multicert
Engineering for digital security

Política de Certificados Qualificados de Assinatura e Selo Eletrónico

Políticas

MULTICERT_PJ.CA3_24.1.2_0002_pt.doc

Identificação do Projeto: PKI da MULTICERT

Identificação da CA: EC MULTICERT

Nível de Acesso: Público

Versão: 4.0

Data: 31/05/2017

MULTICERT, Serviços de Certificação Electrónica, S.A.,
Lagoas Park, Edifício 3, Piso 3 - 2740-266 Porto Salvo – Oeiras
Telefone: +351 217 123 010 Facsimile: +351 217 123 011

Identificador do documento: MULTICERT_PJ.CA3_24.1.2_0002_pt.doc

Palavras-chave: Política de Certificados, EC MULTICERT

Tipologia documental: Políticas

Título: Política de Certificados Qualificados de Assinatura e Selo Eletrónico

Língua original: Português

Língua de publicação: Português

Nível de acesso: Público

Data: 31/05/2017

Versão atual: 4.0

Identificação do Projeto: PKI da MULTICERT

Identificação da CA: EC MULTICERT

Cliente: MULTICERT S.A.

Histórico de Versões

N.º de Versão	Data	Detalhes	Autor(es)
1.0	13/01/2009	Versão inicial	MULTICERT S.A.
1.1	23/03/2009	Atualização de Conteúdos	MULTICERT S.A.
1.2	24/03/2009	Revisão Grupo de Políticas	MULTICERT S.A.
1.3	25/03/2009	Atualização de Conteúdos	MULTICERT S.A.
1.4	25/03/2009	Atualização de Conteúdos	MULTICERT S.A.
1.5	25/03/2009	Atualização de referências bibliográficas	MULTICERT S.A.
1.6	20/04/2010	Revisão de Conteúdos	MULTICERT S.A.
1.8	05/05/2014	Atualização de Algoritmo de Assinatura	MULTICERT S.A.
1.9	09/07/2014	Alteração de Morada	MULTICERT S.A.
2.0	27/02/2015	Versão Aprovada	MULTICERT S.A.
2.1	06/11/2015	Revisão	MULTICERT S.A.
3.0	13/01/2016	Versão Aprovada	MULTICERT S.A.
3.1	26/01/2017	Revisão	MULTICERT S.A.
3.2	29/05/2017	Inclusão do Certificado Qualificado de Selo Eletrónico	MULTICERT S.A.
4.0	31/05/2017	Versão Aprovada	MULTICERT S.A.

Documentos Relacionados

ID Documento	Detalhes	Autor(es)
MULTICERT_PJ.CA3_24.1.1_0001_pt.doc	Declaração de Práticas de Certificação	MULTICERT S.A.
MULTICERT_PJ.CA3_24.1.2_0001_pt.doc	Política de Certificado da raiz auto-assinada da EC MULTICERT	MULTICERT S.A.
MULTICERT_MO.DOC_53_0142_pt.doc	Declaração de Responsabilidade sobre a Utilização de Certificados Espécime	MULTICERT S.A.

Resumo Executivo

Decorrente da implementação de vários programas públicos e privados 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, do governo eletrónico (*eGovernment*) e do comércio eletrónico, os certificados digitais emitidos pela Entidade de Certificação MULTICERT, credenciada pela Entidade Supervisora (conforme previsto na legislação europeia e nacional), fornecem os mecanismos necessários para a autenticação digital forte da identidade do titular do certificado eletrónico, assim como as assinaturas eletrónicas (equivalente legal das assinaturas manuscritas) indispensáveis aos processos de desmaterialização.

A infraestrutura da Entidade de Certificação MULTICERT fornece uma hierarquia de confiança, que promove a segurança eletrónica do titular do certificado digital. A Entidade de Certificação MULTICERT 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 Entidade de Certificação MULTICERT está devidamente credenciada pela Autoridade Nacional de Segurança (http://www.gns.gov.pt/trusted-lists.aspx), com credenciação número ANS-ECC-7/2014, à data de 20/06/2014, conforme previsto na legislação portuguesa e europeia, estando deste modo habilitada legalmente a emitir todo o tipo de certificados digitais, incluindo os certificados digitais qualificados (certificados digitais de mais elevado grau de segurança previsto na legislação).

Este documento define a Política de certificados utilizada na emissão dos certificado qualificados de assinatura digital e selo eletrónico, que complementa e está de acordo com a Declaração de Práticas de Certificação (DPC) da EC MULTICERT[1].

[1] *cf.* MULTICERT_PJ.CA3_24.1.1_0001_pt.doc., Declaração de Práticas de Certificação.

Sumário

Introdução

Objetivos

O objetivo deste documento é definir as políticas utilizadas na emissão dos Certificados Qualificados de Assinatura digital e de Selo Eletrónico, pela EC MULTICERT.

Público-Alvo

Este documento deve ser lido por,

- Recursos humanos atribuídos aos grupos de trabalho da EC MULTICERT,
- Terceiras partes encarregues de auditar a EC MULTICERT,
- 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 MULTICERT[1], presumindo-se que o leitor leu integralmente o seu conteúdo antes de iniciar a leitura deste documento.

1 Introdução

O presente documento é um documento de Política de Certificados, ou PC, cujo objetivo 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, direto 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 dos Certificados Qualificados de Assinatura Digital e de Selo Eletrónico, emitido pela EC MULTICERT.

Os certificados emitidos pela EC MULTICERT 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

Este documento satisfaz e complementa os requisitos impostos pela Declaração de Práticas de Certificação (DPC) da EC MULTICERT[1].

1.2 Designação e Identificação do Documento

Este documento é a Política de Certificados de assinatura digital qualificada. A PC é representada num certificado através de um número único designado de "identificador de objeto" (OID).

Este documento é identificado pelos dados constantes na seguinte tabela:

INFORMAÇÃO DO DOCUMENTO	
Versão do Documento	Versão 4.0
Estado do Documento	Aprovado
OID	1.3.6.1.4.1.25070.1.1.1.1.0.1.2
Data de Emissão	31/05/2017
Validade	1 Ano
Localização	https://pki.multicert.com/index.html

2 Identificação e Autenticação

2.1 Atribuição de Nomes

A atribuição de nomes segue a convenção determinada pela DPC da EC MULTICERT[1].

2.1.1 Tipos de nomes

Os certificados qualificados, de assinatura digital e de selo eletrónico são identificado por um nome único (DN – *Distinguished Name*) de acordo com *standard* X.500.

O nome único do certificado é identificado pelos componentes descritos nas secções seguintes, conforme certificado.

