multicert
Engineering for digital security

Política de Certificado da MULTICERT Root CA

Política

MULTICERT_PJ.ECRAIZ_24.1.2_0001_pt.doc

Identificação do Projeto: EC Raiz da MULTICERT

Identificação da CA: MULTICERT Root CA

Nível de Acesso: Público

Versão: 3.0

Data: 23/11/2016

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

Identificador do documento: MULTICERT_PJ.ECRAIZ_24.1.2_0001_pt.doc

Palavras-chave: PC, Política, Certificado

Tipologia documental: Política

Título: Política de Certificado da MULTICERT Root CA

Língua original: Português

Língua de publicação: Português

Nível de acesso: Público

Data: 23/11/2016

Versão atual: 3.0

Identificação do Projeto: EC Raiz da MULTICERT

Identificação da CA: MULTICERT Root CA

Cliente: ----

Histórico de Versões

N.º de Versão	Data	Detalhes	Autor(es)
1.0	06/02/2014	1ª Versão para Aprovação	MULTICERT S.A.
1.1	26/06/2014	Alteração de Morada	MULTICERT S.A.
2.0	10/07/2014	Versão aprovada	MULTICERT S.A.
2.1	22/11/2016	Revisão	MULTICERT S.A.
3.0	23/11/2016	Versão aprovada	MULTICERT S.A.

Documentos Relacionados

ID Documento	Detalhes	Autor(es)
MULTICERT_PJ.ECRAIZ_24.1.1_0001_pt.pdf	Declaração de Práticas de Certificação	MULTICERT S.A.
MULTICERT_PJ.ECRaiz_24.1.13_0001_pt.pdf	Declaração de Divulgação de Princípios	MULTICERT S.A.

Resumo Executivo

Decorrente da implementação de vários programas públicos e privados para a promoção das tecnologias de informação e comunicação e a introdução de novos processos de relacionamento em sociedade, entre pessoas singulares, empresas, organizações não-governamentais e o Estado, com vista ao fortalecimento da sociedade de informação, do governo eletrónico (*eGovernment*) e do comércio eletrónico, a Entidade de Certificação Raiz da MULTICERT, fornece os mecanismos necessários para a emissão de certificados para Entidades de Certificação Subordinadas, constituindo uma hierarquia de confiança, que promove a segurança eletrónica do titular do certificado digital emitido nesta hierarquia.

A Entidade de Certificação Raiz da MULTICERT estabelece uma estrutura de confiança eletrónica que proporciona a realização de transações eletrónicas seguras, a autenticação forte, um meio de assinar eletronicamente transações ou informações e documentos eletrónicos, assegurando a sua autoria, integridade e não repúdio, e assegurando a confidencialidade das transações ou informação.

Este documento define a Política de certificados utilizada na emissão do certificado auto-assinado da Entidade de Certificação MULTICERT Root CA, que complementa e está de acordo com a Declaração de Práticas de Certificação da Entidade de Certificação Raiz da MULTICERT[1].

Objetivos

O objetivo deste documento é definir as políticas utilizadas na emissão do certificado auto assinado da Entidade de Certificação Raiz da MULTICERT.

Público-Alvo

Este documento deve estar disponível publicamente e é destinado a todas as entidades que se relacionem de alguma forma com a EC Raiz da MULTICERT.

Estrutura do Documento

Assume-se que o leitor é conhecedor dos conceitos de criptografia, infraestruturas de chave pública e assinatura eletrónica. Caso esta situação não se verifique recomenda-se o aprofundar de conceitos e conhecimento nos tópicos anteriormente focados antes de proceder com a leitura do documento.

Este documento complementa a Declaração de Práticas de Certificação da Entidade de Certificação Raiz da MULTICERT1, presumindo-se que o leitor leu integralmente o seu conteúdo antes de iniciar a leitura deste documento.

Definições e Acrónimos

Encontra-se disponível uma lista com definições e acrónimos pertinentes para a leitura deste documento, no final do mesmo.

[1] Cf. MULTICERT_PJ.ECRAIZ_24.1.1_0001_pt.doc, 2014, Declaração de Práticas de Certificação da Entidade de Certificação Raiz da MULTICERT.

