

# **Política de Certificado de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão**

Políticas

---

PJ.CMDA\_34

**Identificação do Projeto:** Chave Móvel Digital

**Identificação da CA:** CMD

**Nível de Acesso:** Público

**Versão:** 1.0

**Data:** 25/02/2018

**Identificador do documento:** PJ.CMDA\_34

**Palavras-chave:** Chave Móvel Digital, Política de Certificados, EC CMD

**Tipologia documental:** Políticas

**Título:** Política de Certificado de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão

**Língua original:** Português

**Língua de publicação:** Português

**Nível de acesso:** Público

**Data:** 25/02/2018

**Periodicidade de Revisão:** 1 ano

**Versão atual:** 1.0

**Identificação do Projeto:** Chave Móvel Digital

**Identificação da CA:** CMD

**Cliente:** AMA

#### Histórico de Versões

Versão	Data	Detalhes	Autor(es)
1.0	Fevereiro 2018	Versão Aprovada	AMA

#### Documentos Relacionados

ID	Detalhes	Autor(es)
PJ.CMDA_33	Declaração de Práticas de Certificação da EC de Chave Móvel Digital de Assinatura Qualificada do Cartão de Cidadão	MULTICERT S.A.

#### Apêndices

ID Documento	Detalhes	Autor(es)
PJ.CMD_35	Formulário de emissão de certificado "espécimen" de CMD	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<sup>1</sup> (SCEE) – Infra-Estrutura de Chaves Públicas do Estado.

Assim, a EC CMD 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 de Chave Móvel Digital de Assinatura Qualificada, emitido pela EC de Chave Móvel Digital de Assinatura Qualificada do Cartão de Cidadão, em complemento das secções 3 e 7 da Política de Certificados do SCEE.

---

<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.

# Sumário

Política de Certificado de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão.....	1
Resumo Executivo .....	3
Sumário.....	4
Introdução .....	5
Objetivos .....	5
Público-Alvo.....	5
Estrutura do Documento.....	5
1 Contexto Geral.....	6
1.1 Visão Geral.....	6
1.2 Designação e Identificação do Documento .....	6
2 Identificação e Autenticação .....	7
2.1 Atribuição de Nomes.....	7
2.1.1 Tipos de nomes .....	7
2.2 Uso do certificado e par de chaves pelo titular.....	7
3 Perfis de Certificado .....	9
3.1 Perfil de Certificado.....	9
3.1.1 Número da Versão .....	9
3.1.2 Extensões do Certificado.....	10
3.1.3 OID do Algoritmo .....	21
3.1.4 Formato dos Nomes .....	21
3.1.5 Condicionamento nos Nomes.....	21
3.1.6 OID da Política de Certificados.....	21
3.1.7 Utilização da extensão <i>Policy Constraints</i> .....	21
3.1.8 Sintaxe e semântica do qualificador de política.....	21
3.1.9 Semântica de processamento para a extensão crítica <i>Certificate Policies</i> .....	22
3.2 Certificado “espécimen” .....	22
Conclusão .....	23
Referências Bibliográficas.....	24
Aprovação.....	25

# Introdução

## Objetivos

O objetivo deste documento é apresentar o perfil do certificado de Chave Móvel Digital de Assinatura Qualificada do Cidadão emitido, pela Entidade de Certificação de Chave Móvel Digital de Assinatura Qualificada do Cidadão (EC CMD).

## Público-Alvo

Este documento deve ser lido por:

- Recursos humanos atribuídos aos grupos de trabalho da EC CMD;
- Terceiras partes, encarregues de auditar a EC CMD;
- 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.

# I Contexto Geral

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

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

## I.1 Visão Geral

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

## I.2 Designação e Identificação do Documento

Este documento é a Política de Certificado de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão. A PC é representada num certificado através de um número único designado de “identificador de objeto” (OID), sendo o valor do OID associado a este documento o “2.16.620.1.1.1.2.4.3.0.1.1”.

