Politica de Certificado da raiz auto-assinada da EC MULTICERT

Políticas

MULTICERT_PJ.CA3_24.1.2_0001_pt.pdf

Identificação do Projecto: MULTICERT CA03

Identificação da CA: MULTICERT CA

Nível de Acesso: Público

Versão: 1.0

Data: 13/01/2009

MULTICERT, Serviços de Certificação Electrónica, S.A.,
Estrada Casal de Canas, Lote 6 – Alfragide, 2720-092 Amadora, Portugal
Telefone: +351 217 123 010 Facsimile: +351 217 123 011

Identificador do documento: MULTICERT_PJ.CA3_24.1.2_0001_pt.pdf

Palavras-chave: Politica de Certificados, EC MULTICERT

Tipologia documental: Políticas

Título: Politica de Certificado da Raíz Auto-Assinada da EC MULTICERT

Língua original: Português

Língua de publicação: Português

Nível de acesso: Público

Data: 13/01/2009

Versão actual: 1.0

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)
1.0	13/01/2009	Versão inicial	José Pina Miranda

Documentos Relacionados

ID Documento	Detalhes	Autor(es)
MULTICERT_PJ.CA3_24.1.1_0001_pt..pdf	Declaração de Práticas de Certificação	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, registada junto da 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 registada junto da 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 auto-assinado da Entidade de Certificação (EC) MULTICERT, que complementa e está de acordo com a Declaração de Práticas de Certificação da EC MULTICERT.[1]

[1] *cf.* MULTICERT_PJ.CA3_24.1.1_0001_pt.pdf. 2009, Declaração de Práticas de Certificação.

Sumário

Introdução

Objectivos

O objectivo deste documento é definir as políticas utilizadas na emissão do certificado auto-assinado da Entidade de Certificação (EC) MULTICERT, 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 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 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 auto-assinado de Entidade de Certificação da MULTICERT, 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 da EC MULTICERT[1].

1.2 Designação e Identificação do Documento

Este documento é a Política de Certificados da raiz auto-assinada da EC MULTICERT. 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 1.3.6.1.4.1.25070.1.1.1.1.0.1.1.

Este documento é identificado pelos dados constantes na seguinte tabela:

INFORMAÇÃO DO DOCUMENTO	
Versão do Documento	Versão 1.0
Estado do Documento	Aprovado
OID	1.3.6.1.4.1.25070.1.1.1.1.0.1.1
Data de Emissão	21/Janeiro/2009
Validade	Não aplicável
Localização	http://pki.multicert.com/pol/cp/root.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

O certificado da EC MULTICERT 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	PT
Organization	O	MULTICERT - Serviços de Certificação Electrónica S.A.
Organization Unit	OU	Entidade de Certificação Credenciada
Common Name	CN	Entidade de Certificação Credenciada <nnn>[2]

2.2 Uso do certificado e par de chaves pelo titular

A Entidade de Certificação MULTICERT é a titular do certificado auto-assinado de EC MULTICERT, utilizando a sua chave privada para a assinatura de certificados de operação e serviços, certificados para utilizadores finais, assim como para a assinatura da respectiva Lista de Certificados Revogados (LRC), de acordo com a sua DPC[1].

[2] <nnn> é um valor sequencial iniciado em "001" na emissão do primeiro certificado deste tipo.

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.[3]

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.[3]

O perfil do certificado da raiz auto-assinada da EC MULTICERT está de acordo com:

- Recomendação ITU.T X.509[4],
- RFC 5280[3], 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).

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] cf. RFC 5280. 2008, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
[4] cf. ITU-T Recommendation X.509. 1997, (1997 E): Information Technology - Open Systems Interconnection – The Directory: Authentication Framework.

