

Política de Certificado de Assinatura Digital Qualificada

Políticas

MULTICERT_PJ.CA3_24.1.2_0002_pt.doc

Identificação do Projecto: MULTICERT CA03

Identificação da CA: MULTICERT CA

Nível de Acesso: Público

Versão: 1.4

Data: 25/03/2009

Aviso Legal Copyright © 2009 MULTICERT — Serviços de Certificação Electrónica, S.A. (MULTICERT)

Todos os direitos reservados: a MULTICERT detém todos os direitos de propriedade intelectual sobre o conteúdo do presente documento ou foi devidamente autorizada a utilizá-los. As marcas constantes deste documento são utilizadas apenas para identificar produtos e serviços e encontram-se sujeitas às regras de protecção legalmente previstas. Nenhuma parte deste documento poderá ser fotocopiada, reproduzida, guardada, traduzida ou transmitida a terceiros, seja por que meio, sem o consentimento prévio por escrito da MULTICERT. Igualmente, o Cliente deverá garantir que não utilizará fora do âmbito ou transmitir a terceiras entidades o "*know-how*" e as metodologias de trabalho apresentadas pela MULTICERT.

Confidencialidade

As informações contidas em todas as páginas deste documento, incluindo conceitos organizacionais, constituem informações sigilosas comerciais ou financeiras e confidenciais ou privilegiadas e são propriedade da MULTICERT. São fornecidas ao Cliente de forma fiduciária, com o conhecimento de que não serão utilizadas nem divulgadas, sem autorização da MULTICERT. O cliente poderá permitir a determinados colaboradores, consultores e agentes que tenham necessidade de conhecer o conteúdo deste documento, ter acesso a este conteúdo, mas tomará as devidas providências para garantir que as referidas pessoas e entidades se encontram obrigados pela obrigação do cliente a mantê-lo confidencial.

As referidas restrições não limitam o direito de utilização ou divulgação das informações constantes do presente documento, quando obtidos por outra fonte não sujeita a reservas ou que previamente ao seu fornecimento, já tenha sido legitimamente divulgada por terceiros.

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 Certificado de Assinatura Digital Qualificada

Língua original: Português

Língua de publicação: Português

Nível de acesso: Público

Data: 25/03/2009

Versão actual: 1.4

Identificação do Projecto: MULTICERT CA03

Identificação da CA: MULTICERT CA

Cliente: MULTICERT S.A.

Histórico de Versões

N.º de Versão	Data	Detalhes	Autor(es)
<u>1.0</u>	<u>13/01/2009</u>	<u>Versão inicial</u>	<u>José Pina Miranda</u>
<u>1.1</u>	<u>23/03/2009</u>	<u>Actualização de Conteúdos</u>	<u>José Pina Miranda</u>
<u>1.2</u>	<u>24/03/2009</u>	<u>Revisão Grupo de Políticas</u>	<u>Sara Loja</u>
<u>1.3</u>	<u>25/03/2009</u>	<u>Actualização de Conteúdos</u>	<u>Sara Loja</u>
<u>1.4</u>	<u>25/03/2009</u>	<u>Actualização de Conteúdos</u>	<u>Nuno Ponte</u>
<u>1.5</u>	<u>25/03/2009</u>	<u>Actualização de referências bibliográficas</u>	<u>Nuno Ponte</u>

Documentos Relacionados

ID Documento	Detalhes	Autor(es)
MULTICERT_PJ.CA3_24.1.1_0001_pt.doc	Declaração de Práticas de Certificação	José Pina Miranda
MULTICERT_PJ.CA3_24.1.2_0001_pt.doc	Política de Certificado da raiz auto-assinada da FC. MULTICERT	José Pina Miranda
MULTICERT_PJ.CA3_53.2.1_0001_pt.doc	Formulário de emissão de certificado "espécimen" de Assinatura Digital	José Pina Miranda
MULTICERT_PJ.CA3_53.2.2_0001_pt.doc	Formulário de revogação de certificado de Assinatura Digital Qualificada	José Pina Miranda
MULTICERT_PJ.CA3_53.2.2_0002_pt.doc	Formulário de suspensão de certificado de Assinatura Digital Qualificada	José Pina Miranda

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 electrónico (*eGovernment*) e do comércio electrónico, os certificados digitais emitidos pela Entidade de Certificação MULTICERT, credenciada pela Autoridade Credenciadora (conforme previsto na legislação europeia e nacional), fornecem os mecanismos necessários para a autenticação digital forte da identidade do titular do certificado electrónico, assim como as assinaturas electrónicas (equivalente legal das assinaturas manuscritas) indispensáveis aos processos de desmaterialização.

