DOCUMENTO DE DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO

Entidade Certificadora Comum do Estado – ECCE

SISTEMA DE CERTIFICAÇÃO ELETRÓNICA DO ESTADO (SCEE)

INFRAESTRUTURA DE CHAVES PÚBLICAS

OID: 2.16.620.1.1.1.2.3.1.2

Versão 2.0 de 4 de março de 2016

APROVAÇÃO E ASSINATURA

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

O Diretor do Centro de Gestão da Rede Informática do Governo

Manuel da Costa Honorato

Assinado de forma digital por Manuel da Costa Honorato
DN: c=PT, o=Presidência do Conselho de Ministros, ou=Centro de Gestão da Rede Informática do Governo, cn=Manuel da Costa Honorato
Dados: 2016.03.04 20:45:02 Z

Manuel da Costa Honorato

ÍNDICE DO DOCUMENTO

1. INTRODUÇÃO

1.1 ENQUADRAMENTO

1.1.1 Âmbito

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

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

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

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

Para o efeito a SCEE compreende um Conselho Gestor que dá parecer sobre a aprovação e integração de entidades certificadoras no SCEE pronunciando-se igualmente sobre práticas e políticas de certificação, uma Entidade Certificadora Eletrónica Raiz, que constitui o primeiro nível da cadeia hierárquica de certificação, e as várias Entidades Certificadoras do Estado a esta subordinadas, bem como as Entidades Filiadas (ver esquema da arquitetura funcional do SCEE na Figura 1).

As entidades credenciadas, no âmbito SCEE, que disponibilizam certificados eletrónicos qualificados, de modo a suportar a produção de assinaturas eletrónicas qualificadas, têm de cumprir obrigatoriamente os requisitos mínimos definidos nas disposições legais e regulamentares em vigor,

disponibilizando para o efeito um conjunto de funções/serviços nucleares e opcionalmente determinados serviços suplementares.

São serviços nucleares: o Registo; Emissão; Distribuição; Estado das revogações e Gestão das revogações. Os serviços suplementares são o fornecimento do Dispositivo Seguro de Criação de Assinaturas e o de Validação Cronológica.

A presente Declaração de Práticas de Certificação (DPC) descreve e regula as práticas de certificação da Entidade Certificadora Comum do Estado (ECCE)

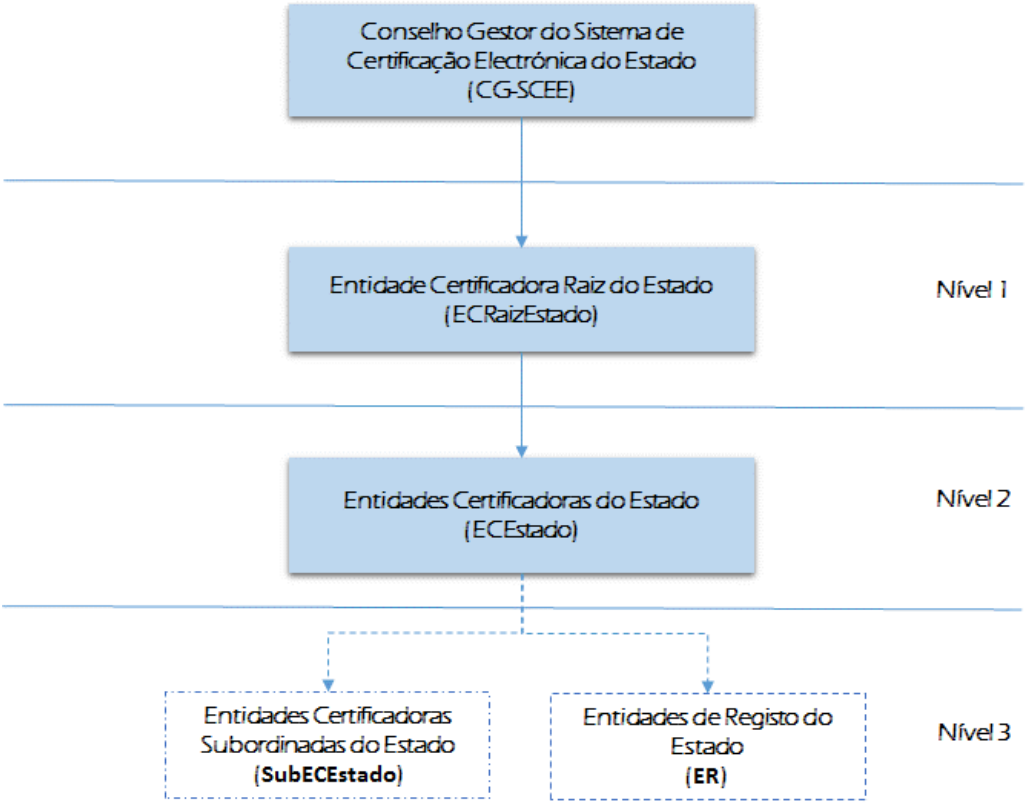

Figura 1 – Arquitetura funcional do SCEE.

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

1.1.2 Estrutura do Documento

Esta DPC assume que o leitor conhece os conceitos de Infraestrutura de Chaves Públicas, certificados e assinatura eletrónica; caso contrário, recomenda-se ao leitor que tente familiarizar-se comos conceitos referidos anteriormente, antes de continuar a leitura do presente documento.

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

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

- ETSI TS 101 456: Policy Requirements for certification authorities issuing qualified certificates;
- ETSI TS 102 042: Policy Requirements for certification authorities issuing public key certificates.

1.1.3 Hierarquia de OID

De acordo com a PCert do SCEE (Ponto 1.1.3).

1.1.3.1. DISTRIBUIÇÃO DA ÁRVORE 2.16.620.1.1 {ID-SCEE})

De acordo com a PCert do SCEE (Ponto 1.1.3.1).

1.2 IDENTIFICAÇÃO DO DOCUMENTO

O presente documento é identificado pelos dados constantes na Tabela 1 seguinte:

Tabela 1. Informação acerca do Documento de Praticas de Certificação da ECCE.

Nome do Documento	**Declaração de Práticas de Certificação da ECCE**
Versão do Documento	Versão 2.0
Estado do Documento	Aprovado
OID	2.16.620.1.1.1.2.3.1.2
Data de Emissão	4 de março de 2016
Validade	1 (um) Ano
Localização	http://www.ecce.gov.pt/repositorio/

1.3 PARTICIPANTES NA INFRA-ESTRUTURA DE CHAVES PÚBLICAS

1.3.1 Entidades Certificadoras (EC)

São entidades que, após devida autorização da Entidade de Certificação Eletrónica do Estado (ECEE), estão habilitadas para criar, assinar, atribuir e gerir certificados. A hierarquia de confiança do SCEE compreende a Entidade Certificadora Raiz do Estado (ECRaizEstado), as Entidades Certificadoras do Estado (ECEstado) e Entidades Certificadoras Subordinadas (subECEstado).

As Entidades Certificadoras que compõem o SCEE são:

1.3.1.1 ENTIDADE CERTIFICADORA RAIZ DO ESTADO

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

1.3.1.2. ENTIDADE CERTIFICADORA COMUM DO ESTADO

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 certificado da ECCE (ver Tabela 2) é assinado pela ECRaizEstado.

Tabela 2. Dados dos Certificados da ECCE.

ATRIBUTO	DESCRIÇÃO
Certificado pkcs1-sha1WithRSAEncryption	
None Distinto	CN=ECCE, OU=ECEstado, O=SCEE, C=PT
Número de série	73 a2 43 85 98 07 f8 3f 44 a9 29 34 78 84 8a 49
Período de validade	De segunda-feira, 3 de Julho de 2006 15:27:00 Até sábado, 23 de Junho de 2018 9:49:47
Marca Digital (SHA-1)	cc 90 54 40 cd f7 fb 2f a5 1c 1c ee de 55 67 08 02 a9 e6 0d
Certificado pkcs1-sha256WithRSAEncryption	
None Distinto	CN=ECCE, OU=ECEstado, O=SCEE, C=PT
Número de série	0a 5b 98 3f 9b ba 46 c7 44 a9 28 cf c0 95 5a 49
Período de validade	De segunda-feira, 3 de Julho de 2006 14:25:19 Até sábado, 23 de Junho de 2018 08:49:47
Marca Digital (SHA-1)	05 a8 c3 0c 1b 69 fe a7 83 88 a0 04 76 d1 88 e0 fc 81 f7 cf

Certificado pkcs1-sha256WithRSAEncryption	
Nome Distinto	CN=ECCE 001, OU=ECEstado, O=SCEE, C=PT
Número de série	5b e0 29 1e 3f 0c 91 e9 55 8a d0 3d 30 37 f5 49
Período de validade	De terça-feira, 24 de Junho de 2015 16:43:57 Até terça-feira, 24 de Junho de 2027 16:43:57
Marca Digital (SHA-1)	f1 8b d1 ba 06 c9 80 a0 b5 98 05 6e cc 19 1f ed 52 eb dc 25

1.3.1.3 ENTIDADES CERTIFICADORAS SUBORDINADAS

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

1.3.2 Entidades de Registo (ER)

As Entidades de Registo desenvolvem a sua atividade de acordo com o estabelecido na presente DPC, na PCert e pelo responsável máximo do CEGER (responsável pela gestão da ECCE).

1.3.3 Entidade de Validação Cronológica

A entidade de validação cronológica da ECCE é parte integrante da estrutura do SCEE. A entidade de validação cronológica emite selos temporais de acordo com as recomendações do ETSI. Cada selo temporal contém um identificador da política, sobre a qual o selo foi emitido (o valor esta descrito na tabela abaixo e no capitulo 7.3). Os selos temporais são assinados utilizando a chave privada destinada para esse efeito.

Tabela 3. Política de Certificado do Selo Temporal.

NOME DO SELO	POLÍTICA DE CERTIFICADO
SELO DE VALIDAÇÃO TEMPORAL	**2.16.620.1.1.1.2.60**

A Entidade de Validação Cronológica daECCE possui sincronização com a fonte internacional de hora (Coordinated Universal Time – UTC) com uma precisão inferior a 1 segundo.

1.3.4 Titulares de Certificados

1.3.4.1 TITULARES

No contexto deste documento, o termo subscritor/titular aplica-se a todos os utilizadores finais a quem tenham sido atribuídos certificados pela ECCE.

No âmbito deste documento, dado que se trata da DPC da ECCE, os titulares dos certificados serão as pessoas individuais ou coletivas, desde que sob responsabilidade humana, que aceitam o certificado e são responsáveis pela sua correta utilização e salvaguarda da chave privada. Preferencialmente, será designado como responsável pelo certificado, o representante legal da pessoa jurídica ou um dos seus representantes legais.

A ECCE tem como titulares, os Membros do Governo ou equiparados, os Chefes do Gabinete, Entidades aderentes à Convenção de Certificação Eletrónica no âmbito do procedimento legislativo, Titulares de cargos de direção superior de 1º e 2º grau ou equiparados de Entidades da Administração Direta e Indireta do Estado, Presidentes e membros de conselhos de administração de institutos públicos ou equiparados, dirigentes com competências especiais delegadas e funcionários e agentes do Estado cuja função determinem a utilização da autenticação e da assinatura qualificada.

1.3.4.2 PATROCINADOR

De acordo com a PCert do SCEE (Ponto 1.3.3.2).

1.3.5 Partes confiantes

De acordo com a PCert do SCEE (Ponto 1.3.4).

1.3.6 Outros participantes

1.3.6.1 A ENTIDADE CERTIFICADORA RAIZ DO ESTADO

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 políticas e das práticas de certificação, a gestão de revogações e disponibilização do estado/situação das mesmas.

A definição em detalhe, composição e seu funcionamento são definidos em documentação e legislação própria – DL nº 116-A/2006 (última alteração e republicação Decreto-Lei n.º 161/2012, de 31 de julho).

1.3.6.2 AUTORIDADE CREDENCIADORA

De acordo com a PCert do SCEE (Ponto 1.3.5.2).

1.3.6.3 AUTORIDADES DE VALIDAÇÃO

De acordo com a PCertdo SCEE (Ponto 1.3.5.3).

1.3.6.4 AUDITORES DE SEGURANÇA

De acordo com a PCert do SCEE (Ponto 1.3.5.4).

1.4 UTILIZAÇÃO DO CERTIFICADO

1.4.1 Utilização adequada

Os certificados da EC do CEGER regulamentados por esta DPC serão utilizados para prestar os serviços de segurança indicados na Tabela 4.

Tabela 4. Utilização Autorizada por Tipo de Certificado.

TIPO DE CERTIFICADO	USOS APROPRIADOS
Certificados de Autenticação	Autenticação perante os sistemas e serviços.
Certificados de Confidencialidade	Cifra de comunicações e informações.
Certificados de Assinatura	Assinatura Eletrónica Qualificada.
Certificados de Servidores	Autenticação do servidor e estabelecimento de comunicações mediante protocolo SSL.
Certificados de Assinatura de Código	Assinatura de ficheiros executáveis e scripts.

1.4.2 Utilização não autorizada

Fica excluída qualquer utilização não incluída na secção anterior (Tabela 4).

1.5 GESTÃO DAS POLÍTICAS

1.5.1 Entidade responsável pela Gestão do Documento

A gestão desta DPC é da responsabilidade do CEGER.

1.5.2 Contacto

Na tabela 5 estão descritos os contactos relevates da Entidade Gestora da ECCE.

Tabela 5. Dados de Contacto da Entidade Gestora da ECEE.

ENTIDADE GESTORA DA ECEE	
Morada:	Rua Almeida Brandão nº 7 1200-602 Lisboa
Correio Eletrónico:	certificacao@ecce.gov.pt
Página Internet:	www.ecce.gov.pt

Telefone	+ 351 213923400/10

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

De acordo com a PCert do SCEE (Ponto1.5.3).

1.5.4 Procedimentos para aprovação da DPC

A presente DPC é anualmente revista. A aprovação da DPC é efetuada pelo Diretor do CEGER, enquanto responsável pela gestão da ECCE.

1.5.5. DEFINIÇÕES E ACRÓNIMOS

Ver Anexo A do presente documento.

2. RESPONSABILIDADE DE PUBLICAÇÃO E REPOSITÓRIO

2.1 REPOSITÓRIOS

Um repositório é o conjunto de equipamentos (*hardware* e *software*), pessoas e procedimentos, construído com o objetivo de publicar informação sobre os certificados e listas de certificados revogados (LCR).

