

# Política de Certificados de Assinatura Digital Qualificada

Políticas

---

PJ.CC\_24.1.2\_0009\_pt\_AsC.pdf

**Identificação do Projecto:** Cartão de Cidadão

**Identificação da CA:** AsC

**Nível de Acesso:** Público

**Versão:** 1.1

**Data:** 10/03/2010

**Identificador do documento:** PJ.CC\_24.1.2\_0009\_pt\_AsC.pdf

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

**Tipologia documental:** Políticas

**Título:** Política de Certificados de Assinatura Digital Qualificada

**Língua original:** Português

**Língua de publicação:** Português

**Nível de acesso:** Público

**Data:** 10/03/2010

**Versão actual:** 1.1

**Identificação do Projecto:** 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 S.A.

#### Apêndices

ID Documento	Detalhes	Autor(es)
PJ.CC_53.2.1_0005_pt_AsC.pdf	Formulário de emissão de certificado "espécimen" de Assinatura Digital Qualificada	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 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.

A infra-estrutura da Entidade de Certificação do Cartão de Cidadão (ou Entidade de Certificação do Cidadão) fornece uma hierarquia de confiança, que promoverá 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 Português<sup>1</sup> (SCEE) – Infra-Estrutura de Chaves Públicas do Estado.

Este documento define a Política de certificados utilizada na emissão do certificado de Assinatura Digital Qualificada, que complementa e está de acordo com a Declaração de Práticas de Certificação da EC de Assinatura Digital Qualificada do Cartão de Cidadão.<sup>2</sup>

---

<sup>1</sup> cf. SCEE 2.16.620.1.1.1.2.1.1.0. 2006, Política de Certificados da SCEE e Requisitos mínimos de Segurança.

<sup>2</sup> cf. MULTICERT\_PJ.CC\_24.1.1\_0002\_pt\_AsC.doc. 2007, Declaração de Práticas de Certificação da EC de Assinatura Digital Qualificada do Cartão de Cidadão.

# Sumário

Resumo Executivo.....	3
Sumário.....	4
Introdução .....	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 e LRC .....	8
3.1 Perfil de Certificado.....	8
3.1.1 Número da Versão .....	8
3.1.2 Extensões do Certificado .....	8
3.1.3 OID do Algoritmo .....	15
3.1.4 Formato dos Nomes .....	15
3.1.5 Condicionamento nos Nomes.....	15
3.1.6 OID da Política de Certificados .....	15
3.1.7 Utilização da extensão Policy Constraints .....	15
3.1.8 Sintaxe e semântica do qualificador de política.....	15
3.1.9 Semântica de processamento para a extensão crítica Certificate Policies.....	16
3.2 Certificado “espécimen” .....	16
3.3 Perfil da lista de revogação de certificados.....	16
3.3.1 Número da Versão .....	16
3.3.2 Extensões da LRC Base da EC AsC .....	17
3.3.3 Extensões da Delta LRC da EC AsC.....	20
Conclusão .....	23
Referências Bibliográficas.....	24
Aprovação do Conselho Executivo.....	25

# Introdução

## Objectivos

O objectivo deste documento é definir as políticas utilizadas na emissão do certificado de Assinatura Digital Qualificada, 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, infra-estruturas de chave pública e assinatura electrónica. 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 Cidadão<sup>2</sup>, presumindo-se que o leitor leu integralmente o seu conteúdo antes de iniciar a leitura deste documento.

# I Contexto Geral

O presente documento é um documento de Política de Certificados, ou PC, cujo objectivo se prende com a definição de um conjunto de políticas e dados para a emissão e validação de Certificados e para a garantia de fiabilidade desses mesmos certificados. 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.

Este documento descreve a política de certificados para a emissão e gestão do certificado de Assinatura Digital Qualificada, emitido pela Entidade de Certificação de Assinatura Digital Qualificada do Cartão de Cidadão (EC AsC).

Os Certificados emitidos pela EC AsC contêm uma referência à 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.

## I.1 Visão Geral

Esta PC satisfaz e complementa os requisitos impostos pela Declaração de Práticas de Certificação da EC de Assinatura Digital Qualificada do Cartão de Cidadão<sup>2</sup>.

## I.2 Designação e Identificação do Documento

Este documento é a Política de Certificados do certificado de Assinatura Digital Qualificada. 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 2.16.620.1.1.1.2.4.1.0.1.1.

