónico assinado.

4.4 ACEITAÇÃO DO CERTIFICADO

4.4.1 Procedimentos para a aceitação de certificado

O responsavel da EC Subordinada assinará de forma electrónica ou manuscrita o documento estabeleçido para esse efeito.

4.4.2 Publicação do certificado

Os certificados da EC Raiz e das EC Subordinada são publicados no repositorio da SCEE.

4.4.3 Notificação da emissão de certificado a outras entidades

Não aplicavel

4.5 USO DO CERTIFICADO E PAR DE CHAVES

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

- A ECRaiz apenas emite certificados à ECE e EC externas e ao pessoal próprio para efeitos de operação dos seus sistemas;
- As ECE emitem certificados ao pessoal próprio para efeitos de operação dos seus sistemas e dependendo da forma como estão organizadas, emitem certificados para o utilizador final (titulares) ou para subEC;

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

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 Politica de Certificados e nesta DPC 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 useo estabelecidas nesta DPC (pontos 1.4.1 e 1.4.2) e só para os que estas estabeleçam.

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

Os certificados auto assinados da EC Raiz podem ser utilizados para prestar os seguintes serviços de segurança:

Tipo de certificado	Usos apropiados
Certificado Auto Assinado CSRS da EC Raiz	Assinatura de certificados, CRLs e informação de estado de certificados
Certificado Auto Assinado Assinatura de AC Raíz	Assinatura

4.5.2 Uso do certificado e da chave pública pelos correspondentes

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

4.6 RENOVAÇÃO DE CERTIFICADOS

Esta Prática não é suportada pela SCEE-ICP, logo em consequencia não se aplicam os pontos 4.6.1 a 4.6.7

4.6.1 Motivos para renovação de certificado

Não aplicável no âmbito da SCEE.

4.6.2 Quem pode submeter o pedido de renovação de certificado

Não aplicável no âmbito da SCEE.

4.6.3 Processamento do pedido de renovação de certificado

Não aplicável no âmbito da SCEE.

4.6.4 Notificação de emissão de novo certificado ao titular

Não aplicável no âmbito da SCEE.

4.6.5 Procedimentos para aceitação de certificado

Não aplicável no âmbito da SCEE.

4.6.6 Publicação de certificado após renovação

Não aplicável no âmbito da SCEE.

4.6.7 Notificação da emissão do certificado a outras entidades

Não aplicável no âmbito da 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 da SCEE, é designado por renovação de certificado com geração de novo par de chaves.

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

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

- Fim do período de validade
- Alteração dos dados constantes no certificado
- Comprometimento das chaves ou perca de fiabilidade das mesmas.
- Alteração de formatos.

Um certificado de AC Subordinada pode ser renovado, entre outros, pelos seguintes motivos:

- Fim do período de validade
- Alteração dos dados constantes no certificado
- Comprometimento das chaves ou perca de fiabilidade das mesmas.
- 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 valido para entidades com certificados em vigor.

A renovação será solicitada respectivamente pelo responsável da AC Raiz e pelo responsável da EC Subordinada correspondente.

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

Os requisitos de renovação são os mesmo que para a emissão inicial do certificado auto assinado da EC Raiz.

Os requisitos de renovação são os mesmo que para a emissão inicial do certificado de EC Subordinada.

Em qualquer caso, a renovação de um certificado está En cualquier caso la renovación de un certificado está sujeita a:

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

4.7.4 Notificação da emissão de novo certificado ao titular

No caso do certificado auto assinado da EC Raiz não existe este procedimento e no caso das EC Subordinadas se efectuará através de correio electrónico

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

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

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

Aplicam-se os mesmos critérios que para a emissão inicial.

4.7.7 Notificação da emissão de novo certificado a outras entidades

Aplicam-se os mesmos critérios que para a emissão inicial.

4.8 ALTERAÇÃO DE CERTIFICADO

A alteração de certificados é o processo em que um titular (ou outro participante) gera um novo par de chaves e o submete para emissão de um novo certificado através de um pedido de certificado que inclui a nova informação que certifica a sua chave pública. Na prática, este processo é um novo pedido de certificado, sendo por isso tratado como tal.

Em consequencia são aplicados os pontos 4.8.1 a 4.8.7

Este processo não é suportado pela SCEE, quando requerido uma modificação no certificado, deve ser efectuado um pedido de certificado em conformidade com o disposto no ponto 4.1.

4.8.1 Motivos para alteração de certificado

Não aplicável no âmbito da SCEE.

4.8.2 Quem pode submeter o pedido de alteração de certificado

Não aplicável no âmbito da SCEE.

4.8.3 Processamento do pedido de alteração de certificado

Não aplicável no âmbito da SCEE.

4.8.4 Notificação da emissão de certificado alterado ao titular

Não aplicável no âmbito da SCEE.

4.8.5 Procedimentos para aceitação de certificado alterado

Não aplicável no âmbito da SCEE.

4.8.6 Publicação do certificado alterado

Não aplicável no âmbito da SCEE.

4.8.7 Notificação da emissão de certificado alterado a outras entidades

Não aplicável no âmbito da SCEE.

4.9 SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO

A revogação e suspensão dos Certificados são mecanismos a utilizar no presuposto que por alguma causa estabelecida na PC ou nesta DPC se deixe de confiar nos ditos certificados antes da finalização do período de validade originalmente previsto.

A revogação de um certificado é o acto 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 operatividade conforme aos usos que lhe são próprios e, em conseqüência a revogação de um certificado desabilita o uso legítimo do mesmo por parte do titular.

No caso de uma suspensão, a validade do certificado pode ser recuperada.

4.9.1 Motivos para a revogação

Um certificado auto assinado da EC Raiz pode ser revogado por:

- Emissão defeitoso de um certificado devido a:

  1 Não se tenham cumprido qualquer requisito fundamental para a emissão do certificado.

  2 A convição de que um dado fundamental relativo ao certifocado pode ser falso.

  3 Existência de um erro de escrita de dados ou outro erro de processo.

- O par de chaves gerado pelo titular é considerado como "fraco".
- A informação contida no certificado ou utilizada para o seu pedido é incorrecta.
- Por ordem formulada do titular ou por terceiro autorizado ou a própria pessoa física solictante em representação de pessoa jurídica.
- Por ocurrencia de qualquer outra causa especificada na PC ou nesta DPC.

Um certificado de EC Subordinada pode ser revogado por:

O roubo, perda, revelação, modificação, ou outro compromisso ou suspeita de compromisso da chave privada do titular.

- O uso indevido deliberado de chaves e certificados, ou a falta de observância ou contravenção dos requerimentos operacionais contidos nesta DPC ou na PCert

- Fim da Actividade da SCEE.
- A EC Subordinada cessa a sua actividade ou deixa de estar subordinada.
- Emissão defeituosa de um certificado debido a:
    1 Não se tenham cumprido qualquer requisito fundamental para a emissão do certificado.
    2 A convição de que um dado fundamental relativo ao certifocado pode ser falso.
    3 Existência de um erro de escrita de dados ou outro erro de processo.

- par de chaves gerado pelo titular é considerado como "fraco".
- A informação contida no certificado ou utilizada para o seu pedido é incorrecta.
- Por ordem formulada do titular ou por terceiro autorizado ou a própria pessoa física solictante em representação de pessoa jurídica.
- Por ocurrencia de qualquer outra causa especificada na PC ou nesta DPC.
- certificado da EC Raíz é revogado.