Os repositórios estão disponíveis 24 horas por dia e sete dias por semana nos seguintes endereços web: http://crls.ecce.gov.pt/crls/crl.crl e http://crls.ecce.gov.pt/crls/crl-001.crl, que poderão ser acedidos através de qualquer navegador de Internet utilizado o protocolo http (80).

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

É indicado o endereço do repositório desta DPC nos certificados da ECCE, EC subordinadas e na LCR da ECCE.

2.2 PUBLICAÇÃO DE INFORMAÇÃO DE CERTIFICAÇÃO

Nos repositórios da ECCE está disponível a seguinte informação:

a) Uma cópia eletrónica do documento de Politica de Certificados (PCert), assinado eletronicamente (www.ecce.gov.pt/repositorio/);

b) Uma cópia eletrónica desta DPC, assinada eletronicamente, pelo administrador de segurança com certificado digital atribuído para o efeito (www.ecce.gov.pt/repositorio/);

c) Listas de Certificados Revogados (LCR);

d) Informações adcionais em www.ecce.gov.pt;

São conservadas todas as versões anteriores da DPC, sendo apenas disponibilizadas a quem justificadamente as solicite.

2.3 PERIODICIDADE DE PUBLICAÇÃO

A informação incluída nos repositórios deverá ser disponibilizada logo que haja informação atualizada.A publicação da CRL da ECCE será publicada no repositório de forma imediata sempre que exista alguma revogação de certificados e a cada 24 horas, quer exista ou não alguma revogação.

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

2.4 CONTROLO DE ACESSO AOS REPOSITÓRIOS

Não existe qualquer restrição de acesso para consulta a esta DPCe às listas de certificados revogados (CRL).

São utilizados mecanismos e controlos de acesso apropriados somente a pessoal autorizado, de forma a restringir o acesso de escrita e ou modificação da informação.

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 RFC3280.

Os certificados emitidos pela ECCE têm o seguinte, DN:

Tabela 6. Regras para o preenchimento do DN.

ATRIBUTO	CÓDIGO	REGRAS PARA PREENCHIMENTO
CountryName	C	Código "PT".
OrganizationName	O	Este campo corresponde, regra geral, à Entidade (ou equivalente) do titular do certificado.
OrganizationUnitName	OU	Neste campo constará informação relativa à unidade organizativa (ou equivalente, caso exista) a que o titular do certificado pertence.
Common Name	CN	É proibida a utilização de "*nicknames*".
		Os equipamentos servidores são designados pelo FQDN (CN = "FQDN"), sendo proibida a sua designação através do endereço IP.
		Os nomes reais correspondem com o nome completo, conforme documento de Identificação.

3.1.2 Necessidade de nomes significativos

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

A ER da ECCE deve garantir que a relação entre o titular e a organização a que pertence é a mesma que consta no certificado e é facilmente percetível e identificável pelos Humanos.

3.1.3Anonimato ou pseudónimo de titulares

Não aplicável.

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.

De acordo com o RFC 3280, todos os atributos *DirectoryString* dos campos *issuer* e *subject* do certificado devem ser codificados numa *UTF8String*, com

exceção dos atributos *country* e *serialnumber*, que devem estar codificados numa *PrintableString*.

3.1.5 Unicidade de nomes

O conjunto de nome distinto (*distinguished name*) e o conteúdo da extensão *KeyUsage* deve ser único e não ambíguo. O Administrador de Registo da ECCE é encarregado de verificar o cumprimento desta norma, suportando-se no sistema de informação de suporte à emissão de certificados (o FORCe) para a atribuição e garantia de unicidade de nomes.

3.1.6 Reconhecimento, autenticação e funções das marcas registadas

AS entidades requisitantes de certificados, devem demonstrar que têm direito à utilização do nome requisitado, não podendo as designações usadas nos certificados emitidos pela ECCE infringir os direitos de propriedade intelectual de outros indivíduos ou entidades

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

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 4210 atualizado pelo RFC 6712.

Para os certificados emitidos pela ECCE, 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, de acordo com o CMP.

3.2.2 Autenticação da identidade de uma pessoa coletiva

O processo de autenticação da identidade de uma pessoa coletiva utilizado pelas EC e ER deve obrigatoriamente garantir que a pessoa coletiva é quem na realidade diz ser.As EC e ER devem guardar toda a documentação utilizada para

verificação da identidade do indivíduo.A ECCE verifica a identidade dos representantes legais de uma entidade requisitante, 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:

- Denominação legal;
- Número de pessoa coletiva;
- 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;
- 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.

3.2.3 Autenticação da identidade de uma pessoa singular

A ER da ECCE guarda toda a documentação utilizada para verificação da identidade do indivíduo. Todas a informação recolhida em formulário próprio para o efeito é validada pelos Administradores de Registo, com base na documentação requerida.

A informação obrigatória para aceitação de um pedido de emissão de certificados, contém, entre outros, os seguintes elementos:

- Nome completo, número do Cartão de Cidadão/Bilhete de Identidade, passaporte ou outro documento de identificação que permita a identificação inequívoca das pessoas singulares que estatutária ou legalmente a representam;
- Endereço, telefone e correio eletrónico;
- Eventual referência a uma qualidade específica, em função da utilização a que o certificado estiver destinado;
- Cargo ou função devidamente comprovada por Despacho de Nomeação ou delagação de competências;
- Nome Organismo do Titular;

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

3.2.4 Informação de subscritor/titular não verificada

De acordo com a PCert do SCEE (Ponto 3.2.4).

3.2.5 Validação dos poderes de autoridade ou representação

A autenticação das autorizações é uma parte formal do pedido de registo de certificado para entidades com personalidade jurídica.Um certificado emitido é uma confirmação de que uma entidade legal é intitulada para utilizar uma chave privada em nome de outra entidade legal. A validação dos poderes de autoridade ou representação é efetuada com base na documentação exigida para o efeito (Despacho de Nomeação ou delegação de competências).

3.2.6 Critérios para interoperabilidade

De acordo com a PCert do SCEE (Ponto 3.2.5).

3.2.7 Critérios para a filiação

De acordo com a PCert do SCEE (Ponto 3.2.6).

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 podem realizar-se utilizado os procedimentos para a autenticação e identificação inicial. Adicionalmente, é validada a existência de certificado previamente emitido (expirado ou a expirar em breve) para o titular em causa.

3.3.2 Identificação e autenticação para renovação de chaves, após revogação

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

A renovação não deve ser concedida quando:

- A revogação ocorreu porque o certificado foi emitido para uma pessoa que não a que está no Subject do certificado;
- Se o certificado foi emitido 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 são as mesmas que para o registo inicial (ver Pontos 3.2.2 e 3.2.3 desta DPC). Os dados de identificação do titular fornecidos com o pedido de revogação são verificados por comparação com os dados que foram registados em base de dados aquando da emissão do(s) certificados(s).

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

4. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

As especificações contidas neste capítulo aplicam-se aos diversos tipos de certificados emitidos pela ECCE.

4.1 PEDIDO DE CERTIFICADO

4.1.1 Quem pode subscrever um pedido de certificado

O pedido de certificados pode ser feito por três tipos de utilizadores:

- Membros do Governo e colaboradores dos seus Gabinetes (mediante autorização do Chefe do Gabinete) que integram a ***Rede Informática do Governo*** (RInG): Entende-se que o pedido se efetua automaticamente pelo simples facto deste utilizador pertencer à RInG. O utilizador da RInG deve dirigir-se ao ponto de registo para que seja identificado e desta forma se possa proceder à emissão dos certificados;

- Utilizadores do Procedimento Legislativo: O utilizador do Procedimento Legislativo deve dirigir-se ao ponto de registo para que seja identificado e desta forma se possa proceder à emissão dos certificados;
- Outros utilizadores do Estado Português: qualquer organização que pretenda certificados digitais e que não tenha condições de constituir-se como Entidade Certificadora, ou que pelo seu tamanho tal não se adeque, poderá solicitar certificados à ECCE. O utilizador deve dirigir-se ao ponto de registo para que seja identificado e desta forma se possa proceder à emissão dos certificados;
- Titulares de Cargos de Direção superior de 1º e 2º nível dos Organismos da Adminisrtração Pública;
- Presidentes e membros dos conselhos de Administração de institutos públicos ou equiparados;
- Funcionários, agentes ou trabalhadores do Estado, cujas funções determinem a utilização da autenticação e da assinatura eletrónica qualificada ou quando tal resulte de atribuição legal;
- Funcionários, agentes ou trabalhadores do Estado que, não sendo dirigentes, tenham por função enviar atos para a Imprensa Nacional Casa da Moeda;
- Funcionários, agentes do Estado que no âmbito de projetos específicos de desmaterialização de procedimentos, careçam de certificados digitais.

O pedido de certificados não implica a sua obtenção se o solicitante não cumprir os requisitos estabelecidos nesta DPC e na PCErty do SCEE. A ER poderá reclamar do solicitante documentação 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, mediante preenchimento de formulário existente para o efeito, em função do tipo de certificado (ver Anexo B);

- Assinatura por parte do requisitante de um documento onde esteja especificado os termos e condições aplicáveis à utilização do(s) certificado(s).
- Obtenção por parte do requisitante, do respectivo par de chaves, por cada certificado requisitado;

É atribuição da ER da ECCE, local ou remota, determinar a adequação do tipo de certificado e as características das funções do solicitante, de acordo com o previsto na PCert do SCEE aplicada a cada caso. A ER poderá autorizar ou negar o pedido de certificação.

Os pedidos de certificados, uma vez completos, serão enviados à ECCE.

Como regra geral, todo o pedido de um certificado digital deverá:

- Proporcionar toda a informação que a ECCE requeira para esse fim. Cabe destacar que nem toda a informação aparecerá no certificado e que esta será conservada, de forma confidencial pela ECCE, de acordo com a normativa vigente em matéria de Proteção de Dados Pessoais;
- Entregar o pedido de certificado, que inclui a chave pública à Entidade de Registo, no caso em que o par de chaves tenha sido gerado pelo solicitante do pedido e o certificado se gere diretamente a partir do pedido.

O pedido do certificado não implica a sua obtenção, principalmente se o solicitante não cumprir os requisitos estabelecidos na DPC e na PCert.

4.2 PROCESSAMENTO DO PEDIDO DE CERTIFICADO

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

- Receção e verificação de toda a documentação e autorizações exigidas, nomeadamente:
  a) Verificação da identidade do requisitante;
  b) Verificação da exatidão e integridade do pedido de certificado;
- Criação e assinatura do certificado;
- Disponibilização do certificado ao titular.

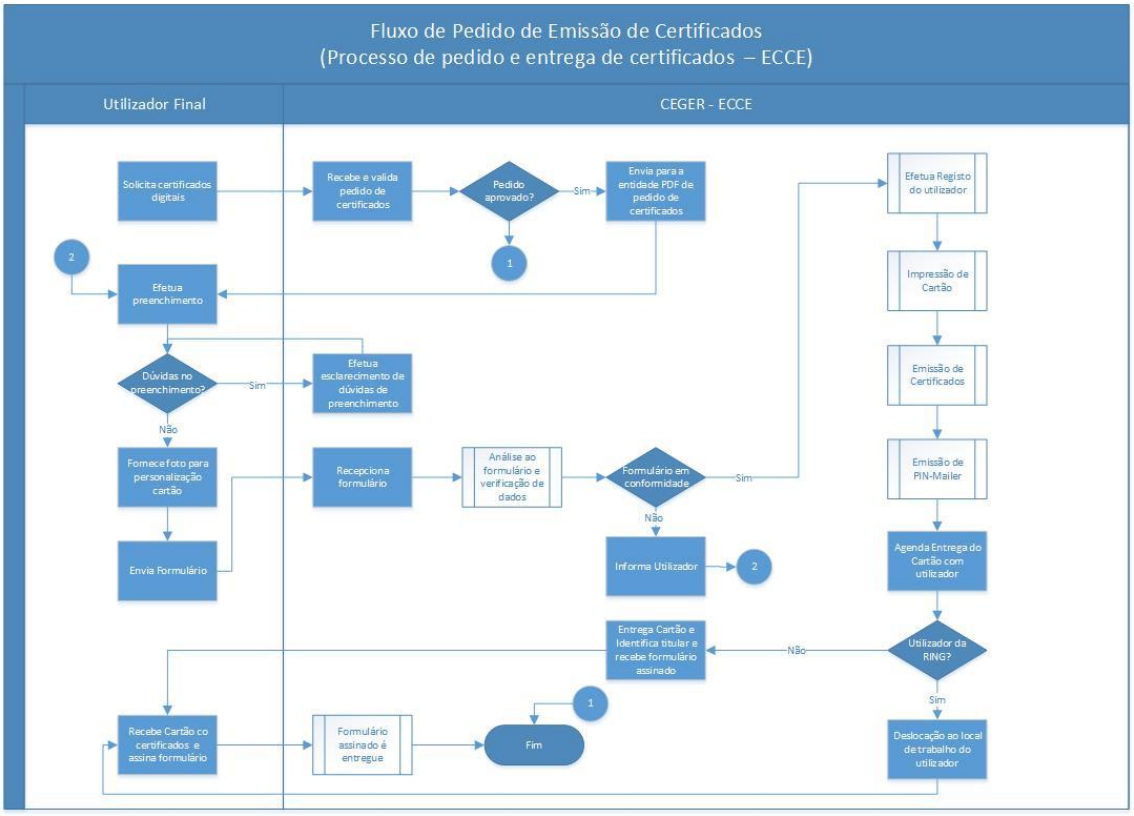

Figura 2 – Fluxo de Pedido de Emissão de Certificados.

4.2.1 Processos para a identificação e funções de autenticação

Conforme o estipulado na secção 3.2 deste documento.

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

- Solicitação assinada eletronicamente: o administrador de registo verifica a validade da assinatura e se o assinante está capacitado para realizar o pedido;
- Solicitação assinada em papel: o administrador de registo verifica a assinatura manuscrita e, caso não conheça o solicitante, é requerida a sua documentação de identificação.

Os pedidos são efetuados mediante formulário existente por tipo de certificado.

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 desta DPC. Quando tal não se verifique, a ECCE pode recusar a emissão do certificado.

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

A ECCE pode negar-se a emitir um certificado de qualquer solicitante baseando-se exclusivamente nos seus próprios critérios, sem que isso implique contrair responsabilidade alguma pelas consequências que possam derivar 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.

