Política de Certificado da EC de Assinatura Digital Qualificada do Cartão de Cidadão

Políticas

PJ.CC_24.1.2_0002_pt_Root.pdf

Identificação do Projeto: Cartão de Cidadão

Identificação da CA: Root

Nível de Acesso: Público

Versão: 1.3

Data: 05/2014

Identificador do documento: PJ.CC_24.1.2_0002_pt_Root.pdf

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

Tipologia documental: Políticas

Título: Política de Certificado da EC de Assinatura Digital Qualificada do Cartão de Cidadão

Língua original: Português

Língua de publicação: Português

Nível de acesso: Público

Data: 05/2014

Versão atual: 1.3

Identificação do Projeto: Cartão de Cidadão

Identificação da CA: Root

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.

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.

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.

No entanto, neste documento é apresentado o perfil de Certificado da Entidade de Certificação de Assinatura Digital Qualificada do Cartão de Cidadão emitido pela EC CC, 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 do certificado da Entidade de Certificação (EC) subordinada de Assinatura Digital Qualificada 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. 2011. Declaração de Práticas de Certificação da EC do Cidadão.

1 Contexto Geral

O presente documento tem como objetivo a definição de um conjunto de parâmetros que definem o perfil de certificado da Entidade de Certificação (EC) subordinada de Assinatura Digital Qualificada 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 ao 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 PC satisfaz e complementa os requisitos impostos pela Declaração de Práticas de Certificação da EC do Cidadão[2].

1.2 Designação e Identificação do Documento

Este documento é a Política de Certificados do certificado de Entidade de Certificação (EC) subordinada de Assinatura Digital Qualificada 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 2.16.620.1.1.1.2.4.0.1.2.

Este documento é identificado pelos dados constantes na seguinte tabela:

INFORMAÇÃO DO DOCUMENTO	
Versão do Documento	Versão 1.3
Estado do Documento	Aprovado
OID	2.16.620.1.1.1.2.4.0.1.2
Data de Emissão	Maio de 2014
Validade	Não aplicável

Localização	http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_sub-ec_cidadao_assinatura_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 do Cidadão[2].

2.1.1 Tipos de nomes

O certificado de Entidade de Certificação (EC) subordinada de Assinatura Digital Qualificada 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 do Cidadão é identificado pelos seguintes componentes:

Atributo	Código	Valor
Country	C	PT
Organization	O	Cartão de Cidadão
Organization Unit	OU	subECEstado
Common Name	CN	EC de Assinatura Digital Qualificada do Cartão de Cidadão <nnnn>[3]

2.2 Uso do certificado e par de chaves pelo titular

A Entidade de Certificação de Assinatura Digital Qualificada do Cartão do Cidadão é a titular do certificado de EC subordinada de Assinatura Digital Qualificada do Cartão de Cidadão, utilizando a sua chave privada para a assinatura dos certificados de Assinatura Digital Qualificada 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[2].

[3] <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.[4]

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.[4]

O perfil do certificado da Entidade de Certificação (EC) subordinada de Assinatura Digital Qualificada do Cartão de Cidadão está de acordo com:

- Recomendação ITU.T X.509[5],
- RFC 5280[4], 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).

[4] cf. *RFC 5280. 2008, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.*
[5] 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[6]	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
	Not Before		<data de emissão>		

[6] 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).

	Not After		<data de emissão + 2.252 dias>		Validade de aproximadamente 6 anos e dois meses. Utilizado para assinar certificados durante o primeiro ano de validade e renovado (com geração de novo par de chaves) após os primeiros onze meses de validade.
	Subject	4.1.2.6		m	
	Country (C)		"PT"		
	Organization (O)		"Cartão de Cidadão"		
	Organization Unit (OU)		"subECEstado"		
	Common Name (CN)		EC de Assinatura Digital Qualificada 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		1.2.840.113549.1.1.1		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) rsaEncryption(1)}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.[7]
	subjectPublicKey		<Chave Pública com modulus n de 2048 bits>		

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

	Unique Identifiers	4.1.2.8			O "*unique identifiers*" está presente para permitir a possibilidade de reutilizar os nomes do *subject* e/ou *issuer*[7].
	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 *subjectKeylidentifier* 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		mc	Esta extensão é marcada CRÍTICA.
	Digital Signature		"0" seleccionado		
	Non Repudiation		"0" seleccionado		
	Key Encipherment		"0" seleccionado		
	Data Encipherment		"0" seleccionado		
	Key Agreement		"0" seleccionado		
	Key Certificate Signature		"1" seleccionado		
	CRL Signature		"1" seleccionado		
	Encipher Only		"0" seleccionado		
	Decipher Only		"0" seleccionado		

	Certificate Policies	4.2.1.5		o	
	policyIdentifier		2.5.29.32.0	m	Identificador da Declaração de Práticas de Certificação ds 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*: http://www.scee.gov.pt/pcert		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/dpc/cc_ec_cidadao_dpc.html	o	
	policyIdentifier		2.16.620.1.1.1.2.4.0.1.2	m	Identificador da Política de Certificados da EC de Assinatura Digital Qualificada do Cartão de Cidadão.

	policyQualifiers		*policyQualifierID*: 1.3.6.1.5.5.7.2.1 *cPSuri*: "http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_sub-ec_cidadao_assinatura_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." (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)}[7] **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[8]).

Até à EC do Cidadão 002 (inclusive), este campo continha o OID 1.2.840.113549.1.1.5 (sha*1WithRSAEncryption*[9]).

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 ("*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 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.

