IGFEJ
INSTITUTO DE GESTÃO FINANCEIRA E EQUIPAMENTOS DA JUSTIÇA I.P.

Declaração de Divulgação de Princípios

Política

Identificação da CA: EC da Justiça

Nível de Acesso: Público

Versão: 1.4

Data: 30-08-2013

Tipologia documental: Política

Título: Declaração de Divulgação de Princípios

Nome do ficheiro: Declaração de Divulgação de Princípios.pdf

Língua original: Português

Língua de publicação: Português

Nível de acesso: Restrito

Data: 30-08-2013

Versão atual: 1.4

Autoria: Claudia Carvalho ..... **Data:** 30-08-2013

Verificação: Claudia Carvalho ..... **Data:** 30-08-2013

Revisão: Sandra Mendonça ..... **Data:** 17-03-2014

Aprovação: Grupo de Gestão da EC Justiça

Identificação da CA: EC da Justiça

Histórico de Versões

N.º de Versão	Data	Autor(es)
1.0	19/01/2009	Sandra Mendonça
1.1	21/03/2011	Claudia Carvalho
1.2	15/03/2012	Claudia Carvalho
1.3	22/01/2013	Claudia Carvalho
1.4	30/08/2013	Claudia Carvalho

Índice

Resumo Executivo

Este documento foi elaborado tendo em conta as especificações técnicas relatadas no anexo B da norma "*ETSI TS 101 456: Policy requirements for certification authorities issuing qualified certificates*".

A Declaração de Divulgação de Princípios da EC da Justiça não constitui uma Política de Certificados sob a qual se regem os certificados emitidos pela EC da Justiça. Para este efeito devem ser consultadas as Políticas de Certificados e Declaração de Práticas de Certificação disponíveis em http://icp.igfej.mj.pt.

1 Introdução

1.1 Objetivos

Este documento pretende resumir, de forma simples e acessível, as características descritas nas Políticas de Certificado e Declaração de Políticas de Certificação da Infraestrutura de chave pública da Entidade de Certificação da Justiça.

A infraestrutura da Entidade de Certificação da Justiça fornece uma hierarquia de confiança, que promove a segurança eletrónica do titular do certificado. A hierarquia de confiança da Entidade de Certificação da Justiça encontra-se englobada na hierarquia do Sistema de Certificação Eletrónica do Estado Português (SCEE) – Infraestrutura de Chaves Públicas do Estado.

1.2 Público-Alvo

Este documento deve ser lido por:

- Titulares de Certificados de Assinaturas Digitais Qualificadas emitidos pela EC da Justiça.

1.3 Estrutura do Documento

Este documento encontra-se dividido em 11 capítulos.

2 Contactos da Entidade de Certificação da Justiça

NOME	ENTIDADE GESTORA DE ENTIIDADE DE CERTIFICAÇÂO ELETRÓNICA DA JUSTIÇA
Gestor:	**Grupo de Gestão da EC da Justiça**
Morada:	**Av. D. João II, nº 1.08.01E, Torre H, Piso 12, 1990-097 Lisboa**
Correio eletrónico:	**AdminCa@igfej.mj.pt**
Página Internet:	**http://icp.igfej.mj.pt**
Telefone:	**+ 351 217907700**
Fax:	**+ 351 217908882**

3 Tipos de Certificados, procedimentos de validação e utilização

A EC da Justiça emite os seguintes tipos de certificados digitais para os titulares:

- Certificado Digital de Assinatura Qualificada (Formato X.509) – A assinatura digital é o único meio legalmente aceite para assinar documentos eletrónicos. Com o certificado digital de assinatura qualificada, o titular pode assinar correio eletrónico e documentos eletrónicos. Ao utilizar o certificado digital de assinatura qualificada, o titular garante a integridade dos conteúdos, autenticidade da sua assinatura e não repúdio, não podendo negar que assinou determinado conteúdo.
- Certificado Digital de Autenticação (Formato X.509) – A utilização do certificado digital de autenticação permite ao titular comprovar a sua identidade perante um sistema de informação.
- Certificado Digital de Cifra (Formato X.509) – A utilização do certificado digital de cifra permite ao titular a utilização em qualquer aplicação garantindo assim confidencialidade.