4.9.2 Quem pode submeter o pedido de revogação

Está autorizado para solicitar a revogação de un certificado:

- titular quando ocorra qualquer uma das circunstâncias expostas no ponto 4.9.1 da DPC
- A pessoa ou organizalção que fez o pedido do certificado e nome de uma organização, dispositivo ou aplicação.
- Uma terceira parte quando tenha a noção que um certificado foi utilizado com fins fraudulentos..
- A própria EC ou ER sempre que tenha conhecimento de qualquer das circunstâncias expostas no ponto 4.9.1 desta DPC.

4.9.3 Procedimento para pedido de revogação

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

No pedido deverá constar o seguinte:

- Indentificação do solicitante.
- Identificar a EC Raiz ou a EC Subordinada para que se solicite a revogação do certificado
- Incluir as causas do pedido

4.9.4 Produção de efeitos da revogação

A revogação será feita de forma imediata. Após terem sido efectuados todos os procedimentos e seja verificado que o pedido é válido, 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 tem como responsabilidade verificar o estado de todo os certificados, através das LCR ou num servidor de verificação do estado on-line (via OCSP).

4.9.7 Periodicidade da emissão da Lista de Certificados Revogados (CRL)

A EC Raiz publicará uma nova CRL no seu repositório no momento em que se produza qualquer revogação e em último caso, em intervalos não spueriores a 3 meses também 3 meses para as ARL geradas pela EC Raíz (mesmo que não existam modificações).

4.9.8 Período máximo entre a emissão e a publicação da CRL

De acordo com o estipulado no ponto 4.9.7

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

SCEE proporciona um servidor web onde publica as CRLs para a verificação do estado dos certificados que emite. Não existe actualmente uma Autoridade de Validação que, mediante o protocolo OCSP, permite verificar o estado dos certificados.

Os endereços de acesso via web às CRL estão referenciadas no ponto 2.1.

4.9.10 Requisitos de verificação on-line de revogação

Não aplicavel

4.9.11 Outras formas disponíveis para divulgação de revogação

Não aplicavel.

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 adoptados os procedimentos descritos na secção 5.7.3.

4.9.13 Motivos para suspensão

Não são permitidos a suspensão de certificados auto assinados da EC Raiz nem dos certificados das EC Subordinadas.

4.9.14 Quem pode submeter o pedido de suspensão

Não são permitidos a suspensão de certificados auto assinados da EC Raiz nem dos certificados das EC Subordinadas.

4.9.15 Procedimentos para pedido de suspensão

Não são permitidos a suspensão de certificados auto assinados da EC Raiz nem dos certificados das EC Subordinadas.

4.9.16 Limite do período de suspensão

Não são permitidos a suspensão de certificados auto assinados da EC Raiz nem dos certificados das EC Subordinadas.

4.10 SERVIÇOS SOBRE O ESTADO DO CERTIFICADO

4.10.1 Características operacionais

Não aplicavel

4.10.2 Disponibilidade de serviço

Não aplicavel

4.10.3 Características opcionais

Não aplicavel

4.11 FIM DE SUBSCRIÇÃO

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

- Revogação do certificado por qualquer das causas descritas no ponto 4.9.1
- 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 efectuado arquivo de chaves privadas de EC Raiz e de EC Subordinada.

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

Não estipulado.

5. MEDIDAS DE SEGURANÇA FÍSICA, DE GESTÃO E OPERACIONAIS

5.1 MEDIDAS DE SEGURANÇA FÍSICA

Todos os aspectos 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 aspectos mais relevantes

5.1.1 Localização física e tipo de construção

A EC Raiz – ECCE - está localizada num Centro de Dados Seguro totalmente construído com paredes de alvenaria betão e tijolo e com tecto e pavimento contruido 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 anti-vandalismo e com fechaduras acionaiaveis electronicamente e respsctivas barras anti-pânico.

A Zona de Alta Segurança (ZAS) tem com 4 layers de protecção perimetrica, de forma a controlar o acesso físico à EC. Isto inclui:

- Uma zona de recepção onde os vistantes se identificam e são reconhecidos com tal
- Uma zona de operações onde o acesso é restricto e é feito através da recepção;
- Uma zona de segurança, onde serão registadas todas os acessos através da zona de operações;
- Uma zona de alta segurança onde tecnologia biometrica será instalada para controlar o acesso à EC.

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

A EC Raiz mantém planos de disaster recovery para as operações da sua EC. As instalações de disaster recovery estão protegidas pelos mesmos níveis de segurança que o local primário.

5.1.2 Acesso físico ao local

O Centro de Dados da ECEE 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 vídeo-vigilância e de gravação, sistemas de detecção 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 actividades 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 é sempre feito através de sistemas de controles de acessos, sendo que qualquer acesso considerado visita é devidamente registado no livro "Diário" onde são registados todos os acessos e qualquer tipo de actividades que ocorram nesta zona.

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 eléctrica durante períodos de falta de corrente e para proteger os equipamentos face a flutuações eléctricas 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.

5.1.4 Exposição à água

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

5.1.5 Prevenção e protecção contra incêndio

O centro de dados da ECEE dispõe de sistemas automáticos de detecção e extinção de incêndios. O gáz 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.

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 informaçãom, cumprindo neste caso a norma EN 1143-1 e com dupla fechadura. O acesso a estas zonas, é restrito a pessoas devidamente autorizadas

5.1.7 Eliminação de resíduos

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

5.1.8 Instalações externas (alternativa) para recuperação de segurança

Todas as cópias de segurança (e.g., base de dados, programas, file system,) são colocadas num site remoto que está geograficamente separado do sítio primário. O acesso físico ao site remoto é restrito a apenas o pessoal autorizado. O site remoto 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 SCEE, são operados de forma segura, seguindo procedimentos preestabelecidos. Por razões de segurança, a informação relativa aos controlos de procedimentos consideram-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 ECEE e que podem materialmente afectar:

- Validação de informação de emissão de Certificado;
- Aceitação, rejeição, pedido de revogação, de renovação ou outro processo de emissão de Certificado;
- Emissão, revogação de Certificados;
- Manipulação de informações de Subscritor ou pedidos.

As funções de confiança incluem além de outras:

a) Administrador de Sistemas
b) Operador de Sistemas
c) Administrador de Segurança
d) Administrador de Registo
e) Auditor de Sistemas
f) Administradores de HSM (Modulo Segurança - Hardware)
g) Operadores de HSM (Modulo Segurança - Hardware)

5.2.1.1 ADMINISTRADOR DE SISTEMAS

É o encarregado pela instalação e configuração de sistemas operativos de produtos de software, da manutenção e actualização dos produtos instalados.

Grante a prestação do serviço com o adequado nível de qualidades e fiabilidade em função do grau de criticidade do mesmo.

Colaborar com os auditores em tudo aquilo que lhe for solicitado.

Não tem acesso a aspectos relacionados com a segurança dos sistemas, da rede.

Mantém o inventário dos equipamentos e servidores que compõem o núcleo da plataforma de certificação digital.

5.2.1.2 OPERADOR DE SISTEMAS

Responsável por operar regularmente os sistemas.

É responsável pela correcta execução da política de cópias de segurança e em particular de as manter actualizadas para que permite recuperar eficientemente qualquer um dos sistemas.

Esta função é acomulada 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 encarrege de qualquer aspecto relativo à segurança: física, das aplicações, da rede, etc

É encarregado pela gestão dos sistemas de protecção perimétrica.

