DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO

Entidade Certificadora **Comum do Estado** – **ECCE**

SISTEMA DE CERTIFICAÇÃO ELETRÓNICA DO ESTADO (SCEE)

INFRAESTRUTURA DE CHAVES PÚBLICAS

OID: 2.16.620.1.1.1.2.3.1.6

Versão 6.0 de 12 de agosto de 2020

Documento Público

EC
Comum
do Estado

REPÚBLICA
PORTUGUESA
PRESIDÊNCIA DO CONSELHO
DE MINISTROS

APROVAÇÃO E ASSINATURA

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

O Diretor do Centro de Gestão da Rede Informática do Governo,

TITO CARLOS
SOARES VIEIRA

Digitally signed by TITO CARLOS SOARES VIEIRA
DN: c=PT, title=DIRETOR, o=Centro de Gestão da Rede Informática do Governo, cn=TITO CARLOS SOARES VIEIRA
Date: 2020.08.14 18:14:00 +01'00'

Tito Soares Vieira

Índice

Ceger

Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt

Government Computer Network
Management Centre
Presidency of the Council of Ministers

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt

Government Computer Network
Management Centre
Presidency of the Council of Ministers

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

1. INTRODUÇÃO

1.1. Enquadramento

1.1.1. Âmbito

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

O SCEE funciona permitindo a interoperabilidade com 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.

O Regulamento (UE) n.º 910/2014, do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno, mais conhecido por regulamento eIDAS, entrou em vigor em 17 de setembro de 2014 e o essencial do seu articulado passou a ser aplicado desde 1 de julho de 2016.

O citado regulamento revogou a Diretiva n.º 1999/93/CE, do Parlamento Europeu e do Conselho, de 13 de dezembro de 1999, relativa a um quadro legal comunitário para as

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

assinaturas eletrónicas, caducando a vigência do Decreto-Lei n.º 290-D/99, de 2 de agosto (regime jurídico dos documentos eletrónicos e da assinatura digital).

O eIDAS tem como objetivo principal, estabelecer uma base europeia comum para uma interação eletrónica segura, aumentando a confiança e segurança das transações *online* na União Europeia, promovendo uma maior utilização de serviços online por parte dos cidadãos, operadores económicos e administração pública.

O eIDAS estabelece um conjunto alargado de serviços de confiança, bem como o reconhecimento mútuo transfronteiriço dos meios de identificação eletrónica (eID). A partir de 29 de setembro de 2018, um cidadão da UE com um cartão eID (notificado de acordo com o regulamento eIDAS), poderá aceder a qualquer serviço público *online* a partir de qualquer Estado-Membro da EU.

A presente Declaração de Práticas de Certificação (DPC) descreve e regula as práticas de certificação da Entidade Certificadora Comum do Estado (ECCE), bem como a sua adequação ao regulamento eIDAS enquanto serviços de confiança previstos no regulamento que são disponibilizados por prestadores de serviços de confiança.

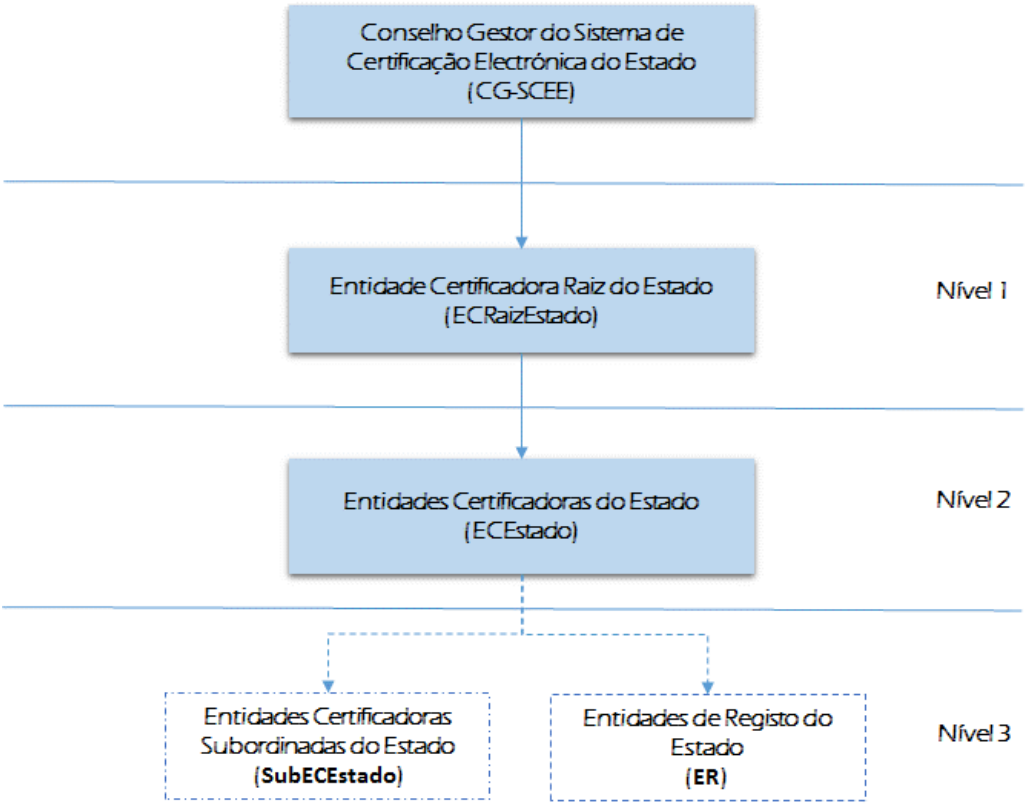

Figura 1 – Arquitetura funcional do SCEE.

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 PCert do SCEE*".

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

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, aparece a frase "*Não aplicável*".

Para a elaboração do seu conteúdo, foram tidos em conta os *standards* europeus, bem como o Regulamento n.º 910/2014, do Parlamento Europeu e do Conselho, de 23 de julho, e respetivos regulamentos de execução.

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 seguinte:

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

Nome do Documento	Declaração de Práticas de Certificação da ECCE
Versão do Documento	Versão 6.0
Estado do Documento	Aprovado
OID	2.16.620.1.1.1.2.3.1.6
Data de Emissão	12 de agosto de 2020
Validade	1 (um) Ano
Localização	https://www.ecce.gov.pt/repositorio/ [1]

[1] O documento está também disponível no *link* alternativo http://www.ecce.gov.pt/dpc (endereço utilizado no *template* dos certificados).

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

1.3. Participantes na Infraestrutura 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 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 24 de junho de 2007 15:43:57 Até 24 de junho de 2027 15:43:57
Emissor	CN=ECRaizEstado, O=SCEE, C=PT

ATRIBUTO	DESCRIÇÃO
Certificado sha256WithRSAEncryption	
Nome Distinto	CN=ECCE 002, OU=ECEstado, O=Centro de Gestão da Rede Informática do Governo, C=PT
Número de série	12 b6 c0 75 cb 90 4e ce 5f 03 3b a3 ec 06 15 7e
Período de validade	De 06 de julho de 2020 15:56:35 Até 06 de julho de 2032 15:56:35
Emissor	CN=ECRaizEstado 002, O=Sistema de Certificação Eletrónica do Estado, C=PT

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

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 está descrito no capítulo 6.3). Os selos temporais são assinados utilizando a chave privada destinada para esse efeito.

A Entidade de Validação Cronológica da ECCE 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 os certificados 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).

Ceger. CENTRO DE GESTÃO DA REDE INFORMÁTICA DO GOVERNO
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

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. Entidade Supervisora

De acordo com a legislação Portuguesa, a Entidade Supervisora é o Gabinete Nacional de Segurança (GNS).

Para efeitos de notificação e comunicação da ECCE à Entidade Supervisora, são estabelecidas as seguintes formas:

a) Para manutenção/alteração de serviços de confiança, mediante preenchimento de formulário disponibilizado pelo GNS, no seu sítio da Internet;
b) Para assuntos técnicos e administrativos, por correio eletrónico dirigido à equipa multidisciplinar de assinatura eletrónica e PKI (AE);
c) Em caso de cessação global ou parcial dos serviços prestados pela ECCE, pelas disposições previstas no Plano de Cessação da Atividade.

1.3.6.3. Entidade gestora das listas de confiança

O Gabinete Nacional de Segurança (GNS) é responsável pela elaboração, conservação, atualização e publicação das listas de confiança nacionais.

1.3.6.4. Organismos de avaliação de conformidade

São entidades competentes para realizar a avaliação da conformidade de prestadores qualificados de serviços de confiança e dos serviços de confiança qualificados prestados. Estes organismos são obrigatoriamente acreditados pelo organismo nacional de acreditação (o IPAC - Instituto Português de Acreditação, I.P).

1.3.6.5. Organismo de reporte

São Organismo de reporte:

a) Agência da União Europeia para a segurança das redes e da informação (ENISA), que recebe anualmente da entidade supervisora um resumo das notificações de violações da segurança e de perda de integridade que tenha recebido dos prestadores de serviços de confiança;
b) Autoridade Nacional de Controlo de Dados Pessoais (Comissão Nacional de Proteção de Dados), que recebe informação da entidade supervisora sobre auditorias ou dos resultados das auditorias realizadas a prestadores qualificados de serviços de confiança, quando haja suspeita de terem sido violadas as regras de proteção dos dados pessoais, assim como é notificada pelos prestadores de

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

serviços de confiança de todas as violações da segurança ou perdas de integridade que tenham um impacto significativo sobre os dados pessoais por eles conservados.