3.1.3 Perfil do Certificado EC do Cidadão (auto-assinado)

Componente do Certificado		Secção no RFC 5280	Valor	Tipo[5]	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 *GeneralisedTime*
	Not Before		<data de emissão>		

[5] 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 + 4.139 dias>		Validade de aproximadamente onze anos e quatro meses. Utilizado para assinar certificados durante os primeiros cinco anos de validade (máximo) e renovado (com geração de novo par de chaves) após os primeiros quatro anos e nove meses de validade.
	Subject	4.1.2.6	<mesmo que *Issuer*>	m	Quando o *subject* é uma EC, tem que conter um DN igual ao *Issuer*.
	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.[6]
	subjectPublicKey		<Chave Pública com modulus n de 4096 bits>		
	Unique Identifiers	4.1.2.8			O "*unique identifiers*" está presente para permitir a possibilidade de reutilizar os nomes do *subject* e/ou *issuer* [6]
	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	

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

	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.
	Digital Signature		"0" seleccionado		
	Non Repudiation		"0" seleccionado		
	Key Encipherment		"0" seleccionado		
	Data Encipherment		"0" seleccionado		
	Key Agreement		"0" seleccionado		
	Key Certificate Signature		"1" seleccionado		
	CRL Signature		"1" seleccionado		
	Encipher Only		"0" seleccionado		
	Decipher Only		"0" seleccionado		
	Certificate Policies	4.2.1.4		o	
	policyIdentifier		1.3.6.1.4.1.25070.1.1.1.1.0.7	m	Identificador da Declaração de Práticas de Certificação da EC MULTICERT
	policyQualifiers		policyQualiflierID: 1.3.6.1.5.5.7.2.1 cPSuri: http://pki.multicert.com/pol/cps/MULTICERT_CA.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."

	policyIdentifier		1.3.6.1.4.1.25070.1.1.1.1.0.1.1	m	Identificador da Política de Certificados da raiz auto-assinada da EC do Cidadão.
	policyQualifiers		policyQualifierID: 1.3.6.1.5.5.7.2.2 userNotice explicitText: "Certificado emitido de acordo com a Política de Certificados em/Certificate issued in accordance with the Certificate Policy in http://pki.multicert.com/pol/cp/root.html."	o	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)
	Basic Constraints	4.2.1.9		mc	Esta extensão é marcada CRÍTICA.
	CA		TRUE		
	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 }[6]
	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 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-1WithRSAEncryption[7])[6].

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 ("*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 pode ser encontrados a Politica 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 Politica de Certificados.

3.1.10 Semântica de processamento para a extensão crítica Certificate Policies

Nada a assinalar.

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

3.2 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. [3]

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. [3]

O perfil da LRC está de acordo com:

- Recomendação ITU.T X.509[4],
- RFC 5280[3], e
- Legislação relevante portuguesa e europeia.

3.2.1 Número da Versão

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

3.2.2 Perfil da LRC Base da EC MULTICERT

As componentes e as extensões definidas para as LRCs X.509 v2 fornecem métodos para associar atributos às LRCs.

Componente da Lista de Revogação de Certificados		Secção no RFC 5280	Valor	Tipo	Comentários
tbsCertList	**Version**	5.1.2.1	1	m	Versão v2 (o valor inteiro é 1)
	Signature	5.1.2.2	1.2.840.113549.1.1.5	m	Contém o identificador do algoritmo utilizado para assinar a LRC. O valor TEM que ser igual ao OID no campo signatureAlgorithm (abaixo)
	Issuer	5.1.2.3		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>"		
	thisUpdate	5.1.2.4	<data de emissão da LRC>	m	Implementações TÊM que utilizar o tempo UTC até 2049, e a partir dessa data devem utilizar o GeneralisedTime.
	nextUpdate	5.1.2.5	<data da próxima emissão da LRC = *thisUpdate* + N>	m	Este campo indica a data em que a próxima LRC vai ser emitida.A próxima LRC pode ser emitida antes da data indicada, mas não será emitida depois dessa data. Os emissores da CRL DEVEM emitir CRL com o tempo de nextUpdate maior ou igual a todas as LRC anteriores. Implementações TÊM que utilizar o tempo UTC até 2049, e a partir dessa data devem utilizar o GeneralisedTime. N será no máximo 1 semana..

revokedCertificates	5.1.2.6	<lista de certificados revogados>	m	
CRL Extensions	5.1.2.7		m	
Authority Key Identifier	5.2.1		o	
keyIdentifier		<O key Identifier é composto pela hash de 160-bit SHA-1 do valor da BIT STRING do subject key identifier do certificado do emissor (excluindo a tag, length, e número de bits não usado)>	m	
CRL Number	5.2.3	<número sequencial único e incrementado>	m	
Issuing Distribution Point	5.2.5		c	
DistributionPointName		http://pki.multicert.comt/crl/crl<ID_CA>.crl		
Freshest CRL	5.2.6		o	
distributionPoint		http://pki.multicert.com/crl/crl<ID_CA>_delta.crl	o	
CRL Entry Extensions	5.3			