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

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 eléctrica.

É responsavel por explicar todos os mecanismos de segurança aos funcionários que devam conhece-los e de consciencializa-los para as questões de segurança levando-os a fazer cumprir as normas e politicas de segurança estabelecidas.

É responsável por estabelecer os calendários para a execução de análise de vulnerabilidades, testes, e trieno, 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 encarregado de:

- Verificar da existência de toda a documentação necessária e devidamente numerada;
- Verificar a coerência da documentação e dos procedimentos;
- Verificar os procedimentos de incidentes e eventos
- Verificar e analisar a protecção dos sistemas (exposição a vulnerabilidades, logs de acesso, utilizadores, etc);
- Verificar a existência e funcionamento dos alarmes e elementos de segurança física;

- Verificar a adequação com a legislação em vigor;
- Verificar o conhecimento dos procedimentos por parte do pessoal implicado
- Deve comprovar todos os aspectos reconhecidos na política de segurança, políticas de cópias de segurança, práticas de certificação, políticas de certificação, etc.

5.2.1.6 ADMINISTRADORES DE HSM (MODULO DE SEGURANÇA EM HARDWARE)

Define-se um conjunto de 7 Administradores para o HSM da EC Raiz, cada um com um cartão criptográfico de contole de acesso às suas funções. Para a realização das operações que requeiram um papel de administrador é necesario introducir no lector do HSM um total de 2 cartões dos 7 atribuidos. Os Administradores de HSM são responsaveis por realizar as seguintes operações:

- Recuperaração da funcionalidade do hardware critográfico em caso de falha de um HSM.
- Recuperação de chaves em caso de terem sido apagadas acidentalmente.
- Sustituição de um conjunto de cartões de administrador. Esta operação só é necesaria ser realizada se se deseja ampliar ou reducir o numero de cartões de administrador
- Sustituição de un conjunto de cartões de operador. Esta operação só é necesaria se se deseja ampliar ou reducir o número de cartões de operador ou substituir algum cartão detriorado.
- Ampliação do número de HSM integrados na infraestructura.
- Dado que se opera em modo FIPS140-2 Nivel 3, autorização para a geração de conjuntos de cartões de operador e claves. Esta operação só se requere durante a ceremónia de geração de chaves para a EC..

5.2.1.7 OPERADORES DE HSM

Define-se um conjunto de 5 operadores para a EC Raíz, cada um com um cartão criptográfico de control de accesso 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 siguientes operações:

- Activação de chaves para sua utilização. Isto significa que cada vez que se inicie a EC, é necessário a inserção dos cartões de operador associados às chaves.
- Autorização para a geração de chaves da aplicação. Esta operação sé é requerida durante a ceremonia de geração de chaves para a EC.
- Arranque do interface de configuração da EC e do resto de entidades que formam a PKI.

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

5.2.2 Número de pessoas exigidas por tarefa

A SCEE 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 multi-utilizador para a geração de chaves nas Ecs.

A atribuição de funções faz com que Sejas sempre requeridos a participação de um mínimo de duas perssoas para todas as actividades relacionadas com o ciclo de vida das chaves das EC.

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.

O resto dos utilizadores da ECEE são identificados mediante certificados lectrónicos emitidos pela própria infraestrutura da ECEE e são autenticados atrvés de cartões criptográficos.

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

5.2.4 Funções que requerem separação de responsabilidades

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

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

5.3 MEDIDAS DE SEGURANÇA DE PESSOAL

5.3.1 Requisitos relativos às qualificações, experiência, antecedentes e credenciação

Todo o pessoal que desempenhe funções na EC Raiz 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 especifica para o seu posto

5.3.2 Procedimentos de verificação de antecedentes

Cada elemento comprovou os antecedentes através das mais diversas formas: Curriculum Vitae, Registo Criminal, etc.

5.3.3 Requisitos de formação e treino

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

Este plano incluí os seguintes aspectos:

- Formação nos aspectos 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 acções 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 afecto à Entidade Certificadora

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

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 acções não autorizadas

No caso da realização de acções não autorizadas respeitantas às Entidades Certificadoras, devem ser tomadas as medidas disciplinares adequadas.

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

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

Adicionalmente em função da gravidade da infracção cometidas, devem aplicar-se as sanções previstas na lei geral da função pública, das organização 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 a DPC e a Políticas de Segurança da Informação.

A Entidades Certificadoras 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 é disponibilizado os seguintes documentos:

- Declaração de Práticas de Certificação
- Politicas de Certificação
- Politicas de Certificado
- Políticas de privacidade
- Politica de Segurança da Informação
- Organigrama e funções do pessoal

É ainda disponibilizada de forma idêntica toda e qualquer documentação técnica necessárias 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 com sucesso ou fracassadas de alteração dos parâmetros de segurança do sistema operativo
- Arranque e paragem de aplicações
- Tentativas com sucesso ou fracassadas de inicio e fim de sessão
- Tentativas com sucesso ou fracassadas de criar, modificar, apagar contas do sistema
- Tentativas com sucesso ou fracassadas de solicitar, gerar, assinar, emitir ou revogar chaves e certificados
- Tentativas com sucesso ou fracassadas de gerar ou emitir CRLs

- Tentativas com sucesso ou fracassadas de criar, modificarmos ou apagar informação dos titulares dos certificados
- Tentativas com sucesso ou fracassadas de acesso às instalações por parte de pessoal autorizado ou não
- Copias de segurança, recuperação ou arquivo dos dados
- Alterações ou actualizações de software e hardware
- Manutenção do sistema
- Mudança de pessoal
- A ceremónia 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 registrados possuem, como mínimo, a siguinte informação:

Categoria: Indica a importancia do evento.

- Informativo: Os eventos desta categoría contém informação sobre operações realizadas com éxito.
- Marca: cada vez que começa e termina uma sessão de administração, regista-se um evento desta categoría.
- Advertência: indica que se detectou 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 excepcional durante uma operação.

Data: Data e hora em que ocurreu 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 possiveis são:

- EC.
- ER.
- Repositório de informação.
- Livrarias de controle de armazenamento de informação

Descrição: Representação textual do evento. Para alguns eventos, a descrição vem seguida duma lista de parametros cujos valores variam dependendo dos dados sobre os quais se executou a operação. Alguns exemplos dos parametros que se incluêm 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 necesario, deste modo definiem-se três niveis de auditorias de control e dos evenetos com uma frecuencia semanal, mensal e anual.

5.4.3 Período de retenção dos registos de auditoria

A informação gerada pelos registos de auditoria são mantidos on-line até que Sejas arquivados. Uma vez arquivados os registos de auditoria são conservados pelo menos durante 15 anos.

5.4.4 Protecção dos registos de auditoria

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

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

A destruição de um arquivo de auditoria só pode ser levado a cabo com a autorização do Administrador de Sistema, Administrador de Segurança e Auditor de 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

São realizadas cópias de segurança de acordo com a Politicas de Cópias de Segurança das ECs

5.4.6 Sistema de recolha de dados de auditoria (interno/externo)

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

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

Todos os elementos significativos existentes na ECEE são acumulados Numa base de dados. Os Procedimentos de controle de segurança epmregues baseiam-se na tecnologia de contrução empregue nas bases de dados.