1.3.6.6. Autoridades de Validação

A ECCE dispõe de autoridades de validação próprias para os serviços disponibilizados utilizando o protocolo OCSP.

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 3.

Tabela 3. 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.

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 da presente DPC é da responsabilidade do CEGER e assinada digitalmente pelo seu Diretor.

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

1.5.2. Contactos

Na tabela seguinte estão descritos os contactos relevantes da Entidade Gestora da ECCE.

Tabela 4. Dados de Contacto da Entidade Gestora da ECEE.

Entidade Gestora da ECEE	
Morada:	Av. Defensores de Chaves, nº6 – 6º Piso 1049-063 Lisboa – Portugal
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

A Entidade Supervisora Portuguesa é o órgão competente para determinar a adequação da presente DPC.

1.5.4. Procedimentos para revisão e aprovação da DPC

A presente DPC é anualmente revista, tendo em conta o ciclo PDCA, da seguinte forma:

a) Em fevereiro de cada ano civil, a versão em vigor é remetida ao Coordenador responsável pela gestão operacional da ECCE;
b) O Gestor Operacional da ECCE efetua uma revisão, colhendo os contributos dos elementos afetos às atividades no âmbito da ECCE, com a finalidade de melhoria continua da DPC;
c) Até ao final do mês de maio de cada ano civil, o Gestor Operacional da ECCE, remete a proposta de nova versão da DPC ao Diretor do CEGER, para discussão em sede de revisão pela gestão da ECCE;
d) A revisão pela gestão da ECCE é efetuada em reunião de coordenação do CEGER.

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.

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

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-001.crl e http://crls.ecce.gov.pt/crls/crl-002.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 da presente 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 Política de Certificados (*PCert*), assinado eletronicamente (www.ecce.gov.pt/repositorio/ e em www.ecce.gov.pt/dpc);
b) Uma cópia eletrónica da presente DPC, assinada eletronicamente, pelo Diretor do CEGER (www.ecce.gov.pt/repositorio/);
c) Listas de Certificados Revogados (LCR);
d) Informações adicionais 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.

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

2.4. Controlo de acesso aos repositórios

Não existe qualquer restrição de acesso para consulta a esta DPC e 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 qualificados de assinatura eletrónica emitidos pela ECCE têm o seguinte, DN:

Tabela 5. Regras para o preenchimento do DN.

Atributo	Código	Regras para preenchimento
CountryName	C	Código "PT".
OrganizationName	O	Este campo corresponde, ao nome formal da 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*".
		Nome real do titular do certificado que deverá corresponder ao nome completo, conforme documento de Identificação nacional.

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.

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

3.1.3. Anonimato ou pseudónimo de titulares

Não aplicável.

3.1.4. Interpretação de formato de nomes

As regras utilizadas pelo SCEE para interpretar o formato dos nomes dos certificados que emite são as contidas na norma ISO9595.

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 verifica o cumprimento desta norma, suportando-se no sistema de informação de suporte à emissão de certificados 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 titular 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

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

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 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 delegação de competências;
- Nome do 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

Toda a informação descrita nos pontos 3.2.2 e 3.2.3 deve ser obrigatoriamente verificada. A ECCE pode autorizar entidades privadas a tomar ações em nome de outras entidades, no entanto, tais autorizações estão associadas com regras particulares das instituições. A autenticação das autorizações é uma parte formal do pedido de registo de certificado para entidades com personalidade jurídica. Um certificado emitido é uma confirmação de que uma entidade legal é intitulada para utilizar uma chave privada em nome de outra entidade legalmente reconhecida.

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

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 da presente 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).

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

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 ação.

3.5. Requisitos operacionais do ciclo de vida do certificado

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

3.6. Pedido de certificado

3.6.1. Quem pode subscrever um pedido de certificado

O pedido de certificados pode ser efetuado pelos seguintes 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 da Administração pública Direta, Indireta e Autónoma do Estado 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 colocar o pedido 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 Administração 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 (Administração pública Direta, Indireta e Autónoma) que, não sendo dirigentes, tenham por função enviar atos para a Imprensa Nacional Casa da Moeda;
- Funcionários, agentes do Estado (Administração pública Direta, Indireta e Autónoma) 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 *PCert* do SCEE. A ER poderá reclamar do solicitante a documentação que considerar oportuna.

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

3.6.2. 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 respetivo 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*.

3.7. 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:
  - Verificação da identidade do requisitante;
  - Verificação da exatidão e integridade do pedido de certificado;
- Criação e assinatura do certificado;
- Disponibilização do certificado ao titular.

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

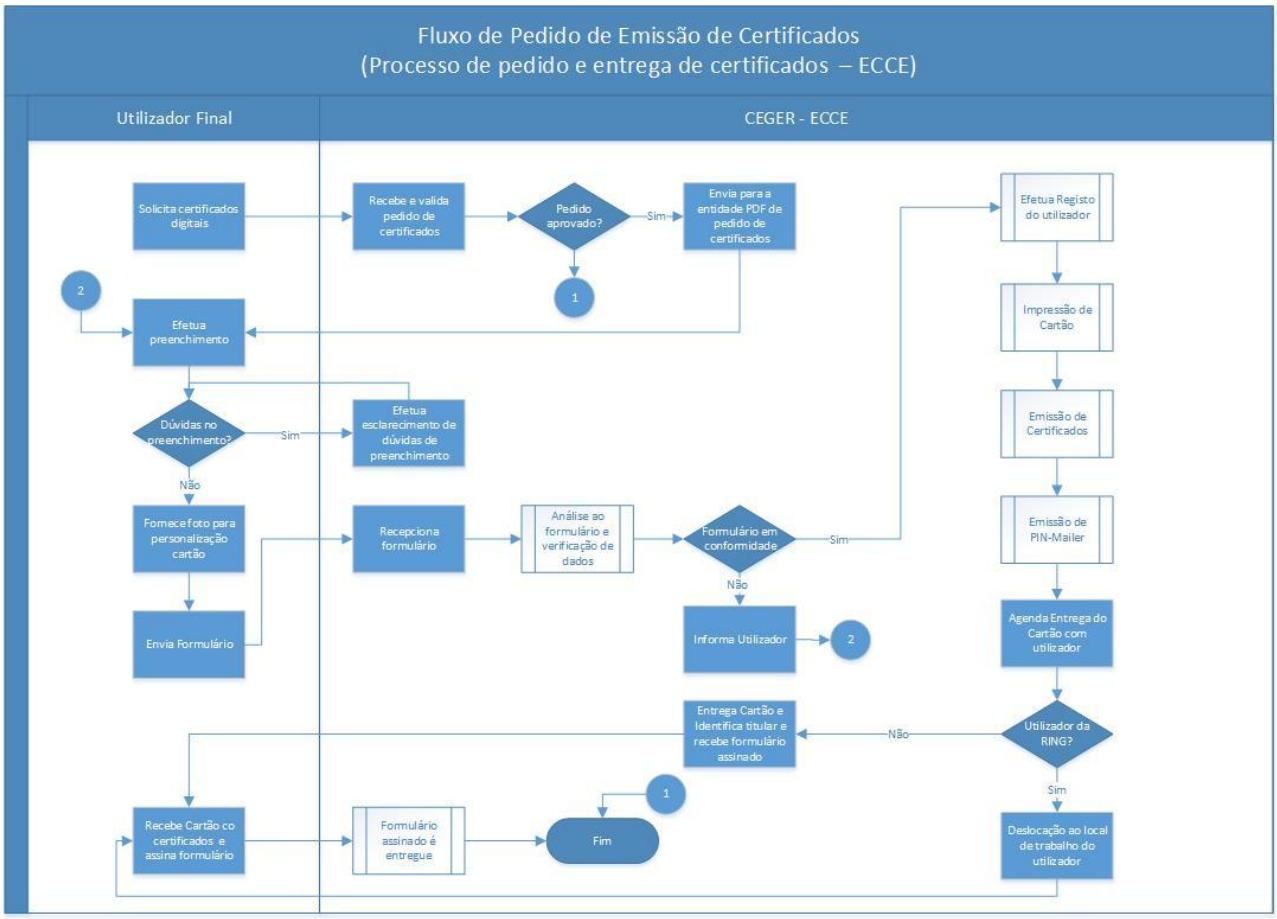

Figura 2 – Fluxo de Pedido de Emissão de Certificados.

3.7.1. 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.

3.7.2. Aprovação ou recusa de pedidos de certificado

A aprovação do certificado passa pelo cumprimento dos requisitos mínimos exigidos no ponto 4.2 da presente 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.

Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

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

3.7.3. 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.

3.8. Emissão de certificado

3.8.1. 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 da renovação 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 pelos sistemas de suporte às tarefas de operação de registo.

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.

3.8.2. Notificação da emissão do certificado ao titular

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

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

3.9. Aceitação do certificado

3.9.1. Procedimentos para a aceitação de certificado

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

3.9.2. Publicação do certificado

Não é efetuada a publicação de certificados emitidos.

3.9.3. Notificação da emissão de certificado a outras entidades

Não aplicável.

3.10. Uso do certificado e par de chaves

3.10.1. 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 Política 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 as seguintes finalidades:

- Certificado de Autenticação: autenticação perante os sistemas de informação das respetivas entidades que exijam a comprovação da identidade do titular mediante certificado eletrónico;
- Certificado de Assinatura: assinatura eletrónica de correio eletrónico, 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 correio eletrónico, cifra de arquivos e cifra de transações.