2.1.1.1 Certificado Qualificado de Assinatura Digital

Atributo	Código	Valor
Country	C	<País de nacionalidade do titular do certificado>
Organization	O (opcional)	<Organização à qual o titular do certificado pertence>
Organization Unit	OU (opcional)	<Área/Departamento da Organização à qual o titular do certificado pertence>
Organization Unit	OU (opcional)	<Área/Departamento da Organização à qual o titular do certificado pertence>
Organization Unit	OU	**Certificado para pessoa singular – Assinatura Qualificada**
Locality	L (opcional)	<Localidade de residência do titular>
State or Province	ST (opcional)	<Província, estado, distrito de residência do titular>
Title	title (opcional)	<Qualidade do titular do certificado, no âmbito da sua utilização para assinatura digital qualificada>
SerialNumber	serialNumber	<**IDC** ou **PAS**>[2]<código país>-<nº identificação>
Surname	SN	<Nomes de família do titular do certificado>
GivenName	givenName	<Nomes próprio do titular do certificado>

[2] **IDC** – Nº de Identificação Civil; **PAS** – Nº do Passaporte

Common Name	CN	<nome do titular do certificado>

A Constituição do DN do certificado qualificado de assinatura digital, pode variar conforme especificações das Entidade de Registo da EC MULTICERT (ver 3.1.3).

2.1.1.2 Certificado Qualificado de Selo Eletrónico

Atributo	Código	Valor
Country	C	<País de nacionalidade da Organização>
Organization	O	<Nome da Organização tal como registada nas entidades competentes>
Organization Unit	OU	**Qualified Certificate for Electronic Seal**
Organization Unit	OU (opcional)	<Área/Departamento da Organização>
Organization Identifier	OI	**VAT**[3]<código país>-<Número do de identificação Fiscal>
Common Name	CN	<Nome da organização pela qual é conhecida>

2.2 Uso do certificado e par de chaves pelo titular

O *Commom Name* do *Distinguished Name* define o titular do certificado, sendo que para o Certificado Qualificado de Assinatura Digital, este assume a identificação de uma pessoa singular. Para o Certificado Qualificado de Selo Eletrónico o valor deste campo assume o nome de uma pessoa coletiva.

Os certificados de assinatura qualificada associam os dados de validação da assinatura eletróncia a uma pessoa singular. Os certificados qualificados de selo eletrónico fazem esta associação a uma pessoa coletiva, garantindo a origem e a integridade dos dados.

Os certificados emitidos segundo esta política são equivalentes a certificados digitais qualificados, nos termos, do definido na Legislação Portuguesa e normativos europeus e internacionais, aplicável para o efeito.

[3] **VAT** – Identificação com base num número nacional de identificação do imposto sobre o valor acrescentado.

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 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, estes podem ser distribuídos através de linhas de comunicação e sistemas públicos, assim como guardados no tipo de unidades de armazenamento mais adequados para cada tipo de certificados[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 de um certificado adicional para obter a chave pública da EC e validar a 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 os certificados das EC's que assinaram este e assim consecutivamente até chegar à EC Raiz[4]

O perfil do certificado de assinatura digital qualificada está de acordo com:

- Recomendação ITU.T X.509[5],
- RFC 5280[4], e
- Legislação relevante portuguesa, europeia e internacional.

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.

[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.*

3.1.3 Perfil de Certificado Qualificado de Assinatura Digital Qualificada

Componente do Certificado		Secção no RFC 5280	Valor	Tipo[6]	Comentários
tbsCertificate	**Version**	4.1.2.1	v3	m	Versão do certificado de acordo com o *standard* X.509
	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)
	Issuer	4.1.2.4		m	
	Country (C)		"PT"		País do titular
	Organization (O)		"MULTICERT - Serviços de Certificação Electrónica S.A"		Designação formal da organização do titular
	Organization Unit (OU)		"Entidade de Certificação Credenciada"		Outra designação da organização do titular
	Common Name (CN)		"MULTICERT - Entidade de Certificação <nnn>"		Nome da EC
	Validity	4.1.2.5		m	Validade do Certificado 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).

Componente do Certificado		Secção no RFC 5280	Valor	Tipo[6]	Comentários
	Not After		<data de emissão + máximo de 5 anos>		Validade máxima de 5 anos.
	Subject	4.1.2.6		m	
	Country (C)		<País de nacionalidade do titular do certificado>		No âmbito das Entidade de Registo (ER) **OF[7], OM[8] e AR[9]**, este campo assume o valor "PT"
	Organization (O)		<Organização à qual o titular do certificado pertence>	o	No âmbito da **ER OF**, este campo assume o valor "Ordem dos Farmacêuticos" No âmbito da **ER OM**, este campo assume o valor "Ordem dos Médicos" No âmbito da **ER AR**, este campo assume o valor "Assembleia da República"
	Organization Unit (OU)		<Área/Departamento da Organização à qual o titular do certificado pertence>	o	Este campo não faz parte da constituição do *subject* do certificado emitido no âmbito da ER AR
	Organization Unit (OU)		**Certificado para pessoa singular – Assinatura Qualificada**		Designação do tipo de certificado. No âmbito da **ER AR** este campo não faz parte da constituição do *subject* dos seus certificados.
	Locality (L)		<Localidade de residência do titular>	o	No âmbito da **ER AR** este campo não faz parte da constituição do *subject* dos seus certificados.
	Common Name (CN)		<nome do titular do certificado>		

[7] Ordem dos Farmacêuticos
[8] Ordem dos Médicos
[9] Assembleia da República

Componente do Certificado		Secção no RFC 5280	Valor	Tipo[6]	Comentários
	Title (title)		<Qualidade do titular do certificado, no âmbito da sua utilização para assinatura digital qualificada> - *Informação confirmada pela Entidade de Certificação apenas na data de emissão e que não foi confirmada posteriormente a essa data*, ou informação similar.	o	A qualidade, no âmbito da **ER OF** é "Farmacêutico", no âmbito da **ER OM** é "Médico". No âmbito da **ER AR** será a qualidade <Qualidade do titular do certificado, no âmbito da sua utilização para assinatura digital qualificada>.
	Surname (SN)		<Nomes de família do titular do certificado>	o	Este campo não faz parte da constituição do *subject* do certificado emitido no âmbito da **ER AR**
	Given Name (givenName)		<Nomes próprio do titular do certificado>	o	Este campo não faz parte da constituição do *subject* do certificado emitido no âmbito da **ER AR**
	Serial Number (serialNumber)		<Identificador único do titular do certificado>	o	Num âmbito geral, este campo assume os valores **IDC** ou **PAS** seguido do código do país do n° associado. A estrutura é a seguinte: <doc de identificação><código do país>-<n° de identificação>, (exemplo IDCPT-12345678) Nas Entidades de Registo específicas com âmbitos restritos, nomeadamente **OF** e **OM**, este campo é constituído por "CP"<N° da cédula profissional> Este campo não faz parte da constituição do *subject* do certificado emitido no âmbito da **ER AR**
	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).