As características deste sistema são as siguintes:

- Permite verificar a integridade da base de dados, detecta uma possivel manipulação fradulenta dos dados
- Assegurar o não repudio por parte dos autores das operações realizadas sobre os dados. Isto consegue-se através das assinaturas electrónicas.
- Guarda um registo histórico de actualização dos dados, armazenar versões sucessivas de cada registro resultante de diferentes operações realizadas sobre ele. Isto permite guardar um registo das operações realizadas e evita

que se percam assinaturas electrónicas realizadas anteriormente por outros utilizadores quando se actualizão os dados.

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

- Inserção ou alteração fraudulenta de um registro de sessão.
- Supressão fraudulenta de sessões intermedias.
- Inserção, alteração ou supressão fraudulenta dum 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

São realizadas pelo menos uma análise mensal de vulnerabilidades e de segurança perimetrica.

O resultado da análise é reportado ao responsável da EC para rever e aprovar um plano de implementação e correcção das vulnerabilidades detectadas.

5.5 ARQUIVO DE REGISTOS

5.5.1 Tipo de dados arquivados

As informações e eventos que são registados são:

- Os registos de auditoria especificados no ponto 5.4 desta Política de Certificação
- Os suportes de Backups dos servidores que compõem a infra-estrutura da EC
- Documentação relativa ao ciclo de vida dos certificados:
  - Contrato/acordo de certificação
  - Cópia da documentação de identificação facultada pelo requerente de certificado
  - Identidade do operador que emitiu o certificado
  - Data da última identificação directa do titular
- Acordos de confidencialidades
- 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 15 anos.

5.5.3 Protecção dos arquivos

O Acessos aos arquivos é restrito a pessoal autorizado.

Os eventos relativos aos certificados emitidos pel EC Raiz está protegido criptograficamente para garantir a detecção 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 anti-fogo dentro da Sala Segura da EC. Uma outra cópia é realizada de forma cifrada e armazenada num cofre anti-fogo na Sala (local) Segura Alternativa.

5.5.5 Requisitos para validação cronológica dos registos

Os sistemas de informação de EC Raiz garantem o registro do tempo nos quais se realizam. O instante de tempo dos sistemas provem de uma fonte segura que constata a data e hora. Os servidores do sistema da ECEE estão sincronizados em data e hora. As fontes de tempos utilizadas, baseadas no protocolo NTP (Network Time Protocol) são utilizadas diferentes fontes, utilizando como referência a do Observatório astronómico de Lisboa

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

O sistema de arquivo é interno à EC Raiz

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 informáticos para levar a cabo acções de verificação de integridade e outras.

São realizadas de forma automática verificações de integridade dos arquivos electrónicos (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 EC Raiz é activado em caso de uma indisponibilidade máxima de 24 horas, estando preparada para a emissão de CRL antes das 12 horas seguintes.

5.7.1 Procedimentos em caso de incidente ou comprometimento

No caso que se veja afetada a segurança dos dados de verificação de assinatura da EC Raiz, esta deverá informar a todos os titulares de seus certificados e terceiros partes

conhecidas que todos os certificados e listas de revogação assinados com estes dados já não são válidos. Logo que possível se procederá 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 são suspeitos de terem sido alterados serão parados os serviços da EC Raiz 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 voltem a existir.

Em caso de afectar certificados emitidos, são notificados os titulares dos mesmos e proceder-se-a à sua rectificação.

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 a SCEE dependentes ou não da Entidade afectada.

Os certificados assinados por entidades dependentes da comprometida, no perido compreendido entre o compromisso da chave e a revogação do certificado, deverão por sua vez ser revogados, informados os seus subscritores e rectificados.

5.7.4 Capacidade de continuidade da actividade em caso de desastre

O Plano de Continuidade da EC Raiz é activado em caso de uma indisponibilidade máxima de 24 horas, estando preparada para a emissão de CRL antes das 12 horas seguintes.

5.8 PROCEDIMENTOS EM CASO DE EXTINÇÃO DE EC OU ER

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

- Compromisso da chave privada da EC
- Decisão política

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

- Informar todos os titulares de certificados e extingir a vigência dos mesmos revogando-os
- Informar todos as terceiras partes com as quais tenha formado acordos de certificação

- Comunicar ào Conselho Gestor do SCEE
- Remeter ao Membro do Governo que tutela a ECEE toda a informação relativa aos certificados electrónico revogados, para que este os tome com sua custodia.

6. MEDIDAS DE SEGURANÇA TÉCNICAS

6.1 GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES

A geração dos pares de chaves dos vários participantes nesta Infra-estrutura de chaves públicas são processados de acordo com os requisitos e algoritmos definidos nesta politica.

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, em que o respectivo par de chaves é gerado num modulo criptográfico, de acordo com requisitos definidos no ponto "6.2.1". O certificado desta entidade é auto-assinado.

As chaves para os certificados auto assinados da EC Raiz emitidos pela EC Raiz são gerados em módulos de hardware criptográficos com validação FIPS 140-2 Nível 3 que têm instalados nos seus respectivos sistemas.

As chaves para os certificados de AC Subordinada emitidos pela AC Raiz são gerados em módulos de hardware criptográficos com validação FIPS 140-2 Nível 3 que têm instalados nos seus respectivos sistemas

6.1.2 Entrega da chave privada ao titular

Não se procede a entrega da chave privada do certificado auto assinado da EC Raiz e do certificado da EC Subordinada ao titular porque já está, em cada caso, na sua posse dentro do HSM.

6.1.3 Entrega da chave pública ao emissor do certificado

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

A entrega ou par das chaves à EC Raiz deve ser efetuada através de um pedido de certificado, segundo o formato descrito no PKCS#10, através de uma transacção on-line de acordo com ou especificado não RFC 2510 (PKI Certificate Management Protocols).

6.1.4 Entrega da chave pública da EC aos correspondentes/destinatários

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

6.1.5 Dimensão das chaves

O que concerne, à dimensão das chaves, os vários participantes devem obedecer aos comprimentos mínimos de chaves:

- Nível 1 (EC Raiz): RSA 4096 bit
- Nível 2 (EC Subordinada): RSA 2048 bit

6.1.6 Geração dos parâmetros da chave pública e verificação da qualidade

A geração dos parâmetros da chave pública e verificação da qualidade deverá ter sempre por base a norma que define o algoritmo. Em termos exemplificativos, para o caso do algoritmo RSA, deverá ser feita de acordo com o estipulado no PKCS#1 y RFC 3280.

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

O campo "keyUsage" dos certificados deve ser utilizados de acordo com o recomendado no RFC 3280.

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

Para tal efeito, nos campos 'Key Usage' y 'Extended Key Usage' do certificado são incluidos os siguintes usos:

Tipo certificado	Key Usage	Extended Key Usage
Certificado auto assinado CSRS da EC Raíz	keyCertSign cRLSign	Não aplicavel
Certificado auto assinado de Assinatura da EC Raíz.	digitalSignature nonRepudiation keyAgreement	clientAuth emailProtection

A chave definida na política e por conseguinte no certificado asociado, é utilizada para a verificação da entidade das EC Subordinadas.

