Política de Certificado da EC de Autenticação do Cartão de Cidadão

Políticas

PJ.CC_24.1.2_0003_pt_Root.pdf

Identificação do Projeto: Cartão de Cidadão

Identificação da CA: Root

Nível de Acesso: Público

Versão: 2.0

Data: Jan 2020

Identificador do documento: PJ.CC_24.1.2_0003_pt_Root.pdf

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

Tipologia documental: Políticas

Título: Política de Certificado da EC de Autenticação do Cartão de Cidadão

Língua original: Português

Língua de publicação: Português

Nível de acesso: Público

Data: Jan 2020

Versão atual: 2.0

Identificação do Projeto: Cartão de Cidadão

Identificação da CA: Root

Cliente: Ministério da Justiça

Histórico de Versões

N.º de Versão	Data	Detalhes	Autor(es)
1.0	13/01/2007	Versão inicial	José Pina Miranda
1.1	10/03/2010	- Atualização do ID do Documento e Logótipo;	MULTICERT
1.2	28/06/2012	- Revisão	MULTICERT
1.3	01/10/2017	- Atualização de referenciais inerentes ao regulamento (EU nº 910/2014 - Alteração da validade do certificado para 12 anos	MULTICERT
1.4	10/11/2019	- Atualização do link do repositório do documento (secção 1.2) - Atualização do DN do certificado (secção 2.1.1) - Atualização da secção 3.1.2 o DN da EC o Tamanho das chaves da EC o URLs das politicas	MULTICERT/INCM/IRN
2.0	**Jan 2020**	**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.

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 têm vindo a ser disponibilizados pelo Estado.

A infraestrutura da Entidade de Certificação do Cartão de Cidadão (ou Entidade de Certificação do Cidadão) fornece uma hierarquia de confiança, que promoverá 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) – Infra-Estrutura de Chaves Públicas do Estado.

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

É ainda apresentado neste documento o perfil dos Certificados da Entidade de Certificação de Autenticação do Cartão de Cidadão, em complemento das secções 3 e 7 da Política de Certificados do SCEE[1].

[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 do certificado de Entidade de Certificação (EC) subordinada de Autenticação do Cartão de Cidadão emitido pela Entidade de Certificação do Cartão do Cidadão (EC do Cidadão).

Público-Alvo

Este documento deve ser lido por:

- Recursos humanos atribuídos aos grupos de trabalho da EC do Cidadão,
- Terceiras partes, encarregues de auditar a EC do Cidadão,
- 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 do Cidadão[2], presumindo-se que o leitor leu integralmente o seu conteúdo antes de iniciar a leitura deste documento.

[2] *cf.* PJ.CC_24.1.1_0001_pt_Root.pdf. Declaração de Práticas de Certificação da EC do Cidadão.

1 Contexto Geral

O presente documento tem como objetivo a definição de um conjunto parâmetros que definem o perfil de certificado da Entidade de Certificação (EC) subordinada de Autenticação do Cartão de Cidadão emitido pela EC do Cidadão, permitindo assim garantir a fiabilidade desse mesmo certificado. 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 CC contêm uma referência à Política de Certificados (PC) de modo a permitir que Partes confiantes e outras 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 do Cidadão[3].

1.2 Designação e Identificação do Documento

Este documento é a Política de Certificados do certificado de Entidade de Certificação (EC) subordinada de Autenticação do Cartão de Cidadão. 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 2.16.620.1.1.1.2.4.0.1.3.

Este documento é identificado pelos dados constantes na seguinte tabela:

INFORMAÇÃO DO DOCUMENTO	
Versão do Documento	Versão 2.0
Estado do Documento	Aprovado
OID	2.16.620.1.1.1.2.4.0.1.3
Data de Emissão	Janeiro 2020
Validade	Não aplicável
Localização	http://pki.cartaodecidadao.pt/publico/politicas/cp.html

[3] *cf.* PJ.CC_24.1.1_0001_pt_Root.pdf. . Declaração de Práticas de Certificação da EC do Cidadão.