A infra-estrutura da Entidade de Certificação MULTICERT fornece uma hierarquia de confiança, que promove a segurança electrónica do titular do certificado digital. A Entidade de Certificação MULTICERT estabelece uma estrutura de confiança electrónica que proporciona a realização de transacções electrónicas seguras, a autenticação forte, um meio de assinar electronicamente transacções ou informações e documentos electrónicos, assegurando a sua autoria, integridade e não repúdio, e assegurando a confidencialidade das transacções ou informação.

A Entidade de Certificação MULTICERT está devidamente credenciada pela Autoridade Nacional de Segurança (<http://www.gns.gov.pt/gns/pt/assinatura/>), 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 do certificado de assinatura digital qualificada, 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. 2009, Declaração de Práticas de Certificação.

Sumário

Resumo Executivo	3
Sumário	4
Introdução.....	7
1 Introdução	8
1.1 Visão Geral	8
1.2 Designação e Identificação do Documento.....	8
2 Identificação e Autenticação	9
2.1 Atribuição de Nomes.....	9
2.1.1 Tipos de nomes.....	9
2.2 Uso do certificado e par de chaves pelo titular	10
3 Perfis de Certificado e LRC.....	11
3.1 Perfil de Certificado	11
3.1.1 Número da Versão	11
3.1.2 Extensões do Certificado.....	12
3.1.3 Perfil de Certificado de Assinatura Digital Qualificada	13
3.1.4 OID do Algoritmo	21
3.1.5 Formato dos Nomes.....	21
3.1.6 Condicionamento nos Nomes.....	21
3.1.7 OID da Política de Certificados.....	21
3.1.8 Utilização da extensão Policy Constraints	21
3.1.9 Sintaxe e semântica do qualificador de política	21
3.1.10 Semântica de processamento para a extensão crítica Certificate Policies	22
3.2 Certificado “espécimen”	22
3.3 Perfil da lista de revogação de certificados	22
4 Identificação e Autenticação	23
4.1 Validação de Identidade no registo inicial	23
4.1.1 Método de comprovação da posse de chave privada	23
4.1.2 Autenticação da identidade de uma pessoa colectiva	23
4.1.3 Autenticação da identidade de uma pessoa singular.....	23
4.1.4 Informação de subscritor/titular não verificada.....	24
4.1.5 Validação de Autoridade	24
4.1.6 Critérios para interoperabilidade	24
4.2 Identificação e Autenticação para pedido de revogação.....	24
5 Requisitos operacionais do ciclo de vida do certificado	26
5.1 Pedido de Certificado.....	26

5.1.1	Quem pode subscrever um pedido de certificado?	26
5.1.2	Processo de registo e responsabilidades	26
5.2	Processamento do pedido de certificado	26
5.2.1	Processos para a identificação e funções de autenticação	27
5.2.1.1	Certificado de pessoa colectiva	27
5.2.1.2	Certificado de pessoa singular	27
5.2.2	Aprovação ou recusa de pedidos de certificado.....	27
5.2.3	Prazo para processar o pedido de certificado	27
5.3	Emissão de Certificado.....	27
5.3.1	Procedimentos para a emissão de certificado	27
5.3.2	Notificação da emissão do certificado ao titular	27
5.4	Aceitação do Certificado	27
5.4.1	Procedimentos para a aceitação de certificado	27
5.4.2	Publicação do certificado	28
5.4.3	Notificação da emissão de certificado a outras entidades	28
5.5	Uso do certificado e par de chaves	28
5.5.1	Uso do certificado e da chave privada pelo titular	28
5.5.2	Uso do certificado e da chave pública pelas partes confiantes.....	28
5.6	Renovação de certificado com geração de novo par de chaves	29
5.6.1	Motivo para a renovação de certificado com geração de novo par de chaves	29
5.6.2	Quem pode submeter o pedido de certificação de uma nova chave pública	29
5.6.3	Processamento do pedido de renovação de certificado com geração de novo par de chaves.....	29
5.6.4	Notificação da emissão de novo certificado ao titular	29
5.6.5	Procedimentos para aceitação de um certificado renovado com geração de novo par de chaves.....	30
5.6.6	Publicação de certificado renovado com geração de novo par de chaves	30
5.6.7	Notificação da emissão de certificado renovado a outras entidades	30
5.7	Suspensão e revogação de certificado	30
5.7.1	Motivos para revogação.....	30
5.7.2	Quem pode submeter o pedido de revogação	31
5.7.3	Procedimento para o pedido de revogação	31
5.7.4	Produção de efeitos da revogação	31
5.7.5	Prazo para processar o pedido de revogação.....	31
5.7.6	Requisitos de verificação da revogação pelas partes confiantes	31
5.7.7	Periodicidade da emissão da lista de certificados revogados (LCR).....	31
5.7.8	Período máximo entre a emissão e a publicação da LCR.....	32
5.7.9	Disponibilidade de verificação on-line do estado / revogação de certificado.....	32
5.7.10	Requisitos de verificação on-line de revogação	32
5.7.11	Outras formas disponíveis para divulgação de revogação	32