	Reason Code	5.3.1		o	Valor tem que ser um dos seguintes: 1 – keyCompromise 2 – cACompromise 3 – affiliationChanged 4 – superseded 5 – cessationOfOperation 6 – certificateHold 8 – removeFromCRL 9 – privilegeWithdrawn 10 - aACompromise
	Signature Algorithm	5.1.1.2	1.2.840.113549.1.1.5	m	TEM que conter o mesmo OID do identificador do algoritmo utilizado no campo signature da sequência tbsCertList. sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 }[6]
	Signature Value	5.1.1.3	<contém a assinatura digital emitida pela EC>	m	Contém a assinatura digital calculada sobre a *tbsCertList*.

3.2.3 Perfil da Delta LRC da EC MULTICERT

As componentes e as extensões definidas para as LRCs X.509 v2 fornecem métodos para associar atributos às LRCs.

Componente da Lista de Revogação de Certificados		**Secção no RFC 5280**	**Valor**	**Tipo**	**Comentários**
tbsCertList	**Version**	5.1.2.1	1	m	Versão v2 (o valor inteiro é 1)

Signature	5.1.2.2	1.2.840.113549.1.1.5	m	Contém o identificador do algoritmo utilizado para assinar a LRC. O valor TEM que ser igual ao OID no campo signatureAlgorithm (abaixo)
Issuer	5.1.2.3		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>"		
thisUpdate	5.1.2.4	<data de emissão da LRC>	m	Implementações TÊM que utilizar o tempo UTC até 2049, e a partir dessa data devem utilizar o GeneralisedTime.
nextUpdate	5.1.2.5	<data da próxima emissão da LRC = *thisUpdate* + N>	m	Este campo indica a data em que a próxima LRC vai ser emitida.A próxima LRC pode ser emitida antes da data indicada, mas não será emitida depois dessa data. Os emissores da CRL DEVEM emitir CRL com o tempo de nextUpdate maior ou igual a todas as LRC anteriores. Implementações TÊM que utilizar o tempo UTC até 2049, e a partir dessa data devem utilizar o GeneralisedTime. N será no máximo 1 dia.
revokedCertificates	5.1.2.6	<lista de certificados revogados>	m	
CRL Extensions	5.1.2.7		m	
Authority Key Identifier	5.2.1		o	
keyIdentifier		<O key Identifier é composto pela hash de 160-bit SHA-1 do valor da BIT STRING do subject key identifier do certificado do emissor (excluindo a tag, length, e número de bits não usado)>	m	

	CRL Number	5.2.3	<número sequencial único e incrementado>	m	
	Delta CRL Indicator	5.2.4	<número da LRC base>	c	Este número da LRC identifica a LRC base utilizada como ponto de partida da geração desta delta CRL.
	Issuing Distribution Point	5.2.5		c	
	DistributionPointName		http://pki.multicert.com/crl/crl<ID_CA>_delta.crl		
	CRL Entry Extensions	5.3			
	Reason Code	5.3.1		o	Valor tem que ser um dos seguintes: 1 – keyCompromise 2 – cACompromise 3 – affiliationChanged 4 – superseded 5 – cessationOfOperation 6 – certificateHold 8 – removeFromCRL 9 – privilegeWithdrawn 10 - aACompromise
	Signature Algorithm	5.1.1.2	1.2.840.113549.1.1.5	m	TEM que conter o mesmo OID do identificador do algoritmo utilizado no campo signature da sequência tbsCertList. sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 }[6]
	Signature Value	5.1.1.3	<contém a assinatura digital emitida pela EC>	m	Contém a assinatura digital calculada sobre a *tbsCertList*.

4 IDENTIFICAÇÃO E AUTENTICAÇÃO

4.1 Validação de Identidade no registo inicial

4.1.1 Método de comprovação da posse de chave privada

No certificado auto-assinado da EC MULTICERT, a comprovação da posse da chave privada será garantida através da presença física dos vários Grupos de Trabalho relevantes, na cerimónia de emissão desse tipo de certificados. Nessa cerimónia, será gerado e apresentado o pedido de certificado no formato PKCS#10[8].