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 do Cidadão[3].

2.1.1 Tipos de nomes

O certificado de Entidade de Certificação (EC) subordinada de Autenticação do Cartão de Cidadão é identificado por um nome único (DN – *Distinguished Name*) de acordo com *standard* X.500.

O nome único do certificado da EC subordinada de Autenticação do Cartão de Cidadão é identificado pelos seguintes componentes:

Atributo	Código	Valor
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 Autenticação do Cartão de Cidadão <nnnn>[4]

2.2 Uso do certificado e par de chaves pelo titular

A Entidade de Certificação de Autenticação do Cartão do Cidadão é a titular do certificado de EC subordinada de Autenticação do Cartão de Cidadão, utilizando a sua chave privada para a assinatura dos certificados de de Autenticação do Cidadão, certificados de operação e serviços, assim como para a assinatura da respetiva Lista de Certificados Revogados (LRC), de acordo com a sua DPC[3].

[4] <nnnn> é um valor sequencial iniciado em "0001" na emissão do primeiro certificado deste tipo.

3 Perfil de Certificado e LRC

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. 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 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 do certificado da Entidade de Certificação (EC) subordinada de Autenticação do Cartão de Cidadão está de acordo com:

- Recomendação ITU.T X.509[6],
- RFC 5280[5], e
- Política de Certificados da SCEE[1].

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 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 5280	Valor	Tipo [7]	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	2.16.840.113549.1.1.11	m	Valor TEM que ser igual ao OID no *signatureAlgorithm* (abaixo) **Nota:** Até à EC do Cartão de Cidadão 002 (inclusive) o algoritmo de assinatura utilizado foi SHA1 (2.16.840.113549.1.1.5)
	Issuer	4.1.2.4		m	
	Country (C)		"PT"		
	Organization (O)		"SCEE – Sistema de Certificação Electrónica do Estado"		
	Organization Unit (OU)		" ECEstado"		
	Common Name (CN)		"Cartão de Cidadão <nnn>"		
	Validity	4.1.2.5		m	TEM que utilizar tempo UTC até 2049, passando a partir daí a utilizar ***GeneralisedTime***

[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).

Componente do Certificado		Secção no RFC 5280	Valor	Tipo [7]	Comentários
	Not Before		<data de emissão>		
	Not After		<data de emissão + 12 anos>		Validade de 12 anos. Utilizado para assinar certificados durante os primeiros dois anos de validade e renovado (com geração de novo par de chaves) após os primeiros 18 e antes de perfazer os 24 meses. Até à EC AsC 0012 a validade da EC era de 6 anos e dois meses.
	Subject	4.1.2.6		m	
	Country (C)		"PT"		
	Organization (O)		"Instituto dos Registos e do Notariado I. P."		O valor deste campo foi "Cartão de Cidadão" até à EC de Autenticação 0013, tendo o valor sido substituído pelo indicado.
	Organization Unit (OU)		"Cartão de Cidadão"		O valor deste campo consta no campo *Organization* (O) até à EC de Autenticação 0013. A partir da EC de Autenticação 0014, passa a estar incluído neste campo *Organization Unit* (OU)
	Organization Unit (OU)		"subECEstado"		
	Common Name (CN)		EC de Autenticação do Cartão de Cidadão <nnnn>		
	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)}

Componente do Certificado		Secção no RFC 5280	Valor	Tipo [7]	Comentários
					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.[8]
	subjectPublicKey		<Chave Pública com *modulus* n de 4096 bits>		Até à EC de Autenticação (AuC) 014 (inclusive) o tamanho da chave é de 2048 bits.
	Unique Identifiers	4.1.2.8			O "*unique identifiers*" está presente para permitir a possibilidade de reutilizar os nomes do *subject* e/ou issuer
	X.509v3 Extensions	4.1.2.9		m	
	Authority Key Identifier	4.2.1.1		o	
	keyIdentifier		<O *key Identifier* é composto pela *hash* de 160-bit SHA-1 do valor da BIT STRING do *subject key identifier* do certificado do emissor (excluindo a *tag*, *length*, e número de bits não usado)>	m	
	Subject Key Identifier	4.2.1.2	<O *key Identifier* 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	Key Certificate Signature CRL Signature	mc	Esta extensão é marcada CRÍTICA.

