Política de Certificado de Validação Cronológica

Políticas

PJ.CC_24.1.2_0007_pt_Root

Identificação do Projeto: Cartão de Cidadão

Identificação da CA: EC AsC

Nível de Acesso: Público

Versão: 5.0

Data: 26/08/2020

Identificador do documento: PJ.CC_24.1.2_0007_pt_Root

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

Tipologia documental: Políticas

Título: Política de Certificado de Validação Cronológica

Língua original: Português

Língua de publicação: Português

Nível de acesso: Público

Data: 26/08/2020

Periodicidade de Revisão: 1 ano

Versão atual: 5.0

Identificação do Projeto: Cartão de Cidadão

Identificação da CA: EC AsC

Cliente: Ministério da Justiça

Histórico de Versões

N.º de Versão	Data	Detalhes	Autor(es)
1.0	07/09/2007	Política de Certificados de Validação Cronológica	José Pina Miranda
1.1	**10/03/2010**	**Versão Aprovada**	**Grupo Gestão**
1.3	**05/2014**	**Versão Aprovada**	**Grupo Gestão**
1.4	17/10/2016	Alteração da Validade do Certificado TSA	Grupo Políticas
1.5	05/05/2017	Revisão	INCM
1.6	**08/2017**	**Versão Aprovada**	**Grupo Gestão**
1.7	19/02/2018	Alteração do *Issuer* do Certificado. Passou a ser emitido pela EC de Assinatura Digital Qualificada do Cartão de Cidadão	Grupo Políticas/IRN
2.0	**08/03/2018**	**Versão Aprovada**	**Grupo Gestão**
2.1	08/03/2018	Alteração do DN do *Issuer* do certificado, inclusão da identificação do TSP	Grupo Políticas
3.0	**09/03/2018**	**Versão Aprovada**	**Grupo Gestão**
3.1	05/01/2019	Alteração ao tamanho das chaves criptográficas	INCM
4.0	**28/01/2019**	**Versão Aprovada**	**GT Gestão**
4.1	24/08/2020	Revisão	INCM/IRN
5.0	26/08/2020	Versão Aprovada	Grupo Gestão

Documentos Relacionados

ID Documento	Detalhes	Autor(es)
PJ.CC_24.1.1_0002_pt_AsC	Declaração de Práticas de Certificação da EC de Assinatura Digital qualificada do Cartão de Cidadão	MULTICERT S.A.

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 eletrónico (*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 eletrónicas indispensáveis aos processos de desmaterialização que estão a ser disponibilizados pelo Estado Português.

A infraestrutura da Entidade de Certificação do Cartão de 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 de Cidadão encontra-se englobada na hierarquia do Sistema de Certificação Electrónica do Estado Português[1] (SCEE) – Infraestrutura de Chaves Públicas do Estado.

Assim, a EC de Assinatura Digital Qualificada do Cartão de Cidadão, 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. Este documento apresenta o perfil de Certificado de Validação Cronológica 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

Introdução

Objetivos

O objetivo deste documento é apresentar o perfil dos Certificados de Validação Cronológica 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 focados 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 Cidadão[2], presumindo-se que o leitor leu integralmente o seu conteúdo antes de iniciar a leitura deste documento.

[2] *https://pki.cartaodecidadao.pt/publico/politicas/PJ.CC_24.1.1_0002_pt_AsC.pdf*, Declaração de Práticas de Certificação da EC de Assinatura Digital Qualificada do Cartão de Cidadão.

1 Contexto Geral

O presente documento tem como objetivo a definição de um conjunto de parâmetros que definem o perfil dos Certificados de Validação Cronológica emitidos pela 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, direto e entendido por um público alargado, incluindo pessoas sem conhecimentos técnicos ou legais.

Os Certificados emitidos pela EC AsC contêm uma referência à 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.

1.1 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 Cidadão[2].

1.2 Designação e Identificação do Documento

Este documento é a Política de Certificados do Certificado de Validação Cronológica. A PC é representada num certificado através de um número único designado de "identificador de objecto" (OID), identificado na tabela abaixo.

Este documento é identificado pelos dados constantes na seguinte tabela:

INFORMAÇÃO DO DOCUMENTO	
Versão do Documento	Versão 5.0
Estado do Documento	Em revisão
OID	2.16.620.1.1.1.2.4.0.1.7
Data de Emissão	Agosto de 2020
Validade	1 ano
Localização	http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_timestamp_pc.html

2 Identificação e Autenticação

2.1 Atribuição de Nomes

A atribuição de nomes segue a convenção determinada pelo SCEE[1] e pela DPC da EC AsC[2].

2.1.1 Tipos de nomes

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

O nome único do certificado da EC do Cidadão 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 Cronológica
Common Name	CN	Serviço de Validação Cronológica do Cartão de Cidadão <*nnnnnn*>[3]

2.2 Uso do certificado e par de chaves pelo titular

A EC AsC é a titular do Certificado de Validação Cronológica, sendo o mesmo emitido para a Entidade de Validação Cronológica (EVC). A chave privada associada a este tipo de certificados é utilizada para assinar as respostas a pedidos de validações cronológicas[4] (aposição de selos temporais), garantindo e permitindo verificar a integridade e não-repúdio dessas mesmas respostas.