4.1.2 Autenticação da identidade de uma pessoa colectiva

Nada a assinalar

4.1.2.1 Certificado auto-assinado da EC MULTICERT

A MULTICERT guarda toda a documentação utilizada para verificação da identidade da entidade de certificação, garantindo a verificação da identidade dos seus representantes legais, por meio legalmente reconhecido, e garantindo, no caso dos seus representantes legais não se encontrarem na cerimónia de emissão de certificado, os poderes bastantes do representante nomeado pela entidade para a referida emissão.

O documento que serve de base à emissão do certificado auto-assinado da EC MULTICERT é um documento formal do Conselho de Administração da MULTICERT que inclui entre outros:

a) a decisão do Conselho de Administração de ser inicializada a EC MULTICERT credenciada,

b) a nomeação do Grupo de Trabalho de Gestão da EC MULTICERT,

c) informação, se necessário, relativas à identificação e aos poderes do(s) representante(s) nomeados pela entidade para estarem presentes na cerimónia de emissão do certificado auto-assinado da EC MULTICERT.

4.1.3 Autenticação da identidade de uma pessoa singular

Nada a assinalar.

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.

[8] cf. RFC 2986. 2000, PKCS #10: Certification Request Syntax Specification, version 1.7.

4.1.6 Critérios para interoperabilidade

Nada a assinalar.

4.2 Identificação e Autenticação para pedido de revogação

Dadas as consequências da revogação do certificado auto-assinado da EC MULTICERT, é exigido um documento formal do Conselho de Administração da MULTICERT que inclui entre outros:

a) a decisão do Conselho de Administração de revogar o certificado auto-assinado da EC MULTICERT,

b) os motivos da revogação do certificado,

c) informação, se necessário, relativas à identificação e aos poderes do(s) representante(s) nomeados pela entidade para estarem presentes na cerimónia de revogação do certificado auto-assinado da EC MULTICERT.

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 auto-assinado da EC MULTICERT apenas pode ser pedido pelo Conselho de Administração da MULTICERT – Serviços de Certificação Electrónica, S.A.

5.1.2 Processo de registo e responsabilidades

O processo de registo do certificado de EC é constituído pelos seguintes passos, a serem efectuados pelos Grupos de Trabalho relevantes:

- Geração do par de chaves (chave pública e privada) em ambiente criptográfico apropriado;
- Geração do PKCS#10 correspondente em ambiente criptográfico apropriado.

5.2 Processamento do pedido de certificado

O pedido de certificado é processado do seguinte modo:

a) Criação do par de chaves e assinatura do certificado em ambiente criptográfico apropriado, de acordo com o perfil indicado nesta política;

b) Disponibilização do certificado.

As secções 6.2.1 e 6.3 descrevem detalhadamente todo o processo

5.2.1 Processos para a identificação e funções de autenticação

Os Grupos de trabalho relevantes executam a identificação e a autenticação de toda a informação necessária de acordo com o estipulado na secção 4 deste documento.

Os Grupos de trabalho relevantes aprovam a candidatura para um certificado auto-assinado da EC MULTICERT quando os seguintes critérios são preenchidos:

- identificação e autenticação bem sucedida de toda a informação necessária nos termos da secção 4 – toda a documentação utilizada para verificação da identidade e de poderes de representação é guardada;
- PKCS#10 válido.

Em qualquer outra situação, será rejeitada a candidatura para emissão de certificado.

Após a emissão do certificado, os Grupos de trabalho relevantes disponibilizam o certificado à EC MULTICERT.

5.2.2 Aprovação ou recusa de pedidos de certificado

A aprovação de certificado passa pelo cumprimento dos requisitos exigidos no ponto 6.2 e 6.2.1. 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 é efectuada por meio de uma cerimónia que decorre na zona de alta segurança da EC CC e, em que se encontram presentes:

- os representantes legais da MULTICERT S.A. ou o(s) representante(s) nomeado(s) para esta cerimónia,
- quatro (4) membros dos Grupo de Trabalho – a segregação de funções não possibilita a presença de um número inferior de elementos,
- quaisquer observadores aceites simultaneamente pelos membros dos Grupo de Trabalho e pelos representantes da MULTICERT S.A..

