

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-CMD

Nível de Acesso: Público

Versão: 2.0

Data: 03/07/2018

Identificador do documento: PJ.CC_24.1.1_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: 03/07/2018

Periodicidade de Revisão: 1 ano

Versão actual: 2.0

Identificação do Projecto: PKI do Cartão de Cidadão

Identificação da CA: Root-AsC-AuC-CMD

Cliente: Ministério da Justiça

Histórico de Versões

Versão	Data	Detalhes	Autor(es)
1.0	29/06/2012	Versão inicial	GT Políticas
1.1-1.2	15/01/2018	Revisão eIDAS	GT Políticas
2.0	03/07/2018	Versão Aprovada	GG

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 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirement.*

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

Declaração de Divulgação de Princípios	1
Resumo Executivo.....	3
Sumário.....	4
Introdução	5
Objetivos.....	5
Público-Alvo	5
Estrutura do Documento.....	5
1 Contactos da Entidade de Certificação do Cartão de Cidadão.....	6
2 Tipos de Certificados, procedimentos de validação e utilização.....	6
3 Limitação de confiança nos certificados	6
4 Responsabilidades dos Cidadãos.....	7
5 Verificação do estado de certificados do Cidadão por outras partes.....	8
6 Verificação do Estado de Certificados.....	9
7 Limitação de responsabilidades	9
8 Acordos aplicáveis, Declaração de Práticas de Certificação e Políticas de Certificação.....	10
9 Política de privacidade	10
10 Indemnizações	10
11 Legislação e normas	10
12 Repositórios, Auditorias e normas de segurança.....	10
Aprovação.....	12

Introdução

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 do Cartão de Cidadão.

A infraestrutura da Entidade de Certificação do Cartão do Cidadão (ou Entidade de Certificação do Cidadão) fornece uma hierarquia de confiança, que promove a segurança eletrónica do Cidadão no seu relacionamento com o Estado. A Entidade de Certificação do Cidadão estabelece uma estrutura de confiança eletrónica que proporciona a realização de transações eletrónicas seguras, a autenticação forte, um meio de assinar eletronicamente transações ou informações e documentos eletrónicos, assegurando a sua autoria, integridade e não repúdio, e assegurando a confidencialidade das transações ou informação.

A hierarquia de confiança da Entidade de Certificação do Cartão do Cidadão encontra-se englobada na hierarquia do Sistema de Certificação Eletrónica do Estado Português (SCEE) – Infraestrutura 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 12 capítulos.

1 Contactos da Entidade de Certificação do Cartão de Cidadão

Nome:	MINISTÉRIO DA JUSTIÇA
Morada:	IRN I.P. - DIC Av. D. João II, nº 1.8.01D Edifício H Campus da Justiça Apartado 8295 1803-001 Lisboa
Correio eletrónico:	cartaodecidadao@irn.mj.pt
Telefone:	211 950 500

2 Tipos de Certificados, procedimentos de validação e utilização

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

- Certificado Digital de Assinatura Qualificada (Formato X.509) – A assinatura digital é um único meio legalmente aceite para assinar documentos eletrónicos. Com o certificado digital de assinatura qualificada, o cidadão pode assinar correio eletrónico, documentos eletrónicos e, inclusivamente, fazer transações eletrónicas. Ao utilizar o certificado digital de assinatura qualificada, o cidadão 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 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 respetivas 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 respetivo 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 objetivo 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, alterada pela Lei n.º 91/2015.

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 Eletrónica 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 Eletrónica 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 correta utilização;
- c) Ler e entender os termos e condições descritos nas Políticas e práticas de certificação;
- d) Verificar os certificados (validação de cadeias de confiança) e 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 PKI do Cartão de Cidadão (PKI CC) 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.

6 Verificação do Estado de Certificados

Outras partes que confiam nos certificados emitidos pela PKI CC devem:

- Verificar o estado do certificado no momento da sua utilização, utilizando os mecanismos
- OCSP e LRC indicados anteriormente, 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 PKI CC:

- Responde pelos prejuízos que cause aos titulares ou a terceiros pela falta ou atraso na inclusão no serviço de consulta sobre a vigência dos certificados, da revogação ou suspensão dum certificado, uma vez que tenha conhecimento dele;
- Só responde pelos danos e prejuízos causados pelo uso indevido do certificado reconhecido, quando não tenha consignado no certificado, de forma clara reconhecida por terceiros o limite quanto ao possível uso.
- A responsabilidade da administração / gestão da PKI assenta sobre base objetiva e cobre todo o risco que os particulares sofram sempre que seja consequência do funcionamento normal ou anormal dos seus serviços;
- Não responde se o destinatário dos documentos assinados eletronicamente não os comprovar e tiver em conta as restrições que figuram no certificado quanto às suas possíveis utilizações;
- Não se responsabiliza pelo uso indevido dos certificados digitais;
- 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 é da exclusiva responsabilidade do Cidadão;
- No âmbito do Cartão de Cidadão a protecção das chaves privada/pública é da exclusiva responsabilidade do Cidadão;
- Não assume qualquer responsabilidade no caso de perda ou prejuízo:
 - Dos serviços que prestam, em caso de guerra, desastres naturais ou qualquer outro caso de força maior;
 - Ocasionalmente pelo uso dos certificados quando excedam os limites estabelecidos pelos mesmo na Política de Certificados e correspondente DPC;
 - Ocasionalmente pelo uso indevido ou fraudulento dos certificados ou LRC emitidos pelas ECs da PKI do CC.

8 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/>.

9 Política de privacidade

A PKI do CC tem medidas implementadas que garantem a privacidade dos dados pessoais, de acordo com a legislação portuguesa, garantindo que a informação do titular, constante nos respetivos certificados digitais, não se encontra publicada, sendo processada de acordo com a Política de Certificação da Sistema de Certificação Eletrónica do Estado.

10 Indemnizações

De acordo com a legislação em vigor.

11 Legislação e normas

A PKI do CC baseia-se essencialmente nos seguintes documentos jurídicos:

- Regulamento n.º 910/2014 de 23 de julho de 2014 do Parlamento Europeu e do Conselho, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE;
- Lei n.º 7/2007, de 5 de fevereiro, alterada pela Lei n.º 91/2015, de 12 de agosto e rege a sua emissão, substituição, utilização e cancelamento;

12 Repositórios, Auditorias e normas de segurança

Toda a informação referente à PKI do CC encontra-se disponível publicamente no repositório acessível em <http://pki.cartaodecidadao.pt>.

Todas as intervenções realizadas à PKI do Cartão de Cidadão são devidamente auditadas por auditores internos. A PKI do CC é auditada por um Organismo de Avaliação da Conformidade (devidamente registado no Organismo Nacional de Acreditação), o qual emite um Relatório de Conformidade (CAR) a ser disponibilizado à Entidade Supervisora, para avaliar a continuidade de disponibilização de serviços de confiança.

As Auditorias de conformidade deverão ocorrer, pelo menos, a cada 12 meses, com intuito de confirmar que a PKI do CC, como prestadora qualificada de serviços de confiança e os serviços de confiança que disponibiliza, cumprem os requisitos estabelecidos pelo Regulamento 910/2014.

Os Certificados Digitais Qualificados emitidos pela PKI do CC 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 EN 319 401 v2.1.1 – Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
- ETSI EN 319 411-1 v1.1.1 – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;
- ETSI EN 319 411-2 v2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part. 2: Requirements for Trust Service providers issuing EU qualified certificates;
- ETSI EN 319 412-1 v1.1.1 – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures;
- ETSI EN 319 412-2 v2.1.1 – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons;
- ETSI EN 319 412-5 v2.1.1 – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements;
- Regulamento (UE) n.o 910/2014 do Parlamento Europeu e do Conselho de 23 de julho de 2014 relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE;

Aprovação