

# Política de Certificado de Assinatura Digital Qualificada

Políticas

---

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

**Identificação do Projeto:** Cartão de Cidadão

**Identificação da CA:** AsC

**Nível de Acesso:** Público

**Versão:** 4.0

**Data:** Jan 2020

**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 Certificado de Assinatura Digital Qualificada

**Língua original:** Português

**Língua de publicação:** Português

**Nível de acesso:** Público

**Data:** Jan 2020

**Periodicidade de Revisão:** 1 ano

**Versão atual:** 4.0

**Identificação do Projeto:** Cartão de Cidadão

**Identificação da CA:** AsC

**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 – 1.3	01/05/2014	- Atualização do algoritmo de assinatura para SHA256 e tamanho de chave para 2048 bits	MULTICERT
1.4	01/10/2017	- Atualização de referenciais inerentes ao regulamento (EU n.º 910/2014) - Inclusão de novo QCStatement e policies - Alteração da validade do certificado para 10 anos	MULTICERT
1.5	14/02/2018	- Atualização de QC Statement (PDS) - Inclusão do Campo <i>Organization</i> no DN da EC	Grupo Políticas
<b>2.0</b>	<b>03/07/2018</b>	<b>Versão Aprovada</b>	<b>Grupo de Gestão</b>
2.1	05/01/2019	Alteração do tamanho de chaves do certificado de assinatura de 2048 para 3072 bits	INCM
<b>3.0</b>	<b>28/01/2019</b>	<b>Versão Aprovada</b>	<b>Grupo de Gestão</b>
3.1	08/11/2019	Revisão anual	MULTICERT
<b>4.0</b>	<b>Jan 2020</b>	<b>Versão aprovada</b>	<b>Grupo de Gestão</b>

#### 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.doc	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 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 AsC não é detentora de uma Política de Certificados, sendo que a emissão de certificados segue as orientações constantes na Política de Certificado do SCEE. Este documento apresenta o perfil dos Certificados de Assinatura Digital Qualificada, emitido pela EC de Assinatura Digital 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 Assinatura Digital Qualificada .....	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 .....	8
3.1 Perfil de Certificado .....	8
3.1.1 Número da Versão.....	8
3.1.2 Extensões do Certificado .....	9
3.1.3 OID do Algoritmo.....	17
3.1.4 Formato dos Nomes.....	17
3.1.5 Condicionamento nos Nomes .....	17
3.1.6 OID da Política de Certificados .....	17
3.1.7 Utilização da extensão <i>Policy Constraints</i> .....	17
3.1.8 Sintaxe e semântica do qualificador de política.....	18
3.1.9 Semântica de processamento para a extensão crítica <i>Certificate Policies</i> .....	18
3.2 Certificado “espécimen” .....	18
Conclusão.....	19
Referências Bibliográficas.....	20
Aprovação .....	21

# Introdução

## Objetivos

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

## Público-Alvo

Este documento deve ser lido por:

- Recursos humanos atribuídos aos grupos de trabalho da EC AsC;
- Terceiras partes, encarregues de auditar a EC AsC;
- Todo o público, em geral.

## Estrutura do Documento

Assume-se que o leitor é conhecedor dos conceitos de criptografia, infraestruturas de chave pública e assinatura eletrónica. Caso esta situação não se verifique recomenda-se o aprofundar de conceitos e conhecimento nos tópicos anteriormente 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 Assinatura Digital Qualificada do Cartão de Cidadão (EC AsC), permitindo assim garantir a fiabilidade dos mesmos. Não se pretende nomear regras legais ou obrigações, mas antes informar, pelo que se pretende que este documento seja simples, direto e entendido por um público alargado, incluindo pessoas sem conhecimentos técnicos ou legais.

Os Certificados emitidos pela EC AsC contêm uma referência à 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 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 objeto” (OID), sendo o valor do OID associado a este documento apresentado na tabela abaixo.

Este documento é identificado pelos dados constantes na seguinte tabela:

<b>INFORMAÇÃO DO DOCUMENTO</b>	
<b>Versão do Documento</b>	Versão 4.0
<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>	Janeiro 2020
<b>Validade</b>	1 ano
<b>Localização</b>	<a href="http://pki.cartaodecidadao.pt/publico/politicas/cp.html">http://pki.cartaodecidadao.pt/publico/politicas/cp.html</a>

<sup>2</sup> cf. PJ.CC\_24.1.1\_0002\_pt\_AsC.pdf, 2018. Declaração de Práticas de Certificação da EC de Assinatura Digital 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> 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>	BI<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

### 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 Assinatura Digital Qualificada 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>.
- Legislação nacional e Europeia, aplicável.

#### 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		Secção no RFC 5280	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	2.16.840.113549.1.1.11	m	Valor TEM que ser igual ao OID no <i>signatureAlgorithm</i> (abaixo) <b>Nota:</b> Até à EC de Assinatura 009 (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)		"Instituto dos Registos e do Notariado I. P."		O valor deste campo foi "Cartão de Cidadão" até à EC de Assinatura 0013, tendo o valor sido substituído pelo indicado.
	Organization Unit (OU)		"Cartão de Cidadão"		O valor deste campo consta no campo <i>Organization</i> (O) até à EC de Assinatura 0013. A partir da EC de Assinatura 0014, passa a estar incluído neste campo <i>Organization Unit</i> (OU)
	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 <i>GeneralisedTime</i>
	Not Before		<data de emissão>		
	Not After		<data de emissão + 10 anos>		Até à EC de Assinatura 0012 (inclusive) a validade do certificado de assinatura qualificada é de 5 anos.