[3] <*nnnnnn*> é um valor sequencial iniciado em "000001" na emissão do primeiro certificado deste tipo.
[4] *cf.* RFC 3161. 2001, Internet X.509 *Public Key Infrastructure Time-Stamp Protocol* (TSP).

3 Perfil de Certificado

3.1 Perfil de Certificado

Para que os utilizadores de uma chave pública tenham a garantia de 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, são utilizados certificados digitais X.509 v3, que pretendem ligar a chave pública ao seu titular, detentor da chave privada associada. Essa ligação é efectuada através da assinatura digital de cada certificado emitido 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 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 ECs assinados por outras ECs.

O perfil dos Certificados de Validação Cronológica está de acordo com os referenciais identificados na secção "Referências Bibliográficas.

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).

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.

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

Componente do Cerificado		Secção RFC 5280	Valor	Tipo Campo	Comentários
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	1.2.840.113549.1.1.11	m	Valor TEM que ser igual ao OID no *signatureAlgorithm* (abaixo)
	Issuer	4.1.2.4		m	
	Country (C)		"PT"		
	Organization (O)		"Instituto dos Registos e do Notariado I.P."		
	Organization Unit (OU)		"Cartão de Cidadão"		
	Organization Unit (OU)		"subECEstado"		
	Common Name (CN)		"EC de Assinatura Digital Qualificada do Cartão de Cidadão <*nnnn*>"		O Certificado de Validação Cronológica fora emitido anteriormente pela EC do Cartão de Cidadão, tendo passado a ser emitido pela EC de Assinatura Digital Qualificada do Cartão de Cidadão a partir da EC de Assinatura 0013.
	Validity	4.1.2.5		m	TEM que utilizar tempo UTC até 2049, passando a partir daí a utilizar ***GeneralisedTime***
	Not Before		<data de emissão>		
	Not After		<data de emissão + 6 anos e 6 meses>		Validade de aproximadamente 6 anos e 6 meses. Utilizado para assinar objetos de tempo durante o primeiro ano de validade, sendo renovado (com geração de novo par de chaves) após o primeiro ano de validade.
	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 Cronológica"		
	Common Name (CN)		"Serviço de Validação Cronológica do Cartão de Cidadão <*nnnnnn*>"		Com a alteração do emissor do certificado, da EC do Cartão de Cidadão para a EC de Assinatura Digital Qualificada do Cartão de Cidadão, o valor <nnnnnn> do primeiro certificado emitido por esta EC iniciou em 000001, sendo que este será incrementado a cada nova emissão.
	Subject Public Key Info	4.1.2.7		m	Utilizado para conter a chave pública e identificar o algoritmo com o qual a chave é utilizada (e.g., RSA, DSA ou *Diffie-Hellman*).
	algorithm		1.2.840.113549.1.1.11		O OID rsaEncryption identifica chaves públicas RSA. pkcs-1 OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 1} rsaEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)} O OID *rsaEncryption* deve ser utilizado no campo *algorithm* com um valor do tipo *AlgorithmIdentifier*. Os parâmetros do campo TÊM que ter o tipo ASN.1 a NULL para o identificador deste algoritmo[6].
	subjectPublicKey		<Chave Pública com modulus n de 3072 bits>		
	X.509v3 Extensions	4.1.2.9		m	
	Authority Key Identifier	4.2.1.1		o	

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

	keyIdentifier		<O *key Identifier* é composto pela *hash* de 160-bit SHA-1 do valor da BIT STRING do *subjectkeyidentifier* do certificado do emissor (excluindo a *tag*, *length*, e número de bits não usado)>	m	
	Subject Key Identifier	4.2.1.2	<O *keyIdentifier* é composto pela *hash* de 160-bit SHA-1 do valor da BIT STRING do *subjectPublicKey* (excluindo a *tag*, *length*, e número de bits não usado)>	m	
	Key Usage	4.2.1.3		mc	Esta extensão é marcada CRÍTICA.
	Digital Signature		"1" selecionado		
	Non Repudiation		"1" selecionado		
	Key Encipherment		"0" selecionado		
	Data Encipherment		"0" selecionado		
	Key Agreement		"0" selecionado		
	Key Certificate Signature		"0" selecionado		
	CRL Signature		"0" selecionado		
	Encipher Only		"0" selecionado		
	Decipher Only		"0" selecionado		
	Certificate Policies	4.2.1.5		o	
	policyIdentifier		2.16.620.1.1.1.2.4.1.0.7	m	Identificador da Declaração de Práticas de Certificação da EC AsC.