Este documento é identificado pelos dados constantes na seguinte tabela:

INFORMAÇÃO DO DOCUMENTO	
<b>Versão do Documento</b>	Versão 1.7
<b>Estado do Documento</b>	Aprovado
<b>OID</b>	2.16.620.1.1.1.2.4.1.0.1.1
<b>Data de Emissão</b>	20-Mar-2009
<b>Validade</b>	Não aplicável
<b>Localização</b>	<a href="http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_sub-ec_cidadao_assinatura_pc.html">http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_sub-ec_cidadao_assinatura_pc.html</a>

## 2 Identificação e Autenticação

### 2.1 Atribuição de Nomes

A atribuição de nomes segue a convenção determinada pelo SCEE<sup>1</sup> e pela DPC da EC de Assinatura Digital Qualificada do Cartão de Cidadão<sup>2</sup>.

#### 2.1.1 Tipos de nomes

O certificado de Assinatura Digital Qualificada é identificado por um nome único (DN – Distinguished Name) de acordo com standard X.500.

O nome único do certificado de Assinatura Digital Qualificada é identificado pelos seguintes componentes:

Atributo	Código	Valor
Country	C	PT
Organization	O	Cartão de Cidadão
Organization Unit	OU	Cidadão Português
Organization Unit	OU	Assinatura Qualificada do Cidadão
Common Name	CN	<concatenação do <i>givenName</i> e <i>SN</i> do Cidadão>
Surname	SN	<nome de família do Cidadão>
Given Name	<i>givenName</i>	<parte do nome do Cidadão que não é o nome de família nem os nomes intermédios>
Serial Number	<i>serialNumber</i>	<identificador único do Cidadão>

### 2.2 Uso do certificado e par de chaves pelo titular

O Cidadão (pessoa singular) identificado pelo *Distinguished Name* é o titular do certificado de Assinatura Digital Qualificada. O certificado emitido segundo esta política é equivalente a um certificado digital qualificado, nos termos, do definido na Legislação Portuguesa, aplicável para o efeito, sendo utilizado em qualquer aplicação para efeitos de assinatura digital qualificada.

## 3 Perfis 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 correcto (pessoa ou sistema) com o qual irão utilizar mecanismos de cifra ou assinatura digital. A confiança é obtida através do uso de certificados digitais X.509 v3, que são estrutura de dados que fazem a ligação entre a chave pública e o seu titular. Esta ligação é afirmada através da assinatura digital de cada certificado por uma EC de confiança. A EC pode basear esta afirmação em meios técnicos (por exemplo, prova de posse da chave privada através de um protocolo desafio-resposta), na apresentação da chave privada, ou no registo efectuado pelo titular.

Um certificado tem um período limitado de validade, indicado no seu conteúdo e assinado pela 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.<sup>3</sup>

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.<sup>3</sup>

O perfil do certificado de Assinatura Digital Qualificada está de acordo com:

- Recomendação ITU.T X.509<sup>4</sup>,
- RFC 3280<sup>3</sup>, e
- Política de Certificados da SCEE<sup>1</sup>.

#### 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).

#### 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.

---

<sup>3</sup> cf. RFC 3280. 2002, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

<sup>4</sup> cf. ITU-T Recommendation X.509. 1997, (1997 E): Information Technology - Open Systems Interconnection – The Directory: Authentication Framework.

Componente do Certificado		Secção no RFC 3280	Valor	Tipo <sup>5</sup>	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	1.2.840.113549.1.1.5	m	Valor TEM que ser igual ao OID no <i>signatureAlgorithm</i> (abaixo)
	Issuer	4.1.2.4		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>"		
	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 + 5 anos>		
	Subject	4.1.2.6		m	
	Country (C)		"PT"		

<sup>5</sup> 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).

Organization (O)		"Cartão de Cidadão"		
Organization Unit (OU)		"Cidadão Português"		
Organization Unit (OU)		"Assinatura Qualificada do Cidadão"		
Common Name (CN)		<concatenação do givenName e SN do cidadão>		
Surname (SN)		<nome de família do cidadão>		
Given Name (givenName)		<nome(s) próprio do cidadão>		
Serial Number (serialNumber)		"BI " <ID do cidadão>		
<b>Subject Public Key Info</b>	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		<p>O OID rsaEncryption identifica chaves públicas RSA.</p> <p>pkcs-1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsads(113549) pkcs(1) 1 }</p> <p>rsaEncryption OBJECT IDENTIFIER ::= { pkcs-1 1 }</p> <p>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.<sup>6</sup></p>
subjectPublicKey		<Chave Pública com modulus n de 1024 bits>		
<b>X.509v3 Extensions</b>	4.1.2.9		m	
<b>Authority Key Identifier</b>	4.2.1.1		o	