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

[9] 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 "*cPSuri*" que contém um apontador, na forma de URI, para a Politica 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. [4]

O perfil da LRC está de acordo com:

- Recomendação ITU.T X.509[5],
- RFC 5280[4], 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 AsC

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	1.2.840.113549.1.1.11	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 Assinatura Digital Qualificada do Cartão de Cidadão 0008 (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)		"Cartão de Cidadão"		
	Organization Unit (OU)		"subECEstado"		
	Common Name (CN)		"EC de Assinatura Digital Qualificada do Cartão de Cidadão <nnnn>"		
	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	
	distributionPoint		http://pki.cartaodecidadao.pt /publico/lrc/cc_ sub-ec_cidadao_assinatura_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_assinatura_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	1.2.840.113549.1.1.11	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 Assinatura Digital Qualificada do Cartão de Cidadão 0008 (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 AsC

Cerificate Revocation List Component		Section in RFC 3280	Value	Field Type	Comments
tbsCertList	**Version**	5.1.2.1	1	m	Versão V2 (o valor inteiro é 1)
	Signature	5.1.2.2	1.2.840.113549.1.1.11	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 Assinatura Digital Qualificada do Cartão de Cidadão 0008 (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)		"Cartão de Cidadão"		
	Organization Unit (OU)		"subECEstado"		
	Common Name (CN)		"EC de Assinatura Digital Qualificada do Cartão de Cidadão <nnnn>"		
	thisUpdate	5.1.2.4	<update date>	m	Implementações TÊM que utilizar o tempo UTC até 2049, e a partir dessa data devem utilizar o *GeneralisedTime*.

	nextUpdate	5.1.2.5	<next update date = update date + 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		<The key Identifier is composed of the 160-bit SHA-1 hash of the value of the BIT STRING subject key identifier in the CRL issuer's certificate (excluding the tag, length, and number of unused bits)>	m	
	CRL Number	5.2.3	<número sequencial único e incrementado>	m	If a CRL issuer generates delta CRLs in addition to complete CRLs for a given scope, the complete CRLs and delta CRLs MUST share one numbering sequence. Given the requirements above, CRL numbers can be expected to contain long integers. CRL verifiers MUST be able to handle CRLNumber values up to 20 octets. Conformant CRL issuers MUST NOT use CRLNumber values longer than 20 octets.
	Delta CRL Indicator	5.2.4	<base CRL number>	c	This CRL number identifies the complete base CRL that was used as the starting point in the generation of this delta CRL.
	Issuing Distribution Point	5.2.5		o	
	distributionPoint		http://pki.cartaodecidadao.pt /publico/lrc/cc_ sub-ec_cidadao_assinatura_crl<ID_CA>_ p<num_seq>.crl	o	
	CRL Entry Extensions	5.3			

	Reason Code	5.3.1		o	Value must be one of the followings: 1 – keyCompromise 2 – cACompromise 3 – affiliationChanged 4 – superseded 5 – cessationOfOperation 6 – certificateHold 8 – removeFromCRL 9 – privilegeWithdrawn 10 - aACompromise
	Signature Algorithm	5.1.1.2	1.2.840.113549.1.1.11	m	MUST contain the same OID algorithm identifier as the signature field in the sequence tbsCertificate. 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 Assinatura Digital Qualificada do Cartão de Cidadão 0008 (inclusive), o algoritmo de assinatura utilizado foi SHA1 (1.2.840.113549.1.1.5)
	Signature Value	5.1.1.3	<contains digital signature issued by the CA>	m	Contains a digital signature computed upon the tbsCertList. The CA certificate is used to digitally sign certificates and CRLs.

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 Assinatura Digital Qualificada do Cartão de Cidadão, emitido pela Entidade de Certificação do Cartão do 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) – 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.

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.

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.

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

Aprovação

ANTÓNIO MANUEL MARTINS DA CRUZ

Digitally signed by ANTÓNIO MANUEL MARTINS DA CRUZ
DN: c=PT, o=Cartão de Cidadão, ou=Cidadão Português, ou=Assinatura Qualificada do Cidadão, sn=MARTINS DA CRUZ, givenName=ANTÓNIO MANUEL, serialNumber=BI103203710, cn=ANTÓNIO MANUEL MARTINS DA CRUZ
Date: 2014.05.26 15:10:58 +01'00'

Carlos Brito (Assinatura)

Assinado de forma digital por Carlos Brito (Assinatura)
DN: givenName=Carlos, sn=Brito, title=Vogal do CD do IGFEJ IP, c=PT, o=MJ, ou=IGFEJ, ou=Conselho Diretivo, cn=Carlos Brito (Assinatura)
Dados: 2014.10.21 09:05:19 +01'00'

João Pedro Monteiro Rodrigues (Assinatura)

Digitally signed by João Pedro Monteiro Rodrigues (Assinatura)
DN: givenName=João Pedro, sn=Monteiro Rodrigues, title=Vogal do Conselho Diretivo, c=PT, o=MJ, ou=IRN, ou=Conselho Diretivo, cn=João Pedro Monteiro Rodrigues (Assinatura)
Date: 2014.10.21 14:36:40 +01'00'

MANUEL PAULO DE OLIVEIRA RICOU

Digitally signed by MANUEL PAULO DE OLIVEIRA RICOU
DN: c=PT, o=Cartão de Cidadão, ou=Cidadão Português, ou=Assinatura Qualificada do Cidadão, sn=DE OLIVEIRA RICOU, givenName=MANUEL PAULO, serialNumber=BI020477953, cn=MANUEL PAULO DE OLIVEIRA RICOU
Date: 2014.10.21 15:51:53 +01'00'