Sumário

1 Introdução

O presente documento é um documento de Política de Certificados (PC), cujo objetivo se prende com a definição de um conjunto de políticas e dados para a emissão e validação de certificados e para a garantia de fiabilidade desses mesmos certificados. Não se pretende nomear regras legais ou obrigações, mas antes informar pelo que se pretende que este documento seja simples, direto e entendido por um público alargado, incluindo pessoas sem conhecimentos técnicos ou legais.

Este documento descreve a política de certificados para a emissão e gestão de certificados emitidos pela MULTICERT Root Certification Authority 01 (MULTICERT Root CA).

Todos os certificados emitidos da hierarquia da MULTICERT CA Root estão em conformidade com os requisitos do ETSI TS 102 042 e do ETSI 101 456 relativamente às políticas de certificados identificados:

0.4.0.2042.1.1	Política de Certificado Avançado (Individual ou Profissional)[2]
0.4.0.2042.1.2	Política de Certificado Avançado (Individual ou Profissional) emitido sobre dispositivo criptográfico[3]
0.4.0.2042.1.7	Política de Certificado de TLS/SSL com verificação da Organização[4]
0.4.0.1456.1.1	Política de Certificado Qualificado[5]

Os Certificados emitidos na Hierarquia da MULTICERT Root CA, contêm uma referência à Politica de Certificados 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 Entidade de Certificação Raiz da MULTICERT.

1.2 Designação e Identificação do Documento

Este documento é a Política de Certificados da raiz auto-assinada da MULTICERT Root CA. A PC, é representada num certificado através de um número único designado de "identificador de objeto" (OID), sendo o valor do OID associado a este documento o 1.3.6.1.4.1.25070.1.1.1.0.1.

Este documento é identificado pelos dados constantes na seguinte tabela:

Informação do Documento	
Versão do Documento	Versão 3.0
Estado do Documento	Aprovado
OID	1.3.6.1.4.1.25070.1.1.1.0.1.1

[2] Denominado de *Normalized Certificate Policy* (NCP) na norma ETSI TS 102 042
[3] Denominado de *Extended Normalized Certificate Policy* (NCP+) na norma ETSI TS 102 042
[4] Denominado de *Organizational Validation Certificate Policy* (OVCP) na norma ETSI TS 102 042
[5] Denominado QCP+SSCD (*Qualified Certificate Policy + Secure Signature Creation Device*) na norma ETSI TS 101 456

Data de Emissão	23/11/2016
Validade	Não aplicável
Localização	https://pki.multicert.com/index.html

1.3 Contato

A gestão desta política de certificados é da responsabilidade do Grupo de Trabalho de Autenticação da PKI da MULTICERT.

NOME	Grupo de Trabalho de Autenticação da PKI da MULTICERT
Morada:	MULTICERT S.A. Lagoas Park, Edifício 3, Piso 3 2740-266 Porto Salvo Oeiras
Correio electrónico:	pki.documentacao@multicert.com
Página Internet:	www.multicert.com
Telefone:	+351 217 123 010
Fax:	+351 217 123 011

2 Identificação e Autenticação

2.1 Atribuição de Nomes

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

2.1.1 Tipos de Nomes

O certificado da MULTICERT Root CA é identificado por nome único (DN – *Distinguished Name*) de acordo com a norma X.500.
O nome único do certificado da MULTICERT Root CA é identificado pelos seguintes componentes:

Atributo	Código	Valor
Country	C	PT
Organization	O	MULTICERT – Serviços de Certificação Electrónica, S.A.
Common Name	CN	MULTICERT Root Certification Authority <nn>[6]

2.2 Uso do Certificado e Par de Chaves pelo Titular

A MULTICERT Root Certification Authority é a titular do certificado auto-assinado de MULTICERT Root CA, utilizando a sua chave privada para a assinatura de certificados de Entidades de Certificação Subordinadas, assinatura da respetiva Lista de Certificados Revogados (LRC) bem como para assinatura de certificados destinados ao serviço OCSP[7], de acordo com a sua DPC[1].

[6] <nn> é um valor sequencial iniciado em "01" na emissão do primeiro certificado deste tipo.
[7] OCSP – Online Certificate Status Protocol

3 Perfis de Certificado e LRC

3.1 Perfil de Certificado

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

Um certificado tem um período limitado de validade, indicado no seu conteúdo e assinado pela EC. Como a assinatura do certificado e a sua validade podem ser verificadas independentemente por qualquer *software* que utilize certificados, 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 certificado[8].