<sup>6</sup> 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 subject key identifier do certificado do emissor (excluindo a tag, length, e número de bits não usado)>	m	
<b>Subject Key Identifier</b>	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	
<b>Key Usage</b>	4.2.1.3		mc	Esta extensão é marcada CRÍTICA.
Digital Signature		"0" seleccionado		
Non Repudiation		"1" seleccionado		Se o bit nonRepudiation for seleccionado, este NÃO DEVE ser combinado com qualquer outro bit do key usage, i.e., se seleccionado, DEVE ser o único seleccionado. <sup>7</sup>
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		
<b>Certificate Policies</b>	4.2.1.5		o	
policyIdentifier		2.16.620.1.1.1.2.10	m	scee-assinatura <sup>1</sup>

<sup>7</sup> cf. RFC 3039, 2001, Internet X.509 Public Key Infrastructure Qualified Certificates Profile.

policyQualifiers		policyQualifierID: 1.3.6.1.5.5.7.2.1 cPSuri: <a href="http://www.scee.gov.pt/pcert">http://www.scee.gov.pt/pcert</a>		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." ( <a href="http://www.alvestrand.no/objectid/submissions/1.3.6.1.5.5.7.2.1.html">http://www.alvestrand.no/objectid/submissions/1.3.6.1.5.5.7.2.1.html</a> )
policyQualifiers		policyQualifierID: 1.3.6.1.5.5.7.2.2 userNotice explicitText: "O certificado emitido segundo esta política é equivalente a um certificado digital qualificado, nos termos, do definido na Legislação Portuguesa, aplicável para o efeito"		Valor do OID: 1.3.6.1.5.5.7.2.2 (id-qt-unotice) Descrição do OID: "User notice é utilizado para apresentar às partes confiantes quando um certificado é utilizado" ( <a href="http://www.alvestrand.no/objectid/submissions/1.3.6.1.5.5.7.2.2.html">http://www.alvestrand.no/objectid/submissions/1.3.6.1.5.5.7.2.2.html</a> )
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: <a href="http://pki.cartaodecidadao.pt/publico/politicas/dpc/cc_sub-ec_cidadao_assinatura_dpc.html">http://pki.cartaodecidadao.pt/publico/politicas/dpc/cc_sub-ec_cidadao_assinatura_dpc.html</a>	o	
policyIdentifier		2.16.620.1.1.1.2.4.1.0.1.1	m	Identificador da Política de Certificados de Assinatura Digital Qualificada.
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	
<b>Basic Constraints</b>	4.2.1.10		c	Esta extensão é marcada CRÍTICA.
CA		FALSE		

PathLenConstraint		0		
<b>CRLDistributionPoints</b>	4.2.1.14		o	
distributionPoint		<a href="http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_assinatura_crl&lt;ID_CA&gt;_p&lt;num_seq&gt;.crl">http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_assinatura_crl&lt;ID_CA&gt;_p&lt;num_seq&gt;.crl</a>	o	
<b>Freshest CRL</b>	4.2.1.16		o	
distributionPoint		<a href="http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_assinatura_crl&lt;ID_CA&gt;_delta_p&lt;num_seq&gt;.crl">http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_assinatura_crl&lt;ID_CA&gt;_delta_p&lt;num_seq&gt;.crl</a>	o	
<b>Netscape Certificate Type</b>	-	S/MIME = 1	o	Não é uma extensão definida no RFC 3280. Definida em <a href="http://www.redhat.com/docs/manuals/cert-system/admin/app_ext.htm">http://www.redhat.com/docs/manuals/cert-system/admin/app_ext.htm</a> .
<b>Subject Directory Attributes</b>	-		o	
dateOfBirth		<data de nascimento do cidadão>		Não é uma extensão definida no RFC 3280. Esta extensão PODE conter atributos adicionais associados com o titular do certificado, como complemento à informação presente no campo subject e na extensão subject alternative name.  ( <a href="http://www.alvestrand.no/objectid/submissions/2.5.29.9.html">http://www.alvestrand.no/objectid/submissions/2.5.29.9.html</a> )
<b>Qualified Certificate Statement</b>	-		o	Não é uma extensão definida no RFC 3280. A extensão QCStatements é uma extensão introduzida pelo PKIX Qualified Certificate Profile <sup>7</sup> e ETSI <sup>8</sup> .  ( <a href="http://javadoc.iaik.tugraz.at/iaik_jce/current/iaik/x509/extensions/qualified/QCStatements.html">http://javadoc.iaik.tugraz.at/iaik_jce/current/iaik/x509/extensions/qualified/QCStatements.html</a> )

