DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO DA ENTIDADE CERTIFICADORA DA JUSTIÇA

VERSÃO 1.5

DATA: Março de 2014

Tipologia documental: Política

Título: Declaração de Práticas de Certificação

Língua original: Português

Língua de publicação: Português

Nível de acesso: Público

Data: 10-03-2014

Versão atual: 1.5

Autoria: Sandra Mendonça..... **Data:** 10-03-2014

Verificação: Claudia Carvalho..... **Data:** 17-03-2014

Aprovação: Carlos Brito / Nuno Fonseca/ Sousa Mendes / Joel Timóteo..... **Data:** 18-03-2014

Identificação da EC: EC da Justiça

Histórico de Versões

N.º de Versão	Data	Autor(es)
1.0	27/02/2009	Claudia Carvalho
1.1	11/03/2011	Claudia Carvalho
1.2	07/03/2012	Claudia Carvalho
1.3	22/01/2013	Claudia Carvalho
1.4	27-09-2013	Claudia Carvalho

Índice Geral

1 Introdução

A presente Declaração de Práticas de Certificação (DPC) descreve as práticas e os procedimentos empregues pelo Instituto de Gestão Financeira e Equipamentos da Justiça (IGFEJ), enquanto entidade certificadora da Justiça (EC Justiça), nos termos da alínea r) do nº 2 do art.º 14º do Decreto-Lei nº 123/2011.

Os serviços de certificação prestados envolvem, entre outros, a emissão, suspensão, revogação e renovação de certificados digitais X.509 v3[1], de acordo com as especificações indicadas nas respetivas Políticas de Certificado (PC), assim como a gestão das listas de certificados revogados (CRL) e dos serviços de diretório X.500[2].

Os serviços fornecidos destinam-se, somente, a utilizadores (pessoas singulares e servidores Web e de Domain Controller (DC)) pertencentes a domínios que integrem a Justiça, estando a utilização do certificado de pessoa singular restrita ao âmbito da atividade profissional do titular enquanto vinculado ao organismo a que pertence. Exceções a esta regra são devidamente autorizadas e documentadas pelo Grupo de Gestão da EC Justiça.

1.1 Âmbito

A presente DPC é designada por "Declaração de Práticas de Certificação da Entidade Certificadora da Justiça", e comummente referida como "DPC Justiça".

A finalidade desta DPC é a de notificar as pessoas que se encontram em situação de utilizar ou de confiar nos certificados digitais emitidos pelo IGFEJ dos seus direitos e obrigações, assim como de as informar sobre as práticas e os procedimentos utilizados pela Entidade Certificadora.

A estrutura da DPC segue o definido pelo RFC 3647[3] (no entanto, algumas das suas secções, por não se aplicarem à estrutura e aos serviços oferecidos pela Entidade Certificadora, não se encontram contempladas) e respeita e implementa o *standard* RFC 5280[4].

Os Certificados emitidos pela EC Justiça contêm uma referência ao DPC de modo a permitir que as Partes Confiantes possam encontrar informação sobre o certificado e sobre a entidade que o emitiu.

A atividade do IGFEJ como Entidade Certificadora para a Justiça, engloba uma Entidade de Registo (ER) e uma Entidade de Certificação (EC).

---

[1] ITU-T Recommendation X.509 Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.

[2] ITU-T Recommendation X.500 Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services.

[3] RFC 3647. November 2003, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

[4] RFC 5280 May 2008, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

A menos que o contrário seja explicitamente declarado, sempre que se fizer referência a Entidade Certificadora consideram-se abrangidos todos os serviços fornecidos pela ER e pela EC.

Esta DPC satisfaz os requisitos impostos pela Política de Certificados do SCEE[5] (Sistema de Certificação Eletrónica do Estado) especificando como implementar os seus procedimentos e controlos e ainda como a EC Justiça atinge os requisitos especificados.

1.2 Identificação do Documento

Este documento é a Declaração de Práticas de Certificação da EC Justiça. A DPC é representada num certificado através de um número único designado de "identificador de objeto" (OID), sendo o valor do OID associado a este documento o 2.16.620.1.1.1.2.6.2. Este documento de DPC é identificado pelos dados constantes na seguinte tabela:

INFORMAÇÃO DO DOCUMENTO	
Versão do Documento	Versão 1.5
Estado do Documento	Aprovado
OID	2.16.620.1.1.1.2.6.2
Data de Emissão	Março 2014
Validade	1 ano
Localização	http://icp.igfej.mj.pt/resources/documentos/CPS.pdf

1.3 Participantes na Infraestrutura de Chaves Públicas

São vários os tipos de entidades que preenchem o perfil de participante numa ICP.

1.3.1 Entidades Certificadoras

A EC Justiça insere-se na hierarquia de confiança do SCEE, constituindo-se numa Entidade Certificadora do Estado (ECEstado), sendo o seu certificado assinado pela entidade certificadora da cadeia de certificação do SCEE (i.e., pela Entidade Certificadora Raiz do Estado Português (ECRaizEstado)). Deste modo, a EC Justiça encontra-se no nível imediatamente abaixo da ECRaizEstado, sendo a sua função principal providenciar a gestão

[5] Política de Certificados da SCEE e requisitos mínimos de Segurança, versão 1.0, Julho 2006.

de serviços de certificação: emissão, operação, suspensão e revogação para os seus subscritores.

A EC Justiça emite certificados de:

- Assinatura de pessoas singulares;
- Autenticação de pessoas singulares;
- Cifra para pessoas singulares;
- *Software*;
- Servidores Web;
- Servidores DC;
- *Code signing*;

O tamanho da chave RSA da EC Justiça é de 4096 bits. Um dispositivo de *hardware* seguro (HSM), com certificação de conformidade com os requisitos de segurança FIPS 140-2, nível 3, é utilizado para gerar e permitir o armazenamento e destruição da chave privada da EC Justiça. A operação deste dispositivo obriga à presença conjunta de dois funcionários autorizados.

O quadro seguinte apresenta os dados mais relevantes relativos aos certificados da EC Justiça, sendo de destacar a adoção da emissão de dois certificados (pkcs1-sha1WithRSAEncryption e pkcs1-sha256WithRSAEncryption), para o mesmo par de chaves.

DN	**CN=Justica; OU=ECEstado; O=SCEE; C=PT**
	Certificado pkcs1-sha1WithRSAEncryption
Número de série	3d6c 218c 41e1 d27e 46e8 ff1b f9b0 2472
Período de validade	De 13/09/2007 10:12:59 a 13/09/2019 10:12:59
Impressão digital	d9e5 2ce6 b203 37ec b1cb 130c d60a dd71 1d72 1727
	Certificado pkcs1-sha256WithRSAEncryption
Número de série	3e02 2678 6a82 91aa 46e8 fe36 e8d7 bce7
Período de validade	De 13/09/2007 10:09:10 a 13/09/2019 10:09:10
Impressão digital	01df 349f c495 4520 db88 dac4 6b8a 5272 b111 7015

1.3.2 Entidades de Registo

A Entidade de Registo (ER) é a entidade que aprova os nomes distintos (DN) dos utilizadores finais e mediante avaliação do pedido, aprova ou rejeita a solicitação de certificados. Para além disso, a ER também tem autoridade para aprovar a revogação ou suspensão de certificados e publicar no diretório público as chaves públicas de cifra dos titulares pessoas singulares.

1.3.3 Titulares de Certificados

1.3.3.1 Titulares

No contexto deste documento, o termo subscritor/titular aplica-se a todos os utilizadores finais a quem tenham sido atribuídos certificados por uma EC do Estado ou EC subordinada do Estado.

De acordo com as regras do SCEE, são considerados titulares de certificados emitidos pela EC Justiça, aqueles cujo nome está inscrito no campo *Subject* do certificado e utilizam o certificado e respetiva chave privada de acordo com o estabelecido nas diversas políticas de certificado, sendo emitidos certificados para as seguintes categorias de titulares:

- Pessoa singular – certificados de Autenticação, de Cifra e de Assinatura Qualificada;
- Equipamentos tecnológicos – certificados para servidor Web, servidores DC, *software* e *Code Signing*.

1.3.3.2 Patrocinadores

A emissão de certificados para equipamentos é efetuada sempre sob responsabilidade humana.

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

1.3.4 Partes confiantes

As partes confiantes ou destinatários são pessoas singulares, entidades ou equipamentos que confiam na validade dos mecanismos e procedimentos utilizados no processo de associação do nome do titular com a sua chave pública, ou seja confiam que o certificado corresponde na realidade a quem diz pertencer.

Nesta DPC, considera-se uma parte confiante, aquela que confia no teor, validade e aplicabilidade do certificado emitido no "ramo" da EC Justiça da hierarquia de confiança do SCEE, podendo ser titular de certificados da comunidade SCEE ou não.

1.3.5 Outros Participantes

1.3.5.1 Autoridade Credenciadora

De acordo com a Política de Certificação do SCEE.

1.3.5.2 Entidades Externas

Entidades que prestam serviços de suporte à EC Justiça, responsáveis pelas seguintes funções:

- Licenciamento, suporte e manutenção da aplicação que gere a infraestrutura de chaves públicas;

- Acesso ao *middleware* e respetivos serviços de suporte e assistência técnica para o correto funcionamento dos *smartcards* emitidos pela EC Justiça;
- Serviços de utilização de espaço físico que reúne os requisitos técnicos e de segurança necessários (ZAS - Zona de Alta Segurança) para a instalação da infraestrutura.
- Serviços de utilização de espaço físico para os restantes componentes que compõem a ICP e que não requerem um nível de segurança tão elevado como o referenciado no ponto anterior.

1.4 Utilização do Certificado

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

- Controlo de acessos;
- Confidencialidade;
- Integridade;
- Autenticação e
- Não-repúdio.

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

Esta política engloba tipos de certificados descritos sumariamente no quadro abaixo:

Tipo de utilização	Identificador	OID
Assinatura pessoal	scee-assinatura	2.16.620.1.1.1.2.10
Autenticação pessoal	scee-autenticação	2.16.620.1.1.1.2.20
Confidencialidade pessoal	scee-confidencialidade	2.16.620.1.1.1.2.30
Autenticação de servidores Web	SSL Server	2.16.620.1.1.1.2.6.1.1.3
Autenticação de servidores DC	Domain Controller	2.16.620.1.1.1.2.6.1.1.5
Assinatura de código	CodeSigning	2.16.620.1.1.1.2.6.1.1.4
Assinatura/Autenticação de dados	Software	2.16.620.1.1.1.2.6.1.1.9

1.4.1 Utilização adequada

Os requisitos e regras definidos neste documento aplicam-se a todos os certificados emitidos pela EC Justiça.

Os certificados emitidos pela EC Justiça são utilizados pelas Partes Confiantes para verificação da cadeia de confiança daquela, assim como para garantir a autenticidade e identidade do emissor de uma assinatura digital gerada pela chave privada correspondente à chave pública contida num certificado emitido sob a EC Justiça.

Os certificados da EC do Justiça regulamentados por esta DPC serão utilizados para prestar os seguintes serviços de segurança:

Tipo de certificado	Uso apropriado
Assinatura	Assinatura Eletrónica Qualificada
Autenticação	Autenticação perante os sistemas e serviços
Confidencialidade	Cifra de comunicações e informações
Servidores Web	Autenticação do servidor e estabelecimento de comunicação mediante protocolo SSL
Servidores DC	Antenticação do servidor e estabelecimento de tráfego LDAP seguro
Code Signing	Assinatura de Código a disponibilizar na Internet
Software	Assinatura/Autenticação de dados

1.4.2 Utilização não autorizada

Os certificados poderão ser utilizados noutros contextos apenas na extensão do que é permitido pelas regras do SCEE e pela legislação aplicável.

Os certificados emitidos pela EC Justiça não poderão ser utilizados para qualquer função fora do âmbito das utilizações descritas anteriormente.

Os serviços de certificação oferecidos pela EC Justiça, não foram desenhados nem estão autorizados a ser utilizados em atividades de alto risco ou que requeiram um atividade isenta de falhas, como as relacionadas com o funcionamento de instalações hospitalares, nucleares, controlo de tráfego aéreo, controlo de tráfego ferroviário, ou qualquer outra atividade onde uma falha possa levar à morte, lesões pessoais ou danos graves para o meio ambiente.

Qualquer uso não incluído na secção anterior fica excluído.

1.5 Gestão das Políticas

1.5.1 Entidade responsável pela gestão do documento

A gestão desta Declaração de Práticas de Certificação é da responsabilidade do Grupo de Gestão da EC da Justiça.

1.5.2 Contacto

NOME	ENTIDADE GESTORA DA ENTIDADE DE CERTIFICAÇÃO ELECTRÓNICA DA JUSTIÇA
Gestor	Grupo de Gestão da EC da Justiça
Morada	Avenida D. João II, nº 1.08.01E, Torre H, Piso 17, 1990-097 Lisboa
Correio eletrónico	AdminCa@igfej.mj.pt
Página Internet	**http://icp.igfej.mj.pt**
Telefone	+ 351 21 318 90 00
Fax	+ 351 21 350 60 23

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

A DPC é aprovada por deliberação do Grupo de Gestão da EC Justiça e posteriormente pelo Conselho Gestor do SCEE.