Este documento é identificado pelos dados constantes na seguinte tabela:

INFORMAÇÃO DO DOCUMENTO	
<b>Versão do Documento</b>	Versão 1.0
<b>Estado do Documento</b>	Aprovado
<b>Data de Emissão</b>	Fevereiro de 2018
<b>Validade</b>	Não aplicável
<b>Localização</b>	<a href="https://pki.cartaodecidadao.pt/publico/politicas/cp.html">https://pki.cartaodecidadao.pt/publico/politicas/cp.html</a>

<sup>2</sup> cf. PJ.CMDA\_33, Declaração de Práticas de Certificação da EC de Chave Móvel Digital de Assinatura Qualificada do Cartão de Cidadão.

## 2 Identificação e Autenticação

### 2.1 Atribuição de Nomes

A atribuição de nomes segue a convenção determinada pelo SCEE<sup>1</sup>, pela DPC da EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão<sup>2</sup> e, pelo Despacho 155/2017 (“Criação de assinaturas eletrónicas à distância, com gestão por um prestador qualificado de serviços de confiança em nome do signatário”) do Gabinete Nacional de Segurança.

#### 2.1.1 Tipos de nomes

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

O nome único do certificado é identificado pelos seguintes componentes:

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

### 3.1 Perfil de Certificado

Os utilizadores de uma chave pública têm que ter confiança que a chave privada associada é detida pelo titular remoto correto (pessoa ou sistema) com o qual irão utilizar mecanismos de cifra ou assinatura digital. Essa confiança é dada através do uso de certificados digitais X.509 v3, que são estruturas de dados que fazem a ligação entre a chave pública e o seu titular. Esta ligação é garantida através da assinatura digital de cada certificado por uma EC de confiança. A EC pode basear esta afirmação em meios técnicos (por exemplo, prova de posse da chave privada através de um protocolo desafio-resposta), na apresentação da chave privada, ou no registo efetuado pelo titular.

Um certificado tem um período limitado de validade, indicado no seu conteúdo e assinado pela EC. Como a assinatura do certificado e a sua validade podem ser verificadas independentemente por qualquer *software* que utilize certificados, os certificados podem ser distribuídos através de linhas de comunicação e sistemas públicos, assim como podem ser guardados em qualquer tipo de unidades de armazenamento.<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 Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão está de acordo com:

- Recomendação ITU.T X.509<sup>4</sup>;
- RFC 5280<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).

<sup>3</sup> cf. RFC 5280. 2008, 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.

### 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		Seção no RFC 3280	Valor	Tipo <sup>5</sup>	Comentários
tbsCertificate	<b>Version</b>	4.1.2.1	v3	m	
	<b>Serial Number</b>	4.1.2.2	<atribuído pela EC a cada certificado>	m	
	<b>Signature</b>	4.1.2.3	2.16.840.113549.1.1.11	m	Valor TEM que ser igual ao OID no <i>signatureAlgorithm</i> (abaixo)
	<b>Issuer</b>	4.1.2.4		m	
	Country (C)		"PT"		
	Organization (O)		AMA - AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA I. P.		
	Organization Unit (OU)		"Cartão de Cidadão"		
	Organization Unit (OU)		"subECEstado"		
	Common Name (CN)		"EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão <nnnn>"		
	<b>Validity</b>	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 + 10 anos>		
	<b>Subject</b>	4.1.2.6		m	
	Country (C)		"PT"		
	Organization (O)		"Cartão de Cidadão"		
Organization Unit (OU)		"Cidadão Português"			