5.7.12	Requisitos especiais em caso de comprometimento de chave privada ...	32
5.7.13	Motivos para suspensão	32
5.7.14	Quem pode submeter o pedido de suspensão	33
5.7.15	Procedimentos para pedido de suspensão	33
5.7.16	Limite do período de suspensão	34
5.7.17	Outras formas disponíveis para divulgação de suspensão	34
6	Auditorias e normas de segurança	36
	Conclusão	37
	Referências Bibliográficas	38

Introdução

Objectivos

O objectivo deste documento é definir as políticas utilizadas na emissão do certificado de assinatura digital qualificada, 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, infra-estruturas de chave pública e assinatura electrónica. Caso esta situação não se verifique recomenda-se o aprofundar de conceitos e conhecimento nos tópicos anteriormente focado antes de proceder com a leitura do documento.

Este documento complementa a Declaração de Práticas de Certificação da EC MULTICERT¹, 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 objectivo se prende com a definição de um conjunto de políticas e dados para a emissão e validação de Certificados e para a garantia de fiabilidade desses mesmos certificados. Não se pretende nomear regras legais ou obrigações, mas antes informar pelo que se pretende que este documento seja simples, directo e entendido por um público alargado, incluindo pessoas sem conhecimentos técnicos ou legais.

Este documento descreve a política de certificados para a emissão e gestão do certificado de Assinatura Digital Qualificada, emitido pela 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

Esta PC satisfaz e complementa os requisitos impostos pela Declaração de Práticas de Certificação (DPC) da EC MULTICERT¹.

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 objecto" (OID), sendo o valor do OID associado a este documento o 1.3.6.1.4.1.25070.1.1.1.1.0.1.2.

Este documento é identificado pelos dados constantes na seguinte tabela:

INFORMAÇÃO DO DOCUMENTO	
Versão do Documento	Versão 1.0
Estado do Documento	Aprovado
OID	1.3.6.1.4.1.25070.1.1.1.1.0.1.2
Data de Emissão	21/Janeiro/2009
Validade	Não aplicável
Localização	http://pki.multicert.com/pol/cp/adq.html

2 Identificação e Autenticação

2.1 Atribuição de Nomes

A atribuição de nomes segue a convenção determinada pela DPC da EC MULTICERT¹.

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 da EC MULTICERT é identificado pelos seguintes componentes:

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	Certificado para pessoa singular – Assinatura Qualificada ou Certificado para pessoa colectiva – Assinatura Qualificada
Common Name	CN	<nome do titular do certificado>
Title	title (opcional)	<Qualidade do titular do certificado, no âmbito da sua utilização para assinatura digital qualificada>
Surname	SN (opcional)	<nomes de família do titular do certificado>
GivenName	givenName (opcional)	<nomes próprio do titular do certificado>
SerialNumber	serialNumber	<identificador único do titular do certificado>

2.2 Uso do certificado e par de chaves pelo titular

A pessoa singular ou a pessoa colectiva (conforme identificado no *Organization Unit*) identificada pelo *Distinguished Name* é o titular do certificado de Assinatura Digital Qualificada. O certificado emitido segundo esta política é equivalente a um certificado digital qualificado, nos termos, do definido na Legislação Portuguesa, aplicável para o efeito, sendo utilizado em qualquer aplicação para efeitos de assinatura digital qualificada.

3 Perfis de Certificado e LRC

3.1 Perfil de Certificado

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

Um certificado tem um período limitado de validade, indicado no seu conteúdo e assinado pela EC. Como a assinatura do certificado e a sua validade podem ser verificadas independentemente por qualquer software que utilize certificados, os certificados podem ser distribuídos através de linhas de comunicação e sistemas públicos, assim como podem ser guardados no tipo de unidades de armazenamento mais adequados para cada tipo de certificados.²

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.²

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

- Recomendação ITU.T X.509³,
- RFC 5280², e
- Legislação relevante portuguesa e europeia.