3.10.2. Uso do certificado e da chave pública pelos correspondentes

Na utilização do certificado e da chave pública, as partes confiantes apenas podem confiar nos certificados, tendo em conta apenas o que é estabelecido na presente DPC.

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network
Management Centre
Presidency of the Council of Ministers

Para isso devem, entre outras, garantir o cumprimento das seguintes condições:

a) Ter conhecimento, bem como o entendimento da utilização e funcionalidades proporcionadas pela criptografia de chave pública e certificados;
b) Ser responsável pela sua correta utilização;
c) Ler e entender os termos e condições descritos nas políticas e práticas de certificação;
d) Verificar os certificados (validação de cadeias de confiança) e LCR, tendo especial atenção às suas extensões marcadas como críticas e propósito das chaves;
e) Confiar nos certificados, utilizando-os sempre que estes estejam válidos.

3.11. Renovação de certificados

Não suportada pela ECCE.

3.11.1. Motivos para renovação de certificado

Não aplicável.

3.11.2. Quem pode submeter o pedido de renovação de certificado

Não aplicável.

3.11.3. Processamento do pedido de renovação de certificado

Não aplicável.

3.11.4. Notificação de emissão de novo certificado ao titular

Não aplicável.

3.11.5. Procedimentos para aceitação de certificado

Não aplicável.

3.11.6. Publicação de certificado após renovação

Não aplicável.

3.11.7. Notificação da emissão do certificado a outras entidades

Não aplicável.

3.12. 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.

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

3.12.1. 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 da presente DPC serão realizadas com mudança de chaves.

3.12.2. Quem pode submeter o pedido de certificação de uma nova chave pública

A renovação deverá ser solicitada respetivamente pelo titular do certificado.

3.12.3. 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 como um novo pedido. As regras para validação da informação são as dispostas nos pontos 3.2.2 e 3.2.3 da presente DPC.

A ER da ECCE valida toda a informação submetida, nos termos do ponto 3.2.2 da presente DPC 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 da presente DPC.

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 esse 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.

3.12.4. 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;

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

- 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).

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

Aplicam-se os mesmos critérios que para a emissão inicial (ver ponto 4.4.1 da presente DPC).

3.12.6. 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 da presente DPC).

3.12.7. Notificação da emissão de novo certificado a outras entidades

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

3.13. 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 da presente DPC.

Em consequência, não são aplicados os pontos 4.8.1 a 4.8.7 da presente DPC.

3.13.1. Motivos para alteração de certificado

Não aplicável.

3.13.2. Quem pode submeter o pedido de alteração de certificado

Não aplicável.

3.13.3. Processamento do pedido de alteração de certificado

Não aplicável.

3.13.4. Notificação da emissão de certificado alterado ao titular

Não aplicável.

3.13.5. Procedimentos para aceitação de certificado alterado

Não aplicável.

3.13.6. Publicação do certificado alterado

Não aplicável.

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

3.13.7. Notificação da emissão de certificado alterado a outras entidades

Não aplicável.

3.14. Suspensão e revogação de certificado

A revogação e suspensão de Certificados são mecanismos a utilizar no pressuposto que, por alguma causa estabelecida na PCert do SCEE 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 operação 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.

3.14.1. Motivos para a revogação

Um certificado emitido pela ECCE pode ser revogado 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 revogado 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.

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

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

1. O utilizador 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 e/ou responsável 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.

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 expressa da Direção do Organismo responsável pelo titular;
3. Por decisão da ECCE, quando comprovada a 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.

3.14.2. 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 da presente DPC;
- A pessoa ou organização que fez o pedido do certificado, em nome de uma organização;
- 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 da presente DPC.

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

3.14.3. 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.

É estalecido o seguinte fluxo de operação:

- 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.

3.14.4. Produção de efeitos da revogação

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

3.14.5. 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.

3.14.6. 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).

3.14.7. Periodicidade da emissão da Lista de Certificados Revogados (LCR)

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

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network
Management Centre
Presidency of the Council of Ministers

3.14.8. Período máximo entre a emissão e a publicação da LCR

Conforme o estipulado no ponto 4.9.7 da presente DPC.

3.14.9. 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 da presente DPC.

3.14.10. 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.

3.14.11. Outras formas disponíveis para divulgação de revogação

Não aplicável.

3.14.12. Requisitos especiais em caso de comprometimento de chave privada

Apenas quando se trate do comprometimento da chave privada da ECCE. Neste caso deverão ser adotados os procedimentos descritos na secção 5.7.3. da presente DPC.

3.14.13. 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 levantamento da sua suspensão;
- Resolução judicial ou administrativa que assim o determine.

3.14.14. Quem pode submeter o pedido de suspensão

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

3.14.15. Procedimentos para pedido de suspensão

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

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

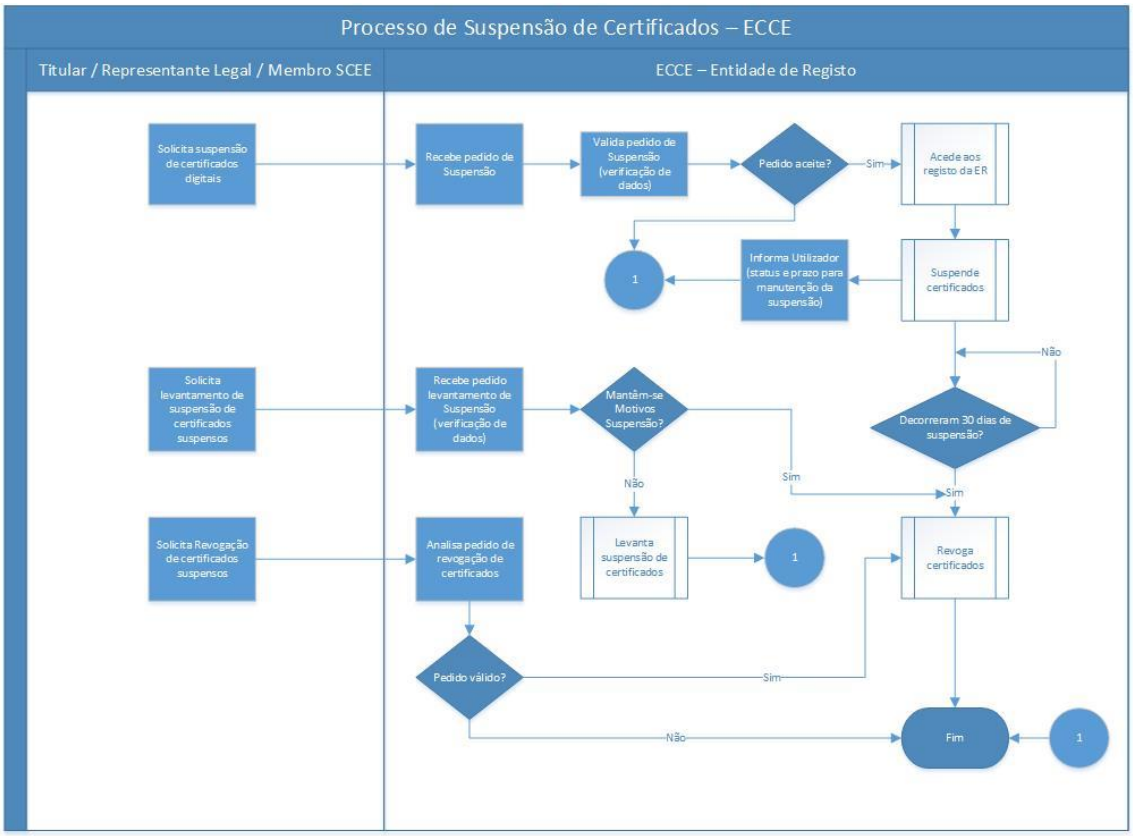

Figura 3 – Processo de Pedido de Suspensão de Certificados.

3.14.16. 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 o mesmo caduca, ou é solicitada a sua revogação, seguem-se os procedimentos utilizados relativamente aos certificados não suspensos nos casos de caducidade e revogação.

3.15. Serviços sobre o estado do certificado

3.15.1. Características operacionais

Não aplicável.

3.15.2. Disponibilidade de serviço

Não aplicável.

3.15.3. Características opcionais

Não aplicável.

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

3.16. Fim de subscrição

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

- Revogação do certificado por qualquer das causas descritas no ponto 4.9.1. da presente DPC;
- Caducidade da vigência do certificado.

3.17. Retenção e recuperação de chaves (*key escrow*)

3.17.1. Políticas e práticas de recuperação de chaves

Não aplicável.

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

Não aplicável.

4. MEDIDAS DE SEGURANÇA FÍSICA, DE GESTÃO E OPERACIONAIS

4.1. 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.

4.1.1. 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 teto e pavimento construído com materiais similares aos das paredes, não tem qualquer janela, sendo totalmente fechado. As suas portas são em aço (alma) e armações igualmente em aço, com características corta-fogo e antivandalismo e com fechaduras acionáveis eletronicamente e respetivas barras antipânico.

A Zona de Alta Segurança (ZAS) tem com 4 *layers* de proteção perimétrica, de forma a controlar o acesso físico 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.

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

A ECCE mantém planos de Recuperação de Incidentes e Continuidade de Serviço para as operações da sua EC, bem como um Plano de Cessação da sua Atividade, global ou parcial.

As instalações de secundárias estão protegidas pelos mesmos níveis de segurança que o local primário.