Componente do Certificado		Secção no RFC 5280	Valor	Tipo[6]	Comentários
	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 ::= { pkcs-1 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.[10]
	subjectPublicKey		<Chave Pública com *modulus* n de 2048 bits>		
	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 *subjectPublicKey* (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. Confere o tipo de utilização do certificado.
	Digital Signature		"0" selecionado		

[10] *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[6]	Comentários
	Non Repudiation		"1" selecionado		certKeyUsage KeyUsage ::= {nonRepudiation}[11]
	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		
	Certificate Policies	4.2.1.4		o	
	policyIdentifier		**1.3.6.1.4.1.25070.1.1.1.1.0.1.2**	m	Identificador da Politica de Certificado de Assinatura Digital Qualificada
	policyQualifiers		policyQualifierID: 1.3.6.1.5.5.7.2.1 cPSuri: https://pki.multicert.com/index.html		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 Politica de Certificados Qualificados (Assinatura Digital e Selo Eletrónico) publicada pela EC. O apontador está na forma de um URI."

[11] *cf.* RFC 3739. 2004, *Internet X.509 Public Key Infrastructure: Qualified Certificates Profile.*

Componente do Certificado		Secção no RFC 5280	Valor	Tipo[6]	Comentários
	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 o Regulamento (EU 910/2014"		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" (http://www.alvestrand.no/objectid/submissions/1.3.6.1.5.5.7.2.2.html)
	policyIdentifier		**1.3.6.1.4.1.25070.1.1.1.1.0.7**	o	Identificador da Declaração de Práticas de Certificação da EC MULTICERT
	policyQualifiers		policyQualifierID: 1.3.6.1.5.5.7.2.1 cPSuri: https://pki.multicert.com/index.html	o	
	policyIdentifier		policyQualifierID: 0.4.0.1862.1.5		Valor do OID: 0.4.0.1862.1.5 (esi4-qcStatement-5)[12] {itu-t(0) identified-organization(4) etsi(0) id-qc-profile (1862) policy-identifiers(1) id-etsi-qcs-QcPDS(5)}
	policyQualifiers		policyQualifierID: 1.3.6.1.5.5.7.2.1 cPSuri: https://pki.multicert.com/index.html		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 Divulgação de Princípios publicada pela EC. O apontador está na forma de um URI."
	policyQualifiers		policyQualifierID: 1.3.6.1.5.5.7.2.2 userNotice explicitText: "PKI Disclosure Statement/Declaração de Divulgação de Princípios"		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"

[12] 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[6]	Comentários
					(http://www.alvestrand.no/objectid/submissions/1.3.6.1.5.5.7.2.2.html)
	policyIdentifier		policyQualifierID: 0.4.0.194112.1.2		Valor do OID: 0.4.0.194112.1.2[13] Identifica que o certificado é emitido para pessoa natural sendo que a chave privada se encontra armazenada num dispositivo seguro. {itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies (194112) policy-identifiers(1) qcp-natural-qscd (2)}
	Basic Constraints	4.2.1.9		c	Esta extensão é marcada CRÍTICA.
	CA		FALSE		
	Extended Key Usage	4.2.1.12			
	KeyPurposeId		id-kp-emailProtection		OID: 1.3.6.1.5.5.7.3.4
	CRLDistributionPoints	4.2.1.13		o	
	distributionPoint		https://pki.multicert.com/CA.html	o	-
	Freshest CRL	4.2.1.15		o	
	distributionPoint		https://pki.multicert.com/CA.html	o	-
	Subject Alternative name	4.2.1.6	RFC822 name = <endereço do correio eletrónico do titular do certificado>	o	

[13] ETSI EN 319 411-2 V2.1.1 - *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*

Componente do Certificado		Secção no RFC 5280	Valor	Tipo[6]	Comentários
	Qualified Certificate Statement	-	id-pe-qcStatements = "1.3.6.1.5.5.7.1.3"[14]		A extensão *QCStatements* é uma extensão introduzida pelo PKIX Qualified Certificate Profile[11] e ETSI[15].
	id-qcs-pkixQCSyntax-v2		id-etsi-qcs-QcCompliance = "0.4.0.1862.1.1"		Declaração da EC MULTICERT, representada por um OID, indicando que este certificado é emitido de acordo com o Anexo III do Regulamento (EU) 910/2014).
	id-qcs-pkixQCSyntax-v2		id-etsi-qcs-QcRetentionPeriod = " 0.4.0.1862.1.3" QcEuRetentionPeriod = "7"		Esta extensão contém a indicação do período de retenção da informação relevante à emissão e uso do certificado, expresso em número de anos após a data expiração do certificado.
	id-qcs-pkixQCSyntax-v2		id-etsi-qcs-QcSSCD = " 0.4.0.1862.1.4"		Declaração efetuada pela EC MULTICERT, indicando que a chave privada associada à chave pública no certificado está guardada num dispositivo qualificado de criação de selo eletrónico, de acordo com o Anexo III do Regulamento (EU) 910/2014. Esta declaração indica que os certificados são emitidos em conformidade com a política ***SSCD***, conforme ETSI TS 101 456.
	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 da EC MULTICERT, representada por um OID, indicando que este certificado é emitido como um certificado qualificado de selo eletrónico, de acordo com o Anexo III do Regulamento (EU) 910/2014.
	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: 1.3.6.1.5.5.7.48.1 (id-ad-ocsp) Descrição do OID: *Online Certificate Status Protocol*

[14] http://www.alvestrand.no/objectid/1.3.6.1.5.5.7.1.3.html
[15] *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[6]	Comentários
	accessLocation		http://ocsp.multicert.com/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)} **Nota:** Na EC da MULTICERT 001 o algoritmo de assinatura utilizado foi SHA1 (2.16.840.113549.1.1.5). A partir da MULTICERT CA 002 será o indicado no presente documento.
	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.

3.1.4 Perfil de Certificado Qualificado de Selo Eletrónico

Componente do Certificado		Secção no RFC 5280	Valor	Tipo[16]	Comentários
tbsCertificate	**Version**	4.1.2.1	v3	m	Versão do certificado de acordo com o *standard* X.509
	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)
	Issuer	4.1.2.4		m	
	Country (C)		"PT"		País do titular
	Organization (O)		"MULTICERT - Serviços de Certificação Electrónica S.A"		Designação formal da organização do titular
	Organization Unit (OU)		"Entidade de Certificação Credenciada"		Outra designação da organização do titular
	Common Name (CN)		"MULTICERT - Entidade de Certificação <nnn>"		Nome da EC
	Validity	4.1.2.5		m	Validade do Certificado TEM que utilizar tempo UTC até 2049, passando a partir daí a utilizar *GeneralisedTime*
	Not Before		<data de emissão>		
	Not After		<data de emissão + máximo de 5 anos>		Validade máxima de 5 anos.