O utilizador de um serviço de segurança que requeira o conhecimento da chave pública do utilizador necessita, normalmente, de obter e validar o certificado que contém essa chave. Se o serviço não dispuser de uma cópia fidedigna da chave pública da EC que assinou o certificado, assim como do nome da EC e informação relacionada (tal como o período de validade), então poderá necessitar de um certificado adicional para obter a chave pública da EC e validar a 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 EC's assinados por outras EC's[8].

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

- Recomendação ITU.T X.509[9];
- RFC 5280[8];
- Legislação relevante portuguesa e europeia;
- CA/Browser Forum: Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.1.6; e
- *ETSI TS 102 042: Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.*

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.

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

3.1.3 Perfil do Certificado

Componente do Certificado		Secção na RFC 5280	Valor	Tipo[10]	Comentários
tbsCertificate	**Version**	4.1.2.1	V3	m	Versão do certificado de acordo com o standard X.509
	Serial Number	4.1.2.2	<Atribuído pela EC a cada certificado>	m	
	Signature	4.1.2.3	1.2.840.113549.1.1.11	m	Valor TEM que ser igual ao OID no signatureAlgorithm (abaixo)
	Issuer	4.1.2.4		m	
	Country (C)		"PT"		País do titular
	Organization (O)		"MULTICERT – Serviços de Certificação Electrónica, S.A."		Designação formal da organização do titular
	Common Name (CN)		"MULTICERT Root Certification Authority <nn>"		Constituído por <nome da CA> <nn> Sendo que <nn> é um valor sequencial iniciado em "01" na emissão do primeiro certificado deste tipo.
	Validity	4.1.2.5		m	Validade do certificado TEM que utilizar tempo UTC até 2049, passando a partir daí a utilizar *GeneralizedTime*
	Not Before		<Data de emissão>		
	Not After		<Data de emissão + 25 anos>		Validade de vinte e cinco anos. Utilizado para assinar certificados durante os primeiros 12 anos de validade (máximo) e renovado (com geração de novo par de

[10] O perfil utiliza 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 como crítica, o que significa que as aplicações que utilizem os certificados TÊM que processar esta extensão).

Componente do Certificado		Secção na RFC 5280	Valor	Tipo[10]	Comentários
					chaves) antes de atingir 12 anos e 6 meses de validade.
	Subject	4.1.2.6	<mesmo que o *Issuer*>	m	Contém o nome da EC titular do certificado 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		1.2.840.113549.1.1.11		O OID rsaEncryption identifica chaves públicas RSA. sha256WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)} O OID rsaEncryption deve ser utilizado no campo algoritmo com um valor do tipo AlgorithmIdentifier. Os parâmetros do campo TÊM que ser do tipo ASN.1 a NULL para o identificador deste algoritmo.[11]
	SubjectPublicKey		<Chave pública com modulus n de 4096 bits>		
	X.509 v3 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, lenght e número de bits não usado)>	m	

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

Componente do Certificado		Secção na RFC 5280	Valor	Tipo[10]	Comentários
	Key Usage	4.2.1.3		mc	Confere o tipo de utilização do certificado. Esta extensão é marcada CRÍTICA
	Digital Signature		"0" selecionado		
	Non Repudiation		"0" selecionado		
	Key Encipherment		"0" selecionado		
	Data Encipherment		"0" selecionado		
	Key Agreement		"0" selecionado		
	Key Certificate Signature		"1" selecionado		Para assinatura de certificados
	CRL Signature		"1" selecionado		Para assinatura de CRLs
	Encipher Only		"0" selecionado		
	Decipher Only		"0" selecionado		
	Basic Constraints	4.2.1.9		mc	Esta extensão é marcada como CRÍTICA
	CA		TRUE		
	Path length		nenhum		
	Signature Algorithm	4.1.1.2	1.2.840.113549.1.1.11	m	TEM que conter o mesmo OID do identificador do algoritmo do campo signature no campo da sequência tbsCertificate. OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}
	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: 1.2.840.113549.1.1.11(sha256WithRSAEncryption[12])[11].