Sempre que possível, a ECCE processará as petições em menos de 24 horas úteis, 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 da ECEE é iniciada quando todos os procedimentos de validação da informação requerida foram concluídos sucesso.

Os procedimentos estabelecidos nesta secção também se aplicam no caso darenovação de certificados, já que na ECCE a renovação de certificados implica a emissão de novos.

A emissão dos certificados da ECCE:

- 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 registo.

O processo de emissão do certificado na CA está automatizado e é assegurado pelo sistema aplicacional FORCe.

Quando a ER da ECCE emite um certificado de acordo com um pedido, efetuará as notificações estabelecidas no ponto 4.3.2 do presente capítulo.

Todos os certificados iniciam a sua vigência no momento da sua emissão. O período de vigência está sujeito a uma possível extinção antecipada, temporal

ou definitiva, quando se expliquem as causas que motivem a suspensão e/ou revogação do certificado.

4.3.2 Notificação da emissão do certificado ao titular

A notificação é efetuada através de correio eletrónico destinado ao titular do certificado.

4.4 ACEITAÇÃO DO CERTIFICADO

4.4.1 Procedimentos para a aceitação de certificado

Para certificados de assinatura, autenticação e cifra, os titulares leêm e assinam o termo de responsabilidade por ocasião da entrega dos certificados, em formulário próprio para o efeito (ver Anexo B).

No caso dos certificados de servidor e de code signing, a ceitação dos termos de utilização e termo de responsabilidade é efetuado por ocisião do pedido de certificado em formulário próprio para o efeito (Anexo B).

4.4.2 Publicação do certificado

Não é efetuada a publicação de certificados emitidos.

4.4.3 Notificação da emissão de certificado a outras entidades

Não aplicável.

4.5 USO DO CERTIFICADO E PAR DE CHAVES

De acordo com a PCert do SCEE (Ponto 4.5).

4.5.1 Uso do certificado e da chave privada pelo titular

O titular só pode utilizar a chave privada e o certificado para os fins 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 uso estabelecidas nesta DPC (Pontos 1.4.1 e 1.4.2) e só para os fins que estas estabeleçam.

Depois da extinção da vigência ou a revogação do certificado, o titular deverá deixar de usar a chave privada associada.Os certificados emitidos pela ECCE só podem ser utilizados com os seguintes propósitos:

- **Certificado de Autenticação**: autenticação perante os sistemas de informação das respectivas entidades que exijam a comprovação da identidade do titular mediante certificado eletrónico;
- **Certificado de Assinatura**: assinatura eletrónica de e-mail, arquivos e transações informáticas aos que se queira dotar de controlo de identidade do assinante, controlo de integridade e não repúdio;
- **Certificado de Confidencialidade**: cifra de e-mail, cifra de arquivos e cifra de transações;
- **Certificados de Equipamentos e Servidores**;
- **Certificados para Assinatura de Código**.

4.5.2 Uso do certificado e da chave pública pelos correspondentes

De acordo com a PCert do SCEE (Ponto 4.5.2).

4.6 RENOVAÇÃO DE CERTIFICADOS

Esta Prática não é suportada pelo SCEE., logo, em consequência, não se aplicam os pontos 4.6.1 a 4.6.6.

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 gera um novo par de chaves e submete o pedido para emissão de novo certificado que irá certificar 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 pode ser renovado pelos seguintes motivos:

1. Fim do período de validade;
2. Mudança de dados contidos no certificado;
3. Chaves comprometidas ou perda de fiabilidade das mesmas;
4. Alteração de formato.

Todas as renovações de certificados no âmbito desta DPC serão realizadas com mudança de chaves.

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

A renovação deverá ser solicitada respectivamente pelo titular do certificado ou pelo responsável de um componente ou servidor.

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

A renovação de um certificado na ECCE corresponde à emissão de um novo par de chaves. Assim sendo, o titular submete um pedido de renovação preenchendo novamente o formulário existente para o efeito (ver Anexo B), como um novo pedido. As regras para validação da informação são as dispostas nos Pontos 3.2.2 e 3.2.3.

A ER da ECCE valida toda a informação submetida (nos termos do Ponto 3.2.2.) e procede a eventuais alterações no registo do titular.

Dado se tratar de um processo de renovação, é em seguida validado e verificado o *status* do certificado anteriormente emitido para aquele titular. Caso o certificado anteriormente emitido esteja válido, o mesmo será revogado antes da emissão do novo certificado.

A emissão do certificado seguirá o disposto no ponto 4.3.

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

- Que se solicite em devido tempo e forma, seguindo as instruções e normas que a ECCE especifica para tal efeito;
- Que a ECCE não tenha tido conhecimento certo da ocorrência de nenhuma causa de revogação / suspensão do certificado;
- Que a solicitação de renovação dos serviços de prestação se refira ao mesmo tipo de certificado emitido inicialmente.

4.7.4 Notificação da emissão de novo certificado ao titular

A notificação ao titular é efetuada através de correio eletrónico. A mensagem enviada é constituída pela seguinte informação:

- Disponibilidade dos certificados para levantamento;
- Local e horário para o levantamento dos certificados;
- Indicação e *link* para download dos certificados da cadeia de certificação (site da ECCE);
- Indicação e *link* para download do Middleware para manipulação do *smartcard* (site da ECCE).

4.7.5 Procedimentos para aceitação de um certificado renovadocom geração de novo par de chaves

Aplicam-se os mesmos critérios que para a emissão inicial (ver Ponto 4.4.1desta DPC).

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 (ver Ponto 4.4.2 desta DPC).

4.7.7 Notificação da emissão de novo certificado a outras entidades

Aplicam-se os mesmos critérios que para a emissão inicial (ver Ponto 4.4.3 desta DPC).

4.8 ALTERAÇÃO DE CERTIFICADO

Este processo não é suportado pela ECCE. Sempre que for requerida uma modificação no certificado, deverá ser efetuado um pedido de certificado em conformidade com o disposto no ponto 4.1.

Em consequência não são aplicados os pontos 4.8.1 a 4.8.7.

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 de Certificados são mecanismos a utilizar no pressuposto que, por alguma causa estabelecida na PCert ou nesta DPC, se deixe de confiar nos referidos certificados antes da finalização do período de validade originalmente previsto.

A revogação de um certificado é o ato pelo qual se torna sem efeito a validade de um certificado, antes de sua data de caducidade. O efeito da revogação de um certificado é a perda de validade do mesmo, originando a cessação permanente de sua operatividade conforme aos usos que lhe são próprios. Em consequência, a revogação de um certificado desabilita a utilização legítima do mesmo por parte do titular.No caso de uma suspensão, a validade do certificado pode ser recuperada, sendo restituída ao titular a capacidade da normal utilização do mesmo.

4.9.1 Motivos para a revogação

Um certificado emitido pela ECCE pode ser revogado por devido a:

- Roubo, perda, revelação, modificação, ou outro compromisso ou suspeita de compromisso da chave privada do titular;
- Utilização indevida ou deliberada de chaves e certificados, ou a falta de observância ou contravenção dos requisitos operacionais expressos no documento de Aceitação das condições de utilização dos certificados pessoais, na PCert;
- Ordem expressa do titular.
- O titular de um certificado deixar de ter relação com uma entidade através da qual obteve o seu certificado;

- Cessação da atividade da ECCE;
- Emissão defeituosa de um certificado porque:
    1. Não se cumpriu um requisito material para a emissão do certificado;
    2. Existe uma convicção razoável que um dado fundamental relativo ao certificado é ou pode ser falso;
    3. Se verificou a existência de um erro de entrada de dados ou outro erro de processo.
    4. O par de chaves gerado por um titular se revela como "débil" ou "fraco".
    5. Não é exata a informação contida num certificado ou a informação utilizada para realizar sua solicitação.
    6. Foi dada ordem – pelo titular (ou por terceiro autorizado) ou pessoa física solicitante, em representação de uma pessoa jurídica;
    7. É revogcado o certificado da ECEE (superior na hierarquia de confiança do certificado);
    8. Pela ocorrência de qualquer outra causa especificada na presente DPC ou nas correspondentes Políticas de Certificado estabelecidas para cada tipo de Certificado.

Podem ainda ser revogados os certificados dos titulares que exerçam funções na RING sempre que:

1. Outilizador deixar de exercer funções no Gabinete Governamental;
2. O utilizador deixar de exercer o cargo para o qual foram emitidos os certificados digitais;
3. O utilizador deixar de ter uma conta ativa na Rede do Governo;
4. O Chefe de Gabinete respetivo der instruções para que sejam revogados os certificados emitidos para o titular;
5. Por decisão do CEGER – ECCE, resultante da violação do acordo de Subscrição e das Práticas de Certificação;
6. Por decisão da direção do CEGER, face a – práticas indevidas na utilização do cartão criptográfico na RInG.

Podem também ser revogados os certificados de dirigentes ou funcionários da Administração Pública sempre que:

1. O titular deixe de exercer o cargo para o qual foram emitidos os certificados digitais;
2. Por decisão da Direção expressa do Organismo responsável pelo titular;
3. Por decisão daECCE, quando comprovadaa violação do Acordo de Subscrição e/ou das Práticas de Certificação;

Podem também ser revogados os certificados de intervenientes no procedimento legislativo eletrónico sempre que:

1. O titular deixe de exercer o cargo para o qual foram emitidos os certificados digitais;
2. O responsável máximo do órgão de soberania der instruções para que sejam revogados os certificados emitidos para o titular;
3. Por decisão da ECCE, quando comprovada a violação do Acordo de Subscrição e/ou das Práticas de Certificação.

A revogação tem como principal efeito sobre o certificado o fim imediato e antecipado do seu período de validade, originado um certificado como não válido. A revogação não afetará as obrigações subjacentes criadas ou comunicadas por esta DPC nem terá efeitos retroativos.

4.9.2 Quem pode submeter o pedido de revogação

Está autorizado a solicitar a revogação de um certificado:

- O seu titular, quando ocorra qualquer uma das circunstâncias expostas no ponto 4.9.1 deste DPC;
- A pessoa ou organização que fez o pedido do certificado, em nome de uma organização, dispositivo ou aplicação;
- Uma terceira parte, quando tenha a noção que um certificado foi utilizado com fins fraudulentos e ilícitos;
- A própria ECCE, sempre que tenha conhecimento de qualquer das circunstâncias expostas no ponto 4.9.1 deste DPC.

4.9.3 Procedimento para pedido de revogação

A solicitação de revogação deverá ser assinada eletronicamente ou de forma manuscrita, sendo que neste último caso se deverá identificar previamente o solicitante. A solicitação deve ser dirigida à ECCE e no pedido deverão constar:

- A identificação do solicitante;
- As causas do pedido.

São admitidos dois tipos de pedido de revogação:

- **Remotos**: Devem estar assinados eletronicamente com um certificado qualificado;
- **Presenciais**: Devem cumprir-se os requisitos de identificação estabelecidos para o registo inicial:

- O pedido de revogação será processado por um operador da ECCE:
- Será comunicado ao titular do certificado a revogação do mesmo através de correio eletrónico;
- Após a revogação do certificado o titular do mesmo deverá cessar o uso da sua chave privada correspondente ao certificado revogado;
- A revogação de um certificado de autenticação comporta a revogação do resto de certificados associados a um titular.
- A solicitação de revogação de um certificado recebida posteriormente a sua data de caducidade não será atendida.

4.9.4 Produção de efeitos da revogação

A revogação será feita de forma imediata, após terem sido efetuados todos os procedimentos de verificaçãoda validade do pedido conforme procedimento detalhado no Ponto 4.9.3.

4.9.5 Prazo para processar o pedido de revogação

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

4.9.6 Requisitos de verificação da revogação pelos correspondentes/destinatários

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

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

A ECCE publicará uma nova LCR no seu repositório no momento em que se produza qualquer revogação ou suspensão de certificados e em último caso, em intervalos não superiores a 24 horas (mesmo que não existam modificações).

4.9.8 Período máximo entre a emissão e a publicação da LCR

Conforme o estipulado no ponto 4.9.7desta DPC.

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

A ECCE proporciona um servidor web onde publica as LCR para a verificação do estado dos certificados que emite. Existe atualmente uma Autoridade de Validação que, mediante o protocolo OCSP, permite verificar o estado dos certificados. Os endereços de acesso via web às LCR estão referenciadas no ponto 2.1.

4.9.10 Requisitos de verificação *on-line* de revogação

As partes confiantes deverão dispor de *software* capaz de operar o protocolo OCSP de forma a obter informação acerca do estado do certificado.

4.9.11 Outras formas disponíveis para divulgação de revogação

Não aplicável.

4.9.12 Requisitos especiais em caso de comprometimento de chave privada

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

4.9.13 Motivos para suspensão

A suspensão da vigência dos certificados aplicar-se-á aos certificados pessoais, entre outros, nos seguintes casos:

- Mudança temporária de alguma das circunstâncias do titular do certificado que aconselhem a suspensão dos certificados durante o período de mudança. Ao retornar-se à situação inicial será levantada a suspensão do certificado;
- Comunicação pelo titular do certificado de um possível comprometimento das suas chaves. No caso em que a suspeita, pelo seu grau de certeza, não aconselhe a revogação imediata, serão suspensos os certificados do titular enquanto se averigua o possível compromisso

das chaves. A análise determinará uma possível revogação dos certificados ou então o levantamentoda sua suspensão.

- Resolução judicial ou administrativa que assim o determine.

4.9.14 Quem pode submeter o pedido de suspensão

O pedido pode ser feito pelo titular do certificado ou pela pessoa com poderes de representação legal.

4.9.15 Procedimentos para pedido de suspensão

A Figura 3 descreve em detalhe o processo de suspensão de certificados.