	policyQualifiers		*policyQualifierID*: 1.3.6.1.5.5.7.2.1 *cPSuri*: http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_sub-ec_cidadao_assinatura_dpc.html	o	Valor do OID: 1.3.6.1.5.5.7.2.1 (id-qt-cps PKIX CPS *Pointer Qualifier*) Descrição do OID: "O atributo *cPSuri* contém um apontador para a Declaração de Práticas de Certificação publicada pela EC. O apontador está na forma de um URI."
	policyIdentifier		2.16.620.1.1.1.2.4.1.0.1.3	m	Identificador da Política de Certificados de Validação Cronológica.
	policyQualifiers		*policyQualifierID*: 1.3.6.1.5.5.7.2.1 *cPSuri*: "http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_timestamp_pc.html"	o	Valor do OID: 1.3.6.1.5.5.7.2.1 (id-qt-cps PKIX CPS Pointer Qualifier) Descrição do OID: "O atributo *cPSuri* contém um apontador para esta política.
	Qualified Certificate Statement		id-pe-qcStatements= "1.3.6.1.5.5.7.1.3"[7]		A extensão QCStatements é uma extensão introduzida pelo PKIX Qualified Certificate Profile e ETSI[8]
	id-qcs-pkixQCSyntax-v2		Id-etsi-tsts-EuQCompliance="0.4.0.19422.1.1" Text= "By inclusion of this statement the issuer claims that this time-stamp token is issued as a qualified electronic time-stamp according to the REGULATION (EU) No 910/2014"		
	Basic Constraints	4.2.1.10		c	Esta extensão é marcada CRÍTICA.
	CA		FALSE		
	Extended Key Usage	4.2.1.13	1.3.6.1.5.5.7.3.8	c	Descrição do OID: *id-kp-timeStamping* indica que o certificado é utilizado para ligar um objeto a uma hora e data obtida de uma fonte fiável de tempo. Esta extensão TEM de ser crítica[4].
	CRLDistributionPoints	4.2.1.14		o	

[7] http://www.alvestrand.no/objectid/1.3.6.1.5.5.7.1.3.html

[8] cf. ETSI EN 319 422 - Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles

	distributionPoint		http://pki.cartaodecidadao.pt /publico/lrc/cc_sub-ec_cidadao_assinatura_crl<ID_CA>_p<num_seq>.crl	o	
	Freshest CRL	4.2.1.16			
	distributionPoint		http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_assinatura_crl<ID_CA>_delta_p<num_seq>.crl		
	Internet Certificate Extensions				
	Authority Information Access	4.2.2.1		o	
	accessMethod		1.3.6.1.5.5.7.48.1	o	Valor do OID value: 1.3.6.1.5.5.7.48.1 (id-ad-ocsp) Descrição do OID: *Online Certificate Status Protocol*
	accessLocation		http://ocsp.asc.cartaodecidadao.pt/publico/ocsp	o	
	Signature Algorithm	4.1.1.2	1.2.840.113549.1.1.11	m	TEM que conter o mesmo OID do identificador do algoritmo do campo *signature* no campo da sequência *tbsCertificate*. sha-256WithRSAEncryption OBJECT IDENTIFIER::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}
	Signature Value	4.1.1.3	<contains digital signature issued by the CA>	m	Ao gerar esta assinatura, a EC certifica a ligação entre a chave pública e o titular (*subject*) do certificado.

3.1.3 OID do Algoritmo

O campo "*signatureAlgorithm*" do certificado contém o OID do algoritmo criptográfico utilizado pela EC para assinar o certificado: "1.2.840.113549.1.1.11" (*sha-256WithRSAEncryption*[9]).

Até à EC do Cidadão 002 (inclusive), este campo continha o OID 1.2.840.113549.1.1.5 (sha*1WithRSAEncryption*[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 Diretório X.500. A utilização de caracteres acentuados será da única responsabilidade do Grupo 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 ("*policyQualifIierID*: 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*" e para o URI desta política, identificado pelo *policyIdentifier*.

3.1.7 Utilização da extensão *Policy Constraints*

Nada a assinalar.

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

[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 }

apontador, na forma de URI, para a Declaração de Práticas de Certificação publicada pela EC e, outro "*cPSuri*" que contém um apontador, na forma de URI, para a Politica de Certificados.

3.1.9 Semântica de processamento para a extensão crítica *Certificate Policies*

Nada a assinalar.

Conclusão

Este documento especifica o perfil de certificado de Validação Cronológica, emitido pela EC de Assinatura Digital Qualificada do Cartão de Cidadão no suporte à sua atividade de certificação digital. A hierarquia de confiança da EC AsC encontra-se englobada na hierarquia do Sistema de Certificação Electrónica do Estado Português (SCEE) – Infraestrutura de Chaves Públicas do Estado:

- Fornecendo uma hierarquia de confiança, que promoverá a segurança eletrónica do Cidadão no seu relacionamento com o Estado;
- Proporcionando 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.

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 3161. 2001, Internet X.509 *Public Key Infrastructure Time-Stamp Protocol* (TSP).

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*.

ETSI 319 421 - *Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps*

ETSI EN 319 422 - Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles

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.pdf - Declaração de Práticas de Certificação da EC de Assinatura Digital Qualificada do Cartão de Cidadão.

Aprovação

Assinado por : **ANTÓNIO PAULO VICENTE SIMÕES MAIO**
Num. de Identificação: BI097771120