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 carateres alfanuméricos não acentuados, espaço, traço de sublinhar, sinal negativo e ponto final ([a-z], [A-Z], [0-9], ' ', '_', '-', '.') sejam utilizados em entradas do Diretório X.500. A utilização de carateres acentuados será da única responsabilidade do Grupo de Trabalho de Gestão da PKI da MULTICERT.

3.1.7 OID da Política de Certificados

A extensão "*certificate policies*" não se encontra ativa no certificado auto-assinado da MULTICERT Root CA.

3.1.8 Utilização da Extensão Policy Constraints

Nada a assinalar.

3.1.9 Sintaxe e Semântica do Qualificador de Política

Nada a assinalar.

3.1.10 Semântica de Processamento para a Extensão Crítica Certificate Policies

Nada a assinalar.

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.[8]

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

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

(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.

O perfil da LRC está de acordo com:

- Recomendação ITU.T X.5094;
- RFC 52803 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 MULTICERT ROOT CA

As componentes e as extensões definidas para as LRC`s X.509 v2 fornecem métodos para associar atributos às LRC´s.

Componente da Lista de Revogação de Certificados		Secção na 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	1.2.840.113549.1.1.11	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."		
	Common Name (CN)		"MULTICERT Root Certification Authority <nn>"		
	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 *GeneralizedTime*.
	nextUpdate	5.1.2.5	<data da próxima emissão da LRC = thisUpdate + N>		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 LRC DEVEM emitir a LRC 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 *GeneralizedTime*. N será no máximo 4 meses.
	revokedCertificates	5.1.2.6	<lista de certificados revogados>	m	
	CRL Extensions	5.1.2.7		m	

Componente da Lista de Revogação de Certificados		Secção na RFC 5280	Valor	Tipo	Comentários
	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, lenght 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		**https://pki.multicert.com/index.html**		
	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 – Compromise

Componente da Lista de Revogação de Certificados		Secção na RFC 5280	Valor	Tipo	Comentários
	Signature Algorithm	5.1.1.2	1.2.840.113549.1.1.11	m	TEM que conter o mesmo OID do identificador do algoritmo utilizado no campo *signature* da sequência tbsCertificate. OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}
	Signature Value	5.1.1.3	<contém a assinatura digital emitida pela EC>	m	Contém a assinatura digital calculada sobre a *tbsCertList*.

3.3 Perfil de Certificado de OCSP

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

Um certificado tem um período limitado de validade, indicado no seu conteúdo e assinado pela EC. Como a assinatura do certificado e a sua validade podem ser verificadas independentemente por qualquer *software* que utilize certificados, os certificados podem ser distribuídos através de linhas de comunicação e sistemas públicos, assim como podem ser guardados em qualquer tipo de unidades de armazenamento[13].

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.

O perfil dos Certificados de Validação *on-line* OCSP está de acordo com:

- Recomendação ITU.T X.509[14];
- RFC 5280[13] e
- Outras normas e legislação aplicável.

3.3.1 Número da Versão

O campo "*version*" do certificado descreve a versão utilizada na codificação do certificado. Neste perfil, a versão utilizada é a 3 (três).

3.3.2 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.

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

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

Componente do Certificado		Secção no RFC 5280	Valor			Tipo[15]	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	1.2.840.113549.1.1.11			m	Valor TEM que ser igual ao OID no *signatureAlgorithm* (abaixo)
	Issuer	4.1.2.4	**EC RAIZ MC**	**MULTICERT Trust Services Certification Authority**	**MULTICERT Certification Authority**	m	
	Country (C)		"PT"				
	Organization (O)		"MULTICERT – Serviços de Certificação Electrónica, S.A."				
	Organization Unit (OU)		--	"MULTICERT Trust Services Provider"	"Accredited Certification Authority"		
	Common Name (CN)		"MULTICERT Root Certification Authority <nn>"	"MULTICERT Trust Services Certification Authority <nnn>"	"MULTICERT Certification Authority <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>				
	Not After		<data de emissão + 2.150 dias>				Validade de aproximadamente 6 anos e 6 meses. Utilizada para assinar respostas OCSP durante aproximadamente quatro meses e renovado (com geração de novo par de chaves) após este período.