1.5.4 Procedimentos para aprovação da DPC

A elaboração da DPC e seguintes correções (ou atualizações) deverão ser submetidas à aprovação do Grupo de Gestão da EC Justiça. As correções (ou atualizações) deverão ser publicadas sob a forma de novas versões desta DPC, substituindo qualquer DPC anteriormente definida.

A DPC é revista/atualizada com uma periodicidade máxima de 1 ano, ou sempre que, antes desse prazo, se verifique qualquer alteração nas práticas ou procedimentos adotados.

Qualquer alteração da DPC só entra em vigor após aprovação pelo Grupo de Gestão da EC Justiça. Este deverá apresentar esta nova versão ao Conselho Gestor do SCEE, que procederá à avaliação da conformidade com a sua Política de Certificados.

1.6 Definições e Acrónimos

Para uma boa interpretação do apresentado no documento, apresenta-se a lista dos acrónimos que surgem neste, bem como a definição de alguns termos considerados importantes.

Lista de Acrónimos:

CRL	Certificate Revocation List
CWA	CEN Workshop Agreement
DC	Domain Controller

DN	Distinguished Name
DPC	Declaração de Práticas de Certificação
C	Country
CC	Comon Criteria
CN	Comon Name
CNPD	Comissão Nacional de Proteção de Dados
CSR	Certificate Signing Request
EC	Entidade de Certificação
SCEE	Sistema de Certificação Eletrónica do Estado
ECEstado	Entidade Certificadora do Estado
EC Justiça	Entidade Certificadora da Justiça
ECRaizEstado	Entidade Certificadora de Raiz do Estado
ER	Entidade de Registo
ERL	Entidade de Registo Local
ETSI	European Telecommunications Standard Institute
FIPS	Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
GNS	Gabinete Nacional de Segurança
HSM	Hardware Security Module.
HTTP	HyperText Transfer Protocol
ICP	Infra-Estrutura de Chaves Públicas
IGFEJ	Instituto de Gestão Financeira e Equipamentos da Justiça
MJ	Ministério da Justiça
O	Organization
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OU	Organization Unit
PC	Política de Certificados
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
RFC	Request For Comments
RSA	Algoritmo criptográfico (Rivest | Shamir | Adleman)

SAN	Subject Alternative Name
SSCD	Secure Signature Creation Device
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
ZAS	Zona de Alta Segurança

Lista de Definições:

Algoritmo

Sequência de instruções para efetuar determinado processo passo a passo.

Browser

Programa que permite navegar na Internet

S/MIME

Secure Multipropose Internet Mail Extensions – *Standard* para envio de correio eletrónico seguro. O protocolo MIME define como uma mensagem eletrónica é organizada e suportada pela maioria das aplicações de correio eletrónico. O S/MIME constrói segurança sobre aquele protocolo ao permitir informação cifrada e a inclusão de um certificado digital como componentes da mensagem.

SSL

Secure Sockets Layer – Protocolo não proprietário desenvolvido pela Netscape que providencia segurança em comunicações consideradas sensíveis. É aceite como um *standard* Web para comunicações cliente-servidor autenticadas e cifradas, sendo tipicamente utilizado entre *browsers* e servidores. Permite confidencialidade, autenticidade e integridade sob a forma de conexões cifradas, autenticação de servidores e clientes e integridade das mensagens. Necessita de utilizar certificados digitais.

Como é que o SSL funciona?

- O cliente e o servidor trocam informação segura. É o designado "*handshaking*";
- O cliente apresenta a identificação da sessão, os algoritmos de encriptação e os métodos de compressão por ele suportados;
- O servidor faz a sua seleção usando esta informação. Se tal for requerido, ambos trocam certificados;
- O servidor define uma chave de sessão apropriada para o algoritmo de cifra, na fase do "*handshaking*".

Servidor e cliente poderão a partir deste momento comunicar de forma segura.

TLS

Transport Layer Security – Baseado em SSL. Parte integrante dos *browsers* de clientes e de servidores.

2 Responsabilidade de Publicação e Repositório

2.1 Repositórios

Um repositório é o conjunto de equipamentos (*hardware* e *software*), pessoas e procedimentos, construído com o objetivo de publicar, entre outras, informação para os titulares/destinatários, sobre os certificados e CRL).

O repositório está disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, sendo acessível através da página http://icp.igfej.mj.pt.

É obrigação da Entidade Certificadora publicar as chaves públicas de cifra dos utilizadores pessoais, assim que os correspondentes certificados são emitidos e cuja publicação foi devidamente aprovada pelos seus titulares, de forma a poderem ser publicamente acedidas. Estas podem ser consultadas e/ou descarregados em http://icp.igfej.mj.pt/faces/PesquisaCertificados.jsp. Estes também são publicados nas respetivas contas de utilizador na *Active Directory* do Ministério da Justiça (MJ).

Também estão publicados os certificados da hierarquia de certificação da EC Justiça em http://icp.igfej.mj.pt/faces/DownloadCertificadoCA.jsp.

2.2 Publicação de informação de certificação

A Entidade Certificadora compromete-se a publicar, a seguinte informação:

- Política de Certificados da SCEE e requisitos mínimos de segurança (http://www.scee.gov.pt/NR/rdonlyres/A50AAF96-F464-4A42-8A62-A80AE5A18633/0/PCert_SCEE_V1.pdf);
- Políticas de certificação disponíveis em http://icp.igfej.mj.pt/faces/Politica.jsp:
  - ✓ Declaração de Práticas de Certificação;
  - ✓ Política de Certificados para Pessoa Singular (Assinatura);
  - ✓ Política de Certificados para Pessoa Singular (Autenticação);
  - ✓ Política de Certificados para Pessoa Singular (Confidencialidade);
  - ✓ Política de Certificados para Servidores Web;
  - ✓ Política de Certificados para Servidores DC;
  - ✓ Política de Certificados para Assinatura de Código;
  - ✓ Política de Certificados para Software;
  - ✓ Declaração de Divulgação de Princípios.
- Lista de Certificados Revogados disponível em http://icp.igfej.mj.pt/crl/crl-itij.crl.
- Documentação de suporte (apenas acessível na intranet da Justiça):
  - ✓ Autorização para emissão de certificado digital – Pessoa Singular (http://icp.igfej.mj.pt/resources/documentos/Autorizacao_Emissao_Certificado_Digital_Pessoa_Singular.doc);
  - ✓ Condições Gerais do Contrato de Emissão de Certificado Digital da EC Justiça (http://icp.igfej.mj.pt/resources/documentos/condicoes_gerais_do_contrato.pdf);
  - ✓ Autorização para emissão de certificado digital – Servidores Web (http://icp.igfej.mj.pt/faces/EmissaoCertificadoServidoresWeb.jsp)

- ✓ Autorização para emissão de certificado digital – Domain Controllers (http://icp.igfej.mj.pt/faces/EmissaoCertificadoServidoresWeb.jsp)
- ✓ Autorização para emissão de certificado digital – Assinatura de código (http://icp.igfej.mj.pt/faces/EmissaoCertificadoAssinaturaCodigo.jsp)
- ✓ Autorização para emissão de certificado digital – Software (http://icp.igfej.mj.pt/faces/EmissaoCertificadoSoftware.jsp)
- ✓ Pedido de revogação de certificado digital – Pessoa singular (http://icp.igfej.mj.pt/resources/documentos/Pedido%20Revogacao%20Certificado%20Digital_Pessoa_Singular.doc);
- ✓ Pedido de revogação de certificado digital – Servidor http://icp.igfej.mj.pt/resources/documentos/Pedido%20Revogacao%20Certificado%20Digital_Servidor.doc;
- ✓ Pedido de revogação de certificado digital – Assinatura Código http://icp.igfej.mj.pt/resources/documentos/Pedido%20Revogacao%20Certificado%20Digital_Code_Signing.doc;
- ✓ Pedido de revogação de certificado digital – Software (http://icp.igfej.mj.pt/faces/PedidoRevogacao.jsp);
- ✓ Autorização para modificação de certificado digital – Pessoal Singular (http://icp.igfej.mj.pt/resources/documentos/Autorizacao_Modificacao_Certificado_Digital_Pessoa_Singular.doc)

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

2.3 Periodicidade de Publicação

A documentação incluída nos repositórios deverá ser atualizada sempre que haja alteração da informação disponibilizada e revista numa base anual.

A CRL deverá ser atualizada sempre que houver uma revogação/suspensão ou a cada 12 horas, sendo a sua validade de 24 horas.

2.4 Controlo de acesso aos repositórios

O acesso ao repositório é público, sem qualquer restrição de acesso, efetuado através de qualquer navegador de Internet utilizando o protocolo HTTP (Porta TCP/80).

O IGFEJ garante, através de controlos de acesso apropriados, que apenas os seus funcionários competentes e designados especialmente para esse fim, têm privilégios de escrita ou alteração das referidas informações.

3 Identificação e Autenticação

3.1 Atribuição de nomes

A atribuição de nomes segue a seguinte convenção:

- aos certificados de pessoa singular é atribuído o nome real do titular, ou pseudónimo;
- aos certificados de equipamentos tecnológicos é atribuído o nome qualificado do domínio (FQDN).

3.1.1 Tipos de nomes

Os titulares de certificados emitidos pela EC Justiça têm um DN, de acordo com o standard X.500 que os identifica unívoca e inequivocamente no âmbito da ICP da Justiça.
Os certificados atribuídos a cada entidade deverão conter no campo "*Subject*" um DN para utilização como identificador único de cada entidade, de acordo com o preconizado no RFC 5280 pelo que:

- Os certificados de pessoa singular apresentam a organização a que o titular pertence;
- Os certificados de equipamentos tecnológicos apresentam a organização responsável pela sua operação (patrocinador).

3.1.2 Necessidade de nomes significativos

O uso de nomes significativos possibilita determinar a identidade da pessoa ou organização a que se referem, para a identificação dos titulares dos respetivos certificados.

A ER assegura que o conjunto de atributos que constituem o DN tem um valor significativo e identifica unívoca e inequivocamente o titular do certificado.

A EC Justiça irá assegurar, dentro da sua hierarquia de confiança:

- a não existência de certificados que, tendo o mesmo nome único identifiquem entidades distintas,
- 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 (com exceção dos certificados com pseudónimos).

3.1.3 Anonimato ou pseudónimo dos titulares

A EC Justiça emite certificados com pseudónimo de titulares, garantindo para o efeito que:

- o certificado contém o pseudónimo do titular, claramente identificado como tal, através da colocação da palavra "pseudo:" antes daquele;
- conserva os elementos que comprovam a verdadeira identidade dos requerentes titulares de certificados com pseudónimo;
- a ER reserva-se o direito de recusar a aceitação de pseudónimos considerados ostensivos;

– comunicará à autoridade judiciária, sempre que esta o ordenar nos termos legalmente previstos, os dados relativos à identidade dos titulares de certificados que sejam emitidos com pseudónimo seguindo-se, no aplicável, o regime do artigo 182.º do Código de Processo Penal.

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

3.1.4 Interpretação de formato de nomes

Os certificados emitidos contêm o campo *subject*) não vazio, preenchido com o DN, que identifica unívoca e inequivocamente o indivíduo ou o equipamento tecnológico, de acordo com a norma ITU-T X.500 (ISO/IEC 9594-1)[6].

As regras utilizadas para interpretar o formato dos nomes seguem o estabelecido no RFC 5280 assegurando que todos os atributos *DirectoryString* dos campos *Issuer* e *Subject* do certificado são codificados numa *UTF8String*, com exceção dos atributos *Country* e *SerialNumber* que são codificados numa *PrintableString*.

3.1.5 Unicidade de nomes

A unicidade dos certificados é efetuada tendo em conta o conteúdo do *Subject Alternative Name* (SAN), mais concretamente o atributo *RFC822 Name*. A ER assegura que não é emitido mais que um certificado por perfil para o mesmo SAN. Exceção a esta regra ocorre nos 2 meses anteriores à expiração do certificado, em que é permitido proceder à renovação do mesmo com geração de novo par de chaves (*certificate re-key*).

3.1.6 Reconhecimento, autenticação e funções das marcas registadas

Não aplicável.

3.2 Validação de identidade no registo inicial

Os certificados da EC Justiça são emitidos para equipamentos tecnológicos ou para pessoas físicas que são funcionários ou agentes, com ou sem poderes de representação, de organismos que pertencem à Justiça.

A ligação do titular do certificado ao organismo a que pertence tem de ser satisfatoriamente comprovada:

a) Certificados para pessoas físicas
É obrigatório que o registo inicial seja efetuado presencialmente, isto é, a validação da identidade do requerente é feita pelo método “cara-a-cara”.
A ER só aprovará o pedido de emissão de certificado após receção de uma declaração, assinada pelo responsável do organismo/superior hierárquico, em que é comprovada a

[6] ITU-T Recommendation X.500 (11/2008) | ISO/IEC 9594-1:2008, Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services

ligação profissional da pessoa ao organismo e autorizada a emissão do respetivo certificado. Essa declaração pode ser enviada através de documento eletrónico ao qual é aposta uma assinatura digital, ou, por escrito, com assinatura autógrafa.
A falta da declaração, no prazo máximo de seis semanas após subscrição do pedido, implica a rejeição, pela ER, do pedido de emissão de certificado.

b) Certificados equipamento tecnológico
A ER só aprovará o pedido de emissão de certificado após receção de uma declaração, assinada pelo responsável técnico (patrocinador), em que é comprovada a responsabilidade técnica pela aplicação/projeto em causa. Essa declaração pode ser enviada através de documento eletrónico assinado digitalmente, ou, por escrito, com assinatura autógrafa.
A falta da declaração, no prazo máximo de dez dias úteis após subscrição do pedido, implica a rejeição, pela ER, do pedido de emissão de certificado.