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).

² cf. RFC 5280. 2008, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

³ 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.

3.1.3 Perfil de Certificado de Assinatura Digital Qualificada

Componente do Certificado		Secção no RFC 5280	Valor	Tipo ⁴	Comentários
tbsCertificate	Version	4.1.2.1	v3	m	
	Serial Number	4.1.2.2	<atribuído pela EC a cada certificado>	m	
	Signature	4.1.2.3	1.2.840.113549.1.1.5	m	Valor TEM que ser igual ao OID no signatureAlgorithm (abaixo)
	Issuer	4.1.2.4		m	
	Country (C)		"PT"		
	Organization (O)		"MULTICERT - Serviços de Certificação Electrónica S.A."		
	Organization Unit (OU)		" Entidade de Certificação Credenciada "		
	Common Name (CN)		"MULTICERT - Entidade de Certificação <nnn>"		
	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>		

⁴ O perfil utilize a terminologia seguinte para cada um dos tipos de campo no certificado X.509:

m – obrigatório (o campo TEM que estar presente)

o – opcional (o campo PODE estar presente)

c – crítico (a extensão é marcada crítica o que significa que as aplicações que utilizem os certificados TÊM que processar esta extensão).

	Not After		<data de emissão + máximo de 5 anos>		Validade máxima de 5 anos.
	Subject	4.1.2.6		m	
	Country (C)		<País de nacionalidade do titular do certificado>		
	Organization (O)		<Organização à qual o titular do certificado pertence>		Opcional
	Organization Unit (OU)		<Área/Departamento da Organização à qual o titular do certificado pertence>		Opcional
	Organization Unit (OU)		“Certificado para pessoa singular – Assinatura Qualificada” ou “Certificado para pessoa colectiva – Assinatura Qualificada”		
	Common Name (CN)		<nome do titular do certificado>		
	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.		Opcional
	Surname (SN)		<nomes de família do titular do certificado>		Opcional
	Given Name (givenName)		<nomes próprio do titular do certificado>		Opcional
	Serial Number (serialNumber)		<identificador único do titular do certificado>		

	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. ⁵
	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.

⁵ cf. RFC 3279. 2002, Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

	Digital Signature		"0" seleccionado		
	Non Repudiation		"1" seleccionado		certKeyUsage KeyUsage ::= {nonRepudiation} ⁶
	Key Encipherment		"0" seleccionado		
	Data Encipherment		"0" seleccionado		
	Key Agreement		"0" seleccionado		
	Key Certificate Signature		"0" seleccionado		
	CRL Signature		"0" seleccionado		
	Encipher Only		"0" seleccionado		
	Decipher Only		"0" seleccionado		
	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 Política de Certificado de Assinatura Digital Qualificada
	policyQualifiers		policyQualifierID: 1.3.6.1.5.5.7.2.1 cPSuri: http://pki.multicert.com/pol/cp/adq.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 Práticas de Certificação publicada pela EC. O apontador está na forma de um URI."

⁶ cf. RFC 3739. 2004, Internet X.509 Public Key Infrastructure: Qualified Certificates Profile.

	policyQualifiers		policyQualifierID: 1.3.6.1.5.5.7.2.2 userNotice explicitText: "O certificado emitido segundo esta política é equivalente a um certificado digital qualificado, nos termos, do definido na Legislação Portuguesa, aplicável para o efeito."		Valor do OID: 1.3.6.1.5.5.7.2.2 (id-qt-notice) 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	Declaração de Práticas de Certificação da EC MULTICERT
	policyQualifiers		policyQualifierID: 1.3.6.1.5.5.7.2.1 cPSuri: http://pki.multicert.com/pol/cps/MULTICERT_CA.html	o	
	Basic Constraints	4.2.1.9		c	Esta extensão é marcada CRÍTICA.
	CA		FALSE		
	Extended Key Usage	4.2.1.12			
	KeyPurposeld		id-kp-emailProtection		
	CRLDistributionPoints	4.2.1.13		o	
	distributionPoint		<a href="http://pki.multicert.com/crl/crl<ID_CA>.crl">http://pki.multicert.com/crl/crl<ID_CA>.crl	o	
	Freshest CRL	4.2.1.15		o	
	distributionPoint		<a href="http://pki.multicert.com/crl/crl<ID_CA>_delta.crl">http://pki.multicert.com/crl/crl<ID_CA>_delta.crl	o	