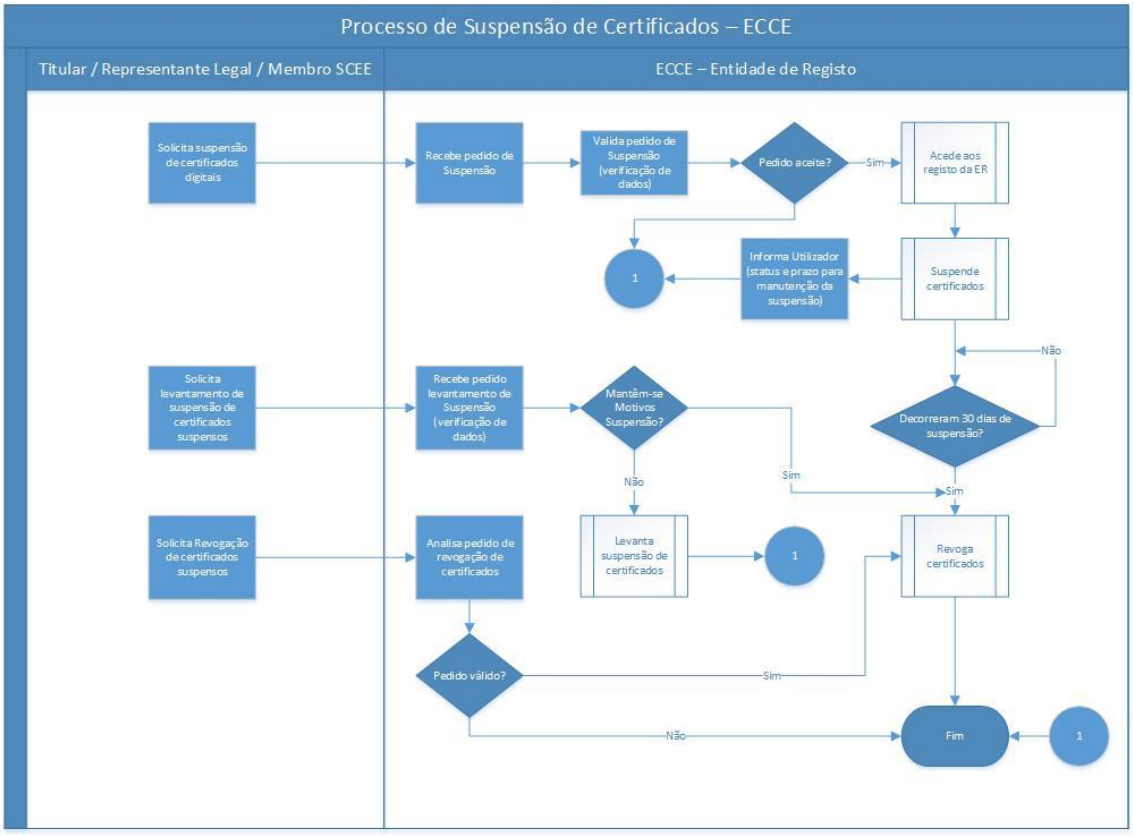

Figura 3 – Processo de Pedido de Suspensão de Certificados.

4.9.16 Limite do período de suspensão

Sem prejuízo do definido na respetiva PCert, a ECCE suspenderá a vigência dos certificados por um período máximo de 30 dias, prazo findo o qual se revogará o certificado.

Se durante o tempo de suspensão do certificado este caduca ou é solicitada a sua revogação, seguem-se os procedimentos utilizados relativamente aos certificados não suspensos nos casos de caducidade e revogação.

4.10 SERVIÇOS SOBRE O ESTADO DO CERTIFICADO

4.10.1 Características operacionais

Não aplicável.

4.10.2 Disponibilidade de serviço

Não aplicável.

4.10.3 Características opcionais

Não aplicável.

4.11 FIM DE SUBSCRIÇÃO

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

- Revogação do certificado por qualquer das causas descritas no ponto 4.9.1desta DPC;
- 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 aplicável.

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

Não aplicável.

5. MEDIDAS DE SEGURANÇA FÍSICA, DE GESTÃO E OPERACIONAIS

5.1 MEDIDAS DE SEGURANÇA FÍSICA

Todos os aspectos relacionados com as medidas de segurança física exigidas às instalações onde operam a ECCE, estão definidos no documento "***Normas de Acesso, Funcionamento de Segurança das instalações da ECCE***". Nesta secção apenas são descritos os aspectos mais relevantes.

5.1.1 Localização física e tipo de construção

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

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

- Uma zona de receção onde os visitantes se identificam e são reconhecidos com tal;
- Uma zona de operações onde o acesso é restrito e é feito através da receção;
- Uma zona de segurança, onde serão registados todos os acessos à zona de operações;
- Uma zona de alta segurança onde está instalada tecnologia biometria para controlo do acesso à EC.

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

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

5.1.2 Acesso físico ao local

O Centro de Dados da ECCE 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 deteção de intrusões, entre outros.

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

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

O acesso a esta ZAS é sempre feito através de sistemas de controlo- de acessos, sendo que qualquer acesso considerado *visita* é devidamente registado no "livro-diário" onde são registados todos os acessos e todo o tipo de atividades que ocorram nesta zona.

5.1.3 Energia e ar condicionado

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

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

5.1.4 Exposição à água

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

5.1.5 Prevenção e proteção contra incêndio

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

Os materiais da sala e portas utilizados são de natureza 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 informação, 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

A eliminação de suportes magnéticos e informação em papel é realizado de forma segura, sendo utilizados equipamentos desmagnetizadores para os suportes magnéticos e destruidores de papel (corte cruzado) para a informação em papel. 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 ao pessoal autorizado. O local 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 ECCE, 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 ECCE e que podem materialmente afetar a:

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

As funções de confiança incluem:

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

5.2.1.1 ADMINISTRADOR DE SISTEMAS

O Administrador de Sistemas:

- É o responsável pela instalação e configuração de sistemas operativos e outros produtos de *software* e pela manutenção e atualização dos produtos instalados;
- Garante a prestação do serviço com o adequado nível de qualidades e fiabilidade em função do grau de criticidade do mesmo;
- Colabora com os auditores em tudo aquilo que lhe for solicitado;
- Não tem acesso a aspetos 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

O Operador de Sistemas:

- É o responsável pela operação regular dos sistemas;
- Garante a correta execução da política de cópias de segurança e, em particular, de as manter atualizadas, permitindo a recuperação eficiente de qualquer um dos sistemas;

Esta função é acumulada pelo Administrador de Sistemas.

5.2.1.3 ADMINISTRADOR DE SEGURANÇA

O Administrador de Segurança:

- É o responsável pela gestão e implementação das regras e práticas de segurança;
- Faz cumprir as políticas de segurança da SCEE e encarrega-se de qualquer aspeto relativo à segurança (física, das aplicações, da rede, etc…);

- Gere os sistemas de proteção perimétrica;
- Resolve todos os incidentes de segurança e elimina todas as vulnerabilidades detectadas;
- Efetua a gestão e controlo dos sistemas de segurança física da sala de operações da EC e de todos os controlos de acesso, dos sistemas de acondicionamento ambiental e de alimentação elétrica;
- Explica todos os mecanismos de segurança aos funcionários que devam conhecê-los e de os sensibilizar para as questões de segurança, tendo em vista o cumprimento das normas e políticas de segurança estabelecidas;
- Estabelece os calendários para a execução de análises de vulnerabilidades, testes e treino, bem como dos planos de continuidade de serviço e auditoria dos sistemas de informação;
- Colabora com os Auditores em tudo aquilo que lhe for solicitado.

5.2.1.4 ADMINISTRADOR DE REGISTO

O Administrador de Registo:

- É 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

O Auditor de Sistemas corresponde a um perfil de auditor interno, sem prejuízo de existir pessoal externo responsável pelas auditorias.

O Auditor de Sistemas é responsável por verificar:

- A existência de toda a documentação necessária e devidamente numerada;
- A coerência da documentação e dos procedimentos;
- Os procedimentos de incidentes e eventos;
- E analisar a proteção dos sistemas (exposição a vulnerabilidades, logs de acesso, utilizadores, etc…);
- A existência e funcionamento dos alarmes e elementos de segurança física;
- A adequação com a legislação em vigor;
- O conhecimento dos procedimentos por parte do pessoal implicado;
- E comprovar todos os aspetos reconhecidos na política de segurança, políticas de cópias de segurança, práticas de certificação e de políticas de certificação.

5.2.1.6 ADMINISTRADORES DE HSM (MÓDULO DE SEGURANÇA EM *HARDWARE*)

Define-se um conjunto de 7 Administradores para o HSM da ECCE, cada um com um cartão criptográfico de controlo de acesso às suas funções. Para a realização das operações que requeiram um papel de administrador será necessário introduzir no leitor do HSM um total de 2 cartões dos 7 atribuídos. Os Administradores de HSM são responsáveis por realizar as seguintes operações:

- Recuperação da funcionalidade do *hardware* criptográfico em caso de falha de um HSM;
- Recuperação de chaves em caso de terem sido apagadas acidentalmente;
- Substituição de um conjunto de cartões de administrador. Esta operação só é necessária se for necessário ampliar ou reduzir o número de cartões de administrador;
- Substituição de um conjunto de cartões de operador. Esta operação só é necessária se for necessário ampliar, reduzir o número de cartões de operador ou substituir algum cartão deteriorado;
- Ampliação do número de HSMs integrados na infraestrutura;
- Autorização para a geração de conjuntos de cartões de operador e chaves, dado que se opera em modo FIPS140-2 Nível 3. Esta operação só é necessária durante a cerimónia de geração de chaves para a EC.

5.2.1.7 OPERADORES DE HSM

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

- Ativação de chaves para sua utilização. Isto significa que de cada vez que se inicie a EC será necessária a inserção dos cartões dos operadores associados às chaves;
- Autorização para a geração de chaves da aplicação. Esta operação é requerida durante a cerimónia 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. Os administradores têm de intervir sempre que seja necessário voltar a configurar a EC ou voltar a arrancar um dos processos envolvidos na EC da ECCE.

5.2.2 Número de pessoas exigidas por tarefa

A ECCE 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 seja sempre requerida a participação de um mínimo de duas pessoas para todas as atividades relacionadas com o ciclo de vida das chaves da 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.

Os restantes utilizadores da ECCE são identificados mediante certificados eletrónicos, emitidos pela própria infraestrutura da ECCE, sendo autenticados através de cartões criptográficos.

A autenticação complementa-se com as correspondentes autorizações para o acesso a determinados recursos de informação dos sistemas da ECCE.

5.2.4Funções que requerem separação de responsabilidades

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

- Incompatibilidade entre a função de **Auditor** (i.e. Auditor de Sistema) e **qualquer outra função**;
- Incompatibilidade entre as funções de **administrador** (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 ECCE:

- Possui qualificações e experiência na prestação de serviços de certificação;

- Cumpre os requisitos de segurança da organização
- É devidamente credenciado pela Autoridade Nacional de Segurança, para manuseamento de matéria secreta;
- Formação básica sobre segurança em sistemas de informação;
- Formação específica para a sua função de confiança.

5.3.2 Procedimentos de verificação de antecedentes

Os antecedentes de cada elemento são comprovados através do processo de credenciação pela Autoridade Nacional de Segurança.

5.3.3 Requisitos de formação e treino

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

Este plano inclui os seguintes aspetos:

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

5.3.4 Frequência e requisitos para ações de reciclagem

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

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

5.3.5 Frequência e sequência da rotação de funções

Não está definido nenhum plano de rotação na atribuição de tarefas ao pessoal da ECCE.

5.3.6 Sanções para ações não autorizadas

No caso da realização de ações não autorizadas respeitantes à ECCE, deverão ser tomadas as medidas disciplinares adequadas.

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

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

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

5.3.7 Requisitos para a contratação de pessoal

Todo o pessoal da ECCE 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 conforme a DPC e a Políticas de Segurança da Informação.

A ECCE 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 a ECCE serão disponibilizados os seguintes documentos:

- Declaração de Práticas de Certificação;
- Políticas de Certificação;
- Políticas de Certificado;
- Políticas de Privacidade;
- Política de Segurança da Informação;
- Organigrama e funções do pessoal.

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

5.4 PROCEDIMENTOS DE AUDITORIA DE SEGURANÇA

5.4.1 Tipo de eventos registados

A ECCE 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 início 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 LCR;
- 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;
- Cópias de segurança, recuperação ou arquivo dos dados;
- Alterações ou atualizações de *software* e *hardware*;
- A manutenção do sistema;
- A mudança de pessoal;
- A cerimónia de geração de chaves e as bases de dados de gestão de chaves.

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

Categoria: Indica a importância do evento;

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

Data: Data e hora em que ocorreu o evento;

Autor: Nome único da Entidade que gerou o evento;

Função: Tipo de Entidade que gerou o evento;

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

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

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

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

5.4.2 Frequência da auditoria de registos

Os registos são analisados seguindo procedimentos manuais e automáticos quando seja necessário. Deste modo, definem-se dois níveis de auditorias de controlo e dos eventos com uma frequência semanal.

5.4.3 Período de retenção dos registos de auditoria

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

5.4.4 Proteção dos registos de auditoria

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

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

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 da ECCE.

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

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

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

Todos os elementos significativos existentes na ECCE são registados numa base de dados. Os Procedimentos de Controlo de Segurança empregues baseiam-se na tecnologia de construção das bases de dados.As características deste sistema são as seguintes:

- Permite verificar a integridade da base de dados, detectando uma possível manipulação fraudulenta dos dados;
- Assegura o não repúdio por parte dos autores das operações realizadas sobre os dados. Isto consegue-se através de assinaturas electrónicas;
- Guarda um registo histórico de atualização dos dados, armazenando versões sucessivas de cada registro resultante de diferentes operações realizadas sobre ele. É assim possível guardar um registo das operações realizadas, evitando que se percam assinaturas eletrónicas realizadas anteriormente por outros utilizadores na atualização dos dados.

Os possíveis perigos a que uma base de dados pode estar exposta e que podem detectar-se com as provas de integridade são:

- Inserção ou alteração fraudulenta de um registro de sessão;
- Supressão fraudulenta de sessões intermédias;
- 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

Serão realizadas, pelo menos anualmente, uma análise de vulnerabilidades e uma de segurança perimétrica.

O resultado das análises é reportado ao responsável da ECCE para revisão e aprovação de um plano de implementação e correção das vulnerabilidades detetadas.

5.5 ARQUIVO DE REGISTOS

5.5.1 Tipo de dados arquivados

As informações e eventos que são registados são:

1. Os registos de auditoria especificados no ponto 5.4 desta DPC;
2. Os suportes de salvaguarda de informação dos servidores que compõem a infraestrutura da ECCE;
3. Documentação relativa ao ciclo de vida dos certificados:
   a) Contrato/Acordo de Certificação;
   b) Cópia da documentação de identificação facultada pelo requerente do certificado;
   c) Identidade do operador que emitiu o Certificado;
   d) Data da última identificação direta do titular.
4. Acordos de confidencialidade;
5. Autorizações de acesso aos sistemas de informação.