3.2.1 Método de comprovação da posse de chave privada

No caso das pessoas singulares, os pares de chaves e respetivos certificados são fornecidos em cartão com chip criptográfico, personalizado fisicamente para o titular. A posse da chave privada é garantida pelo processo de personalização do chip, através do Ciclo de Vida do Certificado, que garante que:

- As chaves privadas são geradas no chip criptográfico do cartão, personalizado para o titular das mesmas;
- Um conjunto de parâmetros integrantes da chave privada é enviado para a EC para geração das correspondentes chaves públicas e emissão dos respetivos certificados digitais, sendo estes, tal como aquelas, arquivados no chip;
- Os certificados apenas são ativados (mantendo-se no estado “suspenso” até lá) pelo próprio titular, mediante alteração do PIN inicial enviado para o endereço pessoal do mesmo (*vide* ponto 3.2.3).

No caso do equipamento tecnológico, a comprovação da posse da chave privada será garantida através da apresentação, por parte do patrocinador, do pedido de certificado (CSR) no formato PKCS#10, acompanhado do respetivo documento de autorização de emissão de certificado (*vide* ponto 3.2.4).

3.2.2 Autenticação da identidade de uma pessoa coletiva

Não aplicável.

3.2.3 Autenticação da identidade de uma pessoa singular

A comprovação da identidade da pessoa singular é realizada, pela ER, em duas fases:

— Através do contrato assinado pelo requerente onde constam os seguintes elementos:

- ✓ Nome completo[7];
- ✓ Nº do cartão de identificação[7];
- ✓ Endereços profissional[8] e não profissional;
- ✓ Categoria/função profissional[8];
- ✓ E-mail profissional[9];
- ✓ Indicação quanto ao uso do certificado ser restrito a determinados tipos de utilização[10].

— Através da declaração do responsável/superior hierárquico do organismo a que o requerente pertence, onde constam, entre outros, os seguintes elementos:

- ✓ Instituto/organismo a que pertence;
- ✓ Serviço;
- ✓ Cargo.

A indicação da necessidade de associação de um pseudónimo ao titular será devidamente fundamentada, mediante ofício assinado pelo responsável pelo organismo que o solicita.

3.2.4 Autenticação da identidade de um patrocinador

Relativamente ao pedido de emissão de certificados para equipamento tecnológico, a ER assegura o arquivo da documentação utilizada para verificação da identidade do patrocinador, garantindo que o mesmo tem os poderes bastantes de representante nomeado pela entidade para a emissão do certificado em causa.

O documento que serve de base ao registo do pedido do certificado de equipamento tecnológico contém, entre outros, os seguintes elementos:

- Denominação do organismo/instituição;
- Identificação do patrocinador (nome completo, cargo e contacto);
- Indicação de que o certificado digital de equipamento tecnológico é emitido para a entidade, na hierarquia de confiança da SCEE, de acordo com a presente DPC;
- DN a ser atribuído ao certificado;
- Informação relativa à identificação e aos poderes do patrocinador nomeado pela entidade para efetuar o pedido do certificado digital de equipamento tecnológico no formato PKCS#10;

O certificado e restantes dados necessários serão entregues ao patrocinador.

3.2.5 Informação de subscritor/titular não verificada

Toda a informação descrita no ponto 3.2.3 é verificada.

[7] Validados por intermédio de um documento de identificação legal (Bilhete de Identidade/Cartão de Cidadão, Passaporte, Cartão Militar ou cartão de identificação estrangeiro, no caso de países pertencentes à Comunidade Europeia)
[8] Validados por intermédio da declaração do responsável/superior hierárquico
[9] Validado mediante pesquisa na *Active Directory* do RCJ
[10] Comunicado no documento "Condições Gerais de Contrato de Emissão de Certificado Digital", anexo ao Contrato

3.2.6 Validação dos poderes de autoridade ou representação

Não aplicável.

3.2.7 Critérios para interoperabilidade

Não aplicável.

3.3 Identificação e autenticação para pedidos de renovação de chaves

Não aplicável.

3.4 Identificação e autenticação para pedido de revogação

Qualquer entidade integrada no domínio do SCEE entre outras como, nomeadamente:

- Titular do certificado, no caso de certificados de pessoa singular;
- Responsável máximo do organismo a que o titular pertence, no caso de certificados de pessoa singular;
- Patrocinador nomeado pela entidade, no caso de certificado de equipamento tecnológico;
- Parte confiante, sempre que demonstre que o certificado foi utilizado com fins diferentes dos previstos;
- ER, sempre que se verifique um motivo plausível para o efeito;

pode solicitar a revogação de um determinado certificado, havendo conhecimento ou suspeita de comprometimento da chave privada do titular ou do equipamento tecnológico ou qualquer outro ato que recomende esta ação.

A EC Justiça guarda toda a documentação utilizada para verificação da identidade e autenticidade da entidade que efetua o pedido de revogação.

Um formulário próprio serve de base ao pedido de revogação de certificado de titular e de equipamento tecnológico e contém, entre outros, os seguintes elementos de identificação da entidade que inicia o pedido de revogação:

- Nome completo, organismo a que pertence e cargo/função que desempenha, para uma identificação inequívoca da entidade (ou seu representante) que inicia o pedido de revogação;
- Endereço ou outras formas de contacto;
- Indicação do pedido de revogação, indicando o DN e o SAN atribuídos ao certificado, assim como a sua validade;
- Indicação do motivo para revogação do certificado.

Este formulário poderá ser assinado digitalmente e entregue por correio eletrónico para o *e-mail* da Administração de Registo (pki@igfej.mj.pt), caso o seu autor seja detentor de um certificado de assinatura qualificada. Caso contrário, será remetido normalmente.

O pedido de revogação poderá ser iniciado telefonicamente[11]. Neste caso, até ao envio do formulário acima referido, encontrar-se-á no estado suspenso. Se ao fim de 3 dias o levantamento não for efetuado, será automaticamente revogado.

[11] Exceto as Partes Confiantes

4 Requisitos Operacionais do Ciclo de Vida do Certificado

4.1 Pedido de certificado

4.1.1 Quem pode subscrever um pedido de certificado

Os certificados da EC Justiça são emitidos para equipamento tecnológico e para pessoas físicas (funcionários ou agentes, com ou sem poderes de representação) pertencentes a organismos da Justiça.

4.1.2 Processo de registo e de responsabilidades

4.1.2.1 Pedido de certificado para pessoa singular

Os pedidos de certificados quando chegam à EC já se encontram com os titulares devidamente identificados e autenticados pela ER e pelas ERL's.

O registo inicial do requerente tem de cumprir o estabelecido no ponto 3.2.

O requerente tem a responsabilidade de fornecer aos Serviços da ER ou às ERL's, toda a informação por elas solicitada e tem de garantir a sua veracidade.

É de salientar que nem toda a informação solicitada aparecerá no certificado e que aquela constará do processo do titular, sendo conservado o registo, em papel, durante 20 anos. O armazenamento destes dados encontra-se devidamente autorizado pela CNPD.

Importa referir que o facto de se efetuar um pedido de certificado, não significa que este seja emitido. Tal requer o cumprimento por parte do requerente dos requisitos estabelecidos na DPC, caso contrário a ER tem a legitimidade para negar o pedido de certificado.

4.1.2.2 Pedido de certificado para equipamento tecnológico

Para se efetuar um pedido de certificado deste tipo, o patrocinador deverá preencher o documento correspondente ao certificado em questão (*Software*, *Code Signing*, Servidor) indicando os dados que pretende que constem naquele. Este documento será assinado e autenticado com o selo branco do organismo. Caso o patrocinador possua certificado digital qualificado, poderá enviar o documento assinado digitalmente.

Para além deste documento, no caso dos certificados para servidor, deverá ser enviado através de correio eletrónico cifrado ou por suporte magnético, o CSR originado pelo servidor em questão.

4.2 Processamento do pedido de certificado

O pedido de certificado digital para pessoa singular, depois de recebido pela ER, é considerado válido se os seguintes requisitos forem cumpridos:

- O formulário está corretamente preenchido;
- O contrato de Emissão de Certificado Digital foi assinado quer pelo requerente quer pelo operador da ERL;
- A declaração do responsável/superior hierárquico do organismo a que o requerente pertence foi devidamente assinada e autenticada com o selo branco do organismo.

4.2.1 Processos para a identificação e funções de autenticação

De acordo com o estipulado nos pontos 3.2 e 3.2.3 ou 3.2.4, conforme sejam certificados para pessoa singular ou para equipamento tecnológico, respetivamente.

4.2.2 Aprovação ou recusa de pedidos de certificado

A aprovação do certificado passa pelo cumprimento dos requisitos exigidos nos ponto 3.2.3. ou 3.2.4 e 4.2. Quando tal não se verifique, a ER pode recusar a emissão do certificado.

Uma notificação automática a informar a rejeição, será enviada ao requerente.

4.2.3 Prazo para processar os pedidos de certificados

Os pedidos de certificados serão processados sem atrasos, a partir do momento em que toda a documentação exigida esteja na posse da ER. Dentro do possível, a ER processará os pedidos de certificados em menos de 24 horas.

4.3 Emissão de certificado

4.3.1 Procedimentos para a emissão de certificado

4.3.1.1 Certificado para pessoa singular

A emissão dos certificados por parte da EC Justiça, indica que todos os procedimentos de processamento do pedido foram concluídos com sucesso.

Os procedimentos estabelecidos neste ponto são também aplicados aos casos de renovação de certificados, uma vez que implica a emissão de novos certificados.

A EC Justiça utiliza um procedimento de geração de certificados que vincula de forma segura o certificado com a informação de registo, incluindo a chave pública, e protege a confidencialidade e integridade dos dados de registo.

Quando a EC Justiça emite um certificado, efetuará as notificações que se estabelecem no ponto 4.3.2.

Os certificados são emitidos no estado suspenso, para garantia de que apenas o seu titular os ativa. Iniciam a sua vigência apenas nesse momento (ativação), ou seja, é-lhes levantada a suspensão. O período de vigência está sujeito a uma possível extinção antecipada, provisória (suspenso) ou definitiva (revogação), quando se expliquem as causas que a motivem.

Após os procedimentos de validação referidos em 3.2, a ER determina se aceita ou rejeita o pedido de certificado.

Se o pedido for rejeitado, a ER notifica automaticamente o requerente, através de e-mail, indicando o motivo da rejeição.

Se o pedido for aceite, os pares de chaves são gerados no *smartcard* e os correspondentes certificados são emitidos na EC.

Todos os procedimentos relacionados com a emissão de certificados são registados e arquivados.

4.3.1.2 Certificado para equipamento tecnológico

Após os procedimentos de validação referidos em 3.2, a ER determina se aceita ou rejeita o pedido de certificado.

Se o pedido for rejeitado, a ER notifica o requerente, através de e-mail, indicando o motivo da rejeição.

Se o pedido for aceite, a ER procede à colocação do ficheiro no ciclo de emissão, enviando-o à EC que se encarregar de o assinar e devolver à ER.

A ER envia ao patrocinador, através de correio eletrónico ou suporte magnético, o ficheiro assinado, ou seja, o certificado.

Os certificados iniciam a sua vigência no momento da sua emissão, salvo quando se indique no mesmo uma data ou hora posterior para a sua entrada em vigor. O período de vigência está sujeito a uma possível extinção antecipada, provisória ou definitiva, quando se expliquem as causas que motivem a suspenso ou revogação do certificado.

4.3.2 Notificação da emissão do certificado ao titular

É acionado o Sistema de Notificação que informa o requerente, através de correio eletrónico, que o certificado foi criado com sucesso e que o respetivo *smartcard* será entregue, no prazo máximo de dez dias úteis, no local de trabalho.

4.4 Aceitação do certificado

4.4.1 Procedimentos para a aceitação de certificado

4.4.1.1 Certificado de pessoa singular

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

- Toma conhecimento dos seus direitos e aceita as obrigações e as responsabilidades, bem como as condições de utilização do certificado, que lhe são impostas pelo Termo de Responsabilidade integrado no contrato assinado quer pelo titular como pelo operador do registo presencial, e por esta DPC;
- Toma conhecimento das funcionalidades do certificado;

Depois de receber o *smartcard*, o requerente fica detentor de 3 certificados (de autenticação, de cifra e de assinatura) e das chaves públicas e privadas correspondentes. A aceitação do conteúdo daqueles ocorre mediante a evocação de um aplicativo que exige a alteração do PIN inicial de 7 dígitos para um outro que jamais poderá ter o mesmo tamanho. Ocorrendo esta alteração de PIN, fica garantida a aceitação do conteúdo do certificado.