Para esse efeito nos campos 'Key Usage' y 'Extended Key Usage' do certificado são incluidos os siguintes usos:

Tipo certificado	Key Usage	Extended Key Usage

Tipo certificado	Key Usage	Extended Key Usage
Certificados CSRS de EC Subordinada.	keyCertSign cRLSign	Não Aplicavel
Certificados de Assinatura de EC Subordinada.	digitalSignature nonRepudiation keyAgreement	clientAuth emailProtection
Certificados de Servidor de EC Subordinada.	digitalSignature nonRepudiation keyEncipherment keyAgreement	serverAuth

6.2 PROTECÇÃO 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 EC Raiz e ECs Subordinadas do SCEE 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 Eutoridades 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 efectuadas com um mínimo de 2 pessoas (com funções qualificadas dentro da entidade) por tarefa.

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

A chave privada da EC Raiz encontra-se sob controlo de mais que uma pessoamulti perssoa. Esta apenas se activachave é activada mediante a iniciação do software da de EC por meio de uma combinação de operadores da ACEC, administradores do

HSM e utilizadores de Sistema Operativo. Este é o único método de activação de dita 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 EC Raiz dispoêm 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 30 anos após expiração da sua validade.

6.2.6 Transferência da chave privada para/do módulo criptográfico

A transferência da chave privada das EC Raiz é feita apenasECs só se pode fazer entre módulos criptográficos (HSM) e requer da intervenção de de um mínimo de dois administradores do HSM, operadores do HSM, um Administrador de Sistemas. e os custódios 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 Entidade de CertificaçãoEntidades Certificadoras que fazem uso de ditos módulos.

6.2.8 Processo para activação da chave privada

A chave privada deverá ser activada quando o sistema quando o sistema/aplicação da EC é ligado ("startup process"). Esta activação só deverá ser efectivada quando previamente tiver sido feita a autenticação no módulo criptográfico pelos operadores indicados para o efeito.

Tal e como se estipula na cláusula no ponto 6.2.2 Controlo multiutilizador Controle multi pessoa da chave privada, a chave privada da EC Raiz ativa-se atravésé activada mediante a iniciação do software de EC por meio da combinação mínima de operadores da EC correspondente. Este é o único método de ativação de dita chavecódigo privada.

6.2.9 Processo para desactivação da chave privada

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

6.2.10 Processo para destruição da chave privada

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

Em termos gerais a destruição debe sempre ser precedida por uma revogação do certificado asociado à chave, mesmo que esta esteja vigente

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

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

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

- Sem formatação do modulo criptográfico:

  Nas situações renovação de chaves (de rotina), a destruição da chave privada antiga é efectuada reescrevendo a nova chave privada do titular.

- Com formatação do modulo 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

6.3 OUTROS ASPECTOS DA GESTÃO DO PAR DE CHAVES

6.3.1 Arquivo da chave pública

As Entidades Certificadoras devem efectuar 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, para verificação de assinaturas geradas durante seu prazo de validade.

6.3.2 Períodos de validade do certificado e das chaves

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

Neste sentido a tabela seguinte apresenta a validade 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]	[3] – [3]	[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 continuar a utilizar-se o mesmo

.

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

6.4 DADOS DE ACTIVAÇÃO

6.4.1 Geração e instalação dos dados de activação

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

A EC Raiz utiliza dispositivos/mecanismos criptográficos (p.e. smartcards) para suporte às actividades, nomeadamente no seu funcionamento.

A actividade da EC Raiz é efectuada com base em funções diferenciadas, cada uma com o correspondente dispositivo onde se encontram os respectivos dados de activação.

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

Para a activação das chaves das ECs 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 que permite activar as chaves privadas.

6.4.2 Protecção dos dados de activação

Só o pessoal autorizado, neste caso os Operadores e Administradores dadas EC correspondentes, possuem os cartões criptográficascriptográficos com capacidade de ativação dadas ECs e conhecem os pinconhece as palavras passe para aceder aos dados de ativaçãoactivação.

No caso dos códigosdas chaves associadas aos certificados pessoais, só o titular conhece o códigoa chave pessoal de acesso ou PIN, sendo portanto o único

responsável da proteção dos dados de ativação de seus códigosactivação das suas chaves privadas.

6.4.3 Outros aspectos dos dados de activação

Não aplicavel

6.5 MEDIDAS DE SEGURANÇA INFORMÁTICA

Os dados referentesrespeitantes a esta secçãoeste ponto são considerados como informação confidencial e só se proporcionam a quem se reconheça real acredite ter a necessidade de os conhecerconhecê-los, como no caso de auditoríasauditorias externas ou internas e inspecçõesinspeções.

A EC Raiz tem estabelecidos os controlos necesarios, referentes à segurança da informção de acordo com a Politica de Certificados e dos standards aplicaveis.

6.6 REQUISITOS TÉCNICOS ESPECÍFICOS

Os dados referentesrespeitantes a esta secçãoeste ponto são considerados como informação confidencial e só se proporcionam a quem se reconheça real acredite ter a necessidade de os conhecer.conhecê-los
De modo geral a EC RaizA ECEE segue as boas práticas estabelecidasestsbelcidas na norma ISO 17799:2005 *Code of practice for information security management*.

6.6.1 Avaliação/nível de segurança

Os vários sistemas e produtos empregues pela ECEE, 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 ECEE, apenas são fornecidos à Autoridade Credenciadora.

A EC raiz implementa um conjunto de medidas de segurança consideradas adequadas, em resultado da arquitectura 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 de 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 ECEE, para garantir que os sistemas são seguros.

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

A infra-estrutura das EC é dotada de ambiente de desenvolvimento, pré-produção e produção claramente diferenciados e independentes.

6.7.2 Medidas para a gestão da segurança

A ECEE mantém um inventário de todos os activos, quer Sejas equipamentos, quer sejam dados ou pessoal e clasifica os mesmo de acordo com a sua necesidade de proteção e o os riscos a que podem estar expostos. Assim é feita uma análise de risco para que se consiga fazer uma eficaz gestão de risco.

.

As configurações dos sistemas são auditadas de forma peridódica e verifica-se as necesidades e capacidade

6.7.3 Ciclo de vida das medidas de segurança

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

A actualização e manutenção dos produtos e sistemas que compoêm os o sistema e ambiente da ECEE são efectuadas de acordo com as recomedações dos respectivos fabricantes e são sempre efectuadas por por pessoal com funções de confiança da ECEE.

6.8 MEDIDAS DE SEGURANÇA DA REDE

Os dados respeitantes a este ponto consideram-se informação confidencial e só se proporcionam a quem se reconheça real necessidade de os conhecer

.

Não obstante indicar que, a infra-estrutura da rede utilizada pelos sistemas de SCEE está dotada de todos os mecanismos de segurança necessários para garantir um serviço confiável e íntegro (p.e. utilização de firewall ou troca de dados cifrados entre redes). Esta rede também é auditada periodicamente.

A EC Raiz tem um nível de segurança máximo em nível de rede:

- Em modo de operação encontra-se desligada fisicamente da rede.
- Quando não esta em operação é mantida desligada ou seja em modo offline

6.9 VALIDAÇÃO CRONOLÓGICA (TIME-STAMPING)

Não aplicavel

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 3280, 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 correctamente todas as extensões identificadas no RFC 3280 (PKIX certificate and CRL profile).

7.1.2.1 AUTHORITYKEYIDENTIFIER:

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

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 critica. 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 Politicas de Certificados que dão suporte e regem o ambiente em que se processou a emissão do certificado. Deve ser incluir o OID das Politicas de Certificados.

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 activo (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 activo ("True"), ou o processo de verificação do certificado falha.

De seguida descriminamA seguir identificam-se os perfis dos quatros tipos de certificados auto assinados que emite a ECEE

da AC Raíz.