	Subject Alternative name	4.2.1.6	RFC822 name = <endereço do correio electrónico do titular do certificado>	o	
	Qualified Certificate Statement	-	id-pe-qcStatements = "1.3.6.1.5.5.7.1.3" ⁷ <pre>qcStatements EXTENSION ::= { SYNTAX QCStatements IDENTIFIED BY id-pe-qcStatements ;</pre>		A extensão <i>QCStatements</i> é uma extensão introduzida pelo PKIX Qualified Certificate Profile ⁶ e ETSI ⁸ .
	id-qcs-pkixQCSyntax-v2		id-etsi-qcs-QcCompliance = "0.4.0.1862.1.1"		<p>Declaração da EC MULTICERT, representada por um OID, indicando que este certificado é emitido como um certificado qualificado, de acordo com o Anexo I e II da Directiva EU 1999/93/EC, de acordo com a lei do país onde a EC está estabelecida.</p> <p>A declaração QcEuCompliance (id-etsi-qcs-QcCompliance) está associada com um identificador específico que corresponde ao OID "0.4.0.1862.1.1".</p> <p>Esta declaração indica que os certificados são emitidos em conformidade com a política <i>QCP public</i>, conforme ETSI TS 101 456.</p>

⁷ <http://www.alvestrand.no/objectid/1.3.6.1.5.5.7.1.3.html>

⁸ cf. ETSI TS 101 862, 2004-06, Qualified certificate profile, v1.3.2.

	id-qcs-pkixQCSyntax-v2		id-etsi-qcs-QcLimitValue = " 0.4.0.1862.1.2" currency = "EUR" amount = "0" exponent = "1"		Declaração pela qual a EC MULTICERT impõe um limite no valor da transacção para o qual este certificado pode ser utilizado, de acordo com a Directiva 1999/93/EC e a lei do país onde a EC está estabelecida.
	id-qcs-pkixQCSyntax-v2		id-etsi-qcs-QcRetentionPeriod = " 0.4.0.1862.1.3" QcEuRetentionPeriod = "20"		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 efectuada pela EC MULTICERT, indicando que a chave privada associada à chave pública no certificado está guardada num dispositivo seguro de criação de assinaturas (<i>Secure Signature Creation Device</i>), de acordo com o anexo III da Directiva 1999/93/EC e da lei do país onde a EC está estabelecida. Esta declaração indica que os certificados são emitidos em conformidade com a política SSCD , conforme ETSI TS 101 456.
	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
	accessLocation		http://ocsp.multicert.com/ocsp	o	

	Signature Algorithm	4.1.1.2	1.2.840.113549.1.1.5	m	TEM que conter o mesmo OID do identificador do algoritmo do campo signature no campo da sequência tbsCertificate. sha-1WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 } ⁵
	Signature Value	4.1.1.3	<contém a assinatura digital emitida pela EC>	m	Ao gerar esta assinatura, a EC certifica a ligação entre a chave pública e o titular (<i>subject</i>) do certificado.

3.1.4 OID do Algoritmo

O campo "*signatureAlgorithm*" do certificado contém o OID do algoritmo criptográfico utilizado pela EC para assinar o certificado: 1.2.840.113549.1.1.5 (sha-1WithRSAEncryption⁹)⁵.

3.1.5 Formato dos Nomes

Tal como definido na secção 2.1.

3.1.6 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 MULTICERT.

3.1.7 OID da Política de Certificados

A extensão "*certificate policies*" contém a sequência de um ou mais termos informativos sobre a política, cada um dos quais consiste num identificador da política e qualificadores opcionais.

Os qualificadores opcionais ("*policyQualifierID*: 1.3.6.1.5.5.7.2.1" e "*cPSuri*") apontam para o URI onde pode ser encontrada a Declaração de Práticas de Certificação com o OID identificado pelo "*policyIdentifier*". Os qualificadores opcionais ("*policyQualifierID*: 1.3.6.1.5.5.7.2.2" e "*userNotice explicitText*") apontam para o URI onde pode ser encontrados a Política de Certificados com o OID identificado pelo "*policyIdentifier*" (i.e., este documento).

3.1.8 Utilização da extensão Policy Constraints

Nada a assinalar.