É possível verificar o estados dos certificados de assinatura, autenticação e cifra emitidos pela Entidade Certificadora da Justiça, através da consulta da CRL (Lista de Certificados Revogados) disponível em http://icp.igfej.mj.pt.

4 Limitação de confiança nos certificados

A utilização dos certificados emitidos para os titulares deve obedecer ao descrito nas respetivas políticas de certificados disponíveis em http://icp.igfej.mj.pt.

O certificado de Assinatura Digital Qualificada emitido segundo esta política é equivalente a um certificado digital qualificado, nos termos do definido na Legislação Portuguesa aplicável para o efeito, sendo utilizado em qualquer aplicação para efeitos de assinatura digital qualificada.

O titular do certificado de Assinatura Digital Qualificada encontra-se devidamente identificado pelo nome único (*distinguished name*) do respetivo certificado.

5 Responsabilidades dos Titulares

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) a quem estiver designado no campo "*Subject*" do certificado;

b) enquanto o certificado se mantiver válido e não estiver na CRL da Entidade de Certificação.

Adicionalmente, o certificado de assinatura digital qualificada atribuído a pessoa singular tem como objetivo a sua utilização em qualquer aplicação para efeitos de assinatura digital qualificada.

O titular pode solicitar a revogação de um determinado certificado, havendo conhecimento ou suspeita de compromisso da chave privada do titular ou qualquer outro ato que recomende esta ação. A Entidade de Certificação guarda toda a documentação utilizada para verificação da identidade e autenticidade da entidade que efetua o pedido de revogação.

Um certificado pode ser revogado por uma das seguintes razões:

- Comprometimento ou suspeita de comprometimento da chave privada;

- Perda da chave privada;
- Inexatidões graves nos dados fornecidos;
- Comprometimento ou suspeita de comprometimento da senha de acesso à chave privada (PIN);
- Comprometimento ou suspeita de comprometimento da chave privada da Entidade de Certificação da Justiça;
- Perda, destruição ou deterioração do dispositivo de suporte da chave privada (por exemplo, suporte/token criptográfico);
- Revogação do certificado da Entidade de Certificação da Justiça;
- Incumprimento por parte da Entidade de Certificação ou do titular das responsabilidades previstas;
- Sempre que haja razões credíveis que induzam que os serviços de certificação possam ter sido comprometidos, de tal forma que coloquem em causa a fiabilidade dos certificados;
- Por resolução judicial ou administrativa.

Na utilização do certificado e da chave pública deve ser garantido o cumprimento das seguintes condições:

a) Ter conhecimento de que o certificado se destina, exclusivamente, a ser utilizado no exercício das sua funções profissionais, carecendo a sua emissão de autorização do dirigente máximo ou responsável competente do organismo a que pertence, e no âmbito da respetiva Política de Certificado, de acordo com o especificado na Declaração de Práticas de Certificação, comprometendo-se a fazer dele um uso próprio;

b) Ser o único detentor da sua chave privada mantendo sobre ela um controlo exclusivo, assegurando a privacidade do *smartcard* e a confidencialidade do respetivo PIN de acesso;

c) Ter conhecimento e perceber a utilização e funcionalidades proporcionadas pela criptografia de chave pública e certificados;

d) Ser responsável pela sua correta utilização;

e) Ler e entender os termos e condições descritos nas Políticas e Práticas de Certificação;

f) Verificar os certificados (validação de cadeias de confiança) e Lista de Certificados Revogados tendo especial atenção às suas extensões marcadas como críticas e propósito das chaves;

g) Confiar nos certificados, utilizando-os sempre que estes estejam válidos;

h) Ter conhecimento de que a informação atualizada acerca das suas responsabilidades e obrigações como titular de um certificado digital emitido pelo IGFEJ, pode ser consultada em http://icp.igfej.mj.pt/ ou solicitada por carta ao Administrador da Autoridade de Registo (Av. D. João II, nº 1.08.01E, Torre H, Piso 12, 1990-097 Lisboa).

Os utilizadores de uma chave pública têm que ter confiança que a chave privada associada é detida pelo titular remoto correto (pessoa ou sistema) com o qual irão utilizar mecanismos de cifra ou assinatura digital. A confiança é obtida através do uso de certificados digitais X.509 v3, que são estrutura de dados que fazem a ligação entre a chave pública e o seu titular. Esta ligação é afirmada através da assinatura digital de cada certificado por uma Entidade de Certificação (EC) de confiança. A EC pode basear esta afirmação em meios técnicos (por exemplo, prova de posse da chave privada através de um protocolo desafio-resposta), na apresentação da chave privada, ou no registo efetuado pelo titular.