Certificado auto assinado de CSRS EC Raíz		
CAMPO	**CONTEÚDO**	**CRÍTICA para extensões**
Campos de X509v1		
1. Versión	V3	
2. Serial Number	Aleatorio	
3. Signature Algorithm	Sha256withRsaEncryption [1]	
4. Issuer Distinguished Name	CN=ECRaizEstado O=ECEE-ICP C=PT	
5. Validez	24 anos.	
6. Subject	CN=ECRaizEstado O=ECEE-ICP C=PT	
7. Subject Public Key Info	Algoritmo: RSA Encryption Tamanho da Chavechave: 4096 (big string)	
Campos de X509v2		
1. issuerUniqueIdentifier	Não será utilizado Não será utilizado	
2. subjectUniqueIdentifier	Não será utilizado	
Extensiones de X509v3		
1. Subject Key Identifier	Derivada de utilizar a função de hash SHA-1 sobre a chave pública do *subject*.	NO
2. Authority Key Identifier	Não aplicavel	Não
3. KeyUsage		Sim
Digital Signature	0	
Non Repudiation	0	

[1] Além do certificado com algoritmo de assinatura sha256withRsaEncryption será emitirá, para o mesmo par de chaves, um certificado assinado com sha1. Este será distribuido por razões de interoperabilidade para facilitar todos aqueles sistemas e aplicações que não suportem este algoritmo, construir a cadeia de confiança nos processos de validação de certificados e assinatura, dando-se um prazo até 31 Dezembro de 2007 para realizar as adaptações que sejam necessárias. A partir dessa data a DPC será revista para indicar de forma expressa que dito certificado não pode ser utilizado

Certificado auto assinado de CSRS EC Raíz		
CAMPO	**CONTEÚDO**	**CRÍTICA para extensões**
Key Encipherment	0	
Data Encipherment	0	
Key Agreement	0	
Key Certificate Signature	1	
CRL Signature	1	
4. extKeyUsage	Não será utilizado	
5. privateKeyUsagePeriod	Não será utilizado	
6. Certificate Policies		Não
Policy Identifier	*2.5.29.32.0*	
URL CPS	http://www.ecee.gov.pt/dpc	
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. Policy Constraints	Não utilizado	Não
13. CRLDistributionPoints	Não utilizado	
14. Auth. Information Access	Não aplicavel	
15.netscapeCertType	Não aplicavel	Não
16. netscapeRevocationURL	Não aplicavel	
17. netscapeCAPolicyURL	Não aplicavel	
18. netscapeComment	Não aplicavel	

Certificado Auto Assinado de Assinatura da EC Raiz		
CAMPO	**CONTEÚDO**	**CRÍTICA para extensões**
Campos de X509v1		
1. Versión	V3	
2. Serial Number	Aleatorio	
3. Signature Algorithm	Sha256withRsaEncryption [2]	
4. Issuer Distinguished Name	CN=ECRaizEstado O=SCEE-ICP C=PT	
5. Validez	24 anos.	
6. Subject	CN=ECRaizEstado O=SCEE-ICP C=PT	
7. Subject Public Key Info	Algoritmo: RSA Encryption Tamanho da Chavechave: 4096 (big string)	
Campos de X509v2		
1. issuerUniqueIdentifier	Não será utilizado	
2. subjectUniqueIdentifier	Não será utilizado	
Extensiones de X509v3		
1. Subject Key Identifier	Derivada de utilizar a función 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
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.ecee.gov.pt/dpc	
Notice Reference	Não será utilizado	

[2] Além do certificado com algoritmo de assinatura sha256withRsaEncryption será emitirá, para o mesmo par de chaves, um certificado assinado com sha1. Este será distribuido por razões de interoperabilidade para facilitar todos aqueles sistemas e aplicações que não suportem este algoritmo, construir a cadeia de confiança nos processos de validação de certificados e assinatura, dando-se um prazo até 31 Dezembro de 2007 para realizar as adaptações que sejam necessárias. A partir dessa data a DPC será revista para indicar de forma expressa que dito certificado não pode ser utilizado

Certificado Auto Assinado de Assinatura da EC Raiz		
CAMPO	**CONTEÚDO**	**CRÍTICA para extensões**
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 aplicable Não será utilizado	
17. netscapeCAPolicyURL	Não aplicavelNão será utilizado	
18. netscapeComment	Não aplicavelNão será utilizado	

De seguida descriminam-se os perfis dos cuatrosquatro tipos de certificados de EC Subordinada que a EC Raiz emite

Certificado CSRS de EC Subordinada		
CAMPO	**CONTEÚDO**	**CRÍTICA para extensões**
Campos de X509v1		
1. Versión	V3	
2. Serial Number	Aleatorio	
3. Signature Algorithm	Sha256withRsaEncryption [3]	
4. Issuer Distinguished Name	CN=ECRaizEstado O=ECEE-ICP C=PT	
5. Validez	12 anos.	
6. Subject	CN=ECESTADO-<OBJECTO> OU=<ENTIDADE RESPONSÁVEL> O=ECEE C=PT	
7. Subject Public Key Info	Algoritmo: RSA Encryption Tamanho da Chavechave: 2048 (big string)	
Campos de X509v2		
1. issuerUniqueIdentifier	Não será utilizado	

[3] Além do certificado com algoritmo de assinatura sha256withRsaEncryption será emitirá, para o mesmo par de chaves, um certificado assinado com sha1. Este será distribuido por razões de interoperabilidade para facilitar todos aqueles sistemas e aplicações que não suportem este algoritmo, construir a cadeia de confiança nos processos de validação de certificados e assinatura, dando-se um prazo até 31 Dezembro de 2007 para realizar as adaptações que sejam necessárias. A partir dessa data a DPC será revista para indicar de forma expressa que dito certificado não pode ser utilizado.

Certificado CSRS de EC Subordinada		
CAMPO	**CONTEÚDO**	**CRÍTICA para extensões**
2. subjectUniqueIdentifier	Não será utilizado	
Extensiones de X509v3		
1. Subject Key Identifier	Função hash SHA-1 sobre a chave pública do subject (EC subordinada).	Não
2. Authority Key Identifier	Função de hash SHA-1 sobre a chave pública da EC emissora (EC Raíz). NÃO SE INCLUI a identificação do certificado da EC emissora (neste caso, DN da EC Raíz, número de série da AC Raíz).	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 aplicavelNão aplicável	
5. privateKeyUsagePeriod	Não utilizadoNão será utilizado	
6. Certificate Policies		Não
Policy Identifier	*2.5.29.32.0*	
URL CPS	http://www.ecee.gov.pt/dpc	
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. Policy Constraints		
13. CRLDistributionPoints	(1) HTTP: http://crls.ecee.gov.pt/crls/ARL.crl	Não
14. Auth. Information Access	OCSP: https://ocsp.ecee.gov.pt	
15.netscapeCertType	Não aplicavel	Não
16. netscapeRevocationURL	Não aplicavel	
17. netscapeCAPolicyURL	Não aplicavel	
18. netscapeComment	Não aplicavel	