4.1.2. 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 videovigilância e de gravação, sistemas de deteção de intrusões, entre outros.

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

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

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.

4.1.3. 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.

4.1.4. Exposição à água

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

4.1.5. 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.

4.1.6. 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 os referenciais e com dupla fechadura. O acesso a estas zonas é restrito a pessoas devidamente autorizadas.

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

4.1.7. 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 respetivos fabricantes.

4.1.8. Instalações externas (alternativa) para recuperação de segurança

Todas as cópias de segurança (ex.: base de dados, programas, *file system*) são colocadas num sítio remoto que está geograficamente separado do sítio primário. O acesso físico ao sítio remoto é restrito ao pessoal autorizado. O local remoto está protegido pelos mesmos níveis de segurança que o local primário.

4.2. 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 dos procedimentos considera-se matéria confidencial, sendo os mesmos explicados de forma resumida.

4.2.1. 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*).

4.2.1.1. 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;

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network
Management Centre
Presidency of the Council of Ministers

- 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.

4.2.1.2. 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.

4.2.1.3. 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 detetadas;
- 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.

4.2.1.4. 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.

4.2.1.5. 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;

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network
Management Centre
Presidency of the Council of Ministers

- 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.

4.2.1.6. 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 HSM 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.

4.2.1.7. 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 utilizar dois cartões de operador, num leitor do HSM. 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 da *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.

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

4.2.2. 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 multiutilizador 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.

4.2.3. 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.

4.2.4. Funções 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).

4.3. Medidas de segurança de pessoal

4.3.1. 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.

4.3.2. Procedimentos de verificação de antecedentes

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

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

4.3.3. 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.

4.3.4. 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 Políticas de Certificação ou Declaração de Práticas de Certificação serão realizadas sessões formativas aos elementos da ECCE.

4.3.5. Frequência e sequência da rotação de funções

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

4.3.6. 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.

4.3.7. 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.

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network
Management Centre
Presidency of the Council of Ministers

4.3.8. 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.

4.4. Procedimentos de auditoria de segurança

4.4.1. 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 registados possuem, como mínimo, a seguinte informação:

Categoria: indica a importância do evento;

- Informativo: os eventos desta categoria contêm informação sobre operações realizadas com êxito;
- Marca: cada vez que começa e termina uma sessão de administração, regista-se um evento desta categoria;
- Advertência: indica que se detetou um acontecimento não habitual durante uma operação, mas não provocou uma falha na operação;

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

- 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.

4.4.2. 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 anual.

4.4.3. 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.

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

4.4.5. Procedimentos para a cópia de segurança dos registos

São realizadas cópias de segurança de acordo com a Políticas de Cópias de Segurança da ECCE.

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

4.4.6. 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, detetando 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 eletrónicas;
- Guarda um registo histórico de atualização dos dados, armazenando versões sucessivas de cada registo 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 são detetáveis com as provas de integridade são:

- Inserção ou alteração fraudulenta de um registo 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.

4.4.7. Notificação da causa do evento

Não é necessária qualquer notificação quando um evento é auditado.

4.4.8. 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.

4.5. Arquivo de registos

4.5.1. Tipo de dados arquivados

As informações e eventos que são registados são:

1. Os registos de auditoria especificados no ponto 5.4 da presente DPC;

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network
Management Centre
Presidency of the Council of Ministers

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) Identidade do operador que emitiu o Certificado;
   c) Data da última identificação direta do titular.
4. Acordos de confidencialidade;
5. Autorizações de acesso aos sistemas de informação.

4.5.2. 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.

4.5.3. Proteção dos arquivos

O Acesso 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.

4.5.4. 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 antifogo, dentro da Sala Segura da ECCE. Uma outra cópia é realizada de forma cifrada e será armazenada num cofre antifogo na sala segura alternativa (local).

4.5.5. Requisitos para validação cronológica dos registos

Os sistemas de informação da ECCE garantem o registo 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.

4.5.6. Sistema de recolha de dados de arquivo (interno/externo)

O sistema de arquivo é interno à ECCE.

4.5.7. 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.

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

4.6. Renovação de chaves

Não aplicável. A renovação de chaves consiste na emissão de novo par de chaves conforme descrito nas secções 4.1 e 4.2.

4.7. Recuperação em caso de desastre ou comprometimento

Em caso de desastre ou comprometimento, serão seguidos os procedimentos previstos no Plano de Contingência e Continuidade de Serviço da ECCE, que será ativado em caso de uma indisponibilidade máxima de 24 horas, estando preparada para a emissão de LCR antes das 12 horas seguintes.

4.7.1. 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.

4.7.2. 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.

4.7.3. 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 os titulares/subscritores e as entidades deste facto, bem como as restantes entidades que compõem o SCEE e a Entidade Supervisora.

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.

4.7.4. Capacidade de continuidade da atividade em caso de desastre

Conforme o Plano de Contingência e Continuidade de Serviço da ECCE.

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

4.8. Procedimentos em caso de extinção da ECCE ou ER

A ECCE dispõe de um Plano de Cessação da Atividade, podendo esta ser global ou parcial.

5. MEDIDAS DE SEGURANÇA TÉCNICAS

5.1. 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.

5.1.1. 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 respetivo par de chaves gerado num módulo criptográfico, de acordo com requisitos definidos no ponto 6.2.1da presente 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).

5.1.2. 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.

5.1.3. 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.

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

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.

5.1.4. Entrega da chave pública da ECCE aos correspondentes/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 estará à disposição dos titulares de certificados e terceiras partes confiantes para realizar qualquer tipo de comprovação.

5.1.5. Dimensão das chaves

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

- Nivel 1 (EC Raíz): RSA 4096 bit;
- Nivel 2 (EC Subordinada): RSA 2048 bit;
- O Tamanho mínimo para certificados pessoais e certificados de componentes ou servidores é de RSA 2048 bit.

5.1.6. 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.

5.1.7. 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 6. 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
Certificado de Controlador de Dominio	• digitalSignature • keyEncipherment	• serverAuth • clientAuth

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

5.2. Proteção da chave privada e características do módulo criptográfico

5.2.1. 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.

5.2.2. 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.

5.2.3. Retenção da chave privada (key escrow)

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

5.2.4. 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.

5.2.5. 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.

5.2.6. 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.

5.2.7. Armazenamento da chave privada no módulo criptográfico

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

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.

5.2.8. 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;
- Administrador de Sistemas;
- Administrador de Segurança.

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

5.2.9. 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;
- Administrador de Sistemas;
- Administrador de Segurança.

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

5.2.10. 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 respetivas cópias de segurança devem também ser alvo de destruição.

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

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

- 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).

5.2.11. Avaliação/nível do módulo criptográfico

Conforme o descrito no ponto 6.2.1 da presente DPC.

5.3. Outros aspetos da gestão do par de chaves

5.3.1. 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 da presente DPC, para verificação de assinaturas geradas durante o seu prazo de validade.

5.3.2. 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 7. 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.

5.4. Dados de ativação

5.4.1. 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.

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

A ECCE utiliza dispositivos/mecanismos criptográficos (*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 respetivos dados de ativação.

5.4.2. 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, por essa razão, o único responsável pela ativação e proteção dos dados de ativação das suas chaves privadas.

5.4.3. Outros aspetos dos dados de ativação

Não aplicável.

5.5. 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 Política de Certificados e os *standards* aplicáveis.

5.6. 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.

A ECCE segue as boas práticas estabelecidas na norma ISO27001:2005.

5.6.1. 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.

5.7. 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.

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

5.7.1. 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.

5.7.2. 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.

5.7.3. 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 formação e 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.

5.8. 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:

- Está devidamente protegida, quer por *Firewalls*, quer por equipamentos de deteção de intrusão (IDS/IPS);

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

- 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 às ferramentas de operação de registo são efetuados através;
- De canal seguro e encriptado, recorrendo à utilização de SSL e certificados digitais.

5.9. 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 Política de Validação Cronológica da ECCE (o documento encontra-se disponível no repositório da ECCE).

6. PERFIS DE CERTIFICADO, CRL E OCSP

6.1. 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.

6.1.1. 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.

6.1.2. Extensões do certificado

Todos os sistemas das várias entidades deverão processar corretamente todas as extensões identificadas no RFC 3280.

6.1.2.1. 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).

6.1.2.2. 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

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

mesmo "*subject*" e que sejam facilmente diferenciadas. O valor utilizado é um *hash* da chave pública que consta no campo do certificado "*subjectPublicKeyInfo*".

6.1.2.3. KeyUsage

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

Especificado na secção 6.1.7 da presente DPC.

6.1.2.4. certificatePolicies

Extensão obrigatória e não critica. Esta extensão lista as Políticas de Certificados que dão suporte e regem o ambiente em que se processou a emissão do certificado. Deve incluir o OID das Políticas de Certificados.

6.1.2.5. 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 ativo ("*True*"), caso contrário o processo de verificação do certificado falha.

Discriminam-se, nas tabelas seguintes, os perfis dos certificados emitidos pela ECCE.

Tabela 8. Perfil do Certificado de Assinatura.

CAMPO	CONTEÚDO	EXTENSÕES CRÌTICAS
Campos de X509v1		
1. Versão	V3	
2. Serial Number	Aleatório	
3. Signature Algorithm	SHA256WithRSAEncryption	
4. Issuer Distinguished Name	CN=ECCE 002, OU=ECEstado, O=Centro de Gestão da Rede Informática do Governo, 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		

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

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	
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 (2) HTTP: http://crls.ecce.gov.pt/crls/crl-002.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(1): URL=http://trust.ecce.gov.pt/ecce-001.crt Alternative Name(2): 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	

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

Tabela 9. Perfil do Certificado de Confidencialidade.