[15] O perfil utilize a terminologia seguinte para cada um dos tipos de campo no certificado X.509:
m – obrigatório (o campo TEM que estar presente);
o – opcional (o campo PODE estar presente);
c – crítico (a extensão é marcada crítica o que significa que as aplicações que utilizem os certificados TÊM que processar esta extensão).

Componente do Certificado		Secção no RFC 5280	Valor	Tipo[15]	Comentários
	Subject	4.1.2.6		m	
	Country (C)		"PT"		
	Organization (O)		"MULTICERT – Serviços de Certificação Electrónica, S.A"		
	Organization Unit (OU)		"Revocation Status Services"		
	Serial Number (SN)		<nnnnnn>		
	Common Name (CN)		"OCSP Validation Service"		
	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		1.2.840.113549.1.1.11		O OID rsaEncryption identifica chaves públicas RSA. Sha-256WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)} 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.[16]
	subjectPublicKey		<Chave Pública com modulus n de 2048 bits>		

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

Componente do Certificado		Secção no RFC 5280	Valor	Tipo[15]	Comentários
	X.509v3 Extensions	4.1.2.9		m	
	Authority Key Identifier	4.2.1.1		o	
	keyIdentifier		<O key Identifier é composto pela hash de 256-bit SHA-256 do valor da BIT STRING do *subjectKeyIdentifier* do certificado do emissor (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 256-bit SHA-256 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		"1" selecionado		
	Non Repudiation		"1" selecionado		
	Key Encipherment		"0" selecionado		
	Data Encipherment		"0" selecionado		
	Key Agreement		"0" selecionado		
	Key Certificate Signature		"0" selecionado		
	CRL Signature		"0" selecionado		
	Encipher Only		"0" selecionado		
	Decipher Only		"0" selecionado		
	Certificate Policies	4.2.1.5		o	

Componente do Certificado		Secção no RFC 5280	Valor			Tipo[15]	Comentários
	policyIdentifier		1.3.6.1.4.1.25070.1.1.1.0.7			m	Identificador da Declaração de Práticas de Certificação da MULTICERT Root CA.
	policyQualifiers		*policyQualifierID*: 1.3.6.1.5.5.7.2.1[17] *cPSuri*: http://pkiroot.multicert.com/pol/index.html			o	Valor do OID: 1.3.6.1.5.5.7.2.1 (id-qt-cps)
	policyIdentifier		1.3.6.1.4.1.25070.1.1.1.0.1.3			m	
	policyQualifiers		**EC RAIZ MC**	**MULTICERT Trust Services Certification Authority**	**MULTICERT Certification Authority**	o	Valor do OID: 1.3.6.1.5.5.7.2.1 (id-qt-cps) Valor do OID: 1.3.6.1.5.5.7.2.2 (id-qt-unotice)
			policyQualifierID: 1.3.6.1.5.5.7.2.1[17] *cPSuri*:http://pkiroot.multicert.com/pol/index.html	*policyQualifierID*: 1.3.6.1.5.5.7.2.2[18] *UserNotice: "Certificado emitido de acordo com a Politica de Certificados em /Certificate issued in accordance with the Certificate Policy in http://pkiroot.multicert.com/pol/index.html"*			
	Basic Constraints	4.2.1.10				c	Esta extensão é marcada CRÍTICA.
	CA		FALSE				
	Extended Key Usage	4.2.1.13	1.3.6.1.5.5.7.3.9			o	Descrição do OID: Indica que a chave privada correspondente ao certificado X.509 pode ser utilizada para assinar respostas OCSP.
	OCSPNocheck	-	NULL			o	Não é uma extensão definida no RFC 3280. Definida em http://www.alvestrand.no/objectid/1.3.6.1.5.5.7.48.

[17] Descrição do OID: "O atributo *cPSuri* contém um apontador para a localização da documentação pública da EC. O apontador está na forma de um URI." (http://www.alvestrand.no/objectid/submissions/1.3.6.1.5.5.7.2.1.html)
[18] 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)

Componente do Certificado		Secção no RFC 5280	Valor	Tipo[15]	Comentários
					1.5.html, esta extensão deve ser incluída num certificado de assinatura OCSP. Esta extensão indica ao cliente OCSP que este certificado de assinatura pode ser confiável, mesmo sem validar junto do servidor OCSP (já que a resposta seria assinada pelo servidor OCSP e o cliente teria que novamente validar o estado do certificado de assinatura).
	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 value: 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	1.2.840.113549.1.1.11	m	TEM que conter o mesmo OID do identificador do algoritmo do campo *signature* no campo da sequência *tbsCertificate*. sha-256WithRSAEncryption OBJECT IDENTIFIER ::= ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}[16]
	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.