Certificado de Assinatura de EC Subordinada		
CAMPO	**CONTEÚDO**	**CRÍTICA para extensões**
Campos de X509v1		
1. Versión	V3	
2. Serial Number	Aleatorio	
3. Signature Algorithm	Sha256withRsaEncryption [4]	
4. Issuer Distinguished Name	CN=ECRaizEstado O=SCEE-ICP C=PT	
5. Validez	12 anos.	
6. Subject	CN=ECESTADO-<OBJECTO>, OU=<ENTIDADE RESPONSÁVEL>, O=SCEE, C=PT	
7. Subject Public Key Info	Algoritmo: RSA Encryption Tamanho da chave: 2048 (big string)	
Campos de X509v2		
1. issuerUniqueIdentifier	Não será utilizado	
2. subjectUniqueIdentifier	Não será utilizado	
Extensiones de X509v3		
1. Subject Key Identifier	Derivada de utilizar a função de hash SHA-1 sobre a chave pública do sujeto.	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 utilizadoNão será utilizado	
6. Certificate Policies		Não
Policy Identifier	*2.5.29.32.0*	
URL CPS	http://www.ecee.gov.pt/dpc	
Notice Reference	Não será utilizado	

[4] Além do certificado com algoritmo de assinatura sha256withRsaEncryption será emitirá, para o mesmo par de chaves, um certificado assinado com sha1. Este será distribuido por razões de interoperabilidade para facilitar todos aqueles sistemas e aplicações que não suportem este algoritmo, construir a cadeia de confiança nos processos de validação de certificados e assinatura, dando-se um prazo até 31 Dezembro de 2007 para realizar as adaptações que sejam necessárias. A partir dessa data a DPC será revista para indicar de forma expressa que dito certificado não pode ser utilizado..

Certificado de Assinatura de EC Subordinada		
CAMPO	**CONTEÚDO**	**CRÍTICA para extensões**
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. Policy Constraints	Não utilizadoNão será utilizado	
13. CRLDistributionPoints	(1) HTTP: http://crls.ecee.gov.pt/crls/ARL.crl	Não
14. Auth. Information Access	OCSP: https://ocsp.scee.gov.pt	
15. netscapeCertType	SSL_Client, SMIME_Client	Não
16. netscapeRevocationURL	Não aplicavel	
17. netscapeCAPolicyURL	Não aplicavel	
18. netscapeComment	Não aplicavel	

Certificado de Servidor de EC Subordinada		
CAMPO	**CONTEÚDO**	**CRÍTICA para extensões**
Campos de X509v1		
1. Versión	V3	
2. Serial Number	Aleatorio	
3. Signature Algorithm	Sha256withRsaEncryption [5]	
4. Issuer Distinguished Name	CN=ECRaizEstado O=ECEE-ICP C=PT	
5. Validez	12 anos.	
6. Subject	CN=ECESTADO-<OBJECTO>, OU=<ENTIDADE RESPONSÁVEL>, O=ECEE-ICP, C=PT	
7. Subject Public Key Info	Algoritmo: RSA Encryption Longitud clave: 2048 (big string)	
Campos de X509v2		
1. issuerUniqueIdentifier	Não será utilizado	

[5] Além do certificado com algoritmo de assinatura sha256withRsaEncryption será emitirá, para o mesmo par de chaves, um certificado assinado com sha1. Este será distribuido por razões de interoperabilidade para facilitar todos aqueles sistemas e aplicações que não suportem este algoritmo, construir a cadeia de confiança nos processos de validação de certificados e assinatura, dando-se um prazo até 31 Dezembro de 2007 para realizar as adaptações que sejam necessárias. A partir dessa data a DPC será revista para indicar de forma expressa que dito certificado não pode ser utilizado.

Certificado de Servidor de EC Subordinada		
CAMPO	**CONTEÚDO**	**CRÍTICA para extensões**
1. issuerUniqueIdentifier	Não será utilizado	
2. subjectUniqueIdentifier	Não será utilizado	
Extensiones de X509v3		
1. Subject Key Identifier	Derivada de utilizar a função de hash SHA-1 sobre a chave pública do subject.	Náo
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	1	
Data Encipherment	0	
Key Agreement	1	
Key Certificate Signature	0	
CRL Signature	0	
4. extKeyUsage	ServerAuth	
5. privateKeyUsagePeriod	Não utilizado	
6. Certificate Policies		Não
Policy Identifier	*2.5.29.32.0*	
URL CPS	http://www.scee.gov.pt/dpc	
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. Policy Constraints	Não utilizado	
13. CRLDistributionPoints	(1) HTTP: http://crls.scee.gov.pt/crls/ARL.crl	Não
14. Auth. Information Access	OCSP: https://ocsp.scee.gov.pt	
15. netscapeCertType	SSL_server	Não
16. netscapeRevocationURL	Não será utilizado	
17. netscapeCAPolicyURL	Não será utilizado	
18. netscapeComment	Não será utilizado	

7.1.3 Identificadores de algoritmo

Algoritmo	OID
Sha1WithRSAEncryption	1.2.840.113549.1.1.5
SHA-256 with RSA Encryption	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 da SCEE são referenciados através de um identificador único (DN) no formato X.500, a aplicar nos campos "issuer" e "subject" do certificado.

Os DN 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 codificicado de acordo a "ISO 3166-1-alpha-2 code elements", em PrintableString.

No caso dos certificados auto-assinados da EC Raiz os DN do emissor e do titular são os mesmos:

CN=ECRaizEstado

O=ECEE-ICP

C=PT

No caso dos certificados das EC Subordinadas o DN do titular é:

CN=ECESTADO-<OBJECTO>

OU=<ENTIDADE RESPONSÁVEL>

O=ECEE-ICP

C=PT

No CN tem que se identificar o tipo de EC e no campo O deve identificar-se a sua organização responsável.

7.1.6 Objecto identificador da política de certificado

Com o objectivo de não limitar o conjunto de políticas para as cadeias de certificação na qual se incluem os certificados da EC Raiz e da EC Subordinada utiliza-se a política especial 'anyPolicy' com um valor de {1.5.29.32.}

7.1.7 Utilização da extensão de restrição de políticas

Não aplicavel

7.1.8 Sintaxe e semântica dos qualificadores de políticas

A extensão Certificate Policies contem os seguintes 'Policy Quailifiers':

- URL CPS: contem a URL da DPC e a PC que regem o certificado

7.1.9 Semântica de processamento da extensão de política de certificados críticos

Tendo em consideração as recomendações introduzidas pelo RFC 3280, quanto à utilização desta extensão, os certificados das EC da SCEE devem incluir no OiD o valor 2.5.29.32.0.

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

Nos certificados para titulares serão incluídos os OiD respectivo, 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 CRL emitidas pelas EC, implementam versão 2 padrão ITU X.509, de acordo com o RFC 3280 (Certificate and CRL Profile).