5.5.2 Período de retenção em arquivo

Toda a informação e documentação relativas ao ciclo de vida dos certificados emitidos pela ECCE são conservadas por um período de 20 anos.

5.5.3 Proteção dos arquivos

O Acessos aos arquivos é restrito a pessoal autorizado.

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

5.5.4 Procedimentos para as cópias de segurança do arquivo

Serão 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 ECCE. Uma outra cópia é realizada de forma cifrada e será armazenada num cofre anti-fogo na SalaSegura Alternativa (local).

5.5.5 Requisitos para validação cronológica dos registos

Os sistemas de informação da ECCE garantem o registro do tempo nos quais se realizam. O instante de tempo dos sistemas provém de uma fonte segura que constata a data e hora. Os servidores dos sistemas da ECCE estão sincronizados em data e hora. As fontes de tempos utilizadas, baseadas no protocolo NTP (*Network Time Protocol*) são utilizadas com 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 ECCE.

5.5.7 Procedimentos de recuperação e verificação de informação arquivada

Apenas o pessoal devidamente autorizado tem acesso aos arquivos físicos de suporte (*media*) e arquivo informáticos para levar a cabo ações de verificação de integridade e outras.

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

5.6 RENOVAÇÃO DE CHAVES

Não Aplicável. A renovaçã de chaves consiste na emissão de novo par de chaves conforme descrito nas seções 4.1 e 4.2.

5.7 RECUPERAÇÃO EM CASO DE DESASTRE OU COMPROMETIMENTO

O Plano de Continuidade da ECCE é ativado em caso de uma indisponibilidade máxima de 24 horas, estando preparada para a emissão de LCR 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 ECCE, esta deverá informar todos os titulares de certificados e terceiras 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 dados forem alterados ou se houver suspeita de terem sido alterados, serão parados os serviços da ECCE até ao restabelecimento das condições seguras, com a inclusão de novos componentes de eficácia credível.

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

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

5.7.3 Procedimentos em caso de comprometimento da chave privada da entidade

No caso de comprometimento da chave privada de uma entidade, deverá proceder-se à sua revogação imediata e informar deste facto as restantes entidades que compõem o SCEE (conforme indicado na Tabela 11 do Ponto 5.7.3 da PCert), dependentes ou não da Entidade afetada.

Os certificados assinados por entidades dependentes da comprometida, no período compreendido entre o compromisso da chave e a revogação do certificado, deverão por sua vez ser revogados e retificados, informando deste facto os seus subscritores.

5.7.4 Capacidade de continuidade da atividade em caso de desastre

Conforme o Plano de Continuidade da ECCE.

5.8 PROCEDIMENTOS EM CASO DE EXTINÇÃO DA ECCE OU ER

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

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

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

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

6. MEDIDAS DE SEGURANÇA TÉCNICAS

6.1 GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES

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

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, sendo o respectivo par de chaves

gerado num módulo criptográfico, de acordo com requisitos definidos no ponto 6.2.1desta DPC. O certificado desta entidade é auto-assinado.

As chaves para os certificados de AC Subordinada (ECCE – Nível 2) emitidos pela ECEE são geradas em módulos de *hardware* criptográficos com validação FIPS 140-2 Nível 3, existentes nos seus sistemas.

As chaves para os certificados de autenticação e confidencialidade (Nível 3) emitidos pela ECCE são gerados em módulos de *hardware* criptográficos com credenciação FIPS 140-2 Nível 3.

As chaves para os certificados de assinatura (Nível 3), emitidos pela ECCE, são geradas no próprio cartão criptográfico do titular, o qual cumpre os requisitos de Dispositivo Seguro de Criação de Assinatura (nível de segurança CC EAL4+ SSCD).

6.1.2 Entrega da chave privada ao titular

As chaves privadas de assinatura, autenticação e confidencialidade são geradas no cartão criptográfico do titular, coincidindo a sua entrega com a do cartão criptográfico.

6.1.3 Entrega da chave pública ao emissor do certificado

A chave pública dos certificados de autenticação e confidencialidade é gerado pela própria ECCE, pelo que não se procede a qualquer entrega.

A chave pública de certificados de assinatura será disponibilizada ao solicitante no processo de obtenção do certificado.

Nos casos em que o par de chaves foi gerado pelo componente ou servidor, a chave pública é disponibilizada através de um ficheiro em formato PKCS#10, que acompanha o pedido.

6.1.4 Entrega da chave pública da ECCE aos orrespondentes/destinatários

A chave pública da ECCE está incluída no seu certificado. O certificado da EC Raiz e da ECCE deverá ser obtido no repositório especificado neste documento onde estaráà disposição dos titulares de certificados e terceiras partes confiantes para realizar qualquer tipo de comprovação.

6.1.5 Dimensão das chaves

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

- Nível 1 (EC Raíz): RSA 4096 bit;
- Nível 2 (EC Subordinada): RSA 2048 bit;
- O Tamanho mínimo para certificados pessoais e certificados de componentes ou servidores é de 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, a geração e verificação deverão ser efetuadas de acordo com o estipulado no PKCS#1 e no RFC 3280.

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

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

Para tal efeito, nos campos "Key Usage" e "Extended Key Usage" do certificado serão incluídos os usos indicados na Tabela 7.

Tabela 7. Usos por Tipo de Certificado.

TIPO DE CERTIFICADO	KEY USAGE	EXTENDED KEY USAGE
Certificado de Autenticação	• Digital Signature. • Key Agreement	• clientAuth. • smartCardLogon
Certificado de Assinatura	• Non Repudiation	• emailProtection
Certificado de Confidencialidade	• Key Encipherment • Data Encipherment	• emailProtection
Certificados de servidor web para uso do protocolo SSL	• digitalSignature • keyEncipherment	• Serverauth
Certificados de Autenticação e Assinatura para componentes	• digitalSignature • keyAgreement	• CodeSigning
Certificado de Controlador de Dominio	• digitalSignature • keyEncipherment	• serverAuth • clientAuth

6.2 PROTEÇÃO DA CHAVE PRIVADA E CARACTERÍSTICAS DO MÓDULO CRIPTOGRÁFICO

6.2.1 Normas e medidas de segurança do módulo criptográfico

Os módulos utilizados para a criação das chaves utilizadas pela ECCE 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* utilizados estão conforme as normas CWA 14167-1 e CWA 14167-2.

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

Todas as operações são efetuadas com um mínimo de 2 pessoas (com funções qualificadas dentro da entidade) por tarefa. Na prática, são envolvidas nas diversas funções, pelo menos 2 pessoas (N=2), entre o conjunto total de pessoas com funções atribuídas dentro da ECCE (M=staff).

A chave privada da ECCE encontra-se sob controlo de mais do que uma pessoa. É ativada mediante a iniciação do *software* da ECCE através de uma combinação de operadores, administradores do HSM e utilizadores de Sistema Operativo. Este é o único método de ativação da chave privada.

6.2.3 Retenção da chave privada (*key escrow*)

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

6.2.4 Cópia de segurança da chave privada

As chaves privadas da ECCE dispõem de uma cópia de segurança realizada pela própria entidade. As cópias de segurança têm o mesmo nível de segurança que a chave original.

6.2.5 Arquivo da chave privada

Todas as chaves que tenham sido alvo de cópias de segurança, são arquivadas por um período mínimo de 20 anos após expiração da sua validade.

6.2.6 Transferência da chave privada para/do módulo criptográfico

A transferência da chave privada da ECCE só se pode fazer entre módulos criptográficos (HSM) e requer a intervenção 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 Certificação que fazem uso dos referidos módulos.

6.2.8 Processo para ativação da chave privada

A chave privada é ser ativada quando o sistema/aplicação da ECCE é ligado ("*startup process*"). Esta ativação só deverá ser efetivada quando previamente tiver sido feita a autenticação no módulo criptográfico pelos operadores nomeados para o efeito,conforme se estipula no ponto 6.2.2.

Para a ativação das chaves privadas da ECCE é necessária, no mínimo, a intervenção dos seguintes perfis da ECCE:

- 2 Operadores de HSM
- 1 Administrador de Sistemas
- 1 Administrador de Segurança

Uma vez a chave ativada, esta permanecerá assim até que o processo de desativação seja executado.

6.2.9 Processo para desativação da chave privada

A chave privada da ECCE é desativada quando o sistema da Entidade Certificadora é desligado.

Para a desativação das chaves privadas da ECCE é necessária, no mínimo, a intervenção dos seguintes perfis da ECCE:

- 2 Operadores de HSM
- 1 Administrador de Sistemas
- 1 Administrador de Segurança

. Uma vez desativada, esta permanecerá inativa até que o processo de ativação seja executado.

6.2.10 Processo para destruição da chave privada

Conforme a Política de Certificação do SCEE (Ponto 6.2.10).

Em termos gerais a destruição deve sempre ser precedida por uma revogação do certificado associado 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 módulo criptográfico** (nas situações renovação de chaves de rotina, a destruição da chave privada antiga é efetuada reescrevendo a nova chave privada do titular);
- **Com formatação do módulo criptográfico (**nas situações em a chave privada deixou de poder ser utilizada, nomeadamente, após expiração ou revogação do certificado).

6.2.11 Avaliação/nível do módulo criptográfico

Conforme o descrito no ponto 6.2.1da presente DPC.

6.3 OUTROS ASPETOS DA GESTÃO DO PAR DE CHAVES

6.3.1 Arquivo da chave pública

A ECCE deverá efetuar o arquivo das suas chaves e das chaves por si emitidas (para efeitos de assinatura digital), permanecendo armazenadas após a expiração dos certificados, conforme os requisitos definidos no ponto 5.5 para verificação de assinaturas geradas durante o seu prazo de validade.

6.3.2 Períodos de validade do certificado e das chaves

O período de utilização das chaves é determinado pelo período de validade do certificado, pelo que, após expiração do mesmo, 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 8 apresenta a validade dos diversos tipos de certificados e período em que os mesmos devem ser renovados. Os valores estão expressos em anos.

Tabela 8. Definição dos Períodos Máximos de Validade dos Certificados.

[Validade dos certificados] – [Período de renovação]					
ECRaizEstado	**ECEstado**	**subECEstado**	**Outras Entidades PKI**	**Titulares**	
				Hardware	***Software***
[24] – [12]	[12] – [6]	[6] – [3]	[3] – [3]	[6] – [6]	[3] – [3]

Os períodos de utilização das chaves são os determinados pela duração do certificado.

6.4 DADOS DE ATIVAÇÃO

6.4.1 Geração e instalação dos dados de ativação

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

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

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

6.4.2 Proteção dos dados de ativação

Apenas os Operadores e Administradores da ECCE possuem os cartões criptográficos com capacidade de ativação da mesma e conhecem os *pins* para aceder aos dados de ativação.

No caso das chaves associadas aos certificados pessoais, só o titular conhece o código pessoal de acesso (ou PIN), sendo portanto o único responsável pela ativação e proteção dos dados de ativação das suas chaves privadas.

6.4.3 Outros aspetos dos dados de ativação

Não aplicável.

6.5 MEDIDAS DE SEGURANÇA INFORMÁTICA

Os dados referentes a esta secção são considerados como informação confidencial e só se proporcionam a quem se reconheça ter a necessidade de os conhecer, como é o caso do pessoal diretamente envolvido em auditorias externas ou internas e inspeções.

A ECCE tem estabelecido os controlos necessários referentes à segurança da informação de acordo com a Politica de Certificados e os *standards* aplicáveis.

6.6 REQUISITOS TÉCNICOS ESPECÍFICOS

Os dados referentes a este ponto são considerados como informação confidencial e só se proporcionam a quem se reconheça ter a necessidade de os conhecer.

AECCE segue as boas práticas estabelecidas na norma ISO 17799:2005 Code of practice for information security management.

6.6.1 Avaliação/nível de segurança

Os vários sistemas e produtos utilizados pela ECCE 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 ECCE, apenas são fornecidos à Autoridade Credenciadora.

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

6.7.1 Medidas de desenvolvimento dos sistemas

Os requisitos de segurança são exigíveis, desde seu início, tanto na aquisição de sistemas informáticos como no desenvolvimento dos mesmos uma vez que poderão ter algum impacto sobre a segurança de ECCE.

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 ECCE, para garantia da sua segurança.

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

A infraestrutura da ECCE é dotada de ambientes de desenvolvimento, pré-produção e produção claramente diferenciados e independentes.

6.7.2 Medidas para a gestão da segurança

A ECCE mantém um inventário de todos os ativos, quer sejam equipamentos, quer sejam dados ou pessoal e classifica-os de acordo com a sua necessidade de proteção. Esta classificação tem também em conta os riscos a que podem estar expostos, efetuando-se uma análise de risco para uma gestão mais eficaz.

As configurações dos sistemas são auditadas de forma periódica tendo em vista a identificação de eventuais necessidades adicionais.

6.7.3 Ciclo de vida das medidas de segurança

As operações de atualização e manutenção dos produtos e sistemas da ECCE seguem o mesmo controlo que o equipamento original, devendo ser instalado pelo pessoal com funções de confiança, com a adequada formaçãoe seguindo os procedimentos definidos para o efeito.

A atualização e manutenção dos produtos e sistemas que compõem os sistemas e ambiente da ECCE serão efetuadas de acordo com as recomendações dos respetivos fabricantes e por pessoal com funções de confiança.

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.

A infraestrutura da rede utilizada pelos sistemas de ECCE 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 ECCE possui um nível de segurança máximo em termos de rede, dado que:

- Apesar de estar ligado à RInG, está devidamente protegida, quer por *Firewalls*, quer por equipamentos de deteção de intrusão (IDS/IPS);
- Não existem permissões para acessos remotos aos sistemas onde está instalado o *software* de certificação, tendo todas as operações de ser efetuadas no local onde se encontram os equipamentos;
- O Acesso à LRA ou RA é sempre efetuado através de canal seguro e encriptado, recorrendo à utilização de SSL e certificados digitais.

6.9 VALIDAÇÃO CRONOLÓGICA (*TIME STAMPING*)

Os pedidos efetuados no âmbito dos protocolos CMP e CRS não requerem assinatura com fonte de tempo segura. No caso de outras mensagens trocadas entre a Autoridade Certificadora, a Entidade de Registo e o subscritor, é recomendada a utilização de selos temporais.