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

Componente do Certificado		Secção no RFC 5280	Valor	Tipo [7]	Comentários
	Certificate Policies	4.2.1.5		o	
	policyIdentifier		2.5.29.32.0	m	Identificador da Declaração de Práticas de Certificação da SCEE. Valor do OID: 2.5.29.32.0 (AnyPolicy). Este policyIdentifier TEM de ser incluído[1].
	policyQualifiers		*policyQualifierID*: 1.3.6.1.5.5.7.2.1 *cPSuri*: https://www.scee.gov.pt/rep		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." (http://www.alvestrand.no/objectid/submissions/1.3.6.1.5.5.7.2.1.html)
	policyIdentifier		2.16.620.1.1.1.2.4.0.7	m	Identificador da Declaração de Práticas de Certificação da EC CC.
	policyQualifiers		*policyQualifierID*: 1.3.6.1.5.5.7.2.1 *cPSuri*: http://pki.cartaodecidadao.pt/publico/politicas/cps.html	o	
	policyIdentifier		2.16.620.1.1.1.2.4.0.1.3	m	Identificador da Política de Certificados da EC de Autenticação do Cartão de Cidadão.
	policyQualifiers		*policyQualifierID*: 1.3.6.1.5.5.7.2.1 *cPSuri*: "http://pki.cartaodecidadao.pt/publico/politicas/cp.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"

Componente do Certificado		Secção no RFC 5280	Valor	Tipo [7]	Comentários
					(http://www.alvestrand.no/objectid/submissions/1.3.6.1.5.5.7.2.2.html) **Nota**: Até à EC do Cartão de Cidadão 002 (inclusive), foi utilizado o *userNotice explicitText* para identificar o URL desta política.
	Basic Constraints	4.2.1.10		mc	Esta extensão é marcada CRÍTICA.
	CA		TRUE		
	PathLenConstraint		0		
	CRLDistributionPoints	4.2.1.14		o	
	distributionPoint		http://pki.cartaodecidadao.pt /publico/lrc/cc_ec_cidadao_crl<ID_CA>_crl.crl	o	
	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.root.cartaodecidadao.pt/publico/ocsp	o	
	Signature Algorithm	4.1.1.2	2.16.840.113549.1.1.11	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)}

Componente do Certificado		Secção no RFC 5280	Valor	Tipo [7]	Comentários
					Nota: Até à EC do Cartão de Cidadão 002 (inclusive) o algoritmo de assinatura utilizado foi SHA1 (2.16.840.113549.1.1.5)
	Signature Value	4.1.1.3	<contém a assinatura digital emitida pela EC>	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 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*" e para o URI desta política, identificado com o OID identificado pelo "*policyIdentifier*" (i.e., este documento). No entanto, até à EC do Cartão de Cidadão 002 (inclusive), foi utilizado o "*userNotice explicitText*" para identificar o URL desta política.

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, o "*cPSuri*" que contém um apontador, na forma de URI, para a Política de Certificados. No entanto, até à EC do Cartão de Cidadão 002 (inclusive), foi utilizado o "*userNotice explicitText*" para identificar o URL desta política.

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

Nada a assinalar.