[16] 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[16]	Comentários
	Subject	4.1.2.6		m	
	Country (C)		<País de nacionalidade da Organização>		
	Organization Unit (OU)		<Área/Departamento da Organização>	o	
	Organization Unit (OU)		**Qualified Certificate for Electronic Seal**	m	Designação do tipo de certificado.
	Organization Identifier (OI)		**VAT**<Country>-<Número do de identificação Fiscal>	m	
	Organization (O)		<Nome da Organização tal como registada nas entidades competentes>	m	
	Common Name (CN)		<Nome da organização pela qual é conhecida>	m	
	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 ::= { pkcs-1 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.[17]
	subjectPublicKey		<Chave Pública com *modulus* n de 2048 bits>		

[17] *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[16]	Comentários
	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 *subjectPublicKey* (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. Confere o tipo de utilização do certificado.
	Digital Signature		"0" selecionado		
	Non Repudiation		"1" selecionado		certKeyUsage KeyUsage ::= {nonRepudiation}[18]
	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		

[18] *cf.* RFC 3739. 2004, *Internet X.509 Public Key Infrastructure: Qualified Certificates Profile.*

Componente do Certificado		Secção no RFC 5280	Valor	Tipo[16]	Comentários
	Decipher Only		"0" selecionado		
	Certificate Policies	4.2.1.4		o	
	policyIdentifier		1.3.6.1.4.1.25070.1.1.1.1.0.1.3	m	Identificador da Politica de Certificado Qualificado de Selo Eletrónico
	policyQualifiers		policyQualifierID: 1.3.6.1.5.5.7.2.1 cPSuri: https://pki.multicert.com/index.html		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 Politica de Certificado Qualificado de Selo Eletrónico publicada pela EC. O apontador está na forma de um URI."
	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 no regulamento (EU) 910/2014."		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" (http://www.alvestrand.no/objectid/submissions/1.3.6.1.5.5.7.2.2.html)
	policyIdentifier		1.3.6.1.4.1.25070.1.1.1.1.0.7	o	Identificador da Declaração de Práticas de Certificação da EC MULTICERT
	policyQualifiers		policyQualifierID: 1.3.6.1.5.5.7.2.1 cPSuri: https://pki.multicert.com/index.html	o	
	policyIdentifier		0.4.0.1862.1.5		Valor do OID: 0.4.0.1862.1.5 (qcs-QcPDS)[19] {itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(1456) policy-identifiers(1) qcp-public-with-sscd(1)}

[19] ETSI EN 319 411-1 - *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements*

Componente do Certificado		Secção no RFC 5280	Valor	Tipo[16]	Comentários
	policyQualifiers		policyQualifierID: 1.3.6.1.5.5.7.2.2 userNotice explicitText: "PKI Disclosure Statement/Declaração de Divulgação de Princípios"		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" (http://www.alvestrand.no/objectid/submissions/1.3.6.1.5.5.7.2.2.html)
	policyQualifiers		policyQualifierID: 1.3.6.1.5.5.7.2.1 cPSuri: https://pki.multicert.com/index.html		
	policyIdentifier		policyQualifierID: 0.4.0.194112.1.3		Valor do OID: 0.4.0.194112.1.3[20] Identifica que o certificado é emitido para pessoa legal sendo que a chave privada se encontra armazenada num dispositivo seguro. {itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies (194112) policy-identifiers(1) qcp-natural-qscd (3)}
	Basic Constraints	4.2.1.9		c	Esta extensão é marcada CRÍTICA.
	CA		FALSE		
	Extended Key Usage	4.2.1.12			
	KeyPurposeId		id-kp-emailProtection		OIDU: 1.3.6.1.5.5.7.3.4
	CRLDistributionPoints	4.2.1.13		o	
	distributionPoint		https://pki.multicert.com/CA.html	o	-
	Freshest CRL	4.2.1.15		o	

[20] ETSI EN 319 411-2 V2.1.1 - *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*

Componente do Certificado		Secção no RFC 5280	Valor	Tipo[16]	Comentários
	distributionPoint		https://pki.multicert.com/CA.html	o	-
	Subject Alternative name	4.2.1.6	RFC822 name = <endereço do correio eletrónico do titular do certificado>	o	
	Qualified Certificate Statement	-	id-pe-qcStatements = "1.3.6.1.5.5.7.1.3"[21]		A extensão *QCStatements* é uma extensão introduzida pelo PKIX Qualified Certificate Profile[11] e ETSI[15].
	id-qcs-pkixQCSyntax-v2		id-etsi-qcs-QcCompliance = "0.4.0.1862.1.1"		Declaração da EC MULTICERT, representada por um OID, indicando que este certificado é emitido de acordo com o Anexo III do Regulamento (EU) 910/2014. A declaração QcEuCompliance (id-etsi-qcs-QcCompliance) está associada com um identificador específico que corresponde ao OID "0.4.0.1862.1.1".
	id-qcs-pkixQCSyntax-v2		id-etsi-qcs-QcRetentionPeriod = " 0.4.0.1862.1.3" QcEuRetentionPeriod = "7"		Esta extensão contém a indicação do período de retenção da informação relevante à emissão e uso do certificado, expresso em número de anos após a data expiração do certificado.
	id-qcs-pkixQCSyntax-v2		id-etsi-qcs-QcSSCD = " 0.4.0.1862.1.4"		Declaração efetuada pela EC MULTICERT, indicando que a chave privada associada à chave pública no certificado está guardada num dispositivo qualificado de criação de selo eletrónico, de acordo com o Anexo III do Regulamento (EU) 910/2014. Esta declaração indica que os certificados são emitidos em conformidade com a política ***SSCD***, conforme ETSI TS 101 456.
	id-qcs-pkixQCSyntax-v2		id-etsi-qct-eseal="0.4.0.1862.1.6.2" Text="Certificate for electronic seals as defined in Regulation (EU) No 910/2014"		Declaração da EC MULTICERT, representada por um OID, indicando que este certificado é emitido como um certificado qualificado de selo eletrónico, de acordo com o Anexo III do Regulamento (EU) 910/2014.
	Internet Certificate Extensions				

[21] http://www.alvestrand.no/objectid/1.3.6.1.5.5.7.1.3.html

Componente do Certificado		Secção no RFC 5280	Valor	Tipo[16]	Comentários
	Authority Information Access	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: *Online Certificate Status Protocol*
	accessLocation		http://ocsp.multicert.com/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)} **Nota:** Na EC da MULTICERT 001 o algoritmo de assinatura utilizado foi SHA1 (2.16.840.113549.1.1.5). A partir da MULTICERT CA 002 será o indicado no presente documento.
	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.

3.1.5 OID do Algoritmo

O campo "*signatureAlgorithm*" do certificado contém o OID do algoritmo criptográfico utilizado pela EC para assinar o certificado: 2.16.840.113549.1.1.11 (sha-256WithRSAEncryption[22]).

3.1.6 Formato dos Nomes

Tal como definido na secção 2.1.

3.1.7 Condicionamento nos Nomes

Para garantir a total interoperabilidade entre as aplicações que utilizam certificados digitais, aconselha-se (mas não se obriga) a que apenas caracteres alfanuméricos não acentuados, espaço, traço de sublinhar, sinal negativo e ponto final ([a-z], [A-Z], [0-9], ' ', '_', '-', '.') sejam utilizados em entradas do Diretório X.500. A utilização de caracteres acentuados será da única responsabilidade do Grupo de Trabalho de Gestão da EC MULTICERT.

3.1.8 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*". Os qualificadores opcionais ("*policyQualifIierID*: 1.3.6.1.5.5.7.2.2" e "*userNotice explicitText*") apontam para o URI onde podem ser encontrados a Política de Certificados com o OID identificado pelo "*policyIdentifier*" (i.e., este documento).