CAMPO	CONTEÚDO	EXTENSÕES CRÍTICAS
Campos de X509v1		
1. Versão	V3	
2. Serial Number	Aleatório	
3. Signature Algorithm	SHA256WithRSAEncryption	
4. Issuer Distinguished Name	CN=ECCE 002, OU=ECEstado, O=Centro de Gestão da Rede Informática do Governo, 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(1.3.6.1.5.5.7.3.4)	**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**

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

Subject Type	End Entity	
Path Length Constraint	None	
12. CRLDistributionPoints	(1) HTTP: http://crls.ecce.gov.pt/crls/crl-001.crl (2) HTTP: http://crls.ecce.gov.pt/crls/crl-002.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 (1): URL=http://trust.ecce.gov.pt/ecce-001.crt Alternative Name (2): URL=http://trust.ecce.gov.pt/ecce-002.crt	**NÃO**
14.netscapeCertType	SMIME	
15. netscapeRevocationURL	Não aplicável	
16. netscapeCAPolicyURL	Não aplicável	
17. netscapeComment	Não aplicável	

Tabela 10. Perfil do Certificado de Autenticação.

CAMPO	CONTEÚDO	EXTENSÕES CRÍTICAS
Campos de X509v1		
1. Versão	V3	
2. Serial Number	Aleatório	
3. Signature Algorithm	SHA256WithRSAEncryption	
4. Issuer Distinguished Name	CN=ECCE 002, OU=ECEstado, O=Centro de Gestão da Rede Informática do Governo, 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	

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

CAMPO	CONTEÚDO	EXTENSÕES CRÍTICAS
Key Encipherment	0	
Data Encipherment	0	
Key Agreement	1	
Key Certificate Signature	0	
CRL Signature	0	
4.extKeyUsage	clientAuth(1.3.6.1.5.5.7.3.2), smartCardLogon(1.3.6.1.4.1.311.20.2.2)	**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**
Subject Type	End Entity	
Path Length Constraint	None	
12. CRLDistributionPoints	(1) HTTP: http://crls.ecce.gov.pt/crls/crl-001.crl (2) HTTP: http://crls.ecce.gov.pt/crls/crl-002.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(1): URL=http://trust.ecce.gov.pt/ecce-001.crt Alternative Name(2): URL=http://trust.ecce.gov.pt/ecce-002.crt	**NÃO**
14.netscapeCertType	SSL Client Authentication	
15. netscapeRevocationURL	Não aplicável	
16. netscapeCAPolicyURL	Não aplicável	
17. netscapeComment	Não aplicável	

6.1.3. Identificadores de algoritmo

Na tabela seguinte indicam-se os identificadores de algoritmos:

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

Tabela 11. 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

6.1.4. 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.

6.1.5. 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 de certificados de cartões de assinatura qualificada, o DN é:

CN = <Nome do Titular>
OU = <Unidade Orgânica do Titular>
O = <Organismo do Titular>
C = PT

6.1.6. Objeto identificador da política de certificado

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

6.1.7. Utilização da extensão de restrição de políticas

Não aplicável.

6.1.8. 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*.

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

6.1.9. 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 respetivos, tendo em conta a sua aplicação.

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

6.2. Perfil da LCR

6.2.1. Número(s) da versão

As LCR emitidas pela ECCE, implementam a versão 2 padrão ITU X.509, de acordo com o RFC 3280.

6.2.2. Extensões da LCR e das suas entradas

O SCEE define como extensões de LCR obrigatórias, não críticas, 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 12. Perfil da LCR e suas Extensões.

CAMPO	CONTEÚDO	EXTENSÕES CRÍTICAS
CRL 001		
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	

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

CAMPO	CONTEÚDO	EXTENSÕES CRÍTICAS
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	
CRL 002		
Version	V2	
Signature		
AlgorithmIdentifier		
Algorithm	SHA-1WithRSAEncryption	
Parameters		
IssuerName	CN = ECCE 002 OU = ECEstado O = Centro de Gestão da Rede Informática do Governo C = PT	
ThisUpdate	Data de emissão	
validityPeriod	24 horas	
NextUpdate	24 horas	
revokedCertificates		
Usercertificate		
CertificateSerialNumber		
revocationDate		
crlEntryExtension		
reasonCode		**Não**

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

CAMPO	CONTEÚDO	EXTENSÕES CRÍTICAS
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-002.crl	**Não**
onlyContainsUserCerts	0	
onlyContainsCACerts	0	
IndirectCRL		
DeltaCRLIndicator	Não é utilizado	**Sim**
BaseCRLNumber	Este valor será igual ao do CRLNumber	

6.3. *Time-Stamping Authority* (TSA)

A *Time-Stamping Authority* (TSA) assina eletronicamente 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 13. Perfil do Certificado de Selo de Validação Cronológica.

CAMPO	CONTEÚDO	EXTENSÕES CRÍTICAS
Campos de X509v1		
1. Versão	V3	
2. Serial Number	Aleatório	
3. Signature Algorithm	SHA256WithRSAEncryption	

Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

CAMPO	CONTEÚDO	EXTENSÕES CRÍTICAS
4. Issuer Distinguished Name	CN= ECCE 001, OU=ECEstado, O=SCEE, C=PT	
5. Validity	3 anos	
6. Subject	CN=ECCE-TSA OU=Entidade Certificadora Comum do Estado OU=ECEstado OU=SCEE O=Centro de Gestão da Rede Informática do Governo 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	
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	2.5.29.32.0	
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	Method=OCSP URL=http://ocsp.scee.gov.pt Method=Certification Authority Issuer URL=http://trust.ecce.gov.pt/ecce-001.crt	**NÃO**
14. QC Statment	ETSI TS 101 862 qualified certificates	**NÃO**

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

O selo temporal emitido pela ECCE contém informação do selo (*TSTinfo structure*), 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 OPTIONAL
}

6.4. Perfil do OCSP

No serviço de OCSP implementado, os certificados de *OCSP Responder*, estão em concordância com as 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*".

6.4.1. Número(s) da versão

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

6.4.2. 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 titular no campo "*subject name*".

Tabela 14. Perfil dos Certificados OCSP Responder.

CAMPO	CONTEÚDO	EXTENSÕES CRÍTICAS
Campos de X509v1		
1. Versão	V3	
2. Serial Number	Aleatório	
3. Signature Algorithm	SHA256WithRSAEncryption	
4. Issuer Distinguished Name	CN=ECCE 002, OU=ECEstado, O=Centro de Gestão da Rede Informática do Governo, C=PT	
5. Validity	6 meses	
6. Subject	CN=VA-ECCE, OU=ECEstado, O=SCEE, C=PT	
7. Subject Public Key Info	Algoritmo: RSA Encryption Tamanho mínimo da chave: 2048	

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

CAMPO	CONTEÚDO	EXTENSÕES CRÍTICAS
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	1	
Key Certificate Signature	0	
CRL Signature	0	
4. extKeyUsage	id-kp-OCSPSigning	**SIM**
5. privateKeyUsagePeriod		
		NÃO
Policy Identifier	2.5.29.32.0	
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	URL=http://crls.ecce.gov.pt/crls/crl-001.crl	**NÃO**
13. Auth. Information Access		**NÃO**
14. OCSP No Revocation Checking	Sim	**NÃO**

Ceger. CENTRO DE GESTÃO DA REDE INFORMÁTICA DO GOVERNO

Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt

Government Computer Network
Management Centre
Presidency of the Council of Ministers

7. AUDITORIA E OUTRAS AVALIAÇÕES DE CONFORMIDADE

7.1. Frequência ou motivo da auditoria

A ECCE é alvo de auditoria nas seguintes situações:

- Anualmente;
- A qualquer momento, sem aviso prévio;
- Auditoria interna.

Anualmente será efetuada 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 da presente DPC.

Entre as auditorias a realizar inclui-se uma auditoria anual externa, por entidade acreditada, para o efeito, ao abrigo do Regulamento (EU) n.º 910/2014, do Parlamento Europeu e do Conselho, de 23 de julho (eIDAS).

Os referenciais a auditar são os constantes na tabela abaixo indicada:

Tabela 15. Referenciais a Auditar.