<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).

Componente do Certificado		Secção no RFC 5280	Valor	Tipo <sup>5</sup>	Comentários
	<b>Subject</b>	4.1.2.6		m	
	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 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		1.2.840.113549.1.1.11		<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</p>

Componente do Certificado		Secção no RFC 5280	Valor	Tipo <sup>5</sup>	Comentários
					campo TEM que ter o tipo ASN.1 a NULL para o identificador deste algoritmo. <sup>6</sup>
	subjectPublicKey		<Chave Pública com modulus n de 3072 bits>		Até à EC de Assinatura Digital Qualificada (AsC) 009 (inclusive) o tamanho da chave é de 1024 bits. Da EC AsC 010 até à EC AsC 014 os certificados de assinatura foram emitidos com tamanho da chave de 2048 bits.
	<b>X.509v3 Extensions</b>	4.1.2.9		m	
	<b>Authority Key Identifier</b>	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	
	<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" selecionado		

<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.

Componente do Certificado		Secção no RFC 5280	Valor	Tipo <sup>5</sup>	Comentários
	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>
	policyQualifiers		<i>policyQualifierID</i> : 1.3.6.1.5.5.7.2.1 <i>cPSuri</i> : <a href="https://www.scee.gov.pt/rep">https://www.scee.gov.pt/rep</a>		Valor do OID: 1.3.6.1.5.5.7.2.1 ( <i>id-qt-cps PKIX CPS Pointer Qualifier</i> )  Descrição do OID: "O atributo <i>cPSuri</i> 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> )
	policyIdentifier		2.16.620.1.1.1.2.4.1.0.7	m	Identificador da Declaração de Práticas de Certificação da EC AsC.

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

Componente do Certificado		Secção no RFC 5280	Valor	Tipo <sup>5</sup>	Comentários
	policyQualifiers		policyQualifierID: 1.3.6.1.5.5.7.2.1 cPSuri: http://pki.cartaodecidadao.pt/publico/politicas/cps.html	o	
	policyIdentifier		2.16.620.1.1.1.2.4.1.0.1.1	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/cp.html"	o	
	policyIdentifier		policyQualifierID: 0.4.0.2042.1.2		NCP+: Extended Normalized Certificate policy
	policyIdentifier		policyQualifierID: 0.4.0.194112.1.2		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		http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_assinatura_crl<ID_CA>_p<num_seq>.crl	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>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 <i>subject</i> e na extensão <i>subject alternative name</i> .

Componente do Certificado		Secção no RFC 5280	Valor	Tipo <sup>5</sup>	Comentários
					(http://www.alvestrand.no/objectid/submissions/2.5.29.9.html)
	<b>Qualified Certificate Statement</b>	-	id-pe-qcStatements = "1.3.6.1.5.5.7.1.3"	o	A extensão QCStatements é uma extensão introduzida pelo PKIX Qualified Certificate Profile <sup>7</sup> e ETSI <sup>8</sup>  (http://javadoc.iaik.tugraz.at/iaik_jce/current/iaik/x509/extensions/qualified/QCStatements.html)
	id-qcs-pkixQCSyntax-v2		id-etsi-qcs-QcCompliance = "0.4.0.1862.1.1"		A aposição desta componente no certificado atesta que este é emitido de acordo com o Anexo I do Regulamento (EU) 910/2014).
	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 Regulamento (EU) 910/2014.
	id-qcs-pkixQCSyntax-v2		id-etsi-qct-esign="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		Declaração de Divulgação de Princípios
	<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>

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

Componente do Certificado		Secção no RFC 5280	Valor	Tipo <sup>5</sup>	Comentários
	accessLocation		<a href="http://ocsp.asc.cartaodecidedao.pt/publico/ocsp">http://ocsp.asc.cartaodecidedao.pt/publico/ocsp</a>	o	
	<b>Signature Algorithm</b>	4.1.1.2	2.16.840.1.13549.1.1.11	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) rsadi(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>9</sup>.

Até à EC de Assinatura Digital Qualificada 009 (inclusive), este campo continha o OID 1.2.840.1.13549.1.1.5 (*sha1WithRSAEncryption*)<sup>10</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*”) contem 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.

<sup>9</sup> Sha256WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}

<sup>10</sup> 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 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 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 “*specimen*” seguido de um número sequencial único (que começa em 0000001);
- Emissão do certificado: de acordo com formulário específico<sup>11</sup>;
- Revogação do certificado: o certificado é revogado imediatamente após a sua emissão<sup>11</sup>.

---

<sup>11</sup> cf. PJ.CC\_53.2.1\_0005\_pt\_AsC.doc. 2007, Formulário de emissão de certificado “espécimen” de Assinatura Digital Qualificada.

# 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 Assinatura Digital Qualificada do Cartão de Cidadão no suporte à sua atividade 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 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*.
- NIST FIPS PUB 180-2. 2002, *Secure Hash Standard, U. S. Department of Commerce, Technology Administration, National Institute of Standards and Technology*.
- SCEE 2.16.620.1.1.1.2.1.1.0. 2006, *Política de Certificados da SCEE e Requisitos mínimos de Segurança*.
- PC.CC\_24.1.1\_0002\_pt\_AsC – *Declaração de Práticas de Certificação da EC de Assinatura Digital Qualificada do Cartão de Cidadão*
- 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 319 401 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*;
- 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 319 412-1 v1.1.1 – *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures*;
- ETSI EN 319 412-2 v2.1.1 – *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 – *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements*;
- Regulamento (UE) n° 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