<sup>8</sup> cf. ETSI TS 101 862, 2001-06, Qualified certificate profile, v1.2.1.

id-qcs-pkixQCSyntax-v2		id-etsi-qcs-QcCompliance = "0.4.0.1862.1.1"		<p>A aposição desta componente ao certificado significa que o mesmo é emitido com a qualidade de certificado Qualificado, de acordo com o Anexo I e II da Directiva 1999/93/EC do Parlamento Europeu e do Conselho de 13 de Dezembro de 1999 sobre "a Community framework for electronic signatures", e conforme transposição para a legislação do país identificado na componente "issuer" do certificado.</p> <p>A declaração QcEuCompliance (id-etsi-qcs-QcCompliance) corresponde ao OID "0.4.0.1862.1.1".</p>
id-qcs-pkixQCSyntax-v2		id-etsi-qcs-QcSSCD = " 0.4.0.1862.1.4"		<p>Declaração efectuada pela respectiva EC, indicando que a chave privada associada à chave pública no certificado está guardada num dispositivo seguro de criação de assinaturas (Secure Signature Creation Device), de acordo com o anexo III da Directiva 1999/93/EC e da lei do país onde a EC está estabelecida.</p>
<b>Internet Certificate Extensions</b>				
<b>Authority Information Access</b>	4.2.2.1		o	
accessMethod		1.3.6.1.5.5.7.48.1	o	<p>Valor do OID: 1.3.6.1.5.5.7.48.1 (id-ad-ocsp)</p> <p>Descrição do OID: Online Certificate Status Protocol</p>
accessLocation		http://ocsp.asc.cartaodecidadao.pt/publico/ocsp	o	
<b>Signature Algorithm</b>	4.1.1.2	1.2.840.113549.1.1.5	m	<p>TEM que conter o mesmo OID do identificador do algoritmo do campo signature no campo da sequência tbsCertificate.</p> <p>sha-1WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsads(113549) pkcs(1) pkcs-1(1) 5 }<sup>Erro! Marcador não definido.</sup></p>
<b>Signature Value</b>	4.1.1.3	<contém a assinatura digital emitida pela EC>	m	<p>Ao gerar esta assinatura, a EC certifica a ligação entre a chave pública e o titular (subject) do certificado.</p>

### 3.1.3 OID do Algoritmo

O campo “*signatureAlgorithm*” do certificado contém o OID do algoritmo criptográfico utilizado pela EC para assinar o certificado: 1.2.840.1.13549.1.1.5 (sha-1WithRSAEncryption<sup>9</sup>).

### 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.

### 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, assim como a indicação explícita dos fins para os quais este certificado deverá ser utilizado.

---

<sup>9</sup> sha-1WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsads(113549) pkcs(1) pkcs-1(1) 5

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

Nada a assinalar.

## 3.2 Certificado “espécimen”

O certificado “espécimen” de Assinatura Digital Qualificada poderá ser emitido sempre que seja necessário validar o perfil, o processo de emissão e/ou a sua utilização. Este certificado tem as seguintes diferenças em relação aos certificados usuais de Assinatura Digital Qualificada:

- Perfil de certificado: é adicionado o prefixo “(espécimen)” ao *CommonName* (CN);
- Perfil de certificado: o atributo *serialNumber* contém “especimen” seguido de um número sequencial único (que começa em 0000001);
- Emissão do certificado: de acordo com formulário específico<sup>10</sup>;
- Revogação do certificado: o certificado é revogado imediatamente após a sua emissão<sup>10</sup>.

## 3.3 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.<sup>3</sup>

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.<sup>3</sup>

O perfil da LRC está de acordo com:

- Recomendação ITU.T X.509<sup>4</sup>,
- RFC 3280<sup>3</sup>, e
- Política de Certificados da SCEE<sup>1</sup>.
- 

### 3.3.1 Número da Versão

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

<sup>10</sup> cf. MULTICERT\_PJ.CC\_53.2.1\_0005\_pt\_AsC.doc. 2007, Formulário de emissão de certificado “espécimen” de Assinatura Digital Qualificada.

