CARTÃO DE CIDADÃO

Declaração de Divulgação de Princípios

Política

PJ.CC_24.1_0001_pt_Root-AsC-AuC.doc

Identificação do Projecto: PKI do Cartão de Cidadão

Identificação da CA: Root-AsC-AuC

Nível de Acesso: Público

Versão: 1.1

Data: 29/06/2012

Identificador do documento: PJ.CC_24.1_0001_pt_Root-AsC-AuC.doc

Palavras-chave: declaração ; divulgação ; princípios

Tipologia documental: Política

Título: Declaração de Divulgação de Princípios

Língua original: Português

Língua de publicação: Português

Nível de acesso: Público

Data: 29/06/2012

Versão actual: 1.1

Identificação do Projecto: PKI do Cartão de Cidadão

Identificação da CA: Root-AsC-AuC

Cliente: Ministério da Justiça

Documentos Relacionados

ID Documento	Detalhes	Autor(es)
PJ.CC_24.1.1_0001_pt_Root.pdf	Declaração de Práticas de Certificação da EC do Cidadão	MULTICERT S.A.
PJ.CC_24.1.1_0002_pt_AsC.pdf	Declaração de Práticas de Certificação da EC de Assinatura Digital Qualificada do Cartão de Cidadão	MULTICERT S.A.
PJ.CC_24.1.2_0001_pt_Root.pdf	Política de Certificados da EC do Cidadão	MULTICERT S.A.
PJ.CC_24.1.2_0002_pt_Root.pdf	Política de Certificados da EC de Assinatura Digital Qualificada do Cartão de Cidadão	MULTICERT S.A.
PJ.CC_24.1.2_0009_pt_AsC.pdf	Política de Certificados de Assinatura Digital Qualificada	MULTICERT S.A.

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 PKI do Cartão de Cidadão não constitui uma Política de Certificados sob a qual se regem os certificados emitidos pela PKI do Cartão de Cidadão. Para este efeito devem ser consultadas as Políticas de Certificados e Declaração de Práticas de Certificação disponíveis em https://pki.cartaodecidadao.pt/.

Sumário

Introdução

Objectivos

Este documento pretende resumir, de forma simples e acessível, as características descritas nas Políticas de Certificado e Declaração de Políticas de Certificação da Infra-estrutura de chave pública da Entidade de Certificação do Cartão de Cidadão.

A infra-estrutura da Entidade de Certificação do Cartão do Cidadão (ou Entidade de Certificação do Cidadão) fornece uma hierarquia de confiança, que promove a segurança electrónica do Cidadão no seu relacionamento com o Estado. A Entidade de Certificação do Cidadão estabelece uma estrutura de confiança electrónica que proporciona a realização de transacções electrónicas seguras, a autenticação forte, um meio de assinar electronicamente transacções ou informações e documentos electrónicos, assegurando a sua autoria, integridade e não repúdio, e assegurando a confidencialidade das transacções ou informação.

A hierarquia de confiança da Entidade de Certificação do Cartão do Cidadão encontra-se englobada na hierarquia do Sistema de Certificação Electrónica do Estado Português1 (SCEE) – Infra-Estrutura de Chaves Públicas do Estado.

Público-Alvo

Este documento deve ser lido pelos Titulares de Certificados de Assinaturas Digitais Qualificadas emitidos pela PKI do Cartão de Cidadão

Estrutura do Documento

Este documento encontra-se dividido em 10 capítulos.

1 Contactos da Entidade de Certificação do Cartão de Cidadão

Nome:	MINISTÉRIO DA JUSTIÇA
Morada:	IRN I.P. Av. D. João II, nº 1.8.01D Edifício H Campus da Justiça Apartado 8295 1803-001 Lisboa
Correio electrónico:	cartaodecidadao@dgrn.mj.pt
Telefone:	707200886

2 Tipos de Certificados, procedimentos de validação e utilização

A PKI do Cartão de Cidadão emite os seguintes tipos de certificados digitais para os cidadãos:

- Certificado Digital de Assinatura Qualificada (Formato X.509) – A assinatura digital é um único meio legalmente aceite para assinar documentos electrónicos. Com o certificado digital de assinatura qualificada, o cidadão pode assinar correio electrónico, documentos electrónicos e, inclusivamente, fazer transacções electrónicas. Ao utilizar o certificado digital de assinatura qualificada, o cidadão garante a integridade dos conteúdos, autenticidade da sua assinatura e não repudio, não podendo negar que assinou determinado conteúdo.
- Certificado Digital de Autenticação (Formato X.509) – A utilização do certificado Digital de autenticação permite ao cidadão comprovar a sua identidade perante um sistema de informação.

Ambos os certificados de assinatura e autenticação constam no Cartão de Cidadão, podendo verificar-se o seu estado através do serviço OCSP (*Online Certificate Status Protocol*) e/ou da consulta das LRC (Listas de Revogação de Certificados) emitidas para cada um dos casos e disponíveis em https://pki.cartaodecidadao.pt/publico/lrc/.

3 Limitação de confiança nos certificados

A utilização dos certificados emitidos para os cidadãos deve obedecer ao descrito nas respectivas políticas de certificados disponíveis em http://pki.cartaodecidadao.pt/publico/politicas/cp.html.

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 Cidadão (pessoa singular) é o titular do certificado de Assinatura Digital Qualificada e encontra-se devidamente identificado pelo nome único (*distinguished name*) do respectivo certificado.

4 Responsabilidades dos Cidadãos

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 Lista de Revogação de Certificados da Entidade de Certificação.