3.1.9 Utilização da extensão *Policy Constraints*

Nada a assinalar.

3.1.10 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 Politica de Certificados.

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

Nada a assinalar.

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

3.2 Certificado "espécimen"

Os certificados "espécimen" poderão ser emitidos sempre que seja necessário validar o perfil, o processo de emissão e/ou a sua utilização. O certificado de "espécimen" pode ser emitido para efeito de testes tendo por base um contrato de responsabilidade a celebrar entre a MULTICERT e a Entidade requerente. Este certificado tem as seguintes diferenças em relação aos certificados usuais, considerados finais:

- Perfil de certificado: é adicionado o prefixo "(espécimen)" ao *CommonName* (CN);
- Emissão do certificado: de acordo com formulário específico[23] para usos internos, ou mediante consentimento de utilização, por parte do titular, através de uma declaração de responsabilidade;

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[4].

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 o perfil da LRC indicado na Política de Certificado da raiz auto-assinada da EC MULTICERT.

[23] *cf.* MULTICERT_MO.DOC_53_0142_pt.pdf, Declaração de Responsabilidade sobre a Utilização de Certificados Espécime.

4 Identificação e Autenticação

4.1 Validação de Identidade no registo inicial

Um Certificado Qualificado de Assinatura Digital é emitido para pessoa singular (pessoa natural), sendo este o responsável pela sua utilização. Um Certificado Qualificado de Selo Eletrónico é emitido para uma Organização (pessoa legal), tendo associado, mas não representado no certificado, uma pessoa singular identificada como "responsável técnico", que terá a responsabilidade de manusear e utilizar o certificado em nome da organização.

4.1.1 Autenticação da identidade

Os certificados Qualificados de Assinatura Digital são emitidos "suspensos", sendo que a sua ativação é efetuada através de um mecanismo digital que utiliza um meio de autenticação efetuado com o certificado de Autenticação, emitido para o titular. Os Certificados Qualificados de Selo Eletrónico são emitidos no estado "ativo", sendo a autenticação da identidade do responsável técnico efetuada através da entrega presencial, ou via CTT em correio registado com serviço adicional de entrega pessoal.

Adicionalmente é feita a validação do endereço de correio eletrónico, que constará no certificado. Esta atividade, inicia-se, após a submissão de um pedido de certificado, com o envio de um e*-mail* de confirmação de pedido, da MULTICERT, para o endereço indicado no mesmo. Neste e*-mail,* é solicitado ao titular/responsável do certificado, a confirmação do endereço de correio eletrónico, o qual acede ao *link* disponibilizado para o efeito.

4.1.1.1 Pessoa singular

O processo de autenticação da identidade de uma pessoa singular, garante que esta, para quem vai ser emitido o certificado é quem na realidade diz ser, através da entrega presencial e/ou através da ativação do certificado, que utiliza um mecanismo que permite autenticar o seu titular.

A autenticação é efetuada aquando a receção do certificado pelo titular, por meio digital. O certificado é emitido no estado "suspenso", sendo que para o ativar é disponibilizado um *link* ao titular, através do qual, este se autentica com o certificado de Autenticação, que consta no *token* criptográfico. Ao fazer esta autenticação será enviado para o telemóvel do titular, uma *password* temporária (OTP) que deverá ser introduzida na página de ativação do certificado, ficando este, assim que o processo seja concluído com sucesso, ativo e pronto a ser utilizado.

A autenticidade do titular do certificado na qualidade ou de representação de pessoa coletiva, no âmbito da sua utilização para assinatura digital qualificada a apor no certificado digital, é validada mediante apresentação de documento(s) comprovativo(s), emitido(s) por entidade que legalmente tem poderes para atestar essa qualidade.

O titular de um certificado de Assinatura Digital Qualificada, emitido pela EC MULTICERT, não poderá ativar o certificado caso não seja efetuada a confirmação de e*-mail*.

4.1.1.2 Pessoa coletiva

Os Certificados Qualificados emitidos para pessoas coletivas denominam-se de Certificados Qualificados de Selos Eletrónicos, neste caso o *Common Name* identifica a pessoa coletiva como titular o certificado.

A validação dos dados da pessoa coletiva é efetuada através de documentos emitidos por entidades legais, definidas para o efeito (exemplo Registo Comercial ou Certidão Permanente). Os dados do responsável técnico e do(s) representante(s) da organização são validados mediante cópia do documento de Identificação ou, caso não seja disponibilizado, deverá o contrato de emissão (formulário) ser devidamente autenticado por entidade com poderes para o ato (notário ou advogado).

A autenticação é efetuada aquando a receção do certificado, pelo responsável técnico designado pelos representantes legais da pessoa coletiva. Esta autenticação poderá ser efetuada através de uma das seguintes formas:

1. Entrega presencial:
    a. Ao próprio:
        i. O responsável técnico efetua o levantamento do certificado nas instalações da MULTICERT S.A., num dos seus escritórios (Lisboa ou Porto) acompanhado de documentos de identificação.
    b. A terceiro:
        i. O responsável técnico pode delegar os poderes de levantamento do certificado a terceiro, mediante declaração com assinatura autenticada e reconhecida por entidade com poderes legais para o ato. A pessoa a quem foram delegados poderes de levantamento, deve apresentar a declaração e respetivo documento de identificação, aquando o levantamento do certificado.

4.1.2 Método de comprovação da posse de chave privada

O par de chaves e certificado é fornecido em token criptográfico (SmartCard ou *token* USB) com chip criptográfico, personalizado fisicamente para o titular. A posse da chave privada é garantida pelo processo de emissão e personalização do token criptográfico, garantindo que:

- O par de chaves é gerado no HSM criptográfico e inserido no token criptográfico, por comunicação direta segura e sem ficar registado em qualquer dispositivo,
- O token criptográfico é personalizado para o titular do mesmo,
- A chave pública é enviada à EC MULTICERT para emissão do certificado digital correspondente, sendo este também inserido no token criptográfico.
- O token criptográfico, é entregue como descrito na secção anterior.

No caso de emissão de um certificado qualificado para Selo Eletrónico existe ainda a opção da chave ser gerada pelo Responsável indicado pela pessoa coletiva (Organização) num HSM próprio. Neste caso:

- O responsável e respetiva organização assume a responsabilidade pela chave gerada e pelo HSM utilizado para o efeito;
- Faz chegar à Multicert toda a documentação necessária acompanhada de um CSR;
- O certificado, após validação da documentação entregue, é devolvido ao responsável.

4.1.3 Informação de subscritor/titular não verificada

Toda a informação descrita nos pontos **Erro! A origem da referência não foi encontrada.** é verificada.

4.1.4 Validação de Autoridade

Nada a assinalar.

4.1.5 Critérios para interoperabilidade

Nada a assinalar.

4.2 Identificação e Autenticação para pedido de revogação

Qualquer entidade pode solicitar a revogação de um determinado certificado, havendo conhecimento ou suspeita de compromisso da chave privada do titular ou qualquer outro ato que recomende esta ação.