3.1.9 Sintaxe e semântica do qualificador de política

A extensão "*certificate policies*" contém um tipo de qualificador de política a ser utilizado pelos emissores dos certificados e pelos escritores da política de certificados. O tipo de qualificador é o "*cPSuri*" que contém um apontador, na forma de URI, para a Declaração de Práticas de Certificação publicada pela EC e, o "*userNotice explicitText*" que contém um apontador, na forma de URI, para a Política de Certificados.

⁹ sha-1WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5

3.1.10 Semântica de processamento para a extensão crítica Certificate Policies

Nada a assinalar.

3.2 Certificado “espécimen”

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

- Perfil de certificado: é adicionado o prefixo “(espécimen)” ao *CommonName* (CN);
- Perfil de certificado: o atributo *serialNumber* contém “especimen” seguido de um número sequencial único (que começa em 0000001);
- Emissão do certificado: de acordo com formulário específico¹⁰;
- Revogação do certificado: o certificado é revogado imediatamente após a sua emissão¹⁰.

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.²

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.²

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

¹⁰ cf. MULTICERT_PJ.CA3_53.2.1_0001_pt.doc. 2009, Formulário de emissão de certificado “espécimen” de Assinatura Digital Qualificada.

4 Identificação e Autenticação

4.1 Validação de Identidade no registo inicial

Para os certificados de assinatura digital qualificada emitidos no domínio da EC MULTICERT, é obrigatório que o registo seja efectuado presencialmente, ou seja, a validação inicial da identidade do requerente é feita pelo método de “cara-a-cara” (ou equivalente).

4.1.1 Método de comprovação da posse de chave privada

No caso dos certificados de assinatura digital qualificada para pessoa singular ou pessoa colectiva, o par de chaves e certificado é fornecido em cartão (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 cartão (ou *token* USB) chip, que garante:

- par de chaves é gerado no HSM criptográfico e inserido no cartão (ou *token* USB) com chip criptográfico, por comunicação directa segura e sem ficar registado em qualquer dispositivo,
- o cartão (ou *token* USB) é personalizado para o titular do mesmo,
- chave pública é enviada à EC MULTICERT para emissão do certificado digital correspondente, sendo este também arquivado no cartão,
- cartão é entregue a titular por método “cara-a-cara”, ou equivalente (cf. 4.1.2 e 4.1.3).

4.1.2 Autenticação da identidade de uma pessoa colectiva

O processo de autenticação da identidade de uma pessoa colectiva, inicia-se com o pedido de emissão do certificado de assinatura digital qualificada para pessoa colectiva, através de preenchimento de formulário próprio e reconhecimento notarial da assinatura dos representantes legais da pessoa colectiva com poderes para o acto.

No formulário será indicada uma pessoa singular para recepção do certificado de pessoa colectiva, sendo a autenticação dessa pessoa efectuada de acordo com 4.1.3.

4.1.3 Autenticação da identidade de uma pessoa singular

O processo de autenticação da identidade de uma pessoa singular, garante que a pessoa singular para quem vai ser emitido o certificado é quem na realidade diz ser através da entrega (ou pedido) de certificado pelo titular (ou representante legal para o efeito de pedido/entrega de certificado digital de assinatura digital qualificada,

com reconhecimento notarial da assinatura do titular do certificado) por método "cara-a-cara", ou equivalente.

O método "cara-a-cara" ou equivalente são os seguintes:

- pedido/entrega de certificado nas instalações da MULTICERT S.A., nomeadamente no seu escritório de Lisboa ou Porto;
- entrega de certificado através de correio registado pessoal¹¹, com entrega exclusiva ao destinatário e mediante a sua identificação.

A autenticidade da qualidade do titular do certificado, no âmbito da sua utilização para assinatura digital qualificada, a apor no certificado digital é validada mediante apresentação de documento comprovativo emitido pela entidade que legalmente poder indicar essa qualidade.

4.1.4 Informação de subscritor/titular não verificada

Toda a informação descrita nos pontos 4.1.2 e 4.1.3 é verificada.

4.1.5 Validação de Autoridade

Nada a assinalar.

4.1.6 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 acto que recomende esta acção.

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

- 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 colectiva;
- 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;
- parte confiante, sempre que demonstre que o certificado foi utilizado com fins diferente dos previstos.