Reference	Short Title	Replaces
EN 319 403 v2.2.2	Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers	TS 119 403 v2.1.1 and v1.1.1
EN 319 401 v2.1.1	General Policy Requirements for Trust Service Providers	EN 319 401
EN 319 411-1 v1.1.1	Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements Note: Incorporates requirements for web site certificates with requirements previously specified in 319 411-3	TS 102 042 EV & Baseline policies EN 319 411-3
EN 319 411-2 v2.1.1	Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates *Note: Extends requirements in part 1 with specific requirements for EU qualified certificates*	EN 319 411-2
EN 319 421 v1.1.1	Policy and Security Requirements for Trust Service Providers issuing ElectronicTime-Stamps	TS 102 023
EN 319 412-1 v1.1.1	Certificate Profiles; Part 1: Overview and common data structures	-
EN 319 412-2 v2.1.1	Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons	TS 119 412-2 & TS 102 280
EN 319 412-3 v1.1.1	Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons	-
EN 319 412-4 v1.1.1	Certificate Profiles; Part 4: Certificate profile for web site certificates issued to organisations	-
EN 319 412-5 v2.1.1	Certificate Profiles; Part 5: QCStatements	EN 319 412-5 v1.1.1 & TS 101 862
EN 319 422 v1.1.1	Time stamping protocol and electronic time-tamp profiles	TS 101 861
TS 119 612	Trusted Lists (see section 3 below)	
Introductory documents		
TR 119 000 v1.2.1 "The framework for standardization of signatures: overview"		
This TR is the enry point for the standards related to digital signatures. It describes the general structure for digital signature standardization and outlining existing and potential standards for such signatures.		
TR 119 001 v1.2.1 on Definitions and abbreviations		
Trust Service Providers Supporting Digital Signatures		
TR 119 400 v1.1.1 on Guidance on the use of standards for trust service providers supporting digital signatures and related services		
Signature Creation and Validation		
TR 119 100 v1.1.1 on Guidance on the use of standards for signatures creation and validation		
TS 119 101 v1.1.1 on Policy and security requirements for applications for signature creation and signature validation Technical requirements		
Signature creation and other related devices		
This area is under the responsibility of CEN TC 224 CEN/TC 224/WG 16 - Application Interface for smart cards used as Secure Signature Creation Devices		
Cryptographic Suites		
TR 119 300 v1.2.1 Business guidance on cryptographic suites		
TS 119 312 v1.1.1 Cryptographic Suites		
Trust Service Status Lists Providers		
TR 119 600 v1.2.1 Business guidance for trust service status lists providers		
TS 119 612 v2.2.1 Trusted Lists		
TS 119 614-1 v1.1.1 Specifications for testing conformance of XML representation of Trusted Lists		

Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

7.2. Identidade e qualificações do auditor

O auditor é uma pessoa ou organização acreditada para o efeito pela Entidade Acreditadora nacional.

7.3. Relação entre o auditor e a entidade certificadora

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

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

O Auditor e a ECCE não devem ter nenhuma relação, atual ou prevista, financeira, legal ou de qualquer outro género que possa originar um conflito de interesses.

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

7.4. Âmbito da auditoria

A auditoria anual obrigatória ao abrigo do Regulamento (EU) n.º 910/2014, do Parlamento Europeu e do Conselho, de 23 de julho (eIDAS), sendo prevista no documento e nas normas técnicas da Entidade Supervisora.

A ECCE efetua auditorias internas no âmbito dos serviços de confiança prestados.

7.5. Procedimentos após uma auditoria com resultado deficiente

As auditorias com resultado deficiente serão tratadas de acordo com o estabelecido no Regulamento (EU) n.º 910/2014, do Parlamento Europeu e do Conselho, de 23 de julho (eIDAS), e nas normas técnicas da Entidade Supervisora.

7.6. Comunicação de resultados

De acordo com o estipulado pelo Regulamento (EU) n.º 910/2014, do Parlamento Europeu e do Conselho, de 23 de julho (eIDAS) e pela Entidade Supervisora.

8. OUTRAS SITUAÇÕES E ASSUNTOS LEGAIS

8.1. Taxas

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

8.1.1. Taxas por emissão ou renovação de certificados

Serão aplicadas as taxas definidas no Despacho 7333/2019, de 08 de agosto.

8.1.2. Taxas para acesso a certificado

Não aplicável.

8.1.3. Taxas para acesso a informação do estado certificado ou de revogação

Não aplicável.

8.1.4. Taxas para outros serviços

Serão aplicadas as taxas definidas no Despacho 7333/2019, de 08 de agosto.

8.1.5. Política de reembolso

ECCE esforça-se para garantir o mais alto nível de qualidade de seus serviços. O reembolso não é aplicável aos serviços prestados pela ECCE.

8.2. Responsabilidade financeira

8.2.1. Seguro de cobertura

Não Aplicável.

8.2.2. Outros recursos

Não aplicável.

8.2.3. Seguro ou garantia de cobertura para utilizadores

Não aplicável.

8.3. Confidencialidade da informação processada

8.3.1. Âmbito da confidencialidade da informação

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

a) As chaves privadas da EC;
b) As chaves privadas dos titulares/subscritores;
c) Toda a informação relativa aos parâmetros de segurança, controlo e procedimentos de auditoria;

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network
Management Centre
Presidency of the Council of Ministers

d) Toda a informação de carácter pessoal proporcionada à EC durante o processo de registo dos subscritores de certificados, salvo se houver autorização explícita para a sua divulgação;
e) Planos de recuperação e continuidade de negócio;
f) Planos de cessação da atividade;
g) Registos de transações, incluindo os registos completos e os registos de auditoria das transações.

8.3.2. Informação não protegida pela confidencialidade

Considera-se informação de acesso público:

a) Declaração de Práticas de Certificação;
b) *Disclosure Statement*, na sua versão em PT e ENG;
c) Os certificados, para efeitos de confidencialidade, desde que declarado na respetiva DPC;
d) LCR e LER;
e) Os dados fornecidos pelo serviço OCSP;
f) Toda a informação classificada como "*pública*".

8.3.3. Responsabilidade de proteção 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 atividades, sobre toda a informação e processos da ECCE.

8.4. Privacidade dos dados pessoais

A ECCE mantém atualizada a sua Política de Privacidade nos seus repositórios, onde se declara o cumprimento das disposições estabelecidas na legislação de proteção de dados pessoais.

8.4.1. Medidas para garantia da privacidade

No cumprimento do estabelecido pela lei nacional e comunitária, a informação de carácter pessoal disponibilizada à ECCE pelos titulares de certificados, deve ser tratada de acordo com o Regulamento Geral de Proteção de Dados (RGPD).

8.4.2. Informação privada

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

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

8.4.3. Informação não protegida pela privacidade

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

Esta informação, proporcionada aquando do pedido de certificado é incluída nos certificados. Esta informação não tem carácter privado/reservado, sendo deste modo pública caso seja consentido pelo titular.

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

a) O período de validade do certificado assim como a data de emissão do certificado e a data de caducidade;
b) O número de série do certificado;
c) Os diferentes estados e situações do certificado e a data do início de cada um deles;
d) As LCR e OCSP, assim como o resto das informações de estado de revogação;
e) A informação contida no Repositório da ECCE.

8.4.4. Responsabilidade de proteção da informação privada

A ECCE garante o cumprimento das suas obrigações, como previsto na presente DPC.

8.4.5. Notificação e consentimento para utilização de informação privada

Para a prestação de serviço, a ECCE obtém o consentimento dos titulares dos dados necessários para a prestação do serviço de certificação.

Considera-se obtido o consentimento por parte do titular com a oposição da assinatura no pedido formulado para prestação do serviço.

8.4.6. Divulgação resultante de processo judicial ou administrativo

A ECCE só poderá fornecer dados e informações consideradas, no âmbito da presente DPC, como informação privada, nos pressupostos em que estes são requeridos pela autoridade pública competente no âmbito da lei.

A ECCE está obrigada a revelar a identidade dos assinantes quando lhes for solicitado pelos órgãos judiciais, no exercício das funções que lhe sejam atribuídas.

8.4.7. Outras circunstâncias para revelação de informação

Não aplicável.

8.5. Direitos de propriedade intelectual

Todos os direitos de propriedade intelectual, incluindo os que se referem a certificados e LCR emitidos, OID, DPC, bem como qualquer outro documento da propriedade da ECCE, pertencem àquela entidade certificadora.

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

As chaves privadas e as chaves públicas são propriedade do titular, independentemente do meio físico que se empregue para o seu armazenamento. O titular conserva sempre o direito sobre as marcas, produtos ou nome comercial contido no certificado.

8.6. Representações e garantias

8.6.1. Representação das EC e garantias

A ECCE está obrigada a:

a) Realizar as suas operações de acordo com a presente DPC;
b) Declarar de forma clara todas as suas Práticas de Certificação no documento apropriado – DPC;
c) Proteger as suas chaves privadas;
d) Emitir certificados de acordo com o previsto na presente DPC;
e) Emitir certificados que estejam conformes com a informação conhecida no momento de sua emissão e livres de erros de *input* de dados;
f) Garantir a confidencialidade no processo da geração dos dados da criação da assinatura e a sua entrega por um procedimento seguro ao titular;
g) Utilizar sistemas e produtos fiáveis que estejam protegidos contra toda a alteração e que garantam a segurança técnica e criptográfica dos processos de certificação;
h) Utilizar sistemas fiáveis para armazenar certificados reconhecidos, que permitam comprovar a sua autenticidade e impedir pessoas não autorizadas altere os dados;
i) Arquivar sem alteração os certificados emitidos;
j) Garantir que podem determinar, com precisão da data e hora, em que emitiu, ou revogou, ou suspendeu um certificado;
k) Empregar pessoal com qualificações, conhecimentos e experiência necessárias para a prestação de serviços de certificação;
l) Revogar os certificados nos termos previstos na presente DPC e publicar os certificados revogados na LCR e OCSP do repositório, com a frequência estipulada na presente DPC;
m) Publicar a sua DPC e as Políticas de Certificado aplicáveis no seu repositório garantindo o acesso às versões atuais assim como as versões anteriores;
n) Notificar, com a rapidez necessária, por correio eletrónico, os titulares dos certificados em caso da ECCE proceder à revogação ou suspensão dos mesmos, indicando o motivo que originou a ação;
o) Colaborar com as auditorias externas, para validar a renovação das suas próprias chaves;
p) Operar de acordo com a legislação aplicável;
q) Proteger as chaves que estejam sobre sua custódia;
r) Garantir a disponibilidade da LCR de acordo com as disposições da presente DPC, bem como a disponibilidade do serviço de OCSP;
s) Em caso de cessar a sua atividade, a ECCE deverá aplicar o seu Plano de Cessação da Atividade;
t) Cumprir com as especificações contidas nas normas sobre Proteção de Dados Pessoais;

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

u) Conservar toda a informação e documentação relativa a um certificado reconhecido e as DPC vigentes em cada momento e durante quinze anos desde o momento da emissão;
v) Disponibilizar os certificados da sua EC e da ECRaizEstado.