4.4.1.2 Certificado de equipamento tecnológico

O certificado considera-se aceite após a assinatura do formulário do pedido de emissão de certificado pelo patrocinador.

Note-se que antes de ser disponibilizado o certificado ao patrocinador, e consequentemente lhe serem disponibilizadas todas as funcionalidades na utilização da chave privada e certificado, é garantido que este:

- Toma conhecimento dos seus direitos e responsabilidades;
- Toma conhecimento das funcionalidades e conteúdo do certificado.

4.4.2 Publicação do certificado

O certificado de cifra é publicado em repositório público, mediante consentimento do seu titular. No *Active Directory* é automaticamente publicado.

4.4.3 Notificação da emissão de certificados a outras entidades

A ER é informada da emissão dos certificados, mediante a alteração de estado do registo de pedido destes na sua aplicação. Esta é a única notificação efetuada.

4.5 Uso do certificado e par de chaves

4.5.1 Uso do certificado e da chave privada pelo titular

Os titulares de certificados utilizarão a sua chave privada apenas e só para o fim a que estas se destinam (conforme estabelecido no campo do certificado "*keyUsage*") e sempre com propósitos legais.

A sua utilização apenas é permitida:

- A quem estiver designado no campo "*Subject*" do certificado;
- Depois de aceitar as condições definidas no ponto 1.4 e
- Enquanto este se mantiver válido.

4.5.2 Uso do certificado e da chave pública pelas partes confiantes

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

- Terem conhecimento e perceberem a utilização e funcionalidades proporcionadas pela criptografia de chave pública e certificados;
- Serem responsáveis pela sua correta utilização;
- Lerem e entenderem os termos e condições descritos nas DPC e PC's;
- Verificarem os certificados (validação de cadeias de confiança) e CRL, tendo especial atenção às suas extensões marcadas como críticas e propósito das chaves;
- Confiarem nos certificados, utilizando-os sempre que estes estejam válidos.

4.6 Renovação de certificados

A renovação de um certificado é o processo em que a emissão de um novo certificado utiliza os dados anteriores do certificado, não havendo alteração das chaves ou qualquer outra informação, com exceção do período de validade do certificado.

Esta prática não é suportada na EC Justiça.

4.7 Renovação de certificado com geração de novo par de chaves

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

A renovação de certificado com geração de novo par de chaves é feita de acordo com o estabelecido na secção 4.3.

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

É motivo válido para a renovação de certificado com geração de novo par de chaves, sempre e quando se verifique que:

- O certificado e o *smartcard* (já que ambos têm a mesma validade) estão a expirar (2 meses antes da expiração é possível submeter novo pedido);
- O certificado foi revogado por motivo de comprometimento de chave ou por avaria do *smartcard*.

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

Conforme especificado em 4.1.1.

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

Conforme especificado em 4.2.

4.7.4 Notificação da emissão de novo certificado ao titular

Conforme especificado em 4.3.2.

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

Conforme especificado em 4.4.1.

4.7.6 Publicação do certificado renovado

Conforme especificado em 4.4.2.

4.7.7 Notificação da emissão do novo certificado a outras entidades

Conforme especificado em 4.4.3.

4.8 Modificação de certificados

A modificação de certificados é o processo em que é emitido um certificado para um titular, mantendo as respetivas chaves, havendo apenas alterações na informação do certificado.

4.8.1 Motivos para modificação de certificado

É motivo válido para a modificação de certificado sempre e quando se verifique que:

- a informação do certificado sofre alterações.

4.8.2 Quem pode submeter o pedido de modificação de certificado

Conforme especificado em 4.1.2.1.

4.8.3 Processamento do pedido de modificação de certificado

Conforme especificado em 4.2.

4.8.4 Notificação da emissão de novo certificado ao titular

Conforme especificado em 4.3.2, excetuando o envio do *smartcard*. Neste caso, é enviado um e-mail com uma URL a apontar para a descarga dos certificados.

4.8.5 Procedimentos para aceitação do certificado modificado

Conforme especificado em 4.4.1.1 excetuando a referência à ativação dos certificados. No caso da modificação, a aceitação ocorre no ato de ativação dos certificados, após a descarga dos mesmos.

4.8.6 Publicação do certificado modificado

Conforme especificado em 4.4.2.

4.8.7 Notificação da emissão do novo certificado a outras entidades

Conforme especificado em 4.4.3.

4.9 Suspensão e revogação de certificado

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

A revogação de um certificado é o 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 operabilidade conforme aos usos que lhe são próprios e, em consequência a revogação de um certificado inabilita o uso legítimo do mesmo por parte do titular.

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

4.9.1 Motivos para a revogação

Um certificado será revogado se:

- se constatar que a sua emissão foi imprópria ou defeituosa;
- se constatar que o certificado foi emitido com base em informações erróneas ou falsas, ou que as informações nele contidas deixaram de ser conformes com a realidade;
- se encontrar suspenso há mais de três dias úteis;
- o organismo a que pertence o titular deixar de integrar a Justiça;
- houver comprometimento, ou ameaça de comprometimento, da chave privada do titular;
- houver comprometimento, ou ameaça de comprometimento, do PIN de acesso ao *smartcard*;
- houver perda, destruição, ou estrago que impeça a utilização do *smartcard*;
- por vontade do próprio.

4.9.2 Quem pode submeter o pedido de revogação

Conforme especificado em 3.4.

4.9.3 Procedimento para o pedido de revogação

Conforme especificado em 3.4.

O processo de revogação do certificado inicia-se com a receção do pedido pela ER e termina com a emissão e publicação de uma nova CRL.

Todos os procedimentos relacionados com a revogação de certificados são registados e arquivados.

4.9.4 Produção de efeitos da revogação

A revogação só produz efeitos a partir da data indicada na CRL.

4.9.5 Prazo para processar o pedido de revogação

A Entidade Certificadora assegura o processamento de um pedido de revogação válido e a atualização da CRL num período máximo de 4 horas desde que rececionado entre as 9h e as 0h dos dias úteis e entre as 8h e as 0h nos fins de semana e feriados.

4.9.6 Requisitos de verificação da revogação pelas partes confiantes

O destinatário de um certificado emitido pela EC Justiça, deve verificar sempre a respetiva CRL. Na impossibilidade dessa verificação devido a falha de sistema ou indisponibilidade do serviço, o certificado não deverá ser reconhecido.

A autenticidade das CRL's deve ser confirmada através da verificação das assinaturas digitais da EC Justiça e dos períodos de validade das respetivas CRL's.

4.9.7 Periodicidade da emissão da CRL

A EC Justiça publica uma nova CRL no seu repositório sempre que há uma revogação ou suspensão de certificados.

Não ocorrendo nenhuma revogação, será publicada conforme especificado em 2.3.

4.9.8 Período máximo entre a emissão e a publicação da CRL

O período máximo entre a emissão e a publicação da CRL será 5 minutos.

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

Não aplicável.

4.9.10 Requisitos de verificação on-line de revogação

Não aplicável.

4.9.11 Outras formas disponíveis para divulgação de revogação

Não aplicável.

4.9.12 Requisitos especiais em caso de comprometimento de chave privada

Não tem requisitos especiais. Aplicam-se os procedimentos utilizados na suspensão/revogação de certificados.

4.9.13 Motivos para suspensão

Um certificado será suspenso quando:

- for recebido um pedido de revogação por telefone e aguarda-se a confirmação escrita;
- houver suspeita de perda do *smartcard* ou de comprometimento de chaves mas esta suspeita, pelo seu grau de certeza, não aconselhe a revogação imediata, sendo suspensos os certificados do titular enquanto se analisa a situação. No final da análise, será determinada a revogação dos certificados ou será levantada a suspensão.

4.9.14 Quem pode submeter o pedido de suspensão

Conforme estabelecido em 4.9.2.

4.9.15 Procedimentos para pedido de suspensão

O pedido de suspensão de certificado para pessoa singular, pode ser efetuado pelo titular, através de e-mail ou carta dirigida ao Administrador da ER, ou por telefone.

No caso de suspensão de certificado de equipamento tecnológico, deverá ser efetuado pelo seu Patrocinador.

O motivo para suspensão tem sempre de ser indicado.

O processo de suspensão do certificado inicia-se com a receção do pedido pela ER e termina com a publicação de uma nova CRL.

Todos os procedimentos relacionados com a suspensão de certificados são registados e arquivados.

4.9.16 Limite do período de suspensão

O período de suspensão de certificado não poderá ultrapassar 3 dias úteis[12]. Findo esse período, se a suspensão não for levantada o certificado é revogado com efeitos a partir da data da suspensão.

[12] Alínea b) do artigo 21º do Decreto-Regulamentar nº 25/2004, de 15 de Julho

4.10 Serviços sobre o estado do certificado

4.10.1 Características operacionais

O estado dos certificados emitidos está disponível publicamente através das CRL's.

4.10.2 Disponibilidade de serviço

O Serviço sobre o estado do certificado está disponível 24 horas por dia, 7 dias por semana.

4.10.3 Características opcionais

Não aplicável.

4.11 Fim de subscrição

O fim da operacionalidade de um certificado acontece quando se verificarem uma das seguintes situações:

- revogação do certificado;
- ter caducado o prazo de validade do certificado.

4.12 Retenção e recuperação de chaves (key escrow)

Apenas se efetua a retenção da chave privada de cifra.

4.12.1 Políticas e práticas de retenção e recuperação de chaves

A recuperação da chave privada de cifra de um titular é efetuada por dois elementos do Grupo de Trabalho da EC Justiça. É criada uma chave de sessão bipartida que é distribuída por estes dois elementos para que seja obrigatória a presença de ambos na obtenção da chave privada do requerente. Este procedimento encontra-se devidamente descrito no documento interno com acesso restrito “Procedimento para Recuperação do Par de Chaves de Cifra e respetivo Certificado”.

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

Não aplicável.

5 Medidas de Segurança Física, de Gestão e Operacionais

5.1 Medidas de segurança física

O Ministério da Justiça implementou várias regras e políticas incidindo sobre controlos físicos, procedimentais e humanos, que suportam os requisitos de segurança constantes desta DPC. Esta secção descreve sucintamente os aspetos não técnicos de segurança que possibilitam, de modo seguro, realizar as funções de geração de chaves, autenticação dos titulares, emissão de certificados, revogação de certificados, auditorias e arquivo. Todos estes controlos não técnicos de segurança são críticos para garantir a confiança nos certificados, pois qualquer falta de segurança pode comprometer as operações da EC.

5.1.1 Localização física e tipo de construção

As operações da EC são realizadas numa sala numa Zona de Alta Segurança (ZAS), inserida noutra zona também de alta segurança e dentro de um edifício que reúne diversas condições de segurança, nomeadamente o controlo total de acessos que previne, deteta e impede acessos não autorizados, baseado em múltiplos níveis de segurança física.

- A ZAS é uma área que obedece às seguintes características:
- Paredes em alvenaria, betão ou tijolo;
- Teto e pavimento com construção similar à das paredes;
- Inexistência de janelas;
- Porta de segurança, com chapa em aço, com as dobradiças fixas e ombreira igualmente em aço, com fechadura de segurança acionável eletronicamente, características corta-fogo e funcionalidade antipânico.

5.1.2 Acesso físico ao local

Os sistemas da EC estão protegidos por um mínimo de 4 níveis de segurança física hierárquicos (edifício em si, bloco de alta segurança, área de alta segurança, sala de alta segurança), garantindo-se que o acesso a um nível de segurança mais elevado só é possível quando previamente se tenha alcançado os privilégios necessários ao nível imediatamente anterior.

As atividades operacionais sensíveis da EC, a criação e armazenamento de material criptográfico e quaisquer atividades no âmbito do ciclo de vida do processo de certificação ocorrem dentro da zona mais restrita de alta segurança. O acesso a cada nível de segurança requer o uso de um cartão magnético de autenticação. Acessos físicos são automaticamente registados e gravados em circuito fechado de TV para efeitos de auditorias. É também gerado um relatório mensal de todas as entradas e saídas ocorridas na ZAS.

A pessoal não acompanhado, incluindo colaboradores ou visitantes não autenticados, não é permitida a sua entrada e permanência em áreas de segurança. A não ser que todo o pessoal que circule dentro destas áreas de segurança seja garantidamente reconhecido por todos, é

obrigatório o uso do respetivo cartão de acesso de modo visível, assim como garantir que não circulam indivíduos não reconhecidos sem o respetivo cartão de acesso visível.

O acesso à zona mais restrita de alta segurança requer controlo duplo, cada um deles utilizando dois fatores de autenticação, incluindo autenticação biométrica.

O *hardware* criptográfico e *tokens* físicos seguros dispõem de proteção adicional, sendo guardados em cofres e armários seguros. O acesso à zona mais restrita de alta segurança, assim como ao *hardware* criptográfico e aos *tokens* físicos seguros é restrito, de acordo com as necessidades de segregação de responsabilidades dos vários Grupos de Trabalho.