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 MULTICERT Root CA, 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[19], cuja assinatura sobre a informação da chave pública será validada.

4.1.2 Autenticação da Identidade de uma Pessoa Coletiva

Nada a assinalar.

4.1.2.1 Certificado auto-assinado da MULTICERT Root CA

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 MULTICERT Root CA 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 MULTICERT Root CA;
b) A nomeação do Grupo de Trabalho de Gestão da MULTICERT Root CA;
c) Informação, se necessário, relativa à identificação e aos poderes do(s) representante(s) nomeado(s) pela entidade para estar(em) presente(s) na cerimónia de emissão do certificado auto-assinado da MULTICERT Root CA.

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.

4.1.6 Critérios para Interoperabilidade

Nada a assinalar.

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

4.2 Identificação e Autenticação para Pedido de Revogação

Dadas as consequências da revogação do certificado auto-assinado da MULTICERT Root CA, 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 MULTICERT Root CA;
b) Os motivos da revogação do certificado;
c) Informação, se necessário, relativa à identificação e aos poderes do(s) representante(s) nomeado(s) pela entidade para esta(em) presente(s) na cerimónia de revogação do certificado auto-assinado da MULTICERT Root CA.

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 efetuados 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 5.2.1 e 5.3 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.

1. Os Grupos de trabalho relevantes aprovam a candidatura para emissão do Certificado Auto-assinado MULTICERT Root CA:
    a. Existe consentimento expresso do Grupo de Gestão da PKI da MULTICERT.
2. Certificado para Entidade de Certificação Subordinada:
    a. 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;
    b. 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 ao Grupo de Gestão da PKI da MULTICERT e, se for o caso, aos representantes legais da Entidade de Certificação Subordinada.

5.2.2 Aprovação ou Recusa de Pedidos de Certificado

A aprovação de certificado passa pelo cumprimento dos requisitos exigidos no ponto 5.2 e 5.2.1.

Quando tal não se verifique, é recusada a emissão do certificado.

5.2.3 Prazo para Processar o Pedido de Certificado

Após a aprovação do pedido de certificado, o certificado deverá ser emitido em não mais do que dez (10) dias úteis.

5.3 Emissão de Certificado

5.3.1 Procedimentos para a Emissão de Certificado

A emissão do certificado é efetuada por meio de uma cerimónia que decorre na zona de alta segurança da EC, 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 do Grupo de Trabalho – a segregação de funções não possibilita a presença de um número inferior de elementos;
- Um Auditor Qualificado – para testemunhar a geração do par de chaves da MULTICERT Root CA e a emitir um relatório a relatar o cumprimento dos requisitos do processo de geração de chaves por parte da MULTICERT Root CA e a utilização de controlos para garantir a integridade e confidencialidade do par de chaves - Este ponto apenas para geração do certificado auto-assinado da MULTICERT Root CA;
- Quaisquer observadores aceites simultaneamente pelo Grupo de Gestão da PKI da MULTICERT.

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) e os membros do Grupo de Trabalho têm os poderes necessários para os atos a praticar;
- Os membros do Grupo de Trabalho efetuam o procedimento de arranque de processamento do certificado auto-assinado da MULTICERT Root CA 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 efetuada de forma presencial, de acordo com secção anterior.

5.4 Aceitação do Certificado

5.4.1 Procedimentos para a Aceitação do Certificado

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

Note-se que antes de ser disponibilizado o certificado ao(s) representante(s), 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 receção 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 respetiva Declaração de Práticas de Certificação.

5.4.2 Publicação do Certificado

A MULTICERT Root CA não publica os certificados auto-assinados nem os certificados emitidos para Entidades de Certificação Subordinadas 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 MULTICERT Root CA. 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 1.3.1 e 1.3.2 da Declaração de Práticas de Certificação (DPC);
c) Enquanto o certificado se mantiver válido e não estiver na LRC da MULTICERT Root CA.