Os selos temporais emitidos pela entidade de validação cronologia da ECCE estão de acordo com as recomendações do RFC 3161. Os selos temporais são emitidos respeitando a Politica de Selo de Validação Temporal (o documento encontra-se disponível no repositório da ECCE).

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.

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 pela ECCE na assinatura dos certificados sejam facilmente diferenciadas. O valor do "*keyIdentifier*" deve derivar da chave pública da ECCE (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 um hash da chave pública que consta no campo do certificado "*subjectPublicKeyInfo*".

7.1.2.3 KEYUSAGE:

Extensão obrigatória e crítica. Esta extensão especifica o fim a que o certificado se destina.

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

7.1.2.4 CERTIFICATEPOLICIES:

Extensão obrigatória e não critica. Esta extensão lista as Politicas de Certificados que dão suporte e regem o ambiente em que se processou a emissão do certificado. Deve 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 ativo (cA=True).

Em termos práticos, se o campo "*keyUsage*" de um certificado estiver presente o valor "*keyCertSign*", então no *BasicConstraints*, o valor do campo "cA", deverá ser estar activo ("True"), caso contrário o processo de verificação do certificado falha.

Descriminam-se, nas tabelas seguintes, os perfis dos certificados emitidos pela ECCE, quer para utilizadores finais, quer para servidores ou componentes:

Tabela 9. Perfil do Certificado de Assinatura.

CAMPO	CONTEÚDO	EXTENSÕES CRÌTICAS
Campos de X509v1		
1. Versão	V3	
2. Serial Number	Aleatorio	
3. Signature Algorithm	SHA256WithRSAEncryption	
4. Issuer Distinguished Name	CN= ECCE 001, OU=ECEstado, O=SCEE, C=PT	
5. Validity	Até 5 anos	
6. Subject	CN=<cn do utilizador>, OU=<Unidade Orgânica>, O=<Organismo>, C=PT	
7. Subject Public Key Info	Algoritmo: RSA Encryption Tamanho da chave: 2048	
Campos de X509v2		
1. issuerUniqueIdentifier	Não utilizado	
2. subjectUniqueIdentifier	Não utilizado	
Extensões de X509v3		
1. Subject Key Identifier	Derivada da utilização da função de hash SHA-1 sobre a chave pública do subject.	**NÃO**
2. Authority Key Identifier	Derivada da utilização da função de hash SHA-1 sobre a chave pública da EC emissora.	**NÃO**
3. KeyUsage		**SIM**
Digital Signature	0	
Non Repudiation	1	
Key Encipherment	0	
Data Encipherment	0	
Key Agreement	0	
Key Certificate Signature	0	
CRL Signature	0	
4.extKeyUsage	emailProtection	
5. privateKeyUsagePeriod	Não utilizado	
6. Certificate Policies		**NÃO**
Policy Identifier	2.16.620.1.1.1.2.10	
URL CPS	http://www.ecce.gov.pt/dpc	
Notice Reference	O certificado emitido segundo esta política é equivalente a um certificado digital qualificado, nos termos, do definido na Legislação Portuguesa, aplicável para o efeito	
7.Policy Mappings		**SIM**
qcStatements	Id-etsi-qcs-QcSSCD	
8. Subject Alternate Names	Endereço de e-mail segundo o RFC822 OID: 2.16.620.1.1.1.2.2.0.2.1 = Cargo do Titular	

CAMPO	CONTEÚDO	EXTENSÕES CRÍTICAS
9. Issuer Alternate Names	Não utilizado	
10. Subject Directory Attributes	Não utilizado	
11. Basic Constraints		**SIM**
Subject Type	End Entity	
Path Length Constraint	None	
12. Policy Constraints	Não utilizado	
13. CRLDistributionPoints	(1) HTTP: http://crls.ecce.gov.pt/crls/crl-001.crl	**NÃO**
14. Auth. Information Access	Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.ecce.gov.pt [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://trust.ecce.gov.pt/ecce-001.crt	**NÃO**
15.netscapeCertType	SMIMEClient	
16. netscapeRevocationURL	Não aplicável	
17. netscapeCAPolicyURL	Não aplicável	
18. netscapeComment	Não aplicável	

Tabela 10. Perfil do Certificado de Confidencialidade.

CAMPO	CONTEÚDO	EXTENSÕES CRÍTICAS
Campos de X509v1		
1. Versão	V3	
2. Serial Number	Aleatorio	
3. Signature Algorithm	SHA256WithRSAEncryption	
4. Issuer Distinguished Name	CN= ECCE 001, OU=ECEstado, O=SCEE , C=PT	
5. Validity	Até 5 anos	
6. Subject	CN=<cn do utilizador>, OU=<Unidade Orgânica>, O=<Organismo>, C=PT	
7. Subject Public Key Info	Algoritmo: RSA Encryption Tamanho da Chave: 2048	
Campos de X509v2		
1. issuerUniqueIdentifier	Não utilizado	
2. subjectUniqueIdentifier	Não utilizado	

Extensões de X509v3		
1. Subject Key Identifier	Derivada da utilização da função de hash SHA-1 sobre a chave pública do subject.	**NÃO**
2. Authority Key Identifier	Derivada da utilização da função de hash SHA-1 sobre a chave pública da EC emissora.	**NÃO**
3. KeyUsage		**SIM**
Digital Signature	0	
Non Repudiation	0	
Key Encipherment	1	
Data Encipherment	1	
Key Agreement	0	
Key Certificate Signature	0	
CRL Signature	0	
4.extKeyUsage	emailProtection	**NÃO**
5. privateKeyUsagePeriod	Não aplicável	
6. Certificate Policies		**NÃO**
Policy Identifier	2.16.620.1.1.1.2.30	
URL CPS	http://www.ecce.gov.pt/dpc	
Notice Reference	Certificado sujeito a: Declaração de Práticas de Certificação da ECCE	
7.Policy Mappings	Não utilizado	
8. Subject Alternate Names	Endereço de e-mail segundo RFC 822 OID: 2.16.620.1.1.1.2.2.0.2.1 = Cargo do Titular	
9. Issuer Alternate Names	Não utilizado	
10. Subject Directory Attributes	Não utilizado	
11. Basic Constraints		**SIM**
Subject Type	End Entity	
Path Length Constraint	None	
12. CRLDistributionPoints	(1) HTTP: http://crls.ecce.gov.pt/crls/crl-001.crl	**NÃO**
13. Auth. Information Access	Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.ecce.gov.pt [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://trust.ecce.gov.pt/ecce-001.crt	**NÃO**
14.netscapeCertType	SMIMEClient	
15. netscapeRevocationURL	Não Aplicável	
16. netscapeCAPolicyURL	Não Aplicável	
17. netscapeComment	Não Aplicável	

Tabela 11. Perfil do Certificado de Autenticação.

CAMPO	CONTEÚDO	EXTENSÕES CRITICAS
Campos de X509v1		
1. Versão	V3	
2. Serial Number	Aleatorio	
3. Signature Algorithm	SHA256WithRSAEncryption	
4. Issuer Distinguished Name	CN= ECCE 001, OU=ECEstado, O=SCEE , C=PT	
5. Validity	Até 5 anos	
6. Subject	CN=<cn do utilizador>, OU=<Unidade Orgânica>, O=<Organismo>, C=PT	
7. Subject Public Key Info	Algoritmo: RSA Encryption Tamanho da Chave: 2048	
Campos de X509v2		
1. issuerUniqueIdentifier	Não utilizado	
2. subjectUniqueIdentifier	Não utilizado	
Extensões de X509v3		
1. Subject Key Identifier	Derivada da utilização da função de hash SHA-1 sobre a chave pública do subject.	**NÃO**
2. Authority Key Identifier	Derivada da utilização da função de hash SHA-1 sobre a chave pública da EC emissora.	**NÃO**
3. KeyUsage		**SIM**
Digital Signature	1	
Non Repudiation	0	
Key Encipherment	0	
Data Encipherment	0	
Key Agreement	1	
Key Certificate Signature	0	
CRL Signature	0	
4.extKeyUsage	clientAuth, smartCardLogon	**NÃO**
5. privateKeyUsagePeriod	Não Utilizado	
6. Certificate Policies		**NÃO**
Policy Identifier	2.16.620.1.1.1.2.20	
URL CPS	http://www.ecce.gov.pt/dpc	
Notice Reference	Certificado sujeito a: Declaração de Práticas de Certificação da ECCE.	
7.Policy Mappings	Não utilizado	
8. Subject Alternate Names	UPN (User´s Principal Name de Windows 200X) OID: 2.16.620.1.1.1.2.2.0.2.1 = Cargo do Titular	**NÃO**
9. Issuer Alternate Names	Não utilizado	
10. Subject Directory Attributes	Não utilizado	
11. Basic Constraints		**SIM**

CAMPO	CONTEÚDO	EXTENSÕES CRITICAS
Subject Type	End Entity	
Path Length Constraint	None	
12. CRLDistributionPoints	(1) HTTP: http://crls.ecce.gov.pt/crls/crl-001.crl	**NÃO**
13. Auth. Information Access	Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.ecce.gov.pt [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://trust.ecce.gov.pt/ecce-001.crt	**NÃO**
14.netscapeCertType	Client Authentication	
15. netscapeRevocationURL	Não aplicável	
16. netscapeCAPolicyURL	Não aplicável	
17. netscapeComment	Não aplicável	

Tabela 12. Perfil do Certificado de Servidor Seguro (SSL).

CAMPO	CONTEÚDO	EXTENSÕES CRITICAS
Campos de X509v1		
1. Versão	V3	
2. Serial Number	Aleatorio	
3. Signature Algorithm	SHA256WithRSAEncryption	
4. Issuer Distinguished Name	CN= ECCE 001, OU=ECEstado, O=SCEE , C=PT	
5. Validity	Até 3 anos	
6. Subject	CN=<nome do host>, OU=<Unidade Orgânica>, O=<Organismo> L=Localidade S=Portugal C=PT	
7. Subject Public Key Info	Algoritmo: RSA Encryption Tamanho da chave: 2048	
Campos de X509v2		
1. issuerUniqueIdentifier	Não utilizado	
2. subjectUniqueIdentifier	Não utilizado	
Extensões de X509v3		
1. Subject Key Identifier	Derivada da utilização da função de hash SHA-1 sobre a chave pública do subject.	**NÃO**

CAMPO	CONTEÚDO	EXTENSÕES CRITICAS
2. Authority Key Identifier	Derivada da utilização da função de hash SHA-1 sobre a chave pública da EC emissora.	**NÃO**
3. KeyUsage		**SIM**
Digital Signature	1	
Non Repudiation	0	
Key Encipherment	1	
Data Encipherment	0	
Key Agreement	0	
Key Certificate Signature	0	
CRL Signature	0	
4.extKeyUsage	serverAuth	**NÃO**
5. privateKeyUsagePeriod		
6. Certificate Policies		**NÃO**
Policy Identifier	2.16.620.1.1.1.2.40	
URL CPS	http://www.ecce.gov.pt/dpc	
Notice Reference	Certificado sujeito a: Declaração de Práticas de Certificação da ECCE.	
7.Policy Mappings	Não utilizado	
8. Subject Alternate Names	DNS Name=<FQDN> Direcção de e-mail segundo RFC 822 (opcional) IPAdress (opcional)	**NÃO**
9. Issuer Alternate Names	Não utilizado	
10. Subject Directory Attributes	Não utilizado	
11. Basic Constraints		**NÃO**
Subject Type	End Entitty	
Path Length Constraint	None	
12. CRLDistributionPoints	(1) HTTP: http://crls.ecce.gov.pt/crls/crl-001.crl	**NÃO**
13. Auth. Information Access	1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.ecce.gov.pt [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://trust.ecce.gov.pt/ecce-001.crt	**NÃO**
14.netscapeCertType	Não aplicável	
15. netscapeRevocationURL	Não aplicável	
16. netscapeCAPolicyURL	Não aplicável	
17. netscapeComment	Não aplicável	

Tabela 13. Perfil do Certificado de Assinatura para Componentes.

CAMPO	CONTEÚDO	EXTENSÕES CRÍTICAS
Campos de X509v1		
1. Versão	V3	
2. Serial Number	Aleatorio	
3. Signature Algorithm	SHa256WithRSAEncryption	
4. Issuer Distinguished Name	CN= ECCE 001, OU=ECEstado, O=SCEE , C=PT	
5. Validity	1 ano	
6. Subject	CN=[A/F] Cód_Componente Descrição OU=<Unidade Orgânica>, O=<Organismo> L=Localidade S=Portugal C=PT	
7. Subject Public Key Info	Algoritmo: RSA Encryption Tamanho mínimo chave: 2048	
Campos de X509v2		
1. issuerUniqueIdentifier	Não Utilizado	
2. subjectUniqueIdentifier	Não Utilizado	
Extensões de X509v3		
1. Subject Key Identifier	Derivada da utilização da função de hash SHA-1 sobre a chave pública do subject.	**NÃO**
2. Authority Key Identifier	Derivada da utilização da 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	0	
Key Certificate Signature	0	
CRL Signature	0	
4. extKeyUsage	CodeSigning	**NÃO**
5. privateKeyUsagePeriod		
6. Certificate Policies		**NÃO**
Policy Identifier	2.16.620.1.1.1.2.40	
URL CPS	http://www.ecce.gov.pt/dpc	
Notice Reference	Certificado sujeito a: Declaração de Prácticas de Certificação da ECCE.	
7.Policy Mappings	Não Utilizado	
8. Subject Alternate Names	Endereço de e-mail de acordo com RFC 822 (opcional)	**NÃO**
9. Issuer Alternate Names	Não Utilizado	

CAMPO	CONTEÚDO	EXTENSÕES CRÍTICAS
10. Subject Directory Attributes	Não Utilizado	
11. Basic Constraints		**SIM**
Subject Type	End Entity	
Path Length Constraint	None	
12. CRLDistributionPoints	(1) HTTP: http://crls.ecce.gov.pt/crls/crl-001.crl	**NÃO**
13. Auth. Information Access	Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.ecce.gov.pt [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://trust.ecce.gov.pt/ecce-001.crt	**NÃO**
14.netscapeCertType	Signature	
15. netscapeRevocationURL	Não aplicável	
16. netscapeCAPolicyURL	Não aplicável	
17. netscapeComment	Não aplicável	

Tabela 14. Perfil do Certificado de Controlador de Domínio.