As ERs da EC MULTICERT guardam toda a documentação utilizada para verificação da identidade e autenticidade da entidade que efetua o pedido de revogação do certificado de assinatura digital qualificada, que podem ser, de entre outros:

- Certificado de Pessoa singular:
  - O titular do certificado no caso de certificados de pessoa singular;
  - O(s) representante(s) legal(ais) da entidade que possa atestar a qualidade do titular do certificado, aposta no certificado digital, sempre que essa qualidade deixe de ser válida;
- Parte confiante, sempre que demonstre que o certificado foi utilizado com fins diferentes dos previstos.

Um formulário próprio[24] serve de base ao pedido de revogação de certificado qualificado e contém, entre outros, os seguintes elementos de identificação da entidade que inicia o pedido de revogação:

a) Denominação legal;

b) Número de pessoa coletiva, sede, objeto social, nome dos titulares dos corpos sociais e de outras pessoas com poderes para a obrigarem e número de matrícula na conservatória do registo comercial ou/e nome completo, número do bilhete de identidade ou qualquer outro elemento que permita a identificação inequívoca da entidade (ou seu representante) que inicia o pedido de revogação;

c) Endereço e outras formas de contacto;

d) Indicação de pedido de revogação, indicando o nome único (DN) atribuído ao certificado, assim como a sua validade;

e) Indicação do motivo para revogação do certificado.

O processo de identificação e autenticação para pedido de revogação de certificado de pessoa singular ou pessoa coletiva, é efetuado através de um dos seguintes métodos:

- Assinatura digital qualificada do formulário,
- Assinatura manuscrita do formulário com entrega do mesmo, pelo subscritor, nas instalações da MULTICERT S.A., nomeadamente no seu escritório de Lisboa ou Porto,
- Assinatura manuscrita do formulário com reconhecimento notarial da assinatura,
- Através de mensagens eletrónicas seguras, previamente definidas entre as ERs da EC MULTICERT e a entidade que efetua o pedido de revogação do certificado.

[24] *cf.* Formulário de revogação de certificado Qualificado, disponível em - https://www.multicert.com/media/3668/multicert_prcq_5322_0001_pt.pdf

5 Requisitos operacionais do ciclo de vida do certificado

5.1 Pedido de Certificado

5.1.1 Quem pode subscrever um pedido de certificado?

No âmbito geral da ER da MULTICERT, que emite certificados para público em geral.

Os certificados qualificados de assinatura digital podem ser subscritos:

- Pelo Titular do certificado, quando o certificado é emitido para pessoa natural,
- Pelo Titular e Representantes legais da entidade, quando o certificado é emitido para pessoa singular associada a uma entidade (na qualidade ou em representação).

O Certificado Qualificado de Selo Eletrónico pode ser subscrito:

- Pelos representantes legais da pessoa coletiva com poderes para o ato, sendo designado por estes uma pessoa física, responsável pelo manuseamento e operação do certificado, denominada de "responsável técnico".

Para as Entidades de Registo, a emissão é restrita ao âmbito das mesmas, nomeadamente a Ordem dos Médicos (OM), Ordem dos Farmacêuticos (OF) e Assembleia da República, apenas são emitidos certificados qualificados de assinatura digital. O pedido de certificado será subscrito pelo titular na qualidade ou função atestada pelos representantes legais da Entidade.

5.1.2 Processo de registo e responsabilidades

O pedido de certificado qualificado é da responsabilidade dos intervenientes, identificados na secção anterior, assim como é da sua responsabilidade a veracidade dos dados fornecidos e disponibilização de toda a documentação necessária que a permita verificar.

O processo de registo é considerado efetivo após ser verificada e confirmada toda a informação constante no pedido, pela ER da MULTICERT.

O processo de registo deve iniciar-se através do preenchimento *on-line* do formulário disponível em https://www.multicert.com/pt/produtos/certificados-digitais/qualificados/.

5.2 Processamento do pedido de certificado

Os pedidos de certificado, depois de recebidos pela ER, são considerados válidos se os seguintes requisitos forem cumpridos:

a) Receção e verificação de toda a documentação e autorizações exigidas;

b) Verificação da identidade do requisitante;

c) Verificação da exatidão e integridade do pedido de certificado;

d) Pedido de emissão de certificado à EC MULTICERT

As secções 4.1, 5.2.1 e 5.3 descrevem detalhadamente todo o processo

5.2.1 Processos para a identificação e funções de autenticação

5.2.1.1 Certificado de pessoa singular

Conforme indicado na secção 304.1

5.2.1.2 Certificado de pessoa coletiva

Conforme indicado na secção 4.1

5.2.2 Aprovação ou recusa de pedidos de certificado

A aprovação de certificado passa pelo cumprimento dos requisitos exigidos no ponto 5.2 e 5.2.1. Quando tal não se verifique, é recusada a emissão do certificado.

5.2.3 Prazo para processar o pedido de certificado

Após a aprovação do pedido de certificado, o certificado deverá ser emitido em não mais do que cinco (5) dias úteis.

5.3 Emissão de Certificado

5.3.1 Procedimentos para a emissão de certificado

A emissão do certificado qualificado é realizada automaticamente, pela plataforma EC MULTICERT, após o registo do pedido de certificado, sendo a geração do par de chaves efetuada pelo HSM e o certificado emitido pela EC MULTICERT após receção do pedido de certificado (PKCS#10).

Como medida de exceção, sempre que ocorrer qualquer quebra de serviço na plataforma EC MULTICERT, o par de chaves será gerado no cartão (ou *token* USB) com chip criptográfico sendo o pedido de certificado (PKCS#10) enviado à EC MULTICERT que o emitirá.

5.3.2 Notificação da emissão do certificado ao titular

O titular do certificado considera-se notificado da emissão do certificado aquando da receção do mesmo.

5.4 Aceitação do Certificado

5.4.1 Procedimentos para a aceitação de certificado

O certificado considera-se aceite após a receção do mesmo.

Note-se que antes de ser disponibilizado o certificado ao titular, e consequentemente lhe serem disponibilizadas todas as funcionalidades na utilização da chave privada e certificado, é garantido que,

a) O titular toma conhecimento dos seus direitos e responsabilidades;

b) O titular toma conhecimento das funcionalidades e conteúdo do certificado;

c) O titular aceita formalmente o certificado e as suas condições de utilização, assinando para o efeito um formulário de pedido de certificado;

d) Os procedimentos necessários em caso de expiração, revogação e renovação do certificado, bem como os termos, condições e âmbito de utilização do mesmo estão definidos nesta Política de Certificados e na respetiva Declaração de Práticas de Certificação.

5.4.2 Publicação do certificado

A EC MULTICERT não publica os certificados emitidos, disponibilizando-o integralmente ao titular, com os constrangimentos definidos no ponto 5.4.1.

5.4.3 Notificação da emissão de certificado a outras entidades

Nada a assinalar.