5.5.2 Uso do Certificado e da Chave Pública pelas Partes Confiantes

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

a) Ter conhecimento e perceber a utilização e funcionalidades proporcionadas pela criptografia de chave pública e certificados;
b) Ser responsável pela sua correta utilização;
c) Ler e entender os termos e condições descritos nas Políticas e práticas de certificação;
d) Verificar os certificados (validação de cadeias de confiança) e LRC, tendo especial atenção às suas extensões marcadas como críticas e propósito das chaves;
e) Confiar nos certificados, utilizando-os sempre que estes estejam válidos.

5.6 Renovação do 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 do 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 constante no certificado sofre alterações.

5.6.2 Quem pode Submeter o Pedido de Certificado de uma Nova Chave Pública

Tal como na secção 5.1.1.

5.6.3 Processamento do Pedido de Renovação do Certificado com Geração de Novo Par de Chaves

Tal como na secção 5.1.2 e 5.2.

5.6.4 Notificação da Emissão de Novo Certificado ao Titular

Tal como na secção 5.3.2.

5.6.5 Procedimentos para Aceitação de um Certificado Renovado com Geração de Novo Par de Chaves

Tal como na secção 5.4.1.

5.6.6 Publicação de Certificado Renovado com Geração de Novo Par de Chaves

Tal como na secção 5.4.2.

5.6.7 Notificação da Emissão de Certificado Renovado a Outras Entidades

Tal como na secção 5.4.3.

5.7 Suspensão e Revogação de Certificado

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

Os certificados depois de revogados não podem voltar a ser válidos, enquanto que os certificados suspensos podem recuperar a sua validade.

5.7.1 Motivos para a Suspensão

A MULTICERT Root CA não suspende certificados.

5.7.2 Quem pode Submeter o Pedido de Suspensão

Nada a assinalar.

5.7.3 Procedimentos para Pedido de Suspensão

Nada a assinalar.

5.7.4 Limite do Período de Suspensão

Nada a assinalar.

5.7.5 Motivos para a Revogação

Um certificado pode ser revogado por uma das seguintes razões:

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

O certificado é revogado no prazo máximo de 7 dias.

5.7.6 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 5.7.5:

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

A MULTICERT Root CA guarda toda a documentação utilizada para verificação da identidade e autenticidade da entidade que efetua 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 MULTICERT Root CA.

5.7.7 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 MULTICERT Root CA por escrito ou por mensagem eletrónica assinada digitalmente pelo Conselho de Administração da MULTICERT S.A., indicando o motivo do pedido de revogação;
- Identificação e autenticação da entidade que efetua 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 PKI da MULTICERT, que fornecerá a informação de revogação aos restantes Grupos de Trabalho;
- Sempre que se decidir revogar um certificado, a revogação é publicada na respetiva 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.

5.7.8 Produção de Efeitos da Revogação

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

5.7.9 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.

5.7.10 Requisitos de Verificação da Revogação pelas Partes Confiantes

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

5.7.11 Periodicidade da Emissão da Lista de Certificados Revogados (LCR)

A MULTICERT Root CA disponibiliza uma nova LCR Base a cada 4 (quatro) meses

5.7.12 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.

5.7.13 Disponibilidade de Verificação Online do Estado / Revogação de Certificado

A MULTICERT Root CA não disponibiliza serviços de validação OCSP para o certificado auto-assinado.

5.7.14 Requisitos de Verificação Online de Revogação

Nada a assinalar.

5.7.15 Outras Formas Disponíveis para Divulgação de Revogação

Nada a assinalar.

5.7.16 Requisitos Especiais em Caso de Comprometimento de Chave Privada

No caso da chave privada da MULTICERT Root CA 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 MULTICERT Root CA e de todos os certificados emitidos no "ramo" da hierarquia de confiança da MULTICERT Root CA;
- Notificação da Autoridade Credenciadora e todos os titulares de certificados emitidos no "ramo" da hierarquia de confiança da MULTICERT Root CA;
- Geração de novo par de chaves para a MULTICERT Root CA;
- Renovação de todos os certificados emitidos no "ramo" da hierarquia de confiança da MULTICERT Root CA.