A cerimónia de emissão de certificado é constituída pelos seguintes passos:

- identificação e autenticação de todas as pessoas presentes na cerimónia, garantindo que o(s) representante(s) da MULTICERT S.A. (ou patrocinador no caso de certificado de equipamento tecnológico) e os membros dos Grupo de Trabalho têm os poderes necessários para os actos a praticar;
- os membros do Grupo de Trabalho efectuam o procedimento de arranque de processamento do certificado auto-assinado da EC MULTICERT e emitem o certificado (correspondente ao PKCS#10 gerado no HSM) em formato PEM;
- a cerimónia de emissão fica terminada com a execução do procedimento de finalização de processamento do certificado auto-assinado, pelos membros do Grupo de Trabalho;

O certificado emitido inicia a sua vigência no momento da sua emissão.

5.3.2 Notificação da emissão do certificado ao titular

A emissão do certificado é efectuada de forma presencial, de acordo com secção anterior.

5.4 Aceitação do Certificado

5.4.1 Procedimentos para a aceitação de certificado

O certificado considera-se aceite após a assinatura do formulário de emissão e aceitação de certificado pelo(s) representante(s) da MULTICERT S.A., de acordo com cerimónia de emissão (conforme secção 5.3.1).

Note-se que antes de ser disponibilizado o certificado aos representantes (ou patrocinador), 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 o formulário de recepção e aceitação 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 auto-assinados, 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

Será dado conhecimento à Autoridade Credenciadora da emissão do certificado auto-assinado da EC MULTICERT. A Autoridade Credenciadora será adicionalmente convidada para a cerimónia de emissão do certificado auto-assinado.

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.

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 Politica 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 publica e certificados.

b) ser responsável pela sua correcta utilização;

c) ler e entender os termos e condições descritos nas Politicas 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 patrocinador) 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 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;
- Equipamento tecnológico deixa de ser utilizado no âmbito da EC MULTICERT;
- 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);
- 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.

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

a) o Conselho de Administração da MULTICERT S.A..

A EC MULTICERT guarda toda a documentação utilizada para verificação da identidade e autenticidade da entidade que efectua o pedido de revogação, garantindo a verificação da identidade dos seus representantes legais, por meio legalmente reconhecido, não aceitando poderes de representação para o pedido de revogação do certificado auto-assinado da EC MULTICERT.

5.7.3 Procedimento para o pedido de revogação

Os procedimentos seguidos no pedido de revogação de certificado são os seguintes:

- todos os pedidos de revogação devem ser endereçados para a EC MULTICERT por escrito ou por mensagem electrónica assinada digitalmente pelo Conselho de Administração da MULTICERT S.A., indicando o motivo do pedido de revogação;
- identificação e autenticação da entidade que efectua o pedido de revogação;
- registo e arquivo do documento de pedido de revogação;
- análise do pedido de revogação pelo Grupo de Trabalho de Gestão da EC MULTICERT, que fornecerá a informação de revogação aos restantes Grupos de Trabalho;
- sempre que se decidir revogar um certificado, a revogação é publicada na respectiva LCR.

Em qualquer dos casos, é arquivada a descrição pormenorizada de todo o processo de decisão, ficando documentado:

- data do pedido de revogação,
- nome do titular do certificado,

- exposição pormenorizada dos motivos para o pedido de revogação,
- nome e funções da pessoa que solicita a revogação,
- informação de contacto da pessoa que solicita a revogação,
- assinatura da pessoa que solicita a revogação.

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 deve ser tratado de forma imediata, pelo que em caso algum poderá ser 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 não disponibiliza serviços de validação OCSP para o certificado auto-assinado.

5.7.10 Requisitos de verificação on-line de revogação

Nada a assinalar.

5.7.11 Outras formas disponíveis para divulgação de revogação

Nada a assinalar.

5.7.12 Requisitos especiais em caso de comprometimento de chave privada

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

A EC MULTICERT não suspende certificados auto-assinados.

5.7.14 Quem pode submeter o pedido de suspensão

Nada a assinalar.

5.7.15 Procedimentos para pedido de suspensão

Nada a assinalar.

5.7.16 Limite do período de suspensão

Nada a assinalar.

Conclusão

Este documento define as Políticas de Certificados do certificado auto-assinado da Entidade de Certificação MULTICERT, 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

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