5.5 Uso do certificado e par de chaves

5.5.1 Uso do certificado e da chave privada pelo titular

Os titulares de certificados utilizarão a sua chave privada apenas e só para o fim a que estas se destinam (conforme estabelecido no campo do certificado "*keyUsage*") e sempre com propósitos legais.

A sua utilização apenas é permitida:

a) A quem estiver designado no campo "*Common Name* " do certificado;

b) De acordo com as condições definidas nos pontos 1.4.1 e 1.4.2 da Declaração de Práticas de Certificação (DPC);

c) Enquanto o certificado se mantiver válido e não estiver na LRC da EC MULTICERT.

5.5.2 Uso do certificado e da chave pública pelas partes confiantes

Na utilização do certificado e da chave pública, as partes confiantes apenas podem confiar nos certificados, tendo em conta apenas o que é estabelecido nesta Política de Certificado e na respetiva DPC. Para isso devem, entre outras, garantir o cumprimento das seguintes condições:

a) Ter conhecimento e perceber a utilização e funcionalidades proporcionadas pela criptografia de chave pública e certificados.

b) Ser responsável pela sua correta utilização;

c) Ler e entender os termos e condições descritos nas políticas e práticas de certificação;

d) Verificar os certificados (validação de cadeias de confiança) e LRC, tendo especial atenção às suas extensões marcadas como críticas e propósito das chaves;

e) Confiar nos certificados, utilizando-os apenas se estes estiverem válidos.

5.6 Renovação de certificado com geração de novo par de chaves

A renovação de chaves do certificado (*certificate re-key*) é o processo em que um titular (ou representante legal) gera um novo par de chaves e submete o pedido para emissão de novo certificado que certifica a nova chave pública. Este processo, no âmbito desta Política de Certificado, é designado por renovação de certificado com geração de novo par de chaves.

A renovação de certificado com geração de novo par de chaves é feita de acordo com o estabelecido na secção 5.3.

5.6.1 Motivo para a renovação de certificado com geração de novo par de chaves

É motivo válido para a renovação de certificado com geração de novo par de chaves, sempre e quando se verifique que:

a) O certificado está a expirar;

b) O suporte do certificado está a expirar;

c) A informação do certificado sofre alterações.

5.6.2 Quem pode submeter o pedido de certificação de uma nova chave pública

Tal como na secção 5.1.1.

5.6.3 Processamento do pedido de renovação de certificado com geração de novo par de chaves

Tal como na secção 5.1.2 e 5.2.

5.6.4 Notificação da emissão de novo certificado ao titular

Tal como na secção 5.3.2.

5.6.5 Procedimentos para aceitação de um certificado renovado com geração de novo par de chaves

Tal como na secção 5.4.1.

5.6.6 Publicação de certificado renovado com geração de novo par de chaves

Tal como na secção 5.4.2.

5.6.7 Notificação da emissão de certificado renovado a outras entidades

Tal como na secção 5.4.3.

5.7 Suspensão e revogação de certificado

Na prática, a revogação e suspensão de certificados é uma ação através da qual o certificado deixa de estar válido antes do fim do seu período de validade, perdendo a sua operacionalidade.

Os certificados depois de revogados não voltam ao estado ativo, ou seja, deixam de ser válidos definitivamente, já os certificados suspensos poderão voltar ao estado ativo, recuperando a sua validade.

Mais informação disponível em https://www.multicert.com/pt/apoio-a-cliente/certificados-digitais/revogacao/ e https://pki.multicert.com/politicas/contrato/cgerais.html.

5.7.1 Motivos para suspensão

Um certificado pode ser suspenso por uma das seguintes razões:

- Suspeita de comprometimento da chave privada;
- Suspeita de perda da chave privada;
- Suspeita de comprometimento da senha e acesso à chave privada (exemplo: PIN);
- Suspeita de perda, destruição ou deterioração do dispositivo de suporte da chave privada (por exemplo, suporte/token criptográfico);
- Qualidade do titular do certificado, aposta no certificado digital, é suspensa;
- Poderes de representação inscritos no certificado sejam suspensos ou alterados;
- Sempre que haja razões credíveis que induzam a suspeita que o serviços de certificação possam ter sido comprometidos, de tal forma que coloquem em causa a fiabilidade dos certificados;
- Por resolução judicial ou administrativa.

5.7.2 Quem pode submeter o pedido de suspensão

Está legitimado para submeter o pedido de revogação, sempre que se verifiquem alguma das condições descritas no ponto 5.7.1, os seguintes elementos entre outros:

a) Titular do certificado (ou representante legal para o efeito de suspensão de certificado digital de assinatura digital qualificada, com reconhecimento notarial da assinatura do titular do certificado), no caso de certificados de pessoa singular com efeitos de representação de pessoa coletiva;

b) Representante legal da entidade que possa atestar a qualidade do titular do certificado, aposta no certificado digital, sempre que essa qualidade seja suspensa;

c) Representante legal da entidade que possa conferir os poderes de representação do titular do certificado, inscritos no certificado digital, sempre que esses poderes sejam suspensos ou alterados;

d) Representante legal da pessoa coletiva identificada como titular do certificado qualificado.

e) Parte confiante, sempre que demonstre que o certificado foi utilizado com fins diferente dos previstos.

A EC MULTICERT guarda toda a documentação utilizada para verificação da identidade e autenticidade da entidade que efetua o pedido de suspensão.

5.7.3 Procedimentos para pedido de suspensão

A MULTICERT dispõe de um serviço *online*, disponível 24*7[25] que permite, ao titular de um certificado digital qualificado, emitido pela EC MULTCERT, suspendê-lo de forma imediata, bastando ter acesso à Internet e conhecimento dos dados a inserir.

Para além deste serviço, poderá ser solicitada a suspensão através de contato direto com a MULTICERT (em dias úteis, das 9h às 18h) a qual fornecerá todas as indicações necessárias para proceder a suspensão do certificado.

5.7.4 Limite do período de suspensão

A suspensão será feita de forma imediata.

[25] https://www.multicert.com/3ws/certSuspensionForm

O pedido de suspensão, após a sua aceitação pela EC MULTICERT, deve ser tratado de forma imediata, pelo que em caso algum poderá ser processado em prazo superior a 24 horas.

O certificado permanece no estado "Suspenso" durante um período máximo de 3 dias úteis. Caso seja ultrapassado esse prazo, sem ser efetuada a formalização do pedido de revogação, o certificado voltará ao estado Ativo (ou válido).

5.7.5 Outras formas disponíveis para divulgação de suspensão

O titular do certificado é notificado, sempre que o certificado for suspenso ou reativado.

5.7.6 Motivos para revogação

Um certificado pode ser revogado por uma das seguintes razões:

- Comprometimento ou suspeita de comprometimento da chave privada;
- Perda da chave privada;
- Inexatidões graves nos dados fornecidos;
- Comprometimento ou suspeita de comprometimento da senha e acesso à chave privada (exemplo: PIN);
- Perda, destruição ou deterioração do dispositivo de suporte da chave privada (por exemplo, suporte/token criptográfico);
- Qualidade do titular do certificado, aposta no certificado digital, deixa de ser válida;
- Poderes de representação inscritos no certificado sejam suspensos ou alterados;
- Incumprimento por parte da EC MULTICERT ou titular das responsabilidades prevista na presente Politica de Certificado e/ou correspondente DPC;
- Sempre que haja razões credíveis que induzam que o serviços de certificação possam ter sido comprometidos, de tal forma que coloquem em causa a fiabilidade dos certificados;
- Por resolução judicial ou administrativa;
- Utilização do certificado para atividades abusivas;
- Risco de comprometimento da chave (por exemplo, devido à fraqueza do algoritmo ou tamanho de chave);
- Cessação de funções.