3.2 Perfil da lista de revogação de certificados

Quando um certificado é emitido, espera-se que seja utilizado durante todo o seu período de validade. Contudo, várias circunstâncias podem causar que um certificado se torne inválido antes da expiração do seu período de validade. Tais circunstâncias incluem a mudança de nome, mudança de associação entre o titular e os dados do certificado (por exemplo, um trabalhador que termina o emprego) e, o compromisso ou suspeita de compromisso da chave privada correspondente. Sob tais circunstâncias, a EC tem que revogar o certificado.

O protocolo X.509 define um método de revogação do certificado, que envolve a emissão periódica, pela EC, de uma estrutura de dados assinada, a que se dá o nome de Lista de Revogação de Certificados (LRC). A LRC é uma lista com identificação temporal dos certificados revogados, assinada pela EC e disponibilizada livremente num repositório público. Cada certificado revogado é identificado na LRC pelo seu número de série. Quando uma aplicação utiliza um certificado (por exemplo, para verificar a assinatura digital de um utilizador remoto), a aplicação verifica a assinatura e validade do certificado, assim como obtém a LRC mais recente e verifica se o número de série do certificado não faz parte da mesma. Note-se que uma EC emite uma nova LRC numa base regular periódica. [5]

O perfil da LRC está de acordo com:

- Recomendação ITU.T X.509[6],
- RFC 5280[5], e
- Política de Certificados da SCEE[1].

3.2.1 Número da Versão

O campo "*version*" da LRC descreve a versão utilizada na codificação da LRC. Neste perfil, a versão utilizada é 2 (dois).

3.2.2 Extensões da LRC Base da EC AuC

As componentes e as extensões definidas para as LRCs X.509 v2 fornecem métodos para associar atributos às LRCs.

Componente da Lista de Revogação de Certificados		Secção no RFC 3280	Valor	Tipo	Comentários
tbsCertList	**Version**	5.1.2.1	1	M	Versão v2 (o valor inteiro é 1)
	Signature	5.1.2.2	2.16.840.113549.1.1.11	M	Contém o identificador do algoritmo utilizado para assinar a LRC. O valor TEM que ser igual ao OID no campo *signatureAlgorithm* (abaixo) **Nota:** Até à EC de Autenticação do Cartão de Cidadão 0009 (inclusive), o algoritmo de assinatura utilizado foi SHA1 (1.2.840.113549.1.1.5)
	Issuer	5.1.2.3		M	
	Country (C)		"PT"		
	Organization (O)		"Instituto dos Registos e do Notariado I. P."		O valor deste campo foi "Cartão de Cidadão" até à EC de Autenticação 0013, tendo o valor sido substituído pelo indicado.
	Organization Unit (OU)		"Cartão de Cidadão"		O valor deste campo consta no campo *Organization* (O) até à EC de Autenticação 0013. A partir da EC de Autenticação 0014, passa a estar incluído neste campo *Organization Unit* (OU)
	Organization Unit (OU)		"subECEstado"		
	Common Name (CN)		"EC de Autenticação do Cartão de Cidadão <nnnn>"		

Componente da Lista de Revogação de Certificados		Secção no RFC 3280	Valor	Tipo	Comentários
	thisUpdate	5.1.2.4	<data de emissão da LRC>	M	Implementações TÊM que utilizar o tempo UTC até 2049, e a partir dessa data devem utilizar o *GeneralisedTime*.
	nextUpdate	5.1.2.5	<data da próxima emissão da LRC = *thisUpdate* + N>	m	Este campo indica a data em que a próxima LRC vai ser emitida.A próxima LRC pode ser emitida antes da data indicada, mas não será emitida depois dessa data. Os emissores da CRL DEVEM emitir CRL com o tempo de nextUpdate maior ou igual a todas as LRC anteriores. Implementações TÊM que utilizar o tempo UTC até 2049, e a partir dessa data devem utilizar o *GeneralisedTime*. N será no máximo 1 semana[1].
	revokedCertificates	5.1.2.6	<lista de certificados revogados>	M	
	CRL Extensions	5.1.2.7		M	
	Authority Key Identifier	5.2.1		O	
	keyIdentifier		<O key Identifier é composto pela hash de 160-bit SHA-1 do valor da BIT STRING do subject key identifier do certificado do emissor (excluindo a tag, length, e número de bits não usado)>	M	
	CRL Number	5.2.3	<número sequencial único e incrementado>	M	
	Issuing Distribution Point	5.2.5		O	