5.1.3 Energia e ar condicionado

A ZAS possui equipamento, que garante condições de funcionamento 24 horas por dia / 7 dias por semana, de:

- Alimentação de energia garantindo alimentação contínua 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 e
- Refrigeração/ventilação/ar condicionado que controlam os níveis de temperatura e humidade, garantindo condições adequadas para o correto funcionamento de todos os equipamentos eletrónicos e mecânicos presentes dentro do ambiente.

5.1.4 Exposição à água

As zonas de alta segurança têm instalado os devidos mecanismos (detetores de inundação) para minimizar o impacto de inundações nos sistemas da EC Justiça.

5.1.5 Prevenção e proteção contra incêndio

A ZAS tem instalado os mecanismos necessários para evitar e apagar fogos ou outros incidentes derivados de chamas ou fumos. Estes mecanismos estão em conformidade com os regulamentos existentes:

- Sistemas de deteção e alarme de incêndio instalados nos vários níveis físicos de segurança,
- Equipamento fixo e móvel de extinção de incêndios estão disponíveis, colocados em sítios estratégicos e de fácil acesso de modo a poderem ser rapidamente usados no início de um incêndio e extingui-lo com sucesso,
- Procedimentos de emergência bem definidos, em caso de incêndio.

5.1.6 Salvaguarda de suportes de armazenamento

Todos os suportes de informação sensível contendo *software* e dados de produção, informação para auditoria, arquivo ou cópias de segurança são guardados em cofres e armários de segurança, alguns deles na ZAS e outros em ambientes distintos externos ao edifício onde se localiza aquela. Possuem controlos de acesso físicos e lógicos apropriados para restringir o acesso apenas a elementos autorizados dos Grupos de Trabalho. Para além

das restrições de acessos, também estão adequados para a proteção contra acidentes (e.g., causados por água ou fogo).

Em situações que implique a deslocação física de *hardware* de armazenamento de dados (i.e., discos rígidos,...) para fora da ZAS, por motivos que não o arquivo de cópias de segurança, cada elemento do *hardware* deverá ser verificado para garantir que não contém dados sensíveis. Nestas situações, a informação tem de ser eliminada usando todos os meios necessários para o efeito (formatar o disco rígido, *reset* do *hardware* criptográfico ou mesmo destruição física do equipamento de armazenamento).

5.1.7 Eliminação de resíduos

Documentos e materiais em papel que contenham informação sensível deverão ser triturados antes da sua eliminação.

É garantido que não é possível recuperar nenhuma informação dos suportes de informação utilizados para armazenar ou transmitir informação sensível (através de formatação "segura" de baixo nível ou destruição física), antes dos mesmos serem eliminados. Equipamentos criptográficos ou chaves físicas de acesso lógico são fisicamente destruídos ou seguem as recomendações de destruição do respetivo fabricante, antes da sua eliminação. Outros equipamentos de armazenamento (discos rígidos, *tapes*,...) deverão ser devidamente limpos de modo a não ser possível recuperar nenhuma informação (através de formatações seguras, ou destruição física dos equipamentos).

5.1.8 Instalações externas (alternativa) para recuperação de segurança

Todas as cópias de segurança são guardadas em ambiente seguro em instalações externas, ficando alojadas em cofres e armários seguros situados em zonas com controlos de acesso físicos e lógicos, de modo a restringir o acesso apenas a pessoal autorizado, garantindo também a proteção contra danos acidentais (e.g., causados por água ou fogo).

5.2 Medidas de segurança dos processos

Nesta secção, descrevem-se os requisitos necessários para reconhecer os papéis de confiança e responsabilidades associadas a cada um desses papéis. Esta secção inclui também a separação de deveres, em termos dos papéis que não podem ser executados pelos mesmos indivíduos.

5.2.1 Funções de confiança

Todas as operações da Entidade Certificadora são asseguradas por funcionários do quadro de pessoal do MJ.

A Entidade Certificadora garante a separação das tarefas para funções críticas, a serem desempenhadas por diferentes funcionários, com perfil estabelecido.

5.2.1.1 Software para certificação digital

A Entidade Certificadora estabelece seis perfis distintos para execução das seguintes funções:

1. **Administrador de Sistemas**: responsável pela instalação, configuração e manutenção dos sistemas, pela criação e manutenção dos utilizadores e dos controlos de acesso;
2. **Administrador de Segurança**: responsável por propor, gerir e implementar todas as políticas da EC, assegurando que se encontram atualizadas e garantir que toda a informação indispensável ao funcionamento e auditoria da EC se encontra disponível ao longo do tempo. O Grupo de Trabalho de Administração de Segurança assume também a função de Operador de HSM.
3. **Administrador de Registo**: responsável pela emissão, expedição, distribuição e gestão de certificados, bem como pela manutenção das CRL's e alerta para as novas emissões de certificados;
4. **Operadores de Sistemas**: responsáveis pelas tarefas de rotina da EC, incluindo operações de cópias de segurança dos seus sistemas;
5. **Auditor de Sistemas**: responsável por efetuar a auditoria interna a todas as ações relevantes e necessárias para assegurar a operacionalidade da EC;
6. **Operador de registo**: Assume a função de ER perante a EC.

5.2.1.1.1 Administrador de Sistemas

Assume o papel de Administrador do Sistema, conforme definido no artigo 29º do Decreto Regulamentar n.º 25/2004, de 15 de Julho.

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

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

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

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

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

5.2.1.1.2 Operador de Sistemas

Assume o papel de Operador de Sistema, conforme definido no artigo 29º do Decreto Regulamentar n.º25/2004.

Responsável por operar regularmente os sistemas.

É responsável pela correta execução da política de cópias de segurança e em particular de as manter atualizadas para que permita recuperar eficientemente qualquer um dos sistemas.

5.2.1.1.3 Administrador de Segurança

Assume o papel de Administrador de Segurança, conforme definido no artigo 29º do Decreto Regulamentar n.º 25/2004.

É responsável:

- Pela gestão e implementação das regras e práticas de segurança;
- Por fazer cumprir as políticas de segurança do SCEE e encarregue de qualquer aspeto relativo à segurança física, das aplicações, da rede, etc.;
- Pela gestão dos sistemas de proteção periférica;
- Por resolver todos os incidentes de segurança e eliminar todas as vulnerabilidades detetadas;
- Pela 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;
- Por explicar todos os mecanismos de segurança aos funcionários que devam conhecê-los e de consciencializá-los para as questões de segurança levando-os a fazer cumprir as normas e políticas de segurança estabelecidas;
- Por estabelecer os calendários para a execução de análise de vulnerabilidades, testes e treino, bem como dos planos de continuidade de serviço e auditoria dos sistemas de informação.

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

5.2.1.1.4 Administrador de Registo

Assume o papel de Administrador de Registo, conforme definido no artigo 29º do Decreto Regulamentar n.º 25/2004.

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

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

5.2.1.1.5 Auditor de Sistemas

Assume o papel de Auditor de Sistema, conforme definido no artigo 29º do Decreto Regulamentar n.º 25/2004.

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

O auditor está encarregado de:

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

5.2.1.1.6 Operador de Registo

Encontra-se sob a alçada do Administrador de Registo e é responsável por todas as tarefas inerentes à ER, desde a validação do pedido de certificado à expedição do mesmo.

5.2.1.1.6.1 Operador de Registo Presencial

Subgrupo responsável pela submissão do pedido de certificado, na presença do requerente.

5.2.1.2 Dispositivo Seguro para Criação de Assinaturas

As funções de confiança incluem também:

- Administradores de HSM;
- Operadores de HSM.

5.2.1.2.1 Administradores de HSM

Definiu-se um conjunto de 4 Administradores para o HSM da EC Justiça, cada um com pelo menos um cartão criptográfico de controlo de acesso às suas funções, perfazendo um total de 7 cartões. Para a realização das operações que requeiram um papel de administrador, é necessário introduzir no leitor do HSM um total de 4 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 se desejar ampliar ou reduzir o número de cartões de administrador;
- Substituição de um conjunto de cartões de operador. Esta operação só é necessária se se desejar ampliar ou reduzir o número de cartões de operador ou substituir algum cartão deteriorado;
- Ampliação do número de HSM's integrados na infraestrutura;
- Dado que se opera em modo FIPS140-2 Nível 3, autorização para a geração de conjuntos de cartões de operador e chaves. Esta operação só se pode requerer durante a cerimónia de geração de chaves para a EC.

5.2.1.2.2 Operadores de HSM

Definiu-se um conjunto de 4 operadores para a EC Justiça, 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 inserir no leitor do HSM dois cartões de operador. Os Operadores de HSM estão encarregues de realizar as seguintes operações:

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

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

5.2.1.3 Outros Perfis de Confiança

Existem ainda outros dois Grupos que, embora não sendo exigidos pelo Decreto-Regulamentar, são indispensáveis para a boa organização dos artefactos e serviços, bem como para a tomada de decisões administrativas.

São eles o Grupo de Gestão e o Grupo de Custódia.

5.2.1.3.1 Grupo de Gestão

É responsável pela nomeação dos membros dos restantes grupos e pela guarda de alguns artefactos sensíveis (cartões de administração do HSM). Este grupo deve ter um mínimo de 4 (quatro) elementos.

As responsabilidades deste grupo são:

- Gestão do "Ambiente de Gestão",
- Rever e aprovar as políticas propostas pelo Grupo de Trabalho de Administração de Segurança;
- Designar os membros dos restantes grupos de trabalho (à exceção do Grupo de Trabalho de Custódia);
- Disponibilizar a identificação de todos os indivíduos que pertencem aos vários Grupos de Trabalho, em um ou mais pontos de acesso facilmente acessíveis pelos indivíduos autorizados;
- Submeter a DPC à validação do Conselho Gestor do SCEE.

5.2.1.3.2 Grupo de Custódia

É responsável pela custódia de alguns artefactos sensíveis (*tokens* de autenticação, etc.), que podem ser levantados pelos membros dos outros grupos mediante a satisfação de determinadas condições[13]. Note-se que, no sentido de melhorar os níveis de segurança, operacionalidade e continuidade de negócio da EC, poderão existir várias instâncias deste grupo, cada qual encarregue da custódia de um conjunto distinto de artefactos.

Este grupo deve fazer uso dos vários ambientes seguros disponibilizados para a guarda deste tipo de itens.

As responsabilidades deste grupo são:

- Gestão do "Ambiente de Custódia" respetivo;
- Custódia de artefactos sensíveis usando os meios adequados que respondam às necessidades de segurança respetivas;
- Disponibilização segura destes itens a membros de grupos autorizados e explicitamente indicados com permissões de acesso a esses itens, após o cumprimento dos procedimentos apropriados de segurança.

[13] Definidas para cada um dos artefactos à sua guarda

5.2.2 Número de pessoas exigidas por tarefa

Todas as operações executadas no local onde se encontram instalados os sistemas de certificação exigem, no mínimo, a presença em simultâneo de dois funcionários autorizados e convenientemente identificados.

A EC Justiça garante 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 na EC.

A atribuição de funções faz com que sejam sempre requeridas a participação de um mínimo de duas pessoas para todas as atividades relacionadas com o ciclo de vida dos certificados emitidos pela EC Justiça.

5.2.3 Identificação e autenticação para cada função

O acesso aos sistemas só é permitido após autenticação através de *password*, sendo exigida a presença simultânea de dois funcionários.

A autenticação no HSM é baseada em técnicas de segredo partilhado com cartões criptográficos específicos do HSM

Os restantes utilizadores da EC Justiça são identificados mediante certificados eletrónicos emitidos pela própria infraestrutura da EC Justiça.

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

5.2.4 Funções que requerem separação de responsabilidades

Entre as funções, estabelecem-se as seguintes incompatibilidades, para que um utilizador não possa ter duas funções marcadas como “incompatíveis”:

	AdmSeg	AdmReg	AdmSist	OpSist	Auditor	AdmHSM	OpHSM
AdmSeg			×		×	×	
AdmReg					×	×	
AdmSist	×				×	×	
OpSist						×	
Auditor	×	×	×			×	×
AdmHSM	×	×	×	×	×		×

	AdmSeg	AdmReg	AdmSist	OpSist	Auditor	AdmHSM	OpHSM
OpHSM					×	×	

5.3 Medidas de segurança de pessoal

5.3.1 Requisitos relativos às qualificações, experiência, antecedentes e credenciação

Todo o pessoal que desempenha funções na EC Justiça tem qualificações e experiência na prestação de serviços de certificação.

Todo o pessoal cumpre os requisitos de segurança da organização.

Todo o pessoal que manuseia matéria confidencial encontra-se devidamente credenciado pelo Gabinete Nacional de Segurança na marca "Nacional" grau "Confidencial".

5.3.2 Procedimentos de verificação de antecedentes

Cada elemento comprovou os antecedentes através de diversas formas:

- Curriculum Vitae e Registo Criminal.
- A verificação de antecedentes inclui, nos termos do artigo 29º do Decreto Regulamentar n.º 25/2004, de 15 de Julho:
  - ✓ confirmação de identificação, usando documentação emitida por fontes fiáveis;
  - ✓ investigação de registos criminais.