5.7.7 Quem pode submeter o pedido de revogação

Está legitimado para submeter o pedido de revogação, sempre que se verifiquem alguma das condições descritas no ponto 5.7.6, os seguintes elementos entre outros (cf. secção 4.2):

a) Titular do certificado (ou representante legal para o efeito de revogação de certificado digital de assinatura digital qualificada, com reconhecimento notarial da assinatura do titular do certificado), no caso de certificados de pessoa singular ou pessoa coletiva;

b) Representante legal da entidade que possa atestar a qualidade do titular do certificado, aposta no certificado digital, sempre que essa qualidade deixe de ser válida;

c) Representante legal da entidade que possa conferir os poderes de representação do titular do certificado, inscritos no certificado digital, sempre que esses poderes sejam suspensos ou alterados;

d) Representante legal da pessoa coletiva identificada como titular do certificado qualificado.

e) Parte confiante, sempre que demonstre que o certificado foi utilizado com fins diferente dos previstos.

A EC MULTICERT guarda toda a documentação utilizada para verificação da identidade e autenticidade da entidade que efetua o pedido de revogação.

5.7.8 Procedimento para o pedido de revogação

De acordo com a secção 4.2.

5.7.9 Produção de efeitos da revogação

A revogação será feita de forma imediata, após processamento do pedido de revogação. Após terem sido efetuados todos os procedimentos e seja verificado que o pedido é válido, o pedido não pode ser anulado.

5.7.10 Prazo para processar o pedido de revogação

O pedido de revogação, após a sua aceitação pela EC MULTICERT, deve ser tratado de forma imediata, pelo que em caso algum poderá ser processado em prazo superior a 24 horas.

5.7.11 Requisitos de verificação da revogação pelas partes confiantes

Antes de utilizarem um certificado, as partes confiantes têm como responsabilidade verificar o estado de todo os certificados, através das LCR ou num servidor de verificação do estado on-line (via OCSP).

5.7.12 Periodicidade da emissão da lista de certificados revogados (LCR)

A EC MULTICERT disponibiliza uma nova LCR Base todas as semanas e uma nova delta-LCR todos os dias.

5.7.13 Período máximo entre a emissão e a publicação da LCR

O período máximo entre a emissão e publicação da LCR não deverá ultrapassar os 30 minutos.

5.7.14 Disponibilidade de verificação on-line do estado / revogação de certificado

A EC MULTICERT dispõe de serviços de validação OCSP do estado dos certificados de forma on-line. Esse serviço poderá ser acedido em http://ocsp.multicert.com/ocsp.

O período máximo entre a revogação e a disponibilização através do serviço de validação OCSP, não deverá ultrapassar os 10 minutos.

5.7.15 Requisitos de verificação on-line de revogação

As partes confiantes deverão dispor de *software* capaz de operar o protocolo OCSP, de forma a obter a informação sobre o estado do certificado.

5.7.16 Outras formas disponíveis para divulgação de revogação

O titular do certificado é notificado, sempre que o certificado for revogado.

5.7.17 Requisitos especiais em caso de comprometimento de chave privada

Apenas quando se trate do comprometimento da chave privada de uma EC MULTICERT. No caso da chave privada da EC MULTICERT ser comprometida ou haver suspeita do seu comprometimento, devem ser tomadas medidas apropriadas de resposta ao incidente. As respostas a esse incidente podem incluir:

- Revogação do certificado da EC MULTICERT e de todos os certificados emitidos no "ramo" da hierarquia de confiança da EC MULTICERT,
- Notificação da Entidade Supervisora e todos os titulares de certificados emitidos no "ramo" da hierarquia de confiança da EC MULTICERT,
- Geração de novo par de chaves para a EC MULTICERT,
- Renovação de todos os certificados emitidos no "ramo" da hierarquia de confiança da EC MULTICERT.

6 Auditorias e normas de segurança

Descrito nas secções 8 e 9.14 da Declaração de Práticas de Certificação disponível em http://pki.multicert.com.

7 Conclusão

Este documento define as Políticas de Certificados Qualificados de Assinatura Digital e de selo Eletrónico, utilizada pela EC MULTICERT no suporte à sua atividade de certificação digital. A hierarquia de confiança da Entidade de Certificação MULTICERT:

- Fornece uma hierarquia de confiança, que promoverá a segurança eletrónica do titular do certificado no seu relacionamento com terceiras entidades,
- 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.

Referências Bibliográficas

CA/Browser Forum – Baseline Requirements, v1.3.3;

CWA 14167 - *Cryptographic Module for CSP Signing Operations - Protection Profile*;

CWA 14169:2004 - *Secure signature-creation devices "EAL 4+"*;

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 319 412-3 V1.1.1 (2016-02) - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons;

ETSI EN 319 412-4 V1.1.1 (2016-02) - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates ;

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

FIPS 140-1. 1994, *Security Requirements for Cryptographic Modules*.

ISO/IEC 3166. 1997, *Codes for the representation of names and countries and their subdivisions*.

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

NIST FIPS PUB 180-1. 1995, *The Secure Hash Algorithm* (SHA-1). *National Institute of Standards and Technology, "Secure Hash Standard", U.S. Department of Commerce*.

RFC 1421. 1993, *Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures.*

RFC 1422. 1993, *Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management.*

RFC 1423. 1993, *Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers.*

RFC 1424. 1993, *Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services.*

RFC 2560. 1999, X.509 *Internet Public Key Infrastructure Online Certificate Status Protocol* – OCSP.

RFC 2986. 2000, PKCS #10: *Certification Request Syntax Specification, version* 1.7.

RFC 3161. 2001, *Internet* X.509 *Public Key Infrastructure Time-Stamp Protocol* (TSP).

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

RFC 3647. 2003, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.*

RFC 4510. 2006, *Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map*.

RFC 4210. 2005, *Internet X.509 Public Key Infrastructure Certificate Management Protocol* (CMP).

RFC 5280. 2008, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List* (CRL) *Profile.*

Aprovação

Renato Isaias Rodrigues Portela

Digitally signed by Renato Isaias Rodrigues Portela
Date: 2017.07.13 11:50:05 +01'00'

[Assinatura Qualificada] MULTICERT - SERVIÇOS DE CERTIFICAÇÃO ELECTRÓNICA S.A.

Digitally signed by [Assinatura Qualificada] MULTICERT - SERVIÇOS DE CERTIFICAÇÃO ELECTRÓNICA S.A.
Date: 2017.07.24 13:33:40 +01'00'