CAMPO	CONTEÚDO	EXTENSÕES CRÍTICAS
Campos de X509v1		
1. Versão	V3	
2. Serial Number	Aleatorio	
3. Signature Algorithm	SHA256WithRSAEncryption	
4. Issuer Distinguished Name	CN= ECCE 001, OU=ECEstado, O=SCEE , C=PT	
5. Validity	3 ano	
6. Subject	CN=<Nome DNS do Controlador de Domínio>	
7. Subject Public Key Info	Algoritmo: RSA Encryption Tamanho mínimo da chave: 2048	
Campos de X509v2		
1. issuerUniqueIdentifier	Não utilizado	
2. subjectUniqueIdentifier	Não utilizado	
Extensões de X509v3		
1. Subject Key Identifier	Derivada da utilização da função de hash SHA-1 sobre a chave pública do subject.	**NÃO**
2. Authority Key Identifier	Derivada da utilização da função de hash SHA-1 sobre a chave pública da EC emissora.	**NÃO**

CAMPO	CONTEÚDO	EXTENSÕES CRÍTICAS
3. KeyUsage		**SIM**
Digital Signature	1	
Non Repudiation	0	
Key Encipherment	1	
Data Encipherment	0	
Key Agreement	0	
Key Certificate Signature	0	
CRL Signature	0	
4. extKeyUsage	clientAuth, serverAuth	**NÃO**
5. privateKeyUsagePeriod		
6. Certificate Policies		**NÃO**
Policy Identifier	2.16.620.1.1.1.2.50	
URL CPS	http://www.ecce.gov.pt/dpc	
Notice Reference	Certificado sujeito a: Declaração de Prácticas de Certificação da ECCE.	
7.Policy Mappings	Não utilizado	
8. Subject Alternate Names	Other Name: 1.3.6.1.4.1.311.25.1=<GUID do Controlador de Domínio> DNS Name=<Nome DNS do Controlador de Domínio>	**NÃO**
9. Issuer Alternate Names	Não utilizado	
10. Subject Directory Attributes	Não utilizado	
11. Basic Constraints		**SIM**
Subject Type	End Entity	
Path Length Constraint	None	
12. CRLDistributionPoints	(1) HTTP: http://crls.ecce.gov.pt/crls/crl-001.crl	**NÃO**
13. Auth. Information Access	Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.scee.gov.pt	**NÃO**
14.netscapeCertType	SSL_server	
15. netscapeRevocationURL	Não aplicável	
16. netscapeCAPolicyURL	Não aplicável	
17. netscapeComment		

7.1.3 Identificadores de algoritmo

Na tabela seguinte indicam-se os identificadores de algoritmos:

Tabela 15. Identificadores OID de Algoritmos.

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

7.1.4 Formatos de nome

Os Certificados emitidos para a EC da ECCE 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 codificado de acordo a "ISO 3166-1-alpha-2 code elements", em PrintableString.

No caso dos titulares, o DN é:

CN = <Nome do Titular>

OU = <Unidade Orgânica do Titular>

O = <Organismo do Titular>

C = PT

7.1.6 Objecto identificador da política de certificado

Com o objetivo de não limitar o conjunto de políticas para as cadeias de certificação na qual se incluem os certificados da EC Raiz e da ECCE 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 aplicável.

7.1.8 Sintaxe e semântica dos qualificadores de políticas

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

- URL CPS: contém a URL da DPC e a PCert.

7.1.9 Semântica de processamento da extensão de política de certificados críticos

Tem em consideração as recomendações introduzidas pelo RFC 5280 atualizado pelo RFC 6818 quanto à utilização desta extensão. Os certificados da EC da ECCE incluem no OiD o valor do perfil aplicável.

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

Nos certificados para titulares serão incluídos os OiD respectivos, 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 LCR emitidas pela ECCE, implementam a versão 2 padrão ITU X.509, de acordo com o RFC 3280.

7.2.2 Extensões da LCR e das suas entradas

O SCEE define como extensões de LCR 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;

Tabela 16. Perfil da LCR e suas Extensões.

CAMPO	CONTEÚDO	EXTENSÕES CRÍTICAS
Version	V2	
Signature		
AlgorithmIdentifier		
Algorithm	SHA-1WithRSAEncryption	
Parameters		
IssuerName	CN = ECCE 001 OU = ECEstado O = SCEE C = PT	
ThisUpdate	Data de emissão	
validityPeriod	24 horas	
NextUpdate	24 horas	
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.ecce.gov.pt/crls/crl-001.crl	**Não**
onlyContainsUserCerts	0	
onlyContainsCACerts	0	
IndirectCRL		
DeltaCRLIndicator	Não é utilizado	**Sim**
BaseCRLNumber	Este valor será igual ao do CRLNumber	

7.3 TIME-STAMPING AUTHORITY (TSA)

A *Time-Stamping Authority* (TSA) assina electronicamente selos temporais com uma ou mais chaves privadas reservadas especialmente para este efeito. Segundo a recomendação do RFC 3280, os certificados e as suas chaves públicas contêm um campo que obriga o uso da extensão *ExtKeyUsageSyntax*, marcada como crítica. Isto significa que o certificado pode ser utilizado pela autoridade de Time Stamping somente para propósitos de assinatura do selo temporal publicado pela autoridade. O certificado de selo temporal desta entidade contém a informação sobre contactos possíveis com a entidade. Tal informação é apresentada na extensão privada – *AuthorityInfoAccessSyntax* – classificada como critica. O perfil de selo temporal é descrito na tabela abaixo.

Tabela 17. Perfil do Certificado de Selo de Validação Cronológica.

CAMPO	CONTEÚDO	EXTENSÕES CRÍTICAS
Campos de X509v1		
1. Versão	V3	
2. Serial Number	Aleatorio	
3. Signature Algorithm	SHA256WithRSAEncryption	
4. Issuer Distinguished Name	CN= ECCE-001, OU=ECEstado, O=SCEE , C=PT	
5. Validity	3 anos	
6. Subject	CN=TSA-ECCE,OU=ECEstado,O=SCEE,C=PT	
7. Subject Public Key Info	Algoritmo: RSA Encryption Tamanho mínimo da chave: 2048	
Campos de X509v2		
1. issuerUniqueIdentifier	Não utilizado	
2. subjectUniqueIdentifier	Não utilizado	
Extensões de X509v3		
1. Subject Key Identifier	Derivada da utilização da função de hash SHA-1 sobre a chave pública do subject.	**NÃO**
2. Authority Key Identifier	Derivada da utilização da 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	0	

CAMPO	CONTEÚDO	EXTENSÕES CRÍTICAS
Key Certificate Signature	0	
CRL Signature	0	
4. extKeyUsage	Time Stamping (1.3.6.1.5.5.7.3.8)	**SIM**
5. privateKeyUsagePeriod		
6. Certificate Policies		**NÃO**
Policy Identifier	2.16.620.1.1.1.2.60	
URL CPS	http://www.ecce.gov.pt/dpc	
Notice Reference	Certificado sujeito a: Declaração de Práticas de Certificação da ECCE.	
7.Policy Mappings	Não utilizado	
8. Basic Constraints		**NÃO**
Subject Type	End Entity	
Path Length Constraint	Não utilizado	
12. CRLDistributionPoints	(1) HTTP: http://crls.ecce.gov.pt/crls/crl-001.crl	**NÃO**
13. Auth. Information Access	Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.scee.gov.pt	**NÃO**

O selo temporal emitido pela ECCE contém informação do selo (TSTinfo strucure), localizada na estrutura SignedData (RFC 2630), assinada pela autoridade de validação cronológica e inserida na estrutura ContentInfo (RFC 2630).

A Entidade de Validação Cronológica responde a pedidos de selo temporal de acordo com a notação ASN.1:

```
TimeStampResp ::= SEQUENCE {
status PKIStatusInfo,
timeStampToken TimeStampToken OPTIONAL
}
```

7.4 PERFIL DO OCSP

No serviço de OCSP implementado, os certificados de *OCSP Responder*, estão em concordância com as normas normas:

a) RFC 5280, atualizado pelo RFC 6818;

b) ITU-TX.509 (2005);

c) RFC 6960.

O período de validade dos certificados OCSP Responder é de x meses e é incluída a extensão "id-pkix-ocsp-nocheck".

7.4.1 Número(s) da versão

Os certificados de *OCSP Responder* utilizam a norma X.509 versão3 (X.509 v3).

7.4.2 .Extensões do OCSP

Os certificados de *OCSP Responder* emitidos pela ECCE incluem o DN da entidade emissora no campo "*issuer name*"e o DN do titularno campo "*subject name*".

Tabela 18. Perfil dos Certificados OCSP Responder.

CAMPO	CONTEÚDO	EXTENSÕES CRÍTICAS
Campos de X509v1		
1. Versão	V3	
2. Serial Number	Aleatorio	
3. Signature Algorithm	SHA256WithRSAEncryption	
4. Issuer Distinguished Name	CN= ECCE-001, OU=ECEstado, O=SCEE , C=PT	
5. Validity	6 meses	
6. Subject	CN=OCSP-ECCE,OU=ECEstado,O=SCEE,C=PT	
7. Subject Public Key Info	Algoritmo: RSA Encryption Tamanho mínimo da chave: 2048	
Campos de X509v2		
1. issuerUniqueIdentifier	Não utilizado	
2. subjectUniqueIdentifier	Não utilizado	
Extensões de X509v3		
1. Subject Key Identifier	Derivada da utilização da função de hash SHA-1 sobre a chave pública do subject.	**NÃO**
2. Authority Key Identifier	Derivada da utilização da 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	

CAMPO	CONTEÚDO	EXTENSÕES CRÍTICAS
Key Agreement	0	
Key Certificate Signature	0	
CRL Signature	0	
4. extKeyUsage	id-kp-OCSPSigning	**SIM**
5. privateKeyUsagePeriod		
		NÃO
Policy Identifier	Any Policy	
URL CPS	http://www.ecce.gov.pt/dpc	
Notice Reference	Certificado sujeito a: Declaração de Práticas de Certificação da ECCE.	
7.Policy Mappings	Não utilizado	
		NÃO
Subject Type		
Path Length Constraint		
8. Basic Constraints		**NÃO**
Subject Type	Entidade Final	
Path Length Constraint	Não utilizado	
12. CRLDistributionPoints	(1) HTTP: http://crls.ecce.gov.pt/crls/crl-001.crl	**NÃO**
13. Auth. Information Access		**NÃO**
14. OCSP No Revocation Checking	Sim	**NÃO**

8. AUDITORIA E OUTRAS AVALIAÇÕES DE CONFORMIDADE

8.1 FREQUÊNCIA OU MOTIVO DA AUDITORIA

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

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

Anualmente será efectuada uma auditoria interna à ECCE de acordo com o Plano de Auditorias do SCEE. É assim garantida a adequação do seu funcionamento e operação com os requisitos desta DPC.

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

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

Da mesma forma, a cada três anos será efectuada uma auditoria externa para avaliar o grau de conformidade com a 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 são determinadas de acordo com o estabelecido na PCert (ver Ponto 8.2).

8.3 RELAÇÃO ENTRE O AUDITOR E A ENTIDADE CERTIFICADORA

A relação entre o auditor e a ECCE será feita de acordo com o estabelecido com a PCert (ver Ponto 8.3).

8.4 ÂMBITO DA AUDITORIA

De acordo com a PCert (Ponto 8.4).

8.5 PROCEDIMENTOS APÓS UMA AUDITORIA COM RESULTADO DEFICIENTE

As auditorias com resultado deficiente serão tratadas de acordo com o estabelecido na Política de Certificados.

8.6 COMUNICAÇÃO DE RESULTADOS

De acordo com a PCert (Ponto 8.6).

9. OUTRAS SITUAÇÕES E ASSUNTOS LEGAIS

9.1 TAXAS

9.1.1 Taxas por emissão ou renovação de certificados

Serão aplicada as taxas definidas por Portaria própria para o efeito.

9.1.2 Taxas para acesso a certificado

Não aplicável.

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

Não aplicável.

9.1.4 Taxas para outros serviços

Não aplicável.

9.1.5 Política de reembolso

Não Aplicável.

9.2 RESPONSABILIDADE FINANCEIRA

9.2.1 Seguro de cobertura

Não Aplicável.

9.2.2 Outros recursos

Não aplicável.

9.2.3 Seguro ou garantia de cobertura para utilizadores

Não aplicável.

9.3 CONFIDENCIALIDADE DA INFORMAÇÃO PROCESSADA

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 do SCEE (ver Ponto 9.3.1).

9.3.2 Informação não protegida pela confidencialidade

De acordo com a Política de Certificação do SCEE (ver Ponto 9.3.2).

9.3.3 Responsabilidade de protecção da confidencialidade da informação

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

Todos os elementos assinam um termo de responsabilidade e sigilo, onde afirmam garantir total sigilo sobre todas as actividades, sobre toda a informação e processos da ECCE.

9.4 PRIVACIDADE DOS DADOS PESSOAIS

A ECCE 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 do SCEE (ver Ponto 9.4.1).

9.4.2 Informação privada

De acordo com a Política de Certificação do SCEE (ver Ponto 9.4.2).

9.4.3 Informação não protegida pela privacidade

De acordo com a Política de Certificação do SCEE (ver Ponto 9.4.3).

9.4.4 Responsabilidade de protecção da informação privada

De acordo com a Política de Certificação do SCEE (ver Ponto 9.4.4).

9.4.5 Notificação e consentimento para utilização de informação privada

De acordo com a Política de Certificação do SCEE (ver Ponto 9.4.5).

9.4.6 Divulgação resultante de processo judicial ou administrativo

De acordo com a Política de Certificação do SCEE (ver Ponto 9.4.6).

9.4.7 Outras circunstâncias para revelação de informação

De acordo com a Política de Certificação do SCEE (ver Ponto 9.4.7).

9.5 DIREITOS DE PROPRIEDADE INTELECTUAL

De acordo com a Política de Certificação do SCEE (ver Ponto 9.5).

9.6 REPRESENTAÇÕES E GARANTIAS

9.6.1 Representação das EC e garantias

De acordo com a Política de Certificação do SCEE (ver Ponto 9.6.1).

9.6.2 Representação das ER e garantias

De acordo com a Política de Certificação do SCEE (ver Ponto 9.6.2).