6 Lista de Definições e Acrónimos

Definições

Assinatura digital	Modalidade de assinatura eletrónica avançada baseada em sistema criptográfico assimétrico composto de um algoritmo ou série de algoritmos, mediante o qual é gerado um par de chaves assimétricas exclusivas e interdependentes, uma das quais privada e outra pública, e que permite ao titular usar a chave privada para declarar a autoria do documento eletrónico ao qual a assinatura é aposta e concordância com o seu conteúdo e ao destinatário usar a chave pública para verificar se a assinatura foi criada mediante o uso da correspondente chave privada e se o documento eletrónico foi alterado depois de aposta a assinatura.
Assinatura eletrónica	Resultado de um processamento eletrónico de dados, suscetível de constituir objeto de direito individual e exclusivo e de ser utilizado para dar a conhecer a autoria de um documento eletrónico.
Assinatura eletrónica avançada	Assinatura eletrónica que preenche os seguintes requisitos: i) Identifica de forma unívoca o titular como autor do documento; ii) A sua aposição ao documento depende apenas da vontade do titular; iii) É criada com meios que o titular pode manter sob seu controlo exclusivo; iv) A sua conexão com o documento permite detetar toda e qualquer alteração superveniente do conteúdo deste.
Assinatura eletrónica qualificada	Assinatura digital ou outra modalidade de assinatura eletrónica avançada que satisfaça exigências de segurança idênticas às da assinatura digital baseadas num certificado qualificado e criadas através de um dispositivo seguro de criação de assinatura.
Autoridade Credenciadora	Entidade competente para a credenciação e fiscalização das entidades certificadoras.
Certificado	Documento eletrónico que liga os dados de verificação de assinatura ao seu titular e confirma a identidade desse titular.
Certificado qualificado	Certificado que contém os elementos referidos no artigo 29.º do DL 62/2003 [7] e é emitido por entidade certificadora que reúne os requisitos definidos no artigo 24.º do DL 62/2003.

Chave privada	Elemento do par de chaves assimétricas destinado a ser conhecido apenas pelo seu titular, mediante o qual se apõe a assinatura digital no documento eletrónico, ou se decifra um documento eletrónico previamente cifrado com a correspondente chave pública.
Chave pública	Elemento do par de chaves assimétricas destinado a ser divulgado, com o qual se verifica a assinatura digital aposta no documento eletrónico pelo titular do par de chaves assimétricas, ou se cifra um documento eletrónico a transmitir ao titular do mesmo par de chaves.
Credenciação	Ato pelo qual é reconhecido a uma entidade que o solicite e que exerça a atividade de entidade certificadora o preenchimento dos requisitos definidos no presente diploma para os efeitos nele previstos.
Dados de criação de assinatura	Conjunto único de dados, como chaves privadas, utilizado pelo titular para a criação de uma assinatura eletrónica.
Dados de verificação de assinatura	Conjunto de dados, como chaves públicas, utilizado para verificar uma assinatura eletrónica.
Dispositivo de criação de assinatura	Suporte lógico ou dispositivo de equipamento utilizado para possibilitar o tratamento dos dados de criação de assinatura.
Dispositivo seguro de criação de assinatura	Dispositivo de criação de assinatura que assegure, através de meios técnicos e processuais adequados, que: i) Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura só possam ocorrer uma única vez e que a confidencialidade desses dados se encontre assegurada; ii) Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura não possam, com um grau razoável de segurança, ser deduzidos de outros dados e que a assinatura esteja protegida contra falsificações realizadas através das tecnologias disponíveis; iii) Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura possam ser eficazmente protegidos pelo titular contra a utilização ilegítima por terceiros; iv) Os dados que careçam de assinatura não sejam modificados e possam ser apresentados ao titular antes do processo de assinatura.
Documento eletrónico	Documento elaborado mediante processamento eletrónico de dados.
Endereço eletrónico	Identificação de um equipamento informático adequado para receber e arquivar documentos eletrónicos.
Estampilha temporal	Estrutura de dados que liga a representação eletrónica de um *datum* com

	uma data/hora particular, estabelecendo evidência de que o *datum* existia nessa data/hora.
Parte confiante	Recetor de uma estampilha temporal que confia na mesma.
Sistema TSA (*TSA system*)	Composição de produtos IT e componentes, organizados de modo a suportar o fornecimento de serviços de validação cronológica.
UTC (*Coordinated Universal Time*)	Escala de tