

Política de Certificado de Validação on-line OCSP emitido pela EC AsC

Política

PJ.CC_24.1.2_0010_pt_AsC.pdf

Identificação do Projeto: Cartão de Cidadão

Identificação da CA: AsC

Nível de Acesso: Público

Versão: 1.3

Data: Maio 2014

Identificador do documento: PJ.CC_24.1.2_0010_pt_AsC.pdf

Palavras-chave: Cartão de Cidadão, Política de Certificados, EC do Cidadão

Tipologia documental: Política

Título: Política de Certificado de Validação on-line OCSP emitido pela EC AsC

Língua original: Português

Língua de publicação: Português

Nível de acesso: Público

Data: Maio 2014

Versão atual: 1.3

Identificação do Projeto: Cartão de Cidadão

Identificação da CA: AsC

Cliente: Ministério da Justiça

Documentos Relacionados

ID Documento	Detalhes	Autor(es)
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

Resumo Executivo

Decorrente da implementação de vários programas públicos para a promoção das tecnologias de informação e comunicação e a introdução de novos processos de relacionamento em sociedade, entre cidadãos, empresas, organizações não-governamentais e o Estado, com vista ao fortalecimento da sociedade de informação e do governo electrónico (*eGovernment*), o Cartão de Cidadão fornece os mecanismos necessários para a autenticação digital forte da identidade do Cidadão perante os serviços da Administração Pública, assim como as assinaturas electrónicas indispensáveis aos processos de desmaterialização que estão a ser disponibilizados pelo Estado Português.

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

Assim, a EC AsC não é detentora de uma Política de Certificados (PC), sendo que a emissão de certificados segue as orientações constantes na Política de Certificado do SCEE.

É ainda apresentado neste documento o perfil de Certificado de Validação *on-line* OCSP emitido pela EC AsC, em complemento das secções 3 e 7 da Política de Certificados do SCEE.

¹ cf. SCEE 2.16.620.1.1.1.2.1.1.0. 2006, Política de Certificados da SCEE e Requisitos mínimos de Segurança.

Sumário

Resumo Executivo.....	3
Sumário	4
Introdução	5
Objectivos.....	5
Público-Alvo	5
Estrutura do Documento.....	5
1 Contexto Geral	6
1.1 Visão Geral	6
1.2 Designação e Identificação do Documento.....	6
2 Identificação e Autenticação.....	7
2.1 Atribuição de Nomes.....	7
2.1.1 Tipos de nomes.....	7
2.2 Uso do certificado e par de chaves pelo titular	7
3 Perfis de Certificado.....	8
3.1 Perfil de Certificado	8
3.1.1 Número da Versão.....	8
3.1.2 Extensões do Certificado	9
3.1.3 OID do Algoritmo.....	13
3.1.4 Formato dos Nomes.....	13
3.1.5 Condicionamento nos Nomes	13
3.1.6 OID da Política de Certificados	13
3.1.7 Utilização da extensão <i>Policy Constraints</i>	13
3.1.8 Sintaxe e semântica do qualificador de política.....	14
3.1.9 Semântica de processamento para a extensão crítica <i>Certificate Policies</i>	14
Conclusão.....	15
Referências Bibliográficas.....	16
Aprovação do Conselho Executivo	17

Introdução

Objetivos

O objetivo deste documento é apresentar o perfil dos Certificados de Validação *on-line* OCSP emitidos pela Entidade de Certificação de Assinatura Digital Qualificada do Cartão de Cidadão (EC AsC).

Público-Alvo

Este documento deve ser lido por:

- Recursos humanos atribuídos aos grupos de trabalho da EC AsC;
- Terceiras partes, encarregues de auditar a EC AsC;
- Todo o público, em geral.

Estrutura do Documento

Assume-se que o leitor é conhecedor dos conceitos de criptografia, infraestruturas de chave pública e assinatura eletrónica. Caso esta situação não se verifique recomenda-se o aprofundar de conceitos e conhecimento nos tópicos anteriormente focado antes de proceder com a leitura do documento.

Este documento complementa a Declaração de Práticas de Certificação da EC de Assinatura Digital Qualificada do Cartão de Cidadão².

² cf. PJ.CC_24.1.1_0002_pt_AsC.pdf, 2011, Declaração de Práticas de Certificação da EC de Assinatura Digital Qualificada do Cartão de Cidadão.

I Contexto Geral

O presente documento tem como objectivo a definição de um conjunto parâmetros que definem o perfil dos Certificados de Validação *on-line* OCSP emitidos pela Entidade de Certificação de Assinatura Digital Qualificada do Cartão de Cidadão (EC AsC), permitindo assim garantir a fiabilidade dos mesmos. Não se pretende nomear regras legais ou obrigações, mas antes informar pelo que se pretende que este documento seja simples, directo e entendido por um público alargado, incluindo pessoas sem conhecimentos técnicos ou legais.

Os Certificados emitidos pela EC AsC contêm uma referência à Política de Certificados (PC) de modo a permitir que partes confiantes e outras entidades ou pessoas interessadas possam encontrar informação sobre o certificado e sobre as políticas seguidas pela entidade que o emitiu.

I.1 Visão Geral

Esta política, satisfaz e complementa os requisitos impostos pela Declaração de Práticas de Certificação da EC de Assinatura Digital Qualificada do Cartão de Cidadão².

I.2 Designação e Identificação do Documento

Este documento é a Política de Certificados do Certificado de Validação *on-line* OCSP. A PC é representada num certificado através de um número único designado de “identificador de objecto” (OID), sendo o valor do OID associado a este documento o “2.16.620.1.1.1.2.4.1.0.1.2”.

Este documento é identificado pelos dados constantes na seguinte tabela:

INFORMAÇÃO DO DOCUMENTO	
Versão do Documento	Versão 1.3
Estado do Documento	Aprovado
OID	2.16.620.1.1.1.2.4.1.0.1.2
Data de Emissão	Maio de 2014
Validade	Não aplicável
Localização	http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_sub-ec_cidadao_assinatura_OCSP_pc.html

2 Identificação e Autenticação

2.1 Atribuição de Nomes

A atribuição de nomes segue a convenção determinada pelo SCEE¹ e pela DPC da EC de Assinatura Digital Qualificada do Cartão de Cidadão².

2.1.1 Tipos de nomes

O Certificado de Validação *on-line* OCSP é identificado por um nome único (DN – *Distinguished Name*) de acordo com standard X.500.

O nome único do Certificados de Validação *on-line* OCSP é identificado pelos seguintes componentes:

Atributo	Código	Valor
Country	C	PT
Organization	O	Cartão de Cidadão
Organization Unit	OU	Serviços do Cartão de Cidadão
Organization Unit	OU	Validação <i>on-line</i>
Common Name	CN	Serviço de Validação <i>on-line</i> do Cartão de Cidadão <nnnnn> ³ - EC de Assinatura Qualificada do Cidadão

2.2 Uso do certificado e par de chaves pelo titular

A EC AsC é a titular do Certificado de Validação *on-line* OCSP, sendo o mesmo emitido para o Servidor de OCSP da EC AsC. A chave privada associada a este tipo de certificados é utilizada para assinar as respostas a pedidos de validação *on-line* OCSP⁴ (consulta do estado actual de certificados digitais), garantindo e permitindo verificar a integridade e não-repúdio dessas mesmas respostas.

³ <nnnnn> é um valor sequencial iniciado em "000001" na emissão do primeiro certificado deste tipo.

⁴ cf. RFC 2560. 1999, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.

3 Perfis de Certificado

3.1 Perfil de Certificado

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. Essa confiança é dada 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 garantida através da assinatura digital de cada certificado por uma 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 EC. 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.⁵

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 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 ECs assinados por outras ECs.⁵

O perfil dos Certificados de Validação *on-line* OCSP está de acordo com:

- Recomendação ITU.T X.509⁶;
- RFC 5280⁵ e
- Política de Certificados da SCEE¹.

3.1.1 Número da Versão

O campo “*version*” do certificado descreve a versão utilizada na codificação do certificado. Neste perfil, a versão utilizada é a 3 (três).

⁵ cf. RFC 5280. 2008, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

⁶ cf. ITU-T Recommendation X.509. 1997, (1997 E): Information Technology - Open Systems Interconnection – The Directory: Authentication Framework.

3.1.2 Extensões do Certificado

As componentes e as extensões definidas para os certificados X.509 v3 fornecem métodos para associar atributos a utilizadores ou chaves públicas, assim como para gerir a hierarquia de certificação.

Componente do Certificado		Secção no RFC 3280	Valor	Tipo ⁷	
tbsCertificate	Version	4.1.2.1	v3	m	
	Serial Number	4.1.2.2	<atribuído pela EC a cada certificado>	m	
	Signature	4.1.2.3	2.16.840.1.13549.1.1.11	m	Valor T Nota: algoritmo
	Issuer	4.1.2.4		m	
	Country (C)		"PT"		
	Organization (O)		"SCEE – Sistema de Certificação Electrónica do Estado"		
	Organization Unit (OU)		"subECEstado"		
	Common Name (CN)		"EC de Assinatura Digital Qualificada do Cartão de Cidadão <nnnn>"		
	Validity	4.1.2.5		m	TEM qu General
	Not Before		<data de emissão>		
	Not After		<data de emissão + 1.900 dias>		Validade resposta geração
	Subject	4.1.2.6		m	
	Country (C)		"PT"		
	Organization (O)		"Cartão de Cidadão"		
	Organization Unit (OU)		"Serviços do Cartão de Cidadão"		
	Organization Unit (OU)		"Validação on-line"		
	Common Name (CN)		"Serviço de Validação on-line do Cartão de Cidadão <nnnnnn> - EC de Assinatura Qualificada do Cidadão"		
	Subject Public Key Info	4.1.2.7		m	Utilizad chave é

⁷ O perfil utilize a terminologia seguinte para cada um dos tipos de campo no certificado X.509:

m – obrigatório (o campo TEM que estar presente);

o – opcional (o campo PODE estar presente);

c – crítico (a extensão é marcada crítica o que significa que as aplicações que utilizem os certificados TÊM que processar esta extensão).

algorithm		1.2.840.1.13549.1.1.1		O OID pkc rsads(1 rsab us(840) rsaEncry Algorith NULL p
subjectPublicKey		<Chave Pública com modulus n de 2048 bits>		
X.509v3 Extensions	4.1.2.9		m	
Authority Key Identifier	4.2.1.1		o	
keyIdentifier		<O <i>key Identifier</i> é composto pela hash de 160-bit SHA-1 do valor da <i>BIT STRING</i> do <i>subject key identifier</i> do certificado do emissor (excluindo a <i>tag</i> , <i>length</i> , e número de <i>bits</i> não usado)>	m	
Subject Key Identifier	4.2.1.2	<O <i>key Identifier</i> é composto pela hash de 160-bit SHA-1 do valor da <i>BIT STRING</i> do <i>subjectPublicKey</i> (excluindo a <i>tag</i> , <i>length</i> , e número de <i>bits</i> não usado)>	m	
Key Usage	4.2.1.3		mc	Esta ext
Digital Signature		"1" seleccionado		
Non Repudiation		"1" seleccionado		
Key Encipherment		"0" seleccionado		
Data Encipherment		"0" seleccionado		
Key Agreement		"0" seleccionado		
Key Certificate Signature		"0" seleccionado		
CRL Signature		"0" seleccionado		
Encipher Only		"0" seleccionado		
Decipher Only		"0" seleccionado		
Certificate Policies	4.2.1.5		o	
policyIdentifier		2.16.620.1.1.1.2.4.1.0.7	m	Identific
policyQualifiers		<i>policyQualifierID</i> : 1.3.6.1.5.5.7.2.1 cPSuri: http://pki.cartaodecidadao.pt/publico/politicas/dpc/cc_sub-ec_cidadao_assinatura_dpc.html	o	Valor de Descriç Declara está na (http://v

⁸ cf. RFC 3279. 2002, *Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

	policyIdentifier		2.16.620.1.1.1.2.4.1.0.1.2	m	Identificação emitido
	policyQualifiers		<i>policyQualifierID: 1.3.6.1.5.5.7.2.2</i> <i>userNotice explicitText:</i> "http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_sub-ec_cidadao_assinatura_OCSP_pc.html"	o	Valor de Descrição confiança (http://v
	Basic Constraints	4.2.1.10		c	Esta ext
	CA		FALSE		
	PathLenConstraint		0		
	Extended Key Usage	4.2.1.13	1.3.6.1.5.5.7.3.9	o	Descrição certifica
	OCSPNocheck	-	NULL	o	Não é http://w esta ext extensã ser con resposta novame
	Internet Certificate Extensions				
	Authority Information Access	4.2.2.1		o	
	accessMethod		1.3.6.1.5.5.7.48.1	o	Valor de Descrição
	accessLocation		http://ocsp.asc.cartaodecidadao.pt/publico/ocsp	o	
	Signature Algorithm	4.1.1.2	2.16.840.1.13549.1.1.1.1	m	TEM qu signature sha-256 body(2)
	Signature Value	4.1.1.3	<contém a assinatura digital emitida pela EC>	m	Ao gera titular (

3.1.3 OID do Algoritmo

O campo “*signatureAlgorithm*” do certificado contém o OID do algoritmo criptográfico utilizado pela EC para assinar o certificado: “2.16.840.113549.1.1.11” (*sha-256WithRSAEncryption*⁹).

Até à EC de Assinatura Digital Qualificada 008 (inclusive), este campo continha o OID 1.2.840.113549.1.1.5 (*sha1WithRSAEncryption*¹⁰).

3.1.4 Formato dos Nomes

Tal como definido na secção 2.1

3.1.5 Condicionamento nos Nomes

Para garantir a total interoperabilidade entre as aplicações que utilizam certificados digitais, aconselha-se (mas não se obriga) a que apenas caracteres alfanuméricos não acentuados, espaço, traço de sublinhar, sinal negativo e ponto final ([a-z], [A-Z], [0-9], ‘ ‘, ‘_’, ‘-’, ‘.’) sejam utilizados em entradas do Directório X.500. A utilização de caracteres acentuados será da única responsabilidade do Grupo de Trabalho de Gestão da EC.

3.1.6 OID da Política de Certificados

A extensão “*certificate policies*” contém a sequência de um ou mais termos informativos sobre a política, cada um dos quais consiste num identificador da política e qualificadores opcionais.

Os qualificadores opcionais (“*policyQualifierID: 1.3.6.1.5.5.7.2.1*” e “*cPSuri*”) apontam para o URI onde pode ser encontrada a Declaração de Práticas de Certificação com o OID identificado pelo “*policyIdentifier*”. Os qualificadores opcionais (“*policyQualifierID: 1.3.6.1.5.5.7.2.2*” e “*userNotice explicitText*”) apontam para o URI onde pode ser encontrados a Política de Certificados com o OID identificado pelo “*policyIdentifier*” (i.e., este documento).

3.1.7 Utilização da extensão *Policy Constraints*

Nada a assinalar.

⁹ sha-256WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11) }

¹⁰ sha-1WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 }

3.1.8 Sintaxe e semântica do qualificador de política

A extensão “*certificate policies*” contém um tipo de qualificador de política a ser utilizado pelos emissores dos certificados e pelos escritores da política de certificados. O tipo de qualificador é o “*cPSuri*” que contém um apontador, na forma de URI, para a Declaração de Práticas de Certificação publicada pela EC e, o “*userNotice explicitText*” que contém um apontador, na forma de URI, para a Política de Certificados.

3.1.9 Semântica de processamento para a extensão crítica *Certificate*

Policies

Nada a assinalar.

Conclusão

Este documento rege-se pelo definido na Política de Certificados do SCEE especificando o perfil de certificado de Validação *on-line* OCSP, emitido pela Entidade de Certificação de Assinatura Digital Qualificada do Cartão de Cidadão no suporte à sua atividade de certificação digital. A hierarquia de confiança da Entidade de Certificação de Assinatura Digital Qualificada do Cartão de Cidadão encontra-se englobada na hierarquia do Sistema de Certificação Electrónica do Estado Português (SCEE) – Infra-Estrutura de Chaves Públicas do Estado:

- Fornecendo uma hierarquia de confiança, que promoverá a segurança electrónica do Cidadão no seu relacionamento com o Estado;
- Proporcionando a realização de transações electrónicas seguras, a autenticação forte, um meio de assinar eletronicamente transações ou informações e documentos electrónicos, assegurando a sua autoria, integridade e não repúdio, e assegurando a confidencialidade das transações ou informação.

Referências Bibliográficas

ITU-T Recommendation X.509. 1997, (1997 E): *Information Technology - Open Systems Interconnection – The Directory: Authentication Framework.*

NIST FIPS PUB 180-2. 2002, *Secure Hash Standard, U. S. Department of Commerce, Technology Administration, National Institute of Standards and Technology.*

RFC 2560. 1999, X.509 *Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.*

RFC 3279. 2002, *Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.*

RFC 5280. 2008, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.*

SCEE 2.16.620.1.1.1.2.1.1.0. 2006, *Política de Certificados da SCEE e Requisitos mínimos de Segurança.*

PJ.CC_24.1.1_0002_pt_AsC – *Declaração de Práticas de Certificação da EC de Assinatura Digital Qualificada do Cartão de Cidadão*

Aprovação