### 3.3.2 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	<b>Version</b>	5.1.2.1	1	m	Versão v2 (o valor inteiro é 1)
	<b>Signature</b>	5.1.2.2	1.2.840.113549.1.1.5	m	Contém o identificador do algoritmo utilizado para assinar a LRC. O valor TEM que ser igual ao OID no campo signatureAlgorithm (abaixo)
	<b>Issuer</b>	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>"		
	<b>thisUpdate</b>	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.
	<b>nextUpdate</b>	5.1.2.5	<data da próxima emissão da LRC = <i>thisUpdate</i> + 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 <sup>1</sup> .

<b>revokedCertificates</b>	5.1.2.6	<lista de certificados revogados>	m	
<b>CRL Extensions</b>	5.1.2.7		m	
<b>Authority Key Identifier</b>	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	
<b>CRL Number</b>	5.2.3	<número sequencial único e incrementado>	m	
<b>Issuing Distribution Point</b>	5.2.5		o	
distributionPoint		http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_assinatura_crl<ID_CA>_p<num_seq>.crl	o	
<b>Freshest CRL</b>	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	
<b>CRL Entry Extensions</b>	5.3			

	<b>Reason Code</b>	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
	<b>Signature Algorithm</b>	5.1.1.2	1.2.840.113549.1.1.5	m	TEM que conter o mesmo OID do identificador do algoritmo utilizado no campo signature da sequência tbsCertList. sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 }
	<b>Signature Value</b>	5.1.1.3	<contém a assinatura digital emitida pela EC>	m	Contém a assinatura digital calculada sobre a <i>tbsCertList</i> .

### 3.3.3 Extensões da Delta LRC da EC AsC

Certificate Revocation List Component		Section in RFC 3280	Value	Field Type	Comments
tbsCertList	<b>Version</b>	5.1.2.1	1	m	Version V2 (the integer value is 1)
	<b>Signature</b>	5.1.2.2	1.2.840.113549.1.1.5	m	Contains the algorithm identifier for the algorithm used to sign the CRL. Value MUST match the OID in signatureAlgorithm (below)
	<b>Issuer</b>	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 <nnnnnnnn>"		
	<b>thisUpdate</b>	5.1.2.4	<update date>	m	Implementations MUST specify using UTC time until 2049, from then on using GeneralisedTime
	<b>nextUpdate</b>	5.1.2.5	<next update date = update date + N>	m	This field indicates the date by which the next CRL will be issued. The next CRL could be issued before the indicated date, but it will not be issued any later than the indicated date. CRL issuers SHOULD issue CRLs with a nextUpdate time equal to or later than all previous CRLs.  Implementations MUST specify using UTC time until 2049, from then on using GeneralisedTime. N is at most 1 day.

<b>revokedCertificates</b>	5.1.2.6	<revoked certificates list>	m	
<b>CRL Extensions</b>	5.1.2.7		m	
<b>Authority Key Identifier</b>	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	
<b>CRL Number</b>	5.2.3	<increasing sequence number>	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.
<b>Delta CRL Indicator</b>	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.
<b>Issuing Distribution Point</b>	5.2.5		o	
distributionPoint		http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_assinatura_crl<ID_CA>_p<num_seq>.crl	o	
<b>CRL Entry Extensions</b>	5.3			

	<b>Reason Code</b>	5.3.1		o	Value must be one of the followings: <ul style="list-style-type: none"> <li>1 – keyCompromise</li> <li>2 – cACompromise</li> <li>3 – affiliationChanged</li> <li>4 – superseded</li> <li>5 – cessationOfOperation</li> <li>6 – certificateHold</li> <li>8 – removeFromCRL</li> <li>9 – privilegeWithdrawn</li> <li>10 - aACompromise</li> </ul>
	<b>Signature Algorithm</b>	5.1.1.2	1.2.840.113549.1.1.5	m	MUST contain the same OID algorithm identifier as the signature field in the sequence tbsCertificate.  sha-1WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsads(113549) pkcs(1) pkcs-1(1) 5 } Erro! Marcador não definido.
	<b>Signature Value</b>	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 define as Políticas de Certificados do certificado de Assinatura Digital Qualificada, utilizada pela Entidade de Certificação de Assinatura Digital Qualificada do Cartão de Cidadão no suporte à sua actividade 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 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.

## Referências Bibliográficas

ETSI TS 101 862, 2001-06, Qualified certificate profile, v1.2.1.

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

RFC 3039, 2001, Internet X.509 Public Key Infrastructure Qualified Certificates Profile.

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

RFC 3280. 2002, 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.

# Aprovação do Conselho Executivo