Um certificado tem um período limitado de validade, indicado no seu conteúdo e assinado pela Entidade de Certificação. Como a assinatura do certificado e a sua validade podem ser verificadas independentemente por qualquer *software* que utilize certificados, os certificados podem ser distribuídos

através de linhas de comunicação e sistemas públicos, assim como podem ser guardados em qualquer tipo de unidades de armazenamento.

O utilizador de um serviço de segurança que requeira o conhecimento da chave pública do utilizador necessita, normalmente, de obter e validar o certificado que contém essa chave. Se o serviço não dispuser de uma cópia fidedigna da chave pública da Entidade de Certificação (EC) que assinou o certificado, assim como do nome da EC e informação relacionada (tal como o período de validade), então poderá necessitar de um certificado adicional para obter a chave pública da EC e validar a chave pública do utilizador. Em geral, para validar a chave pública de um utilizador, pode ser necessária uma cadeia de múltiplos certificados, incluindo o certificado da chave pública do utilizador assinado por uma EC e, zero ou mais certificados adicionais de EC assinados por outras EC.

6 Verificação do estado de certificados do Titular por outras partes

Outras partes que confiam nos certificados emitidos pela Entidade de Certificação da Justiça devem:

- Verificar o estado do certificado no momento da sua utilização e assumir a responsabilidade dessa verificação;
- Obedecer ao especificado nas Políticas de Certificado do certificado em causa;
- Utilizar o certificado adequadamente de acordo com os objetivos da sua emissão.

7 Limitação de responsabilidades

A Entidade de Certificação da Justiça não se responsabiliza pelo uso indevido dos certificados digitais.

A Entidade de Certificação da Justiça não se responsabiliza por qualquer utilização dos certificados digitais que não conste na Declaração de Práticas de Certificação ou na Política de Certificados.

A utilização dos certificados digitais emitidos para os titulares e a proteção das chaves privada/pública é da exclusiva responsabilidade do titular.

8 Acordos aplicáveis, Declaração de Práticas de Certificação e Políticas de Certificação

Todos os acordos aplicáveis, Declarações de Práticas de Certificação e Políticas de Certificado encontram-se disponibilizados em http://icp.igfej.mj.pt/.

9 Política de privacidade

A informação do titular constante do pedido de emissão dos certificados digitais não se encontra publicada e é processada de acordo com a Política de Certificação do Sistema de Certificação Eletrónica do Estado.

10 Legislação e normas

A EC da Justiça baseia-se essencialmente nos seguintes documentos jurídicos:

- Diretiva 1999/93/CE de 13 Dezembro 1999, relativa a um quadro legal comunitário para as assinaturas eletrónicas
- Decreto-Lei n.º 290-D/99, de 2 de Agosto, republicado pelo DL 88/2009, de 9 de Abril, que aprova o regime jurídico dos documentos eletrónicos e da assinatura digital.
- Decreto Regulamentar nº 25/2004 de 15 de Julho de 2004, que regulamenta o DL 290-D/99.

11 Auditorias e normas de segurança

Todas as intervenções realizadas à EC da Justiça são devidamente auditadas por auditores internos. A EC da Justiça é ainda auditada por auditores de segurança, conforme o disposto no artigo 33.º do Decreto-Lei 290-D/99, republicado pelo DL 88/2009, de 9 de Abril.

Os Certificados Digitais Qualificados emitidos pela EC da Justiça cumprem todos os requisitos técnicos definidos nas seguintes normas:

- CWA 14167- Cryptographic Module for CSP Signing Operations — Protection Profile
- CWA 14169:2004 - Secure signature-creation devices "EAL 4+"
- ETSI TS 101 456 V1.4.3 (2007-05) Electronic Signatures and Infrastructures (ESI)
- ETSI TS 102 042 V1.1.1 (2002-04) Policy requirements for certification authorities issuing public key certificates
- ETSI TS 101 862 V1.3.1 (2004-03) Qualified Certificate profile

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 09:06:01 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 14:36:01 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 20:39:47 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 15:21:08 Z