Um formulário próprio¹² serve de base ao pedido de revogação de certificado de assinatura digital qualificada e contém, entre outros, os seguintes elementos de identificação da entidade que inicia o pedido de revogação:

¹¹http://www2.ctt.pt/fewcm/wcmervlet/ctt/empresas/Oferta_Nacional/cartasdocumentos/envioscomgartentrg/correregpeessoal.html

- a) denominação legal;
- b) número de pessoa colectiva, sede, objecto 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 colectiva, é efectuado 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 electrónicas seguras, previamente definidas entre a EC MULTICERT e a entidade que efectua o pedido de revogação do certificado.

¹² *cf.* MULTICERT_PJ.CA3_53.2.2_0001_pt.doc. 2009, Formulário de revogação de certificado de Assinatura Digital Qualificada.

5 Requisitos operacionais do ciclo de vida do certificado

5.1 Pedido de Certificado

5.1.1 Quem pode subscrever um pedido de certificado?

O certificado de assinatura digital qualificada para pessoa colectiva pode ser subscrito pelos representantes legais da pessoa colectiva com poderes para o acto.

O certificado de assinatura digital qualificada para pessoa singular pode ser subscrito pelo titular do certificado ou representante legal para o efeito de pedido/entrega de certificado digital de assinatura digital qualificada, com reconhecimento notarial da assinatura do titular do certificado,

5.1.2 Processo de registo e responsabilidades

O processo de registo do pedido de certificado de assinatura digital qualificada é da responsabilidade do titular do certificado (ou representante legal para o efeito de pedido/entrega de certificado digital de assinatura digital qualificada, com reconhecimento notarial da assinatura do titular do certificado) sempre que o formulário de pedido for preenchido *online* através de *interface Web* fornecido pela EC MULTICERT.

O processo de registo do pedido de certificado de assinatura digital qualificada é da responsabilidade da EC MULTICERT sempre que o formulário de pedido for remetido em formato manuscrito. Contudo a veracidade e completude dos dados é sempre da responsabilidade do titular (ou representante legal para o efeito de pedido/entrega de certificado digital de assinatura digital qualificada, com reconhecimento notarial da assinatura do titular do certificado).

5.2 Processamento do pedido de certificado

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

- a) Recepção e verificação de toda a documentação e autorizações exigidas;
- b) Verificação da identidade do requisitante;
- c) Verificação da exactidão e integridade do pedido de certificado;
- d) Criação do par de chaves e assinatura o certificado;
- e) Disponibilização do certificado ao titular.

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 colectiva

Conforme indicado na secção 4.1.2.

5.2.1.2 Certificado de pessoa singular

Conforme indicado na secção 4.1.3.

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 verificar, 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 de assinatura digital qualificada de pessoa colectiva ou pessoa singular é realizada automaticamente, pela plataforma EC MULTICERT, após o registo do pedido de certificado, sendo a geração do par de chaves efectuada pelo HSM e o certificado emitido pela EC MULTICERT após recepção do pedido de certificado (PKCS#10).

Como medida de excepção, 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 recepção do mesmo, de acordo com o método "cara-a-cara" indicado em 4.1.3.

5.4 Aceitação do Certificado

5.4.1 Procedimentos para a aceitação de certificado

O certificado considera-se aceite após a recepção do mesmo, de acordo com o método "cara-a-cara" indicado em 4.1.3.

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.

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 respectiva 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 "*Subject*" 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.

Adicionalmente, o certificado de assinatura digital qualificada tem como objectivo a sua utilização em qualquer aplicação para efeitos de assinatura digital qualificada.

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 respectiva 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 correcta 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 sempre que estes estejam 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 acção 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 podem voltar a ser válidos, enquanto que os certificados suspensos podem recuperar a sua validade.

5.7.1 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;
- Inexactidões 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;
- Incumprimento por parte da EC MULTICERT ou titular das responsabilidades prevista na presente Política de Certificado e/ou correspondente DPC;
- Sempre que haja razões creíveis 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.

5.7.2 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 5.7.1, 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 colectiva;
- 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) 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 efectua o pedido de revogação.

5.7.3 Procedimento para o pedido de revogação

De acordo com a secção 4.2.

5.7.4 Produção de efeitos da revogação

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

5.7.5 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.

5.7.6 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).

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

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

5.7.8 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.

5.7.9 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.

5.7.10 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.

5.7.11 Outras formas disponíveis para divulgação de revogação

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

5.7.12 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 Autoridade Credenciadora 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.

5.7.13 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;
- 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.

5.7.14 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 5.7.13, 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 ou pessoa colectiva;
- 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) 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 efectua o pedido de suspensão.