---

<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 Unit (OU)		"Chave Móvel Digital de Assinatura Qualificada do Cidadão"		
	Organization Unit (OU)		"RemoteQSCDManagement"		
	Surname (SN)		<nome de família do cidadão>		
	Given Name (givenName)		<nome(s) próprio do cidadão>		
	Serial Number (serialNumber)		"BI"<ID do cidadão>		
	Common Name (CN)		<concatenação do givenName e SN 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		1.2.840.113549.1.1.11		<p>O OID <i>rsaEncryption</i> identifica chaves públicas RSA.</p> <p>pkcs-1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 1 }</p> <p>rsaEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}</p> <p>O OID <i>rsaEncryption</i> deve ser utilizado no campo <i>algorithm</i> com um valor do tipo <i>AlgorithmIdentifier</i>. 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 2048 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 256-bit SHA-256 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 256-bit SHA-256 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" selecionado		
	Non Repudiation		"1" selecionado		Se o bit <i>nonRepudiation</i> for selecionado, este NÃO DEVE ser combinado com qualquer outro bit do <i>key usage</i> , i.e., se selecionado, DEVE ser o único selecionado. <sup>7</sup>
	Key Encipherment		"0" selecionado		
	Data Encipherment		"0" selecionado		
	Key Agreement		"0" selecionado		
	Key Certificate Signature		"0" selecionado		
	CRL Signature		"0" selecionado		
	Encipher Only		"0" selecionado		
	Decipher Only		"0" selecionado		
	<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		<p>policyQualifierID: 1.3.6.1.5.5.7.2.1</p> <p>cPSuri: <a href="http://www.scee.gov.pt/pcert">http://www.scee.gov.pt/pcert</a></p>		<p>Valor do OID: 1.3.6.1.5.5.7.2.1 (id-qt-cps PKIX CPS Pointer Qualifier)</p> <p>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."</p> <p>(<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>)</p>
	policyIdentifier		2.16.620.1.1.1.2.4.3.0.7	m	Identificador da Declaração de Práticas de Certificação da EC CMD.
	policyQualifiers		<p>policyQualifierID: 1.3.6.1.5.5.7.2.1</p> <p>cPSuri:</p> <p><a href="http://pki.cartaodecidadao.pt/publico/politicas/dpc/cc_sub-ec_cidadao_cmd_dpc.html">http://pki.cartaodecidadao.pt/publico/politicas/dpc/cc_sub-ec_cidadao_cmd_dpc.html</a></p>	o	
	policyIdentifier		2.16.620.1.1.1.2.4.3.0.1.1	m	Identificador desta Política.
	policyQualifiers		<p>policyQualifierID: 1.3.6.1.5.5.7.2.1</p> <p>cPSuri:</p> <p><a href="http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_sub-ec_cidadao_cmd_pc.html">http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_sub-ec_cidadao_cmd_pc.html</a></p>	o	
	policyIdentifier		policyQualifierID: 0.4.0.2042.1.2		NCP+: Extended Normalized Certificate policy
	policyIdentifier		policyQualifierID: 0.4.0.1941.12.1.2		QCP-n-qscd: certificate policy for EU qualified certificates issued to natural persons with private key related to the certified public key in QSCD
	<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="https://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_cmd_crl&lt;ID_CA&gt;_p&lt;num_seq&gt;.crl">https://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_cmd_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="https://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_cmd_crl&lt;ID_CA&gt;_delta_p&lt;num_seq&gt;.crl">https://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_cmd_crl&lt;ID_CA&gt;_delta_p&lt;num_seq&gt;.crl</a>	o	
	<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, em complemento à informação presente no campo <i>subject</i> e na extensão <i>subject alternative name</i> .  ( <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>	-	id-pe-qcStatements = "1.3.6.1.5.5.7.1.3"	o	Não é uma extensão definida no RFC 3280. A extensão QCStatements é uma extensão introduzida pelo PKIX <i>Qualified Certificate Profile</i> 7 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> )
	id-qcs-pkixQCSyntax-v2		id-etsi-qcs-QcCompliance = "0.4.0.1862.1.1"		A aposição desta componente ao certificado que este este é emitido de acordo com o Anexo III do Regulamento (EU) 910/2014).  A declaração <i>QcEuCompliance</i> (id-etsi-qcs-QcCompliance) corresponde ao OID "0.4.0.1862.1.1".