8.6.2. Representação das ER e garantias

A ER integrada na ECCE está obrigada a:

a) Realizar suas operações de acordo com esta Política de Certificados;
b) Realizar suas operações de acordo com as DPC da sua EC;
c) Comprovar, rigorosamente, a identidade das pessoas as quais se concede o certificado digital por eles tratado, pelo que requer a presença física da pessoa;
d) Não armazenar nem copiar os dados de criação de assinatura da pessoa a quem tenham prestado os seus serviços;
e) Informar, antes da emissão de um certificado, a pessoa que solicite seus serviços, das obrigações que assume, bem com deve guardar os dados de criação de assinatura e que procedimentos devem seguir para comunicar a perca ou utilização indevida dos dados ou dispositivos de criação ou verificação da assinatura, do seu preço, e das condições precisas para a utilização do certificado bem como das suas limitações de uso;
f) Validar e enviar, de forma segura, à EC a que está subordinada a ER, um pedido de certificação devidamente complementada com a informação fornecida pelo titular e assinada digitalmente e receber os certificados emitidos de acordo com esse pedido;
g) Armazenar de forma segura até ao momento do envio, tanto a documentação fornecida pelo titular como a gerada pela própria ER durante o processo de registo ou revogação;
h) Formalizar o contrato de Certificação com o titular segundo o estabelecido na DPC;
i) Solicitar a revogação de um certificado quando tenha conhecimento ou suspeita de compromisso de uma chave privada;
j) Autenticar os pedidos dos utilizadores finais para a renovação ou revogação de seus certificados, gerar pedidos de renovação ou revogação assinados digitalmente e enviados a sua EC;
k) Em caso de aprovação de um pedido de certificação, notificar o titular a emissão do certificado e a forma de obtê-lo;
l) Em caso de negação de um pedido de certificação, notificar o titular desta recusa e o motivo da mesma;
m) Tratando-se de certificados pessoais, deve utilizar ferramentas de pedido e envio na presença da pessoa;
n) Manter sob controlo restrito as ferramentas de tramitação de certificados digitais e notificar a sua EC, de qualquer mal funcionamento ou outra eventualidade que possa fugir ao comportamento normal;
o) Enviar uma cópia assinada do contracto de certificação e dos seus pedidos de revogação à EC;

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

p) Receber e tratar todos os pedido de revogação presenciais que receba, de forma imediata, depois de levar a cabo a respetiva identificação baseada no DN de quem solicita;
q) Colaborar nos vários aspetos da operação, auditoria ou controlo da ER, se tal lhe for solicitado pela EC;
r) Obrigada a confidencialidade durante e posteriormente, à prestação de serviços como Entidade de Registo, no que diz respeito à informação recebida da EC.

8.6.3. Representação e garantias do titular

É obrigação, entre outras, dos titulares dos certificados emitidos pela ECCE:

a) Limitar e adequar a utilização dos certificados, de acordo com as utilizações previstas na DPC;
b) Tomar todos os cuidados e medidas necessárias para garantir a posse da sua chave privada;
c) Solicitar de imediato a revogação de um certificado, em caso de ter conhecimento ou suspeita de compromisso da chave privada correspondente à chave pública contida no certificado;
d) Não utilizar um certificado digital que tenha perdido a sua eficácia, quer por ter sido revogado, suspendido ou por ter expirado o período de validade;
e) Submeter à ER a informação que considerem exata e completa, com relação aos dados que estas solicitem para realizar o processo de registo. Deve informar a EC de qualquer modificação desta informação;
f) Não monitorizar, manipular ou efetuar ações de "engenharia inversa" sobre a implantação técnica (*hardware* e *software*) dos serviços de certificação, sem a devida autorização prévia, por escrito, de EC.

8.6.4. Representação dos correspondentes (Relying party) e garantias

É obrigação das partes que confiem nos certificados emitidos pela ECCE:

a) Limitar a fiabilidade dos certificados às utilizações permitidas para os mesmos em conformidade com o expresso na DPC;
b) Verificar a validade dos certificados no momento de realizar qualquer operação baseada nos mesmos;
c) Assumir a responsabilidade na correta verificação das assinaturas digitais;
d) Assumir a responsabilidade na comprovação da validade, revogação ou suspensão dos certificados em que confia;
e) Ter pleno conhecimento das garantias e responsabilidades aplicáveis na aceitação e uso de certificados em que confia e aceitar sujeitar-se às mesmas;
f) Notificar qualquer acontecimento ou situação anómala relativa ao certificado, que possa ser considerado como causa de revogação do mesmo, utilizando o endereço de correio eletrónico que consta no sítio da internet da ECCE.

8.6.5. Representação e garantias de outros participantes

Não existem outros participantes.

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

8.7. Renúncia de garantias

A ECCE recusa todas as garantias de serviço que não se encontrem vinculadas nas obrigações estabelecidas na presente DPC.

8.8. Limitações às obrigações

De acordo com a legislação em vigor.

8.9. Indemnizações

De acordo com a legislação em vigor.

8.10. Termo e cessação da atividade

8.10.1. Termo

Esta DPC entra em vigor desde o momento de sua publicação no repositório da ECCE e manter-se-á em vigor 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.

Em caso de cessação de atividade serão seguidos os procedimentos previstos no Plano de Cessão de Atividade.

8.10.2. Substituição e revogação da DPC

Esta DPC será substituída por uma nova versão com independência das mudanças efetuadas 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.

8.10.3. Consequências da conclusão da atividade e sobrevivência

As obrigações e restrições que estabelece esta DPC relativamente a auditorias, informação confidencial, obrigações e responsabilidades perante o 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.

8.11. Notificação individual e comunicação aos participantes

Todos os participantes devem utilizar métodos razoáveis para comunicar neste âmbito.

A ECCE adota como notificação individual e comunicação aos participantes, os seguintes meios:

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network
Management Centre
Presidency of the Council of Ministers

a) Correio eletrónico da certificação da ECCE, para o endereço que consta no formulário de requerimento do serviço de certificação;
b) Formulários eletrónicos;
c) Telefone, para o número indicado no formulário de requerimento do serviço de confiança;
d) Informações disponibilizadas no sítio da Internet (www.ecce.gov.pt);
e) Através de correio postal para a morada indicada no ponto 1.5.2 da presente DPC;
f) Outros meios, previstos na presente DPC, por convênio entre as partes ou legalmente/judicialmente estabelecidos.

As comunicações efetuadas pela ECCE deverão ter em conta a criticidade e o assunto da mesma, bem como as regras estabelecidas na presente DPC.

São estabelecidas as seguintes regras excecionais de comunicação:

a) As previstas no Plano de Cessação da Atividade;
b) As previstas no Processo de Gestão de Incidentes;

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

8.12. Alterações

8.12.1. 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 1.5.1 da presente DPC.

8.12.2. Prazo e mecanismo de notificação

As alterações à presente DPC, são de pelo menos, em períodos anuais, sendo a nova versão publicitada no sítio da *internet* www.ecce.gov.pt.

8.12.3. Motivos para mudar de OID

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

8.13. Disposições para resolução de conflitos

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

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network
Management Centre
Presidency of the Council of Ministers

8.14. Legislação aplicável

A legislação relevante aplicável à atividade da ECCE é a constante do sítio da *internet* www.ecce.gov.pt.

8.15. Conformidade com a legislação em vigor

É responsabilidade da ECCE zelar pelo cumprimento da legislação aplicável reconhecida no ponto anterior.

8.16. Providências várias

8.16.1. Acordo completo

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

8.16.2. 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 efetivas.

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

8.16.3. Severidade

Não estipulado.

8.16.4. Execuções (taxas de advogados e desistência de direitos)

Não estipulado.

8.16.5. Força maior

Não estipulado.

8.17. Outras providências

Não estipulado.