5.7.15 Procedimentos para pedido de suspensão

Um formulário próprio¹³ serve de base ao pedido de suspensão de certificado de assinatura digital qualificada e contém, entre outros, os seguintes elementos de identificação da entidade que inicia o pedido de suspensão:

- f) denominação legal;
- g) número de pessoa colectiva, sede, objecto 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 suspensão;
- h) endereço e outras formas de contacto;
- i) indicação de pedido de suspensão, indicando o nome único (DN) atribuído ao certificado, assim como a sua validade;
- j) indicação do motivo para suspensão do certificado.

O processo de identificação e autenticação para pedido de suspensão de certificado de pessoa singular ou pessoa colectiva, é efectuado através de um dos seguintes métodos:

¹³ *cf.* MULTICERT_PJ.CA3_53.2.2_0002_pt.doc. 2009, Formulário de suspensão de certificado de Assinatura Digital Qualificada.

- 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 electrónicas seguras, previamente definidas entre a EC MULTICERT e a entidade que efectua o pedido de suspensão do certificado.

5.7.16 Limite do período de suspensão

A suspensão será feita de forma imediata.

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 de suspenso o tempo suficiente para confirmação da sua eventual reactivação ou revogação. Este período de tempo não pode ultrapassar os três dias úteis – findo esse prazo o certificado é imediatamente revogado, caso não exista comunicação em contrário por parte de quem submete o pedido de suspensão.

5.7.17 Outras formas disponíveis para divulgação de suspensão

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

6 Auditorias e normas de segurança

Todas as intervenções realizadas na Entidade de Certificação da MULTICERT são escrutinadas por auditores internos. A Entidade de Certificação da MULTICERT é auditada por um auditor independente do círculo de influência da Entidade de Certificação, exigida pela Autoridade Credenciadora, conforme o disposto no artigo 33.º do Decreto-Lei n.º 62/2003. A sua missão é auditar a infra-estrutura da Entidade de Certificação, no que respeita a equipamentos, recursos humanos, processos, políticas e regras, tendo que submeter um relatório anual, em Março, à Autoridade Credenciadora. A lista de Auditores de Segurança de Entidades Certificadoras credenciados pela Entidade Credenciadora podem ser encontrados em <http://www.gns.gov.pt/gns/pt/assinatura/>.

Os Certificados Digitais Qualificados emitidos pela Entidade de Certificação da MULTICERT cumprem todos os requisitos técnicos definidos nas seguintes normas:

- CWA 14167- Cryptographic Module for CSP Signing Operations — Protection Profile;
- CWA 14169:2004 - Secure signature-creation devices "EAL 4+" ;
- ETSI TS 101 456 V1.4.3 (2007-05) Electronic Signatures and Infrastructures (ESI);
- ETSI TS 101 862 V1.3.3 (2006-01) Qualified Certificate profile;
- ETSI TS 102 042 V1.4.3 (2007-12) Policy requirements for certification authorities issuing public key certificates;
- ETSI TS 102 176-1 v2.0.0 (2007-11) Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms.
- ETSI TS 102 280 v1.1.1 (2004-03) X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons;

Conclusão

Este documento define as Políticas de Certificados do certificado de Assinatura Digital Qualificada, utilizada pela EC MULTICERT no suporte à sua actividade de certificação digital. A hierarquia de confiança da Entidade de Certificação MULTICERT:

- fornece uma hierarquia de confiança, que promoverá a segurança electrónica do titular do certificado no seu relacionamento com terceiras entidades,
- proporciona a realização de transacções electrónicas seguras, a autenticação forte, um meio de assinar electronicamente transacções ou informações e documentos electrónicos, assegurando a sua autoria, integridade e não repúdio, e assegurando a confidencialidade das transacções ou informação.

Referências Bibliográficas

ETSI TS 101 456, 2007-05. Electronic Signatures and Infrastructures (ESI);Policy requirements for certification authorities issuing qualified certificates, v.1.4.3

ETSI TS 101 862, 2006-01. Qualified certificate profile, v1.3.3.

ETSI TS 102 042, 2007-12. Policy requirements for certification authorities issuing public key certificates, v1.4.3.

ETSI TS 102 176-1, 2007-11. Electronic Signatures and Infrastructures (ESI);Algorithms and Parameters for Secure Electronic Signatures;Part 1: Hash functions and asymmetric algorithms, v2.0.0.

ETSI TS 102 280, 2004-03. X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons, v1.1.1.

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

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

RFC 3739. 2004, Internet X.509 Public Key Infrastructure: Qualified Certificates Profile.

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