Componente da Lista de Revogação de Certificados		Secção no RFC 3280	Valor	Tipo	Comentários
	distributionPoint		http://pki.cartaodecidadao.pt /publico/lrc/cc_ sub-ec_cidadao_ autenticacao_crl<ID_CA>_p<num_seq>.crl	O	
	Freshest CRL	5.2.6		O	
	distributionPoint		http://pki.cartaodecidadao.pt /publico/lrc/cc_ sub-ec_cidadao_autenticacao_crl<ID_CA>_delta_p<num_seq>.crl	O	
	CRL Entry Extensions	5.3			
	Reason Code	5.3.1		O	Valor tem que ser um dos seguintes: 1 – keyCompromise; 2 – cACompromise; 3 – affiliationChanged; 4 – superseded; 5 – cessationOfOperation; 6 – certificateHold; 8 – removeFromCRL; 9 – privilegeWithdrawn; 10 – aACompromise
	Signature Algorithm	5.1.1.2	2.16.840.113549.1.1.11	M	TEM que conter o mesmo OID do identificador do algoritmo utilizado no campo signature da sequência tbsCertList. sha-256WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)} **Nota:** Até à EC de Autenticação do Cartão de Cidadão 0009 (inclusive), o algoritmo de assinatura utilizado foi SHA1 (1.2.840.113549.1.1.5)
	Signature Value	5.1.1.3	<contém a assinatura digital emitida pela EC>	M	Contém a assinatura digital calculada sobre a *tbsCertList*.

3.2.3 Extensões da Delta LRC da EC AuC

Componente da Lista de Revogação de Certificados		Secção no RFC 3280	Valor	Tipo	Comentários
tbsCertList	**Version**	5.1.2.1	1	m	Versão V2 (o valor inteiro é 1)
	Signature	5.1.2.2	2.16.840.113549.1.1.11	m	Contém o identificador do algoritmo utilizado para assinar a LRC. O valor TEM que ser igual ao OID no campo *signatureAlgorithm* (abaixo) **Nota:** Até à EC de Autenticação do Cartão de Cidadão 0009 (inclusive), o algoritmo de assinatura utilizado foi SHA1 (1.2.840.113549.1.1.5)
	Issuer	5.1.2.3		m	
	Country (C)		"PT"		
	Organization (O)		"Instituto dos Registos e do Notariado I. P."		O valor deste campo foi "Cartão de Cidadão" até à EC de Autenticação 0013, tendo o valor sido substituído pelo indicado.
	Organization Unit (OU)		"Cartão de Cidadão"		O valor deste campo consta no campo *Organization* (O) até à EC de Autenticação 0013. A partir da EC de Autenticação 0014, passa a estar incluído neste campo *Organization Unit* (OU)
	Organization Unit (OU)		"subECEstado"		
	Common Name (CN)		"EC de Autenticação do Cartão de Cidadão <nnnnnnnnn>"		
	thisUpdate	5.1.2.4	<data de emissão da delta LRC>	m	Implementações TÊM que utilizar o tempo UTC até 2049, e a partir dessa data devem utilizar o *GeneralisedTime*.