Ceger
Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt
Government Computer Network Management Centre
Presidency of the Council of Ministers

ANEXO A – Acrónimos e Definições

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

Acrónimos

AdmHSM	Administradores de 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 Eletrónica do Estado;
ECEstado	Entidade Certificadora do Estado;
ECRaizEstado	Entidade Certificadora de Raiz do Estado;
EGPC	Entidade Gestora de Políticas 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	Infraestrutura de Chave Pública;
IDS/IPS	*Intrusion Detection System / Intrusion Prevention System*;
IETF	*Internet Engineering Task Force*;
LCR	Lista de Certificados Revogados;
LDAP	*Lightweight Directory Access Protocol*;
LER	Lista de 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;

Ceger

Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt

Government Computer Network
Management Centre
Presidency of the Council of Ministers

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 correção de irregularidades;
RFC	*Request For Comments*;
RPI	Relatório de primeiras impressões;
RSA	Algoritmo criptográfico (Rivest | Shamir | Adleman);
RSAE	Relatório Sumário de Análise de Eventos;
subECEstado	Entidade Certificadora Subordinada de uma ECEstado;
TCP/IP	*Transmission Control Protocol/Internet Protocol*;
TRT	Termo de Responsabilidade do Titular;
OID	Identificador de Objeto;
URL	*Unified Resource Locator*;

Definições

Assinatura digital	Modalidade de assinatura eletrónica avançada baseada em sistema criptográfico assimétrico composto de um algoritmo ou série de algoritmos, mediante o qual é gerado um par de chaves assimétricas exclusivas e interdependentes, uma das quais privada e outra pública, e que permite ao titular usar a chave privada para declarar a autoria do documento eletrónico ao qual a assinatura é aposta e concordância com o seu conteúdo e ao destinatário usar a chave pública para verificar se a assinatura foi criada mediante o uso da correspondente chave privada e se o documento eletrónico foi alterado depois de aposta a assinatura;
Assinatura eletrónica avançada	Assinatura eletrónica que preenche os seguintes requisitos: • 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 detetar toda e qualquer alteração superveniente do conteúdo deste;

Ceger

Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt

Government Computer Network Management Centre
Presidency of the Council of Ministers

Assinatura eletrónica qualificada	Assinatura digital ou outra modalidade de assinatura eletrónica avançada que satisfaça exigências de segurança idênticas às da assinatura digital baseadas num certificado qualificado e criadas através de um dispositivo seguro de criação de assinatura;
Assinatura eletrónica	É o resultado de um processamento eletrónico de dados suscetível de constituir objeto de direito individual e exclusivo e de ser utilizado para dar a conhecer a autoria de um documento eletrónico;
Autoridade credenciadora	Entidade competente para a credenciação e fiscalização das entidades certificadoras;
C	Atributo do DN de um objeto dentro da estrutura de diretório X.500;
Certificado	Estrutura de dados assinado eletronicamente por um prestador de serviços de certificação e que vincula ao titular os dados de validação de assinatura que confirma a sua identidade;
Chave privada	Elemento do par de chaves assimétricas destinado a ser conhecido apenas pelo seu titular, mediante o qual se apõe a assinatura digital no documento eletrónico, ou se decifra um documento eletrónico previamente cifrado com a correspondente chave pública;
Chave pública	Elemento do par de chaves assimétricas destinado a ser divulgado, com o qual se verifica a assinatura digital aposta no documento eletrónico pelo titular do par de chaves assimétricas, ou se cifra um documento eletrónico a transmitir ao titular do mesmo par de chaves;
Chave	Sequência de símbolos;
CN	Atributo do DN de um objeto dentro da estrutura de diretório X.500.
Credenciação	Ato pelo qual é reconhecido a uma entidade que o solicite e que exerça a atividade de entidade certificadora o preenchimento dos requisitos definidos no presente diploma para os efeitos nele previstos;
Dados de ativação	Dados privados, diferentes das chaves, exigidos para o acesso aos módulos criptográficos;
Dados de criação de assinatura	São dados únicos, como códigos ou chaves criptográficas privadas que o titular utiliza para gerar a sua assinatura eletrónica;
Dados de criação de assinatura	Conjunto único de dados, como chaves privadas, utilizado pelo titular para a criação de uma assinatura eletrónica;
Dados de verificação de assinatura	São dados como códigos ou chaves criptográficas públicas, que se utilizam para verificar a assinatura eletrónica;
Dados de verificação de assinatura	Conjunto de dados, como chaves públicas, utilizado para verificar uma assinatura eletrónica;
Declaração de Práticas de Certificação	Documento onde são especificados ao pormenor a forma como Prestador de Serviços de Certificação realiza as atividades relacionadas com a gestão do ciclo de vida do certificado;
Diretório de certificados:	Repositório de informação que segue o standard X500;
Dispositivo de criação de assinatura	Suporte lógico ou dispositivo de equipamento utilizado para possibilitar o tratamento dos dados de criação de assinatura;
Dispositivo seguro de criação de assinatura	Dispositivo de criação de assinatura que assegure, através de meios técnicos e processuais adequados, que: • 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;

Ceger

Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt

Government Computer Network Management Centre
Presidency of the Council of Ministers

	• 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 diretório X.500;
Documento eletrónico	Conjunto de dados lógicos armazenados em suporte suscetível de poder ser lido por equipamentos eletrónicos de processamento de dados;
Endereço eletrónico	Identificação de um equipamento informático adequado para receber e arquivar documentos eletrónicos;
Entidade certificadora	Entidade ou pessoa singular ou coletiva que cria ou fornece meios para a criação e verificação das assinaturas, emite os certificados, assegura a respetiva publicidade e presta outros serviços relativos a assinaturas eletrónicas;
Entidade de Registo	Entidade ou pessoa singular ou coletiva designada pelas Entidades Certificadoras para realizar atividades de comprovação da identidade dos subscritores ou titulares e consequente registo, bem como a gestão de pedidos de revogação de certificados;
Função *hash*	É uma operação que se realiza sobre um conjunto de dados de qualquer tamanho de forma que o resultado obtido é outro conjunto de dados de tamanho fixo independente do tamanho original e que tem a propriedade de estar associado univocamente aos dados inicias e garantir que é impossível obter mensagens distintas que gerem o mesmo resultado ao aplicar esta função;
***Hash* ou impressão digital**	Resultado de tamanho fixo que se obtém após a aplicação de uma função *hash* a uma mensagem e que cumpre a requisito de estar associado univocamente aos dados iniciais;
HSM	Módulo de seguridad criptográfico empleado para almacenar claves y realizar operaciones criptográficas de modo seguro;
Infraestrutura de Chave Pública	Estrutura de hardware, software, pessoas, processos e políticas que usa a tecnologia de assinatura digital para dar a terceiros de confiança uma associação verificável entre a componente pública de um par de chaves assimétrico e um assinante específico;
LCR	Lista de certificados revogados que é criada e assinada pela EC que emitiu os certificados. Um certificado é introduzido na lista quando é revogado (por exemplo, por suspeita de comprometimento da chave). Em determinadas circunstâncias, a EC pode dividir uma LCR num conjunto de LCR mais pequenas;
LER	Lista de certificados de outras CA revogados. Uma ARL é equivalente a uma CRL para os certificados cruzados com outras CA;

Ceger

Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt

Government Computer Network Management Centre
Presidency of the Council of Ministers

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 objeto dentro da estrutura de diretório X.500;
OCSP	protocolo que permite a comprovação do estado do certificado no momento em que o mesmo é utilizado;
OCSP responder	Servidor que responde segundo o protocolo OCSP aos pedidos OCSP com o estado do certificado;
OID	O identificador alfanumérico/numérico único registado em conformidade com a norma de registo ISO, para fazer referência a um objeto específico ou a uma classe de objetos específica;
OU	Atributo do DN de um objeto dentro da estrutura de diretório X.500;
Pedido OCSP	Pedido de consulta de estado de um certificado a um OCSP Responder;
PIN	*Personal Identification Number*;
PIN	número específico apenas conhecido pela pessoa que tem de aceder a um recurso que se encontra protegido por este mecanismo;
PKCS	Conjunto de standard desenvolvido pela RSA *Labs* aceite internacionalmente para definição da sintaxe a utilizar com a criptografia de chave pública;
PKIX	Grupo de trabalho do IETF constituído para desenvolver as especificações relacionadas com PKI e Internet;
Time *stamping*	Constatação da data e hora de um documento eletrónico mediante processos criptográficos, para datar os documentos de forma objetiva;
SHA	Desenvolvido pelo NIST e revisto em 1994 (SHA-1). Este algoritmo consiste em transformar mensagens de menos de 264 bits e gerar um resumo de 160 bits de comprimento. A probabilidade de encontrar duas mensagens distintas que produzam o mesmo resumo é praticamente nula, por esse motivo utiliza-se para assegurar a integridade dos documentos durante o processe de assinatura eletrónica;
SmartCard	Cartão criptográfico utilizado pelo titular para armazenar chaves privadas de assinatura e ou cifra. Os *smartcards* são considerados dispositivos seguros de criação de assinatura e de acordo com a lei permite a geração de assinatura eletrónica qualificadas;
Titular	Pessoa singular ou coletiva identificada num certificado como a detentora de um dispositivo de criação de assinatura;
Validação cronológica	Declaração de entidade certificadora que atesta a data e hora da criação, expedição ou receção de um documento eletrónico;
X.500	Standard desenvolvido pelo ITU que define as recomendações de um diretório. Corresponde ao standard ISO 9594-1;
X.509	Standard desenvolvido pelo ITU que define o formato eletrónico dos certificados eletrónicos;
Zona de alta segurança	Área de acesso controlado através de um ponto de entrada e limitada a pessoal autorizado devidamente credenciado e a visitantes devidamente acompanhados. As zonas de alta segurança devem estar encerradas em todo o seu perímetro e ser vigiadas 24 horas por dia, 7 dias por semana, por pessoal de segurança, por outro pessoal ou por meios eletrónicos.

Ceger

Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt

Government Computer Network Management Centre
Presidency of the Council of Ministers

ANEXO B – Formulários para Emissão de Certificados

O formulário disponibilizado aos titulares de certificados da ECCE para pedido de emissão de certificados está anexado ao Documento de Declaração de Práticas de Certificação na sua versão PDF.

FIM DO DOCUMENTO

Centro de Gestão da Rede Informática do Governo
Av. Defensores de Chaves, nº6 – 6ºPiso • 1049-063 Lisboa
PORTUGAL (+351) 213 923 400
certificacao@ecce.gov.pt • www.ecce.gov.pt

Government Computer Network
Management Centre
Presidency of the Council of Ministers