5.3.3 Requisitos de formação e treino

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

Este plano inclui os seguintes aspetos:

- Formação nos aspetos legais básicos relativos à prestação de serviços de certificação;
- Formação em segurança dos sistemas de informação;
- Serviços disponibilizados pela Entidade Certificadora;
- Conceitos básicos sobre ICP;
- Declaração de Práticas de Certificação e Políticas de Certificados;
- Gestão de ocorrências;
- Formação específica para o seu posto;
- Funcionamento do *software* e hardware usados pela EC;

5.3.4 Frequência e requisitos para ações de reciclagem.

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

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

5.3.5 Frequência e sequência da rotação de funções

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

5.3.6 Sanções para ações não autorizadas

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

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

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

Adicionalmente, em função da gravidade da infração cometida, devem aplicar-se as sanções previstas na lei, nomeadamente a Lei do Cibercrime (Lei nº 109/2009, de 15 de setembro).

5.3.7 Contratação de pessoal

Todo o pessoal da EC Justiça está sujeito ao dever de sigilo mediante a assinatura de um termo de confidencialidade relativo às funções que desempenha. Este acordo descreve as suas tarefas de acordo com a DPC.

A Entidade Certificadora tem como requisito na contratação de pessoal (com exceção do Grupo de Custódia), a Credenciação dos mesmos pelo GNS.

5.3.8 Documentação fornecida ao pessoal

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

- Declaração de Práticas de Certificação;
- Políticas de Certificado;
- Política de Recursos Humanos;
- Funções do pessoal (*job descriptions*);
- Documentação técnica sobre o *software* e *hardware* da EC.

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

5.4 Procedimentos de auditoria de segurança

5.4.1 Tipo de eventos registados

Todas as operações efetuadas pela ER e pela EC são registadas e assinadas. Todos os registos (*logs*) contêm a data do evento e a identificação do operador que o efetuou.

São criados registos eletrónicos para os seguintes eventos:

- iniciação e encerramento dos sistemas;
- criação, alteração e eliminação de passwords e privilégios de acesso dos operadores dos sistemas;
- acessos (*login*) e saídas (*logoff*) efetuados nos sistemas;
- tentativas não autorizadas de acesso aos sistemas;
- geração de chaves de assinatura e de encriptação;
- emissão, suspensão e revogação de certificados;
- geração de CRL's;
- falhas de leitura e escrita no diretório de certificados e CRL's;
- alterações na configuração dos sistemas.

São criados registos manuais relativamente a:

- todos os pedidos a que correspondem certificados emitidos/revogados;
- todos os documentos entregues pelo requerente no ato do pedido de emissão/revogação;
- outra documentação adicional entregue para efeitos de validação.

5.4.2 Frequência da auditoria de registos

Os *logs* são analisados sempre que se verifique suspeita de comprometimento ou falha de segurança.

Ações tomadas baseadas na informação dos registos são também documentadas.

5.4.3 Período de retenção dos registos de auditoria

A informação dos *logs* é mantida nos sistemas durante dois anos e em arquivo durante o período indicado no ponto 5.5.2.

5.4.4 Proteção dos registos de auditoria

Os sistemas incluem mecanismos de segurança para proteção de acessos não autorizados para leitura, modificação e eliminação dos registos de auditoria.

Os registos manuais também estão protegidos contra acessos não autorizados.

Os registos de auditoria apenas deverão estar acedíveis ao Auditor de Sistemas e poderão ser visualizados pelos Auditores Externos.

A destruição de um arquivo de auditoria só poderá ser levada a cabo com a autorização do Administrador de Sistemas, do Administrador de Segurança e do Auditor de Sistemas.

Os registos de auditoria são considerados informação sensível, conforme especificado no ponto 9.4.

5.4.5 Procedimentos para a cópia de segurança dos registos

A cópia dos *logs* é efetuada com a periodicidade definida na política de *backups* da EC Justiça e guardada numa área segura fora das instalações da ZAS.

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

Os registos de auditoria são automaticamente recolhidos através do *software* de certificação e de segurança dos sistemas.

5.4.7 Notificação de agentes causadores de eventos

Não é efetuada qualquer notificação ao sujeito causador da ocorrência do evento.

5.4.8 Avaliação de vulnerabilidades

Em caso de alteração significativa no ambiente global da EC Justiça ou, no mínimo, uma vez por ano, é efetuada uma avaliação das vulnerabilidades.

O resultado da análise é reportado ao Grupo de Gestão da EC Justiça para rever, promover e aprovar, caso se justifique, um plano de tratamento dos riscos avaliados.

5.5 Arquivo de registos

5.5.1 Tipo de dados arquivados

Toda a documentação referente ao funcionamento do serviço de certificação, incluindo avarias, situações operacionais especiais e a informação respeitante ao registo, é mantida em ficheiro eletrónico.

São arquivados os seguintes dados:

- Os registos de auditoria especificados no ponto 5.4;
- As cópias de segurança dos sistemas que compõem a ICP;
- Chaves de cifra.

A Entidade Certificadora conserva em ficheiro manual:

- todos os pedidos a que correspondem certificados emitidos/revogados;

- todos os documentos entregues pelo requerente no ato do pedido;
- outra documentação adicional entregue para efeitos de validação.

5.5.2 Período de retenção em arquivo

Toda a informação de arquivo é conservada durante o período de 20 anos.

5.5.3 Proteção dos arquivos

De acordo com o disposto no ponto 5.4.4.

5.5.4 Procedimentos para as cópias de segurança do arquivo

De acordo com o disposto no ponto 5.4.5.

5.5.5 Requisitos para avaliação cronológica dos registos

Os sistemas de informação da EC Justiça garantem o registo do tempo nos quais se realizam.

O tempo dos sistemas provém de uma fonte segura que sincroniza a data e hora legal portuguesa, via NTP (*Network Time Protocol*).

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

De acordo com o disposto no ponto 5.4.6.

5.5.7 Procedimentos de recuperação e verificação de informação arquivada

Apenas membros autorizados dos Grupos de Trabalho têm acesso aos arquivos para verificação da sua integridade.

São realizadas de forma automática verificações de integridade dos arquivos eletrónicos (cópias de segurança) na altura da sua criação, em caso de erros ou comportamentos imprevistos, realiza-se novo arquivo.

5.6 Renovação de chaves

Não aplicável.

5.7 Recuperação em caso de desastre ou comprometimento

Esta secção descreve os requisitos relacionados com os procedimentos de notificação e de recuperação no caso de desastre ou de comprometimento.

5.7.1 Procedimentos em caso de incidente ou comprometimento

Cópias de segurança das chaves privadas da EC (geradas e mantidas de acordo com a secção 6.2.4) e dos registos arquivados (secção 5.5.1) são guardados em ambientes seguros externos e disponíveis em caso de desastre ou de comprometimento.

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

Se os recursos de *hardware*, *software* e/ou os dados forem alterados ou houver suspeita de que terão sido alterados, serão parados os serviços da EC até ao restabelecimento das condições seguras, com a inclusão de novos componentes de eficácia credível, sendo a ECEE notificada do facto.

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

Caso afete certificados emitidos, os titulares dos mesmos serão notificados e proceder-se-á à sua revogação.

5.7.3 Procedimentos em caso de comprometimento da chave privada da entidade

Em caso de comprometimento da chave privada da EC, proceder-se-á à sua revogação imediata e serão informadas deste facto todas as entidades que compõem a SCEE, dependentes ou não da Entidade afetada.

Os certificados assinados por esta deverão por sua vez ser revogados e informados os seus titulares/patrocinadores.

Serão implementados os seguintes procedimentos:

a) Geração de um pedido de revogação da EC comprometida e de todos os certificados emitidos na sua hierarquia de confiança;

b) Notificação da Autoridade Credenciadora, de todos os titulares de certificados emitidos na sua hierarquia de confiança e de todas as Entidades Subscritoras.

Após o comprometimento da chave privada da EC, será submetida ao Grupo de Gestão a decisão de criação de nova chave.

Em caso de decisão positiva os seguintes procedimentos serão seguidos:

- Gerar nova chave;
- Efetuar pedido de certificado (PKCS#10);
- Receber o novo certificado;

- Disseminar novo certificado;
- Renovar todos os certificados emitidos pela EC.

5.7.4 Capacidade de continuidade da atividade em caso de desastre

O Ministério da Justiça dispõe dos recursos de computação, *software*, cópias de segurança e registos arquivados, necessários para restabelecer ou recuperar operações essenciais (emissão e revogação de certificados, com a publicação de informação de revogação) após um desastre natural ou outro.

5.8 Procedimentos em caso de extinção de EC ou ER

Em caso de cessação de atividade como prestador de serviços de Certificação, a EC Justiça implementará, com uma antecedência mínima de três meses, as seguintes ações:

- Informar o Conselho Gestor do SCEE;
- Informar a ECEE;
- Informar todos os titulares de certificados e extinguir a vigência dos mesmos, revogando-os;
- Informar todas as terceiras partes com as quais tenha formado acordos de certificação;
- Efetuar uma notificação final aos titulares 2 (dois) dias antes da cessação formal da atividade;
- Garantir a transferência para arquivo da informação relativa à atividade da EC.

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

Havendo alterações do organismo/estrutura responsável pela gestão da atividade da EC, as entidades listadas nas alíneas acima, deverão ser informadas de tal facto.

6 Medidas de Segurança Técnicas

Esta secção define as medidas de segurança implementadas para a EC Justiça de forma a proteger chaves criptográficas geradas por esta, e respetivos dados de ativação. O nível de segurança atribuído à manutenção das chaves deve ser máximo para que chaves privadas e dados de ativação estejam sempre protegidos e sejam apenas acedidos por pessoas devidamente autorizadas.

6.1 Geração e instalação do par de chaves

A geração dos pares de chaves da EC Justiça é processada de acordo com os requisitos e algoritmos definidos nesta política.

6.1.1 Geração do par de chaves

Os pares de chaves da EC Justiça são gerados em módulos criptográficos seguros, com certificado de conformidade FIPS 140-2, nível 3. O seu funcionamento efetua-se em modo *on-line* obedecendo, para o efeito, aos requisitos do ponto 6.7. Os seus certificados encontram-se assinados pela ECRaizEstado.

6.1.1.1 Chaves para efeitos de Assinatura Digital e Autenticação

O par de chaves dos certificados de assinatura e de autenticação emitidos pela EC Justiça gera-se no próprio cartão criptográfico do titular, o qual cumpre os requisitos definidos no ponto 6.2.1.

De seguida, as chaves públicas são entregues à RA a qual envia-as, juntamente com os respetivos pedidos de certificado, à CA. Esta gera os certificados contendo a chave pública.

Os certificados (no formato PKCS#11) gerados são inseridos no chip do cartão.

6.1.1.2 Chaves para efeitos de Confidencialidade

O par de chaves do certificado de cifra é gerado na CA e entregue à RA juntamente com o certificado (no formato PKCS#12) para ser posteriormente inserido no cartão.

6.1.2 Entrega da chave privada ao titular

As chaves privadas são entregues ao titular através do cartão criptográfico. É efetuada uma cópia da chave privada de cifra a ser guardada na EC Justiça, para efeitos de recuperação, por parte do próprio titular, de ficheiros cifrados por/para aquele.

As entregas do cartão criptográfico e do PIN são efetuadas desfasadas no tempo e para locais distintos.

6.1.3 Entrega da chave pública ao emissor do certificado

As chaves públicas são geradas e gravadas na EC Justiça, conforme descrito em 6.1.1.

6.1.4 Entrega da chave pública da EC às partes confiantes

A chave pública da EC Justiça está incluída no certificado da dita EC. Este certificado deve ser obtido do repositório especificado neste documento onde fica à disposição dos titulares de certificados e às terceiras partes confiantes para realizar qualquer tipo de comprovação.

A chave é disponibilizada no formato DER.

6.1.5 Dimensão das chaves

O comprimento dos pares de chaves deve ter o tamanho suficiente, de forma a prevenir possíveis ataques de criptanálise que descubram a chave privada correspondente ao par de chaves no seu período de utilização. A dimensão das chaves é a seguinte:

- Nível 2 (EC Subordinada): RSA 4096 bit;
- O Tamanho mínimo para certificados pessoais e certificados de componentes ou servidores é de RSA 1024 bit, para uma validade de 3 anos.

6.1.6 Geração dos parâmetros da chave pública e verificação da qualidade

A geração dos parâmetros da chave pública e verificação da qualidade deverá ter sempre por base a norma que define o algoritmo. Para o caso do algoritmo RSA, utilizado pela EC Justiça, deverá ser feita de acordo com o estipulado no PKCS#1 e RFC 5280.

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

A chave privada da EC Justiça é utilizada para assinatura da sua CRL, para a assinatura de certificados para equipamentos tecnológicos e certificados para utilizadores finais (conforme o indicado na extensão "*key usage*" do certificado). O campo "*keyUsage*" dos certificados deve ser utilizado de acordo com o recomendado no RFC 5280.