7.2.2 Extensões da CRL e das suas entradas

A SCEE define como extensões de CRL obrigatórias, não criticas, as seguintes:

- CRLNumber, implementado de acordo com as recomendações do RFC 3280;
- AuthorityKeyIdentifier: deve conter o hash (SHA-1) da chave pública da EC que assinou a CRL;

CAMPO	CONTEÚDO	CRÍTICA para extensões

CAMPO	CONTEÚDO	CRÍTICA para extensões
Versión	2	
Signature		
AlgorithmIdentifier		
Algorithm	SHA-1WithRSAEncryption	
Parameters		
IssuerName		
ThisUpdate	Data de emissão	
validityPeriod	6 meses	
NextUpdate	6 meses	
revokedCertificates		
Usercertificate		
CertificateSerialNumber		
revocationDate		
crlEntryExtension		
reasonCode		Não
CRLReason		
Unspecified	1	
KeyCompromise	1	
CACompromise	1	
affiliationChanged	1	
superseded	1	
cessationOfOperation	1	
certificateHold	1	
removeFromCRL	0	
certificateissuer		Sim
crlExtensions		
authorityKeyIdentifier	Derivada de utilizar a função hash sha-1 sobre a chave pública da EC emissora	Não
issuerAltName		Não
crlNumber		Não
issuingDistributionPoint	(1) HTTP: http://crls.ecee.gov.pt/crls/ARL.crl	Não
onlyContainsUserCerts		
onlyContainsCACerts	1	
IndirectCRL		
DeltaCRLIndicator	Não se utiliza	Sim
BaseCRLNumber	Este valor será igual ao do CRLNumber	

7.3 PERFIL DO OCSP

A ECEE não proporciona serviços OCSP

7.3.1 Número(s) da versão

A ECEE não proporciona serviços OCSP

7.3.2 Extensões do OCSP

A ECEE não proporciona serviços OCSP

8. AUDITORIA E OUTRAS AVALIAÇÕES DE CONFORMIDADE

8.1 FREQUÊNCIA OU MOTIVO DA AUDITORIA

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

- No processo de integração na SCEE;
- Anualmente; e
- A qualquer momento, sem aviso prévio.

Anulamente será efectuada uma auditoria interna à EC Raiz de acordo com o Plano de Auditorias da SCEE. Com isto garante-se a adequação do seu funcionamento e operação com as estipulações desta DPC..

Sem prejuizo doa anterior, a 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 protecção de dados pessoais.

Da mesma forma a cada tres ano será efectuada uma auditoria externa para avaliar o grau de comformidade relativo à especificação técnica ETSI TS 101 456 "Policy requirements for certification authorities issuing qualified certificates", tendo em conta os critérios da CWA 14172-2 ("EESSI Conformity Assessment Guidance - Part 2: Certification Authority services and processes").

8.2 IDENTIDADE E QUALIFICAÇÕES DO AUDITOR

A identidade e qualificação do auditor é determinada de acordo com o estabelecido na Politica de Certificados.

8.3 RELAÇÃO ENTRE O AUDITOR E A ENTIDADE CERTIFICADORA

A relação entre o auditor e a EC Raiz será feita de acordo com o estabelecido com a Política de Certificados.

8.4 ÂMBITO DA AUDITORIA

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

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

- Politica de Segurança
- Segurança Física
- Avaliação Tecnológica
- Gestão dos serviços da EC
- Selecção de Pessoal
- DPC e PC (em vigor)
- Contratos
- 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 EC Raiz a auditoria deverá incidir também sobre as cerimónias de geração de chaves, tanto do certificado auto-assinado da ECEE como dos certificados das EC Subordinadas 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 Política de Certificados

8.6 COMUNICAÇÃO DE RESULTADOS

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

Comunicação de resultados	Auditor	Entidade	ECEE
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 Direcção da ECEE como entidade máxima responsável.

9. OUTRAS SITUAÇÕES E ASSUNTOS LEGAIS

9.1 TAXAS

9.1.1 Taxas por emissão ou renovação de certificados

Não Aplicavel

9.1.2 Taxas para acesso a certificado

O acesso aos certificados de EC Raiz e de EC Subordinada emitidos, 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 da Entidade Certificadora Raiz do Estado nem por nenhum outro serviço adicional que se tenha conhecimento no momento da redacção deste Documento.

9.1.5 Política de reembolso

Não Aplicavel

9.2 RESPONSABILIDADE FINANCEIRA

9.2.1 Seguro de cobertura

Não Aplicavel

9.2.2 Outros recursos

Não aplicavel.

9.2.3 Seguro ou garantia de cobertura para utilizadores

Não aplicavel

9.3 CONFIDENCIALIDADE DA INFORMAÇÃO PROCESSADA

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

9.3.1 Âmbito da confidencialidade da informação

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

9.3.2 Informação não protegida pela confidencialidade

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

9.3.3 Responsabilidade de protecção da confidencialidade da informação

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

Todo os elementos assinam um termo de responsabilidade e sigilo, onde afirmam garantir total sigilo sobre toda as actividades, sobre todos a informação e processos da ECEE.

9.4 PRIVACIDADE DOS DADOS PESSOAIS

A EC Raiz mantém actualizada a sua Política de Privacidade nos seus repositórios, onde se declara o cumprimento das disposições estabelecidas na legislação de protecção de dados pessoais.

9.4.1 Medidas para garantia da privacidade

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

9.4.2 Informação privada

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

9.4.3 Informação não protegida pela privacidade

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

9.4.4 Responsabilidade de protecção da informação privada (dados pessoais?)

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

9.4.5 Notificação e consentimento para utilização de informação privada

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

9.4.6 Divulgação resultante de processo judicial ou administrativo

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

9.4.7 Outras circunstâncias para revelação de informação

Não aplicável

9.5 DIREITOS DE PROPRIEDADE INTELECTUAL

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

9.6 REPRESENTAÇÕES E GARANTIAS

9.6.1 Representação das EC e garantias

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

9.6.2 Representação das ER e garantias

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

9.6.3 Representação e garantias do titular

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

9.6.4 Representação dos correspondentes (Relying party) e garantias

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

9.6.5 Representação e garantias de outros participantes

Não existem outros participantes.

9.7 RENUNCIA DE GARANTIAS

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

9.8 LIMITAÇÕES ÀS OBRIGAÇÕES

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

9.9 INDEMNIZAÇÕES

De acordo com a legislação em vigor

9.10 TERMO E CESSAÇÃO DA ACTIVIDADE

9.10.1 Termo

Esta DPC entra em vigor desde o momento de sua publicação no repositório de SCEE.

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

9.10.2 Substituição e revogação da DPC

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

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

9.10.3 Consequências da conclusão da actividade e sobrevivência

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

.

9.11 NOTIFICAÇÃO INDIVIDUAL E COMUNICAÇÃO AOS PARTICIPANTES

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

9.12 ALTERAÇÕES

9.12.1 Procedimento para alterações

A autoridade com atribuições para realizar e aprovar alterações sobre esta DPC é a Entidade Gestora da Entidade de Certificação Electrónica do Estado. Os dados de contacto da ECEE encontram-se no ponto *1.5 Administração das Políticas* desta DPC.

9.12.2 Prazo e mecanismo de notificação

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

9.12.3 Motivos para mudar de OID

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

9.13 DISPOSIÇÕES PARA RESOLUÇÃO DE CONFLITOS

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

9.14 LEGISLAÇÃO APLICÁVEL

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

9.15 CONFORMIDADE COM A LEGISLAÇÃO EM VIGOR

É responsabilidade da Conselho Gestor de Políticas de Certificação (CGPC) velar pelo cumprimento da legislação aplicavel reconhecida no ponto anterior.

9.16 PROVIDÊNCIAS VÁRIAS

9.16.1 Acordo completo

Todos as Terceira Partes confiantes assumem na sua totalidade o conteúdo da última versão desta DPC.

9.16.2 Nomeação (Independencia)

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 efectivas.

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

9.16.3 Severidade

Não Estipulado

9.16.4 Execuções (taxas de advogados e desistência de direitos)

Não Estipulado

9.16.5 Força maior

Não Estipulado

9.17 OUTRAS PROVIDÊNCIAS

Não Estipulado.