9.6.3 Representação e garantias do titular

De acordo com a Política de Certificação do SCEE (ver Ponto 9.6.3).

9.6.4 Representação dos correspondentes (Relying party) e garantias

De acordo com a Política de Certificação do SCEE (ver Ponto 9.6.4).

9.6.5 Representação e garantias de outros participantes

Não existem outros participantes.

9.7 RENÚNCIA DE GARANTIAS

De acordo com a Política de Certificação do SCEE (ver Ponto 9.7).

9.8 LIMITAÇÕES ÀS OBRIGAÇÕES

De acordo com a Política de Certificação do SCEE (ver Ponto 9.8).

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 da ECCE.

Esta DPC estará em vigor enquanto não for revogada expressamente pela emissão de uma nova versão ou pela renovação das chaves da EC Raiz, momento em que obrigatoriamente se redigirá 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 Consequência ências da conclusão da actividade e sobrevivência

As obrigações e restrições que estabelece esta DPCrelativamente a auditorias, informação confidencial, obrigações e responsabilidades da SCEE (nascidas sob sua vigência), manter-se-ão após a 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 do SCEE (ver Ponto 9.11).

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 ECCE. Os dados de contacto da ECCE encontram-se no ponto 1.51 desta DPC.

9.12.2 Prazo e mecanismo de notificação

De acordo com a Política de Certificação do SCEE (ver Ponto 9.12.2).

9.12.3 Motivos para mudar de OID

De acordo com a Política de Certificação do SCEE (ver Ponto 9.12.3).

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 do SCEE (ver Ponto 9.14).

9.15 CONFORMIDADE COM A LEGISLAÇÃO EM VIGOR

É responsabilidade do Conselho Gestor do SCEE velar pelo cumprimento da legislação aplicável reconhecida no ponto anterior.

9.16 PROVIDÊNCIAS VÁRIAS

9.16.1 Acordo completo

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

9.16.2 Nomeação (Independência)

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

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

9.16.3 Severidade

Não Estipulado.

9.16.4 Execuções (taxas de advogados e desistência de direitos)

Não Estipulado.

9.16.5 Força maior

Não Estipulado.

9.17 OUTRAS PROVIDÊNCIAS

Não Estipulado.

ANEXO A – ACRÓNIMOS E DEFINIÇÕES

Com o objectivo de conhecer os conceitos que são utilizados no presente documento, indicam-se em seguida acrónimos e definições de conceitos utilizados.

A.1. ACRÓNIMOS

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

SCEE	Sistema de Certificação Electrónica do Estado;
ECEstado	Entidade Certificadora do Estado;
ECRaizEstado	Entidade Certificadora de Raiz do Estado;
EGPC	Entidade Gestora de Politicas de Certificação;
ER	Entidade de registo;
EREstado	Entidade de Registo do Estado;
ETSI	European Telecommunications Standard Institute;
FIPS	Federal Information Processing Standard;
FQDN	Fully Qualified Domain Name;
HSM	Hardware Security Module;
ICP	Infra-Estrutura de Chave Pública;
IDS/IPS	Intrusion Detection System / Intrusion Prevention System;
IETF	Internet Engineering Task Force;
LCR	Lista de Certificados Revogados;
LDAP	Lightweight Directory Access Protocol;
LER	Lista de Certificados de Entidades Certificadoras Revogadas;
O	Organization;
OCSP	Online Certificate Status Protocol;
OID	Object Identifier;
OpHSM	Operadores do HSM;
OpSist	Operador de Sistemas;
OU	Organizacional Unit;
P1	Perfil de Certificado de ECRaizEstado;
P2	Perfil de Certificado de ECEstado;

P3	Perfil de Certificado de Assinatura Digital;
P4	Perfil de Certificado de Autenticação;
P5	Perfil de Certificado de Confidencialidade;
P6	Perfil de Certificado de Time Stamping;
P7	Perfil de Certificado de OCSP;
PC	Política de Certificado;
PCert	Política de Certificados da SCEE;
PED	PIN Entry Device;
PKCS	Public-Key Cryptography Standards;
PKCS#1	RSA Cryptography Standard;
PKCS#10	Certification Request Syntax Standard;
PKCS#11	Cryptographic Token Interface Standard;
PKCS#7	Cryptographic Message Syntax Standard;
RAF	Relatório de auditoria final;
RCI	Relatório de correcção de irregularidades;
RFC	Request For Comments;
RPI	Relatório de primeiras impressões;
RSA	Algoritmo criptográfico (Rivest | Shamir | Adleman);
RSAE	Relatório Sumário de Análise de Eventos;
subECEstado	Entidade Certificadora Subordinada duma ECEstado;
TCP/IP	Transmission Control Protocol/Internet Protocol;
TRT	Termo de Responsabilidade do Titular;
OID	Identificador de Objecto;
URL	Unified Resource Locator;

A.2. DEFINIÇÕES

Assinatura digital	Modalidade de assinatura electrónica avançada baseada em sistema criptográfico assimétrico composto de um algoritmo ou série de algoritmos, mediante o qual é gerado um par de chaves assimétricas exclusivas e interdependentes, uma das quais privada e outra pública, e que permite ao titular usar a chave privada para declarar a autoria do documento electrónico ao qual a assinatura é aposta e concordância com o seu conteúdo e ao destinatário usar a chave pública para verificar se a assinatura foi criada mediante o uso da correspondente chave privada e se o documento electrónico foi alterado depois de aposta a assinatura;
Assinatura electrónica avançada	Assinatura electrónica que preenche os seguintes requisitos: • Identifica de forma unívoca o titular como autor do documento; • A sua aposição ao documento depende apenas da vontade do titular; • É criada com meios que o titular pode manter sob seu controlo exclusivo; • A sua conexão com o documento permite detectar toda e qualquer alteração superveniente do conteúdo deste;
Assinatura electrónica qualificada	Assinatura digital ou outra modalidade de assinatura electrónica avançada que satisfaça exigências de segurança idênticas às da assinatura digital baseadas num certificado qualificado e criadas através de um dispositivo seguro de criação de assinatura;
Assinatura electrónica	É o resultado de um processamento electrónico de dados suscetível de constituir objecto de direito individual e exclusivo e de ser utilizado para dar a conhecer a autoria de um documento electrónico;

Autoridade credenciadora	Entidade competente para a credenciação e fiscalização das entidades certificadoras;
C	Atributo do DN de um objecto dentro da estrutura de directório X.500;
Certificado	Estrutura de dados assinado electronicamente por um prestador de serviços de certificação e que vincula ao titular os dados de validação de assinatura que confirma a sua identidade;
Chave privada	Elemento do par de chaves assimétricas destinado a ser conhecido apenas pelo seu titular, mediante o qual se apõe a assinatura digital no documento electrónico, ou se decifra um documento electrónico previamente cifrado com a correspondente chave pública;
Chave pública	Elemento do par de chaves assimétricas destinado a ser divulgado, com o qual se verifica a assinatura digital aposta no documento electrónico pelo titular do par de chaves assimétricas, ou se cifra um documento electrónico a transmitir ao titular do mesmo par de chaves;
Chave	Sequência de símbolos;
CN	Atributo do DN de um objecto dentro da estrutura de directório X.500.
Credenciação	Acto pelo qual é reconhecido a uma entidade que o solicite e que exerça a actividade de entidade certificadora o preenchimento dos requisitos definidos no presente diploma para os efeitos nele previstos;
Dados de Activação	Dados privados, diferentes das chaves, exigidos para o acesso aos módulos criptográficos;
Dados de criação de assinatura	São dados únicos, como códigos ou chaves criptográficas privadas que o titular utiliza para gerar a sua assinatura electrónica;
Dados de criação de assinatura	Conjunto único de dados, como chaves privadas, utilizado pelo titular para a criação de uma assinatura electrónica;

Dados de verificação de assinatura	São dados como códigos ou chaves criptográficas públicas, que se utilizam para verificar a assinatura electrónica;
Dados de verificação de assinatura	Conjunto de dados, como chaves públicas, utilizado para verificar uma assinatura electrónica;
Declaração de Práticas de Certificação	Documento onde são especificados ao pormenor a forma como Prestador de Serviços de Certificação realiza as actividades relacionadas com a gestão do ciclo de vida do certificado;
Directório de Certificados:	Repositório de informação que segue o standard X500;
Dispositivo de criação de assinatura	Suporte lógico ou dispositivo de equipamento utilizado para possibilitar o tratamento dos dados de criação de assinatura;
Dispositivo seguro de criação de assinatura	Dispositivo de criação de assinatura que assegure, através de meios técnicos e processuais adequados, que: • Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura só possam ocorrer uma única vez e que a confidencialidade desses dados se encontre assegurada; • Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura não possam, com um grau razoável de segurança, ser deduzidos de outros dados e que a assinatura esteja protegida contra falsificações realizadas através das tecnologias disponíveis; • Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura possam ser eficazmente protegidos pelo titular contra a utilização ilegítima por terceiros; • Os dados que careçam de assinatura não sejam modificados e possam ser apresentados ao titular antes do processo de assinatura;

DN	Identificação unívoca de uma entrada dentro da estrutura de directório X.500;
Documento Electrónico	Conjunto de dados lógicos armazenados em suporte susceptível de poder ser lido por equipamentos electrónicos de processamento de dados;
Endereço electrónico	Identificação de um equipamento informático adequado para receber e arquivar documentos electrónicos;
Entidade certificadora	Entidade ou pessoa singular ou colectiva que cria ou fornece meios para a criação e verificação das assinaturas, emite os certificados, assegura a respectiva publicidade e presta outros serviços relativos a assinaturas electrónicas;
Entidade de Registo	Entidade ou pessoa singular ou colectiva designada pelas Entidades Certificadoras para realizar actividades de comprovação da identidade dos subscritores ou titulares e consequente registo, bem como a gestão de pedidos de revogação de certificados;
Função hash	É uma operação que se realiza sobre um conjunto de dados de qualquer tamanho de forma que o resultado obtido é outro conjunto de dados de tamanho fixo independente do tamanho original e que tem a propriedade de estar associado univocamente aos dados inicias e garantir que é impossível obter mensagens distintas que gerem o mesmo resultado ao aplicar esta função;
Hash ou impressão digital	Resultado de tamanho fixo que se obtém após a aplicação de uma função hash a uma mensagem e que cumpre a requisito de estar associado univocamente aos dados iniciais;
HSM	Módulo de seguridad criptográfico empleado para almacenar claves y realizar operaciones criptográficas de modo seguro;
Infra-Estrutura de Chave Pública	Estrutura de hardware, software, pessoas, processos e políticas que usa a tecnologia de assinatura digital para dar a terceiros de confiança uma associação verificável entre a componente pública de um par de chaves assimétrico e um assinante específico;

LCR	Lista de certificados revogados que é criada e assinada pela EC que emitiu os certificados. Um certificado é introduzido na lista quando é revogado (por exemplo, por suspeita de comprometimento da chave). Em determinadas circunstâncias, a EC pode dividir uma LCR num conjunto de LCR mais pequenas;
LER	Lista de certificados de outras CA revogados. Uma ARL é equivalente a uma CRL para os certificados cruzados com outras CA;
Módulo Criptográfico Hardware	Módulo de hardware utilizado para realizar funções criptográficos e armazenar chaves em modo seguro;
Número de série de Certificado	Valor inteiro e único que está associado inequivocamente com um certificado emitido pela SCEE;
O	Atributo do DN de um objecto dentro da estrutura de directório X.500;
OCSP	protocolo que permite a comprovação do estado do certificado no momento em que o mesmo é utilizado;
OCSP Responder	Servidor que responde segundo o protocolo OCSP aos pedidos OCSP com o estado do certificado;
OID	O identificador alfanumérico/numérico único registado em conformidade com a norma de registo ISO, para fazer referência a um objecto específico ou a uma classe de objectos específica;
OU	Atributo do DN de um objecto dentro da estrutura de directório X.500;
Pedido OCSP	Pedido de consulta de estado de um certificado a um OCSP Responder;
PIN	Personal Identification Number;
PIN	número específico apenas conhecido pela pessoa que tem de aceder a um recurso que se encontra protegido por este mecanismo;
PKCS	Conjunto de standard desenvolvido pela RSA Labs aceite internacionalmente para definição da sintaxe a utilizar com a criptografia de chave pública;

PKIX	Grupo de trabalho do IETF constituido para desenvolver as especificações relacionadas com PKI e Internet;
Time Stamping	Constatação da data e hora de um documento electrónico mediante processos criptográficos, para datar os documentos de forma objectiva;
SHA	Desenvolvido pelo NIST e revisto em 1994 (SHA-1). Este algoritmo consiste em transformar mensagens de menos de 264 bits e gerar um resumo de 160 bits de comprimento. A probabilidade de encontrar duas mensagens distintas que produzam o mesmo resumo é praticamente nula, por esse motivo utiliza-se para assegurar a integridade dos documentos durante o processe de assinatura electrónica;
SmartCard	Cartão criptográfico utilizado pelo titular para armazenar chaves privadas de assinatura e ou cifra. Os smartcards são considerados dispositivos seguros de criação de assinatura e de acordo com a lei permite a geração de assinatura electrónica qualificadas;
Titular	Pessoa singular ou colectiva identificada num certificado como a detentora de um dispositivo de criação de assinatura;
Validação cronológica	Declaração de entidade certificadora que atesta a data e hora da criação, expedição ou recepção de um documento electrónico;
X.500	Standard desenvolvido pelo ITU que define as recomendações de um directório. Corresponde ao standard ISO 9594-1;
X.509	Standard desenvolvido pelo ITU que define o formato electrónico dos certificados electrónicos;
Zona de Alta Segurança	Área de acesso controlado através de um ponto de entrada e limitada a pessoal autorizado devidamente credenciado e a visitantes devidamente acompanhados. As zonas de alta segurança devem estar encerradas em todo o seu perímetro e ser vigiadas 24 horas por dia, 7 dias por semana, por pessoal de segurança, por outro pessoal ou por meios electrónicos.

ANEXO B – FORMULÁRIOS PARA EMISSÃO DE CERTIFICADOS

Os fomulários disponibilizados aos titulares de certificados da ECCE para pedido de emissão de certificados estão anexos ao Documento de Declaração de Práticas de Certificação na sua versão PDF.

Os formulários para emissão de certificados são:

- **Formulário para Requerimento de Certificados Pessoais**;
- **Formulário para Requerimento de Certificado SSL/TLS**.