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

Tipo de certificado	Key Usage	Extended Key Usage (Enhanced Key Usage)
Certificado de Assinatura	Non Repudiation	clientAuth (Client Authentication), EmailProtection (Secure Email)
Certificado de Autenticação	Digital Signature	clientAuth (Client Authentication); microsoftSmartCardLogon (Smart Card Logon),

Tipo de certificado	Key Usage	Extended Key Usage (Enhanced Key Usage)
		emailProtection (Secure Email)
Certificado de confidencialidade	Key Encipherment	emailProtection (Secure email), microsoftEncryptedFileSystem (Encrypting file system) BitLocker Drive Encryption
Certificado de Code Signing	Digital Signature	codeSigning
Certificado de Servidor Web	Digital Signature Key Encipherment	serverAuth (Server Authentication)
Certificado de Servidor DC	Digital Signature Key Encipherment	serverAuth (Server Authentication), client auth (client authentication)
Software	Digital Signature, key Encipherment	client auth (client authentication), emailProtection (Secure Email)

6.1.8 Outra utilização para as chaves

As chaves não podem ser utilizadas para outros fins, para além dos que são identificados na secção anterior.

6.2 Proteção da chave privada e características do módulo criptográfico

Nesta secção são considerados os requisitos para proteção da chave privada da EC Justiça e dos titulares bem como as características dos seus módulos criptográficos.

6.2.1 Normas e medidas de segurança do módulo criptográfico

6.2.1.1 EC Justiça

O módulo criptográfico da EC Justiça cumpre a norma FIPS 140-2, nível 3.

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

A implementação da Autoridade de Certificação, comporta as seguintes tarefas:

- Iniciação do estado do módulo HSM;
- Criação dos cartões de administração e de operador;
- Geração das chaves da EC.

6.2.1.2 Titulares

As chaves privadas dos certificados emitidos pela EC Justiça geram-se no próprio cartão criptográfico do titular, o qual cumpre os requisitos de Dispositivo Seguro de Criação de Assinatura (nível de segurança CC EAL4+ SSCD).

Suportam as normas PKCS#11 e CSP.

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

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

A chave criptográfica de ativação do componente seguro de *hardware* que armazena a chave privada da EC Justiça é distribuída por funcionários distintos, sendo obrigatória a presença de dois desses funcionários para ativação da componente de hardware e a consequente utilização da chave privada.

Todas as operações são efetuadas com um mínimo de 2 pessoas (com funções qualificadas dentro da entidade) por tarefa.

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

A chave privada da EC Justiça encontra-se sob controlo de mais que uma pessoa. Esta apenas se ativa mediante a iniciação do *software* da EC por meio de uma combinação de operadores da EC, administradores do HSM e utilizadores de Sistema Operativo. Este é o único método de ativação de dita chave privada.

6.2.3 Retenção da chave privada (*key escrow*)

Não é permitida a recuperação das chaves privadas de assinatura dos utilizadores finais.

A recuperação da chave privada de cifra é efetuado conforme descrito no ponto 4.12.1.

6.2.4 Cópia de segurança da chave privada

A EC e a ER mantêm cópias de segurança das suas chaves privadas de assinatura e encriptação.

A EC Justiça mantém cópias dos pares de chaves de encriptação dos utilizadores finais de forma a permitir recuperações.

6.2.5 Arquivo da chave privada

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

6.2.6 Transferência da chave privada para/do módulo criptográfico

A chave privada da EC Justiça é gerada dentro do módulo criptográfico.

As chaves privadas dos utilizadores finais são geradas no chip do dispositivo físico (*smartcard*), de acordo com a norma FIPS 140-1 nível 2.

A transferência da chave privada da EC Justiça só se pode fazer entre módulos criptográficos (HSM) e requer a intervenção de um mínimo de dois administradores do HSM, operadores do HSM e um Administrador de Sistemas.

6.2.7 Armazenamento da chave privada no módulo criptográfico

As chaves privadas são geradas no módulo criptográfico de acordo com o estipulado no ponto 6.2.1.

6.2.8 Processo para ativação da chave privada

A ativação da chave privada da EC Justiça é realizada através da inicialização do *software* de certificação do módulo criptográfico, após a identificação exigida.

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

A ativação da chave privada dos utilizadores finais é realizada através da inicialização do *software* de certificação do posto de trabalho, após a identificação de acesso exigida (PIN). O nº máximo de tentativas de identificação de acesso é 3.

6.2.9 Processo para desativação da chave privada

A chave privada da EC Justiça é desativada quando o sistema da EC é desligado.

Estas tarefas são executadas pelo Administrador de Sistemas com supervisão do Administrador de Segurança.

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

Quanto à chave privada dos utilizadores, esta é desativada quando se termina a sessão que foi inicializada com ela ou se retira o cartão do leitor.

6.2.10 Processo para destruição da chave privada

De acordo com a Política de Certificação do Sistema de Certificação Eletrónica do Estado.

Em termos gerais, a destruição deve sempre ser precedida por uma revogação do certificado associado à chave.

As várias chaves privadas dos utilizadores 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.

Nas situações em que a chave privada dos utilizadores deixou de poder ser utilizada, nomeadamente, após expiração ou revogação do certificado, o seu módulo criptográfico deverá ser destruído.

6.2.11 Avaliação/nível do módulo criptográfico

Descrito no ponto 6.2.1.

6.3 Outros aspetos da gestão do par de chaves

6.3.1 Arquivo da chave pública

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

6.3.2 Períodos de validade do certificado e das chaves

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

As chaves públicas podem ser utilizadas durante todo o período em que se mantenham em arquivo, para verificação de assinaturas geradas durante o período de validade dos certificados correspondentes.

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

[Validade dos Certificados] – [Período de Renovação]	
EC Justiça	Certificados emitidos
[12] – [9]	[3] – [3]

Não obstante estas validades, a EC Justiça pode deixar de emitir novos certificados a partir de uma data apropriada, anterior à expiração do certificado EC, de tal forma que nenhum certificado emitido possa ter uma data de expiração posterior à data de expiração de qualquer um dos certificados constantes da cadeia de certificação (ou seja, há que ter em conta a validade da ECRaizEstado).

6.4 Dados de ativação

6.4.1 Geração e instalação dos dados de ativação

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

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

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

Para a instauração da EC Justiça são criados cartões criptográficos, que servem para atividades de funcionamento e recuperação. A EC opera com vários tipos de funções, cada um com os seus correspondentes cartões criptográficos onde se armazenam os dados de ativação.

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

6.4.2 Proteção dos dados de ativação

Só o pessoal autorizado, neste caso os Operadores e Administradores do HSM, possuem os cartões criptográficos com capacidade de ativação da EC e conhecem os PINs para aceder aos dados de ativação.

No caso das chaves associadas aos certificados pessoais, só o titular conhece o PIN, sendo portanto o único responsável da proteção dos dados de ativação das suas chaves privadas.

6.4.3 Outros aspetos dos dados de ativação

Não estipulado.

6.5 Medidas de segurança informática

6.5.1 Requisitos técnicos específicos

Os sistemas utilizados pela EC Justiça para emissão, suspensão, revogação, distribuição e gestão de certificados, estão fisicamente protegidos contra modificações não autorizadas e ataques técnicos ao nível do equipamento e dos suportes lógicos, sendo o acesso efetuado de acordo com os níveis de segurança e de atribuição de funções definidos.

Os sistemas instalados:

- exigem a identificação e autenticação prévia do operador;

- têm dispositivos de alarme lógicos com monitorização constante;
- asseguram que qualquer modificação não autorizada é detetada.

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

6.5.2 Avaliação/nível de segurança

Os vários sistemas e produtos utilizados pela EC Justiça são fiáveis e protegidos contra modificações. Os produtos e sistemas referidos, são avaliados, estando em conformidade com os requisitos definidos na especificação técnica CWA 14167-1 e/ou com a norma ISO 15408 ou perfil equivalente.

6.6 Ciclo de vida das medidas técnicas de segurança

Os dados relativos a esta secção são considerados sensíveis, sendo apenas disponibilizados a quem tiver necessidade de os conhecer. No domínio da EC Justiça, apenas são fornecidos à Autoridade Credenciadora e ao auditor devidamente credenciado por aquela.

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

6.6.1 Medidas de desenvolvimento do sistema

Os requisitos de segurança são exigíveis, desde o seu início, tanto na aquisição de sistemas informáticos como no desenvolvimento dos mesmos, dado que podem ter algum impacto sobre a segurança de EC Justiça.

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 EC Justiça, para garantir que os sistemas são seguros.

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

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

6.6.2 Medidas para a gestão da segurança

A EC Justiça tem mecanismos e/ou Grupos de Trabalho para controlar e monitorizar a configuração dos sistemas da EC.

A EC Justiça mantém um inventário de todos os ativos, quer sejam equipamentos, quer sejam dados ou pessoal e classifica os mesmos de acordo com a sua necessidade de proteção e os riscos a que podem estar expostos. Assim é feita uma análise de risco anual para que se consiga fazer uma eficaz gestão de risco.

As configurações dos sistemas são auditadas de forma periódica e verificam-se as necessidades.

6.6.3 Ciclo de vida das medidas da segurança

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

6.7 Medidas de segurança da rede

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

Não obstante indicar que a infraestrutura da rede utilizada pelos sistemas da EC Justiça está dotada de todos os mecanismos de segurança necessários para garantir um serviço confiável e íntegro (p.e. utilização de *firewall*), esta rede também é auditada periodicamente.

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

- Encontra-se ligado à rede, mas devidamente protegida quer por *Firewalls*, quer por equipamentos de deteção de intrusão (IDS/IPS);
- O Acesso da LRA ou ER é sempre efetuado através de canal seguro e encriptado, recorrendo à utilização de SSL com autenticação no cliente.

6.8 Validação cronológica

Certificados, CRL's e outras entradas na base de dados contêm sempre informação sobre a data e hora dessa entrada. Tal informação não é baseada em mecanismos criptográficos.

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 ER e o subscritor, está-se a utilizar o serviço de NTP (*Network Time Protocol*).

7 Perfis de Certificado, CRL e OCSP

7.1 Perfil do certificado

A emissão de certificados é feita segundo o perfil de Certificados ITU-T X.509 versão 3 e de acordo com as recomendações definidas nos RFC's 5280, 3739, ETSI TS 101 862 e ETSI 102 280.

7.1.1 Version

Neste campo os certificados contêm o valor V3 (três), de forma a identificar a utilização de certificados ITU-T X.509 versão 3.

7.1.2 Certificate extension

A EC Justiça contempla todas as extensões identificadas no RFC 5280.

7.1.2.1 AuthorityKeyIdentifier

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

7.1.2.2 SubjectKeyIdentifier

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

7.1.2.3 KeyUsage

Extensão obrigatória e crítica. Esta extensão especifica o fim a que o certificado se destina. Especificado na secção 6.1.7, deste documento.

7.1.2.4 CertificatePolicies

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

7.1.2.5 BasicConstraints

É uma extensão opcional para certificados de titular.

7.1.3 Identificadores de Algoritmo

Algoritmo	OID
Sha1WithRSAEncryption	1.2.840.113549.1.1.5
SHA-256 with RSA Encryption	1.2.840.113549.1.1.11
rsaEncryption	1.2.840.113549.1.1.1

7.1.4 Formatos de Nome

Os Certificados emitidos pela EC Justiça são referenciados através de um DN, a aplicar nos campos "*issuer*" e "*subject*" do certificado.

Os DN's são representados através de uma X.501 UTF8String.

7.1.5 Restrições de Nome

Os nomes contidos nos certificados estão restritos à utilização de DN's únicos e sem ambiguidades. O atributo "C" (*countryName*) é codificado de acordo a "ISO 3166-1-alpha-2 code elements", em *PrintableString*.

7.1.6 Objeto Identificador da Política de Certificado

Todos os certificados emitidos garantem a inclusão do OID da Política de Certificado.

7.1.7 Utilização da Extensão de Restrição de Políticas

Não aplicável.

7.1.8 Sintaxe e Semântica dos Qualificadores de Políticas

A extensão "*Certificate Policies*" contém os seguintes '*Policy Qualifiers*':

- URL: contém a URL da DPC;
- *Notice Reference*: Contém nota sobre a DPC.

7.1.9 Semântica de Processamento da Extensão Crítica de Política de Certificados

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

7.2 Perfil da CRL

As CRL's emitidas pela EC Justiça, implementam a versão 2 padrão ITU X.509, de acordo com o RFC 5280 ("*Certificate and CRL Profile*").

De salientar que, as diversas aplicações e sistemas utilizados pelos participantes que integram a SCEE, devem garantir, entre outras:

- A verificação da assinatura constante na CRL, através da chave pública constante no certificado da EC que a emite;
- A verificação da cadeia de certificação do certificado da EC;
- A verificação de que é utilizada a versão 2;
- Que no momento da verificação, a data está enquadrada nos valores indicados nos campos da CRL "thisUpdate" e "nextUpdate";
- Que a entidade que emite a CRL é a mesma que emitiu o certificado.

7.3 Perfil do OCSP

A EC Justiça não proporciona serviços OCSP.

8 Auditoria e Avaliações de Conformidade

Uma inspeção regular de conformidade a esta DPC e a outras regras, procedimentos, cerimónias e processos será levada a cabo pelos membros do Grupo de Trabalho de Auditoria da EC Justiça.

Para além de auditorias de conformidade, a EC Justiça irá efetuar outras fiscalizações e investigações para assegurar a sua conformidade com a legislação nacional. A execução destas auditorias, fiscalizações e investigações poderá ser delegada a uma entidade externa de auditoria.