<sup>8</sup> cf. ETSI EN 319 412-5 V2.1.1 - *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements*

	id-qcs-pkixQCSyntax-v2		id-etsi-qcs-QcSSCD = " 0.4.0.1862.1.4"		Declaração efetuada, indicando que a chave privada associada à chave pública no certificado está guardada num dispositivo qualificado de criação de assinatura eletrónico, de acordo com o Anexo II do Regulamento (EU) 910/2014.
	id-qcs-pkixQCSyntax-v2		d-etsi-qcs-QcPDS="0.4.0.1862.1.6.1" Text="Certificate for electronic signatures as defined in Regulation (EU) No 910/2014"		Declaração, representada por um OID, indicando que este certificado é emitido como um certificado qualificado de assinatura eletrónica, de acordo com o Anexo I do Regulamento (EU) 910/2014.
	id-qcs-pkixQCSyntax-v2		id-etsi-qcs-QcPDS="0.4.0.1862.1.5" URI= <a href="http://pki.cartaodecidadao.pt/publico/politicas/cps.html">http://pki.cartaodecidadao.pt/publico/politicas/cps.html</a> Language: PT		
	<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	Valor do OID: 1.3.6.1.5.5.7.48.1 (id-ad-ocsp) Descrição do OID: <i>Online Certificate Status Protocol</i>
	accessLocation		<a href="http://ocsp.cmd.cartaodecidadao.pt/publico/ocsp">http://ocsp.cmd.cartaodecidadao.pt/publico/ocsp</a>	o	
	<b>Signature Algorithm</b>	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) rsdsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}
	<b>Signature Value</b>	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: 1.2.840.1.13549.1.1.11(*sha-256WithRSAEncryption*)<sup>6</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 os URI’s onde podem ser encontrados os documentos, Declaração de Práticas de Certificação e Política de Certificado (i.e., este documento), com os OIDs identificados pelo “*policyIdentifier*”. Os qualificadores opcionais (“*policyQualifierID*: 1.3.6.1.5.5.7.2.2” e “*userNotice explicitText*”) contêm um apontador na forma de texto, com a indicação explícita dos fins para os quais este certificado deverá ser utilizado.

### 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 outro para a Política de Certificados. O “*userNotice explicitText*” contém um apontador, na forma de texto com a indicação explícita dos fins para os quais este certificado deverá ser utilizado.

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

Nada a assinalar.

## 3.2 Certificado “espécimen”

O certificado “espécimen” de Chave Móvel Digital de Assinatura Qualificada do Cidadão 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 “(ESPECIMEN)” ao *CommonName* (CN);
- Emissão do certificado: de acordo com formulário específico<sup>9</sup>;
- Revogação do certificado: o certificado é revogado imediatamente após a sua emissão<sup>9</sup>.

---

<sup>9</sup> cf. PJ.CMDA\_35, Formulário de emissão de certificado “espécimen” de certificado de CMD.

# Conclusão

Este documento rege-se pelo definido na Política de Certificados do SCEE especificando o perfil dos certificados de Assinatura Digital Qualificada, emitidos pela Entidade de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão no suporte à sua atividade de certificação digital. A hierarquia de confiança da Entidade de Certificação de Chave Móvel Digital 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 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.*

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 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.*

ETSI TS 102 042 v2.4.1 (2013-02) - *Policy requirements for certification authorities issuing public key certificates;*

ETSI TS 102 176-1 v2.1.1 (2011-07) - *Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms;*

ETSI TS 101 456 V1.4.3 (2007-05) - *Electronic Signatures and Infrastructures (ESI);*

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;*

ETSI EN 319 411-2 V2.1.1 (2016-02) - *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates;*

ETSI EN 319 412-2 v2.1.1 (2016-02) - *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons;*

ETSI EN 319 412-5 v2.1.1 (2016-02) - *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements;*

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