Componente da Lista de Revogação de Certificados		Secção no RFC 3280	Valor	Tipo	Comentários
	nextUpdate	5.1.2.5	<data da próxima emissão da delta LRC = *thisUpdate* + N>	m	Este campo indica a data em que a próxima LRC vai ser emitida. A próxima LRC pode ser emitida antes da data indicada, mas não será emitida depois dessa data. Os emissores da CRL DEVEM emitir CRL com o tempo de *nextUpdate* maior ou igual a todas as LRC anteriores. Implementações TÊM que utilizar o tempo UTC até 2049, e a partir dessa data devem utilizar o *GeneralisedTime*. N será no máximo 1 mês
	revokedCertificates	5.1.2.6	< lista de certificados revogados >	m	
	CRL Extensions	5.1.2.7		m	
	Authority Key Identifier	5.2.1		o	
	keyIdentifier		<O key Identifier é composto pela hash de 160-bit SHA-1 do valor da BIT STRING do subject key identifier do certificado do emissor (excluindo a tag, length, e número de bits não usado)>	m	
	CRL Number	5.2.3	<número sequencial único e incrementado>	m	Se um emissor da LRC gera delta LRCs para além de LRCs completas para um determinado âmbito, as LRCs completas e as delta LRCs DEVEM partilhar uma sequência de numeração.
	Delta CRL Indicator	5.2.4	<número da LRC de base>	c	Este número de LRC identifica a LRC completa de base, correspondente ao ponto de partida para a geração desta delta LRC.
	Issuing Distribution Point	5.2.5		o	
	distributionPoint		http://pki.cartaodecidadao.pt /publico/lrc/cc_ sub-ec_cidadao_autenticacao_crl<ID_CA>_p<num_seq>.crl	o	

Componente da Lista de Revogação de Certificados		Secção no RFC 3280	Valor	Tipo	Comentários
	CRL Entry Extensions	5.3			
	Reason Code	5.3.1		o	Valor tem que ser um dos seguintes: 1 – keyCompromise; 2 – cACompromise; 3 – affiliationChanged; 4 – superseded; 5 – cessationOfOperation; 6 – certificateHold; 8 – removeFromCRL; 9 – privilegeWithdrawn; 10 - aACompromise
	Signature Algorithm	5.1.1.2	2.16.840.113549.1.1.11	m	Contem o mesmo OID do identificador do algoritmo utilizado no campo signature da sequência tbsCertList. sha-256WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)} **Nota:** Até à EC de Autenticação do Cartão de Cidadão 0009 (inclusive), o algoritmo de assinatura utilizado foi SHA1 (1.2.840.113549.1.1.5)
	Signature Value	5.1.1.3	<contém a assinatura digital emitida pela EC>	m	Contém a assinatura digital calculada sobre a *tbsCertList*.

Conclusão

Este documento rege-se pelo definido na Política de Certificados do SCEE especificando o perfil de certificado da Entidade de Certificação (EC) subordinada de Autenticação do Cartão de Cidadão, emitido pela Entidade de Certificação do Cartão de Cidadão no suporte à sua atividade de certificação digital. A hierarquia de confiança da Entidade de Certificação do Cartão do 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 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

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_0001_pt_Root - Declaração de Práticas de Certificação da EC do Cartão de Cidadão.

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

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*.

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

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 (2016-02) – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;

Regulamento (UE) nº 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

Assinado por : **PAULA ISABEL DUARTE MARCELINO**
Num. de Identificação: BI101757026
Data: 2020.01.18 17:21:00+00'00'

CARTÃO DE CIDADÃO

[Assinatura Qualificada] Nuno Fonseca

Assinado de forma digital por [Assinatura Qualificada] Nuno Fonseca
DN: c=PT, o=Instituto de Gestão Financeira e Equipamentos da Justiça, ou=Certificado para pessoa singular - Assinatura Qualificada, title=Diretor - Informação confirmada pela Entidade de Certificação apenas na data de emissão e que não foi confirmada posteriormente a essa data, sn=Fonseca, givenName=Nuno, serialNumber=MLPT-82636941433884l984, cn=[Assinatura Qualificada] Nuno Fonseca
Dados: 2020.01.19 23:24:59 Z