8.1 Frequência ou motivo da auditoria

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

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

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

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

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

8.2 Identidade e qualificações do auditor

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

O auditor deverá ser selecionado no momento da realização de cada auditoria, devendo em termos gerais cumprir os seguintes requisitos:

- experiência em PKI’s, segurança e processos de auditoria em sistema de informação,
- independência a nível orgânico da Entidade Certificadora (para os casos de auditorias externas),
- credenciado pelo Gabinete Nacional de Segurança, no caso das auditorias de conformidade.

8.3 Relação entre o auditor e a entidade certificadora

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

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

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

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

8.4 Âmbito da auditoria

O âmbito das auditorias e outras avaliações inclui a conformidade com a legislação nacional, com o SCEE e com esta DPC e outras regras, procedimentos e processos (especialmente os relacionados com operações de gestão de chaves, recursos, controlos de gestão e operação e gestão do ciclo de vida de certificados).

Devem determinar a adequação referente aos seguintes documentos:

- Política de Segurança;
- Segurança Física;
- Avaliação Tecnológica;
- Gestão dos serviços da EC;
- Seleção de Pessoal;
- DPC e PC (em vigor);
- Contratos;
- Política de Privacidade.

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

8.5 Procedimentos após uma auditoria com resultado deficiente

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

- documenta todas as deficiências encontradas durante a auditoria;
- no final da auditoria reúne com o Grupo de Gestão da EC Justiça e apresenta de forma resumida um Relatório de Primeiras Impressões (RPI);
- elabora o relatório de auditoria;

- depois de apreciado e consolidado, é remetida uma cópia do Relatório de Auditoria Final (RAF), para o Grupo de Gestão da EC Justiça e outra para a Autoridade Credenciadora;
- tendo em conta as irregularidades constantes no relatório, a EC Justiça enviará um Relatório de Correção de Irregularidades (RCI), para a Autoridade Credenciadora, no qual deve estar descrito quais as ações, metodologia e tempo necessário para corrigir as irregularidades encontradas;
- a Autoridade Credenciadora depois de analisar este relatório toma uma das três seguintes opções, consoante o nível de gravidade/severidade das irregularidades:
  - ✓ aceita os termos, permitindo que a atividade seja desenvolvida até à próxima inspeção;
  - ✓ permite que a entidade continue em atividade por um período máximo de 60 dias até à correção das irregularidades antes da revogação;
  - ✓ revogação imediata da atividade.

8.6 Comunicação de resultados

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

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

9 Outras Situações e Assuntos legais

9.1 Taxas

9.1.1 Taxas por emissão ou renovação de certificados

Não aplicável

9.1.2 Taxas para acesso a certificado

Não aplicável

9.1.3 Taxas para acesso a informação do estado ou de revogação

Não aplicável

9.1.4 Taxas para outros serviços

Não aplicável.

9.1.5 Política de reembolso

Não aplicável.

9.2 Responsabilidade Financeira

Não aplicável.

9.3 Confidencialidade de informação processada

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

9.3.1 Âmbito da confidencialidade da informação processada

De acordo com a Política de Certificação do SCEE.

9.3.2 Informação fora do âmbito da confidencialidade da informação

De acordo com a Política de Certificação do SCEE.

9.3.3 Responsabilidade de proteção da confidencialidade da informação

Os elementos dos Grupos de Trabalho ou outras entidades que recebam informação confidencial são responsáveis por assegurar que esta não é copiada, reproduzida, armazenada, traduzida ou transmitida a terceiras partes por quaisquer meios sem antes terem o consentimento escrito da EC Justiça.

9.4 Privacidade dos dados pessoais

A EC Justiça 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.

9.4.1 Medidas para garantia da privacidade

No cumprimento do estabelecido pela lei sobre assinaturas eletrónicas, a informação de carácter pessoal disponibilizada à EC Justiça pelos titulares de certificados, será tratada de acordo com a lei de proteção de dados pessoais.

Existe um ficheiro de dados, único, de titulares de assinaturas eletrónicas no sistema que gere o ciclo de vida dos certificados sendo que o mesmo é responsabilidade da Administração de Registo.

9.4.2 Informação privada

É considerada informação privada a seguinte informação:

- Pedidos de certificados, aprovados ou negados assim como toda a informação pessoal obtida para a emissão e manutenção de certificados;
- Chaves privadas geradas e/ou armazenadas pelas EC;
- Os dados pessoais a que se refere a Lei 67/98, de 26 de Outubro.

9.4.3 Informação não protegida pela privacidade

Não é considerada confidencial a seguinte informação:

- O período de validade do certificado, assim como a sua data de emissão e a data de caducidade;
- O número de série do certificado;
- Os diferentes estados e situações do certificado e a data do início de cada um deles;

- As CRL's assim como o resto da informação do estado de revogação;
- A informação contida no Repositório das EC.

9.4.4 Responsabilidade de proteção da informação privada (dados pessoais)

Todos os participantes nos serviços fornecidos pela EC Justiça são responsáveis pela segurança dos dados pessoais e devem cumprir com a lei nacional.

9.4.5 Notificação e consentimento para utilização de informação privada

Os LRA's obtêm consentimento dos titulares para o tratamento dos dados pessoais por eles fornecidos diretamente e que constarão do formulário de pedido de certificado.

9.4.6 Divulgação resultante de processo judicial ou administrativo

A EC Justiça revelará a identidade dos titulares sempre que lhe for solicitado pelos órgãos judiciais no exercício das funções que lhe sejam atribuídas, ou seja, quando acompanhados de documento com valor jurídico perante a lei nacional em vigor.

De acordo com a Política de Certificação do SCEE.

9.4.7 Outras circunstâncias para revelação de informação

Não aplicável.

9.5 Direitos de propriedade intelectual

Todos os direitos de propriedade intelectual, incluindo os que se referem a certificados e CRL's emitidos, OID's, DPC's e PC's bem como qualquer outro documento propriedade da EC Justiça, pertencem a esta.

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

9.6 Representações e garantias

9.6.1 Representação e garantias das Entidades Certificadoras

De acordo com a Política de Certificação do SCEE.

9.6.2 Representação e garantias das Entidade de Registo

De acordo com a Política de Certificação do SCEE.

9.6.3 Representação e garantias dos titulares

De acordo com a Política de Certificação do SCEE.

9.6.4 Representação e garantias das partes confiantes

De acordo com a Política de Certificação do SCEE.

9.6.5 Representação e garantias de outros participantes

É obrigação das entidades referenciadas no ponto 1.3.5.2 cumprirem todas as cláusulas estipuladas nos respetivos contratos celebrados entre estas e o IGFEJ.

9.7 Renúncia de garantias

De acordo com a Política de Certificação do SCEE.

9.8 Limitações às obrigações

De acordo com a Política de Certificação do SCEE.

9.9 Indemnizações

De acordo com a legislação em vigor.

9.10 Duração e término da DPC

9.10.1 Duração

Esta DPC entra em vigor no momento da sua publicação no repositório da EC Justiça.

Esta DPC estará em vigor enquanto não for substituída por uma nova versão ou pela renovação das chaves da EC Justiça, momento em que obrigatoriamente se redigirá uma nova versão.

9.10.2 Término

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

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

9.10.3 Consequências do término da DPC

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

9.11 Notificação individual e comunicação aos participantes

Todos os participantes devem utilizar métodos razoáveis para comunicar uns com os outros. Esses métodos podem incluir correio eletrónico assinado digitalmente, fax, formulários assinados, ou outros, dependendo da criticidade e assunto da comunicação.

9.12 Alterações

9.12.1 Procedimento para alterações

A autoridade com atribuições para aprovar as alterações sobre esta DPC é o Grupo de Gestão da EC Justiça. Os dados de contacto encontram-se no ponto 1.5. Posteriormente estas alterações são submetidas ao Conselho Gestor do SCEE para aprovação deste.

9.12.2 Prazo e mecanismo de notificação

Caso o Grupo de Gestão da EC Justiça considere que as alterações à especificação podem afetar a aceitabilidade dos certificados para propósitos específicos, comunicar-se-á aos utilizadores destes que se efetuou uma mudança e que devem consultar a nova DPC no repositório estabelecido.

9.12.3 Motivos para mudar de OID

A EC Justiça deve determinar se as alterações à DPC obrigam a uma mudança no OID da política de Certificados ou no URL que aponta para a DPC.

Nos casos em que, a julgamento do Grupo de Gestão da EC Justiça, as alterações da DPC não afetem a aceitação dos certificados, proceder-se-á ao aumento do número menor de versão do documento, mantendo o número maior da versão do documento, assim como o

OID associado. Não se considera necessário comunicar este tipo de modificações aos utilizadores dos certificados.

No caso em que o Grupo de Gestão da EC Justiça julgue que as alterações à especificação podem afetar aceitabilidade dos certificados para propósitos específicos, proceder-se-á ao aumento do número maior de versão do documento e colocado a zero o número menor da mesma. Também se modificarão os dois últimos números do Identificador de Objeto (OID) que o representa. Este tipo de modificações comunicar-se-á aos utilizadores dos certificados segundo o estabelecido no ponto 9.12.2.

9.13 Disposições para resolução de conflitos

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

9.14 Legislação aplicável

É aplicável à atividade das entidades certificadoras a seguinte legislação específica:

- Despacho nº 27008/2004 (2ª série), de 28 de Dezembro, publicado no D.R II, nº 302 de 28 de Dezembro – Estabelece as normas e especificações técnicas elaboradas e publicadas pelo Instituto de Normalização para as Telecomunicações (ETSI) e pelo Comité Europeu de Normalização (CEN), no âmbito da European Electronic Signature Standardisation Initiative (EESSI);
- Portaria nº 597/2009, de 4 de Julho – Fixa os termos a que obedece o registo das entidades certificadoras que emitem certificados qualificados;
- Despacho nº 16445/2004, de 29 de Julho, publicado no D.R II, nº 190 de 13 de Agosto – Estabelece as especificações técnicas emitidas para algoritmos criptográficos e parâmetros elaborados pelo ETSI – Technical Committee Electronic Signatures and Infrastructures (ESI);
- Aviso nº 8134/2004, de 29 de Julho, publicado no D.R II, nº 190 de 13 de Agosto;
- Decreto Regulamentar nº. 25/2004, de 15 de Julho – Aprova as regras técnicas e de segurança exigíveis às entidades certificadoras que emitem certificados qualificados, regulamentando ainda alguns aspetos específicos relacionados com a credenciação das entidades certificadoras;
- Decreto-Lei nº 290-D/99, de 2 de Agosto republicado pelo Decreto-Lei nº 88/2009, de 9 de Abril – Regula a validade, eficácia e valor probatório dos documentos eletrónicos, a assinatura eletrónica e a atividade de certificação de entidades certificadoras;
- Portaria nº 1370/2000, publicada no D.R. nº 211, II série de 12 de Setembro – Define as caraterísticas do contrato de seguro obrigatório de responsabilidade civil a que se refere a alínea d) do art.º 12º do Decreto-Lei nº 290-D/99, de 2 de Agosto.

9.15 Conformidade com a legislação em vigor

É responsabilidade do Grupo de Gestão da EC Justiça velar pelo cumprimento da legislação aplicável listada no ponto anterior.

9.16 Providências várias

9.16.1 Acordo completo

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

9.16.2 Independência

No caso em 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 válida apenas e só nos casos em que tais estipulações não sejam consideradas essenciais. É responsabilidade do Grupo de Gestão da EC Justiça a avaliação da essencialidade das mesmas.

9.16.3 Severidade

Não aplicável.

9.16.4 Execuções (taxas de advogados e desistência de direitos)

Não aplicável.

9.16.5 Força maior

Não aplicável.

9.17 Outras providências

Não aplicável.

Aprovação pelo Grupo de Gestão

Carlos Brito (Assinatura)

Assinado de forma digital por Carlos Brito (Assinatura)
DN: givenName=Carlos, sn=Brito, title=Vogal do CD do IGFEJ IP, c=PT, o=MJ, ou=IGFEJ, ou=Conselho Diretivo, cn=Carlos Brito (Assinatura)
Dados: 2014.03.19 09:05:39 Z

Nuno Fonseca (Assinatura)

Assinado de forma digital por Nuno Fonseca (Assinatura)
DN: givenName=Nuno, sn=Fonseca, title=Director, c=PT, o=MJ, ou=IGFEJ, ou=DSST, cn=Nuno Fonseca (Assinatura)
Dados: 2014.03.19 22:11:27 Z

Joel Pereira (Assinatura)

Assinado de forma digital por Joel Pereira (Assinatura)
DN: givenName=Joel, sn=Pereira, title=Juiz de Direito, c=PT, o=MJ, ou=CSM, ou=Tribunais, cn=Joel Pereira (Assinatura)
Dados: 2014.03.26 20:40:49 Z

Carlos José Sousa Mendes (Assinatura)

Assinado de forma digital por Carlos José Sousa Mendes (Assinatura)
DN: givenName=Carlos José, sn=Sousa Mendes, title=Procurador da República, c=PT, o=MJ, ou=PGR, ou=Tribunal do Trabalho de Lisboa, cn=Carlos José Sousa Mendes (Assinatura)
Dados: 2014.03.27 15:28:44 Z