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

O Cidadão pode solicitar a revogação de um determinado certificado, havendo conhecimento ou suspeita de compromisso da chave privada do titular ou qualquer outro acto que recomende esta acção.

No caso do Certificado de pessoa singular os motivos para a revogação de um certificado está definido nos Artigos 18.º e 33.º da Lei n.º 7/2007 de 5 de Fevereiro.

Para qualquer certificado emitido no Âmbito do Cartão de cidadão podem ser causas para a sua revogação:

a) Comprometimento ou suspeita de comprometimento da chave privada da Entidade de Certificação de Assinatura Digital Qualificada ou de outra EC no "caminho" até à Entidade de Certificação Electrónica do Estado;

b) Perda, destruição ou deterioração do dispositivo de suporte da chave privada (por exemplo, suporte/*token* criptográfico);

c) Revogação do certificado da Entidade de Certificação do Cartão de Cidadão ou de outra EC no "caminho" até à Entidade de Certificação Electrónica do Estado;

d) Incumprimento por parte da Entidade de Certificação ou titular das responsabilidades previstas;

e) 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;

f) Por resolução judicial ou administrativa.

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

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

b) Ser responsável pela sua correcta utilização;

c) Ler e entender os termos e condições descritos nas Politicas e práticas de certificação;

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

e) Confiar nos certificados, utilizando-os sempre que estes estejam válidos.

Os utilizadores de uma chave pública têm que ter confiança que a chave privada associada é detida pelo titular remoto correcto (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 efectuado 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 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.

5 Verificação do estado de certificados do Cidadão por outras partes

Outras partes que confiam nos certificados emitidos pela Entidade de Certificação do Cartão de Cidadão 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 objectivos da sua emissão.

6 Limitação de responsabilidades

A Entidade de Certificação do Cartão de Cidadão (ECCC) não se responsabiliza pelo uso indevido dos certificados digitais.

A ECCC não se responsabiliza por qualquer utilização dos certificados digitais que não conste na Declaração de Políticas de Certificação ou na Política de Certificados.

A utilização dos certificados digitais emitidos para os cidadãos e a protecção das chaves privada/pública é da exclusiva responsabilidade do Cidadão.

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

Todos os acordos aplicáveis, Declarações de Política de Certificação e Políticas de Certificação encontram disponíveis em https://pki.cartaodecidadao.pt/.

8 Política de privacidade

A informação do Cidadão constante nos respectivos certificados digitais não se encontra publicada e é processada de acordo com a Política de Certificação da Sistema de Certificação Electrónica do Estado.

9 Legislação e normas

A PKI do Cartão de Cidadão baseia-se essencialmente nos seguintes documentos jurídicos:

- Directiva 1999/93/CE de 13 Dezembro 1999, relativa a um quadro legal comunitário para as assinaturas electrónicas
- Decreto-Lei nº 62/2003, de 3 de Abril de 2003, altera o Decreto-Lei n.º 290-D/99, de 2 de Agosto, que aprova o regime jurídico dos documentos electrónicos e da assinatura digital.
- Decreto Regulamentar nº 25/2004 de 15 de Julho de 2004, que aprova o regime jurídico dos documentos electrónicos e da assinatura digital.
- Lei n.º 7/2007 de 5 de Fevereiro que cria o cartão de cidadão e rege a sua emissão, substituição, utilização e cancelamento.

10 Auditorias e normas de segurança

Todas as intervenções realizadas à PKI do Cartão de Cidadão são devidamente auditadas por auditores internos. A PKI do Cartão do Cidadão é ainda auditada pela Autoridade Nacional de Segurança, conforme o disposto no artigo 8.º do Decreto-Lei 116-A/2006.

Os Certificados Digitais Qualificados emitidos pela PKI do Cartão de Cidadão 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 do Conselho Gestor

ANTÓNIO MANUEL MARTINS DA CRUZ	Assinado de forma digital por ANTÓNIO MANUEL MARTINS DA CRUZ DN: cn=ANTÓNIO MANUEL MARTINS DA CRUZ, serialNumber=BI103203710, givenName=ANTÓNIO MANUEL, sn=MARTINS DA CRUZ, ou=Assinatura Qualificada do Cidadão, ou=Cidadão Português, o=Cartão de Cidadão, c=PT Dados: 2012.06.29 22:27:01 +01'00'
GONÇALO NUNO MENDES DE ALMEIDA CASEIRO	Assinado de forma digital por GONÇALO NUNO MENDES DE ALMEIDA CASEIRO DN: c=PT, o=Cartão de Cidadão, ou=Cidadão Português, ou=Assinatura Qualificada do Cidadão, sn=MENDES DE ALMEIDA CASEIRO, givenName=GONÇALO NUNO, serialNumber=BI116298120, cn=GONÇALO NUNO MENDES DE ALMEIDA CASEIRO Dados: 2012.07.02 11:52:40 +01'00'
José António Alves Rodrigues	Assinado de forma digital por José António Alves Rodrigues DN: givenName=José António, sn=Alves Rodrigues, title=Especialista de Informática, c=PT, o=MJ, ou=ITIJ, ou=DIEAS, cn=José António Alves Rodrigues Dados: 2012.07.02 10:22:30 +01'00'
João Pedro Monteiro Rodrigues	Assinado de forma digital por João Pedro Monteiro Rodrigues DN: c=PT, o=Ministério da Justiça, ou=Instituto dos Registos e do Notariado IP, cn=João Pedro Monteiro Rodrigues Dados: 2012.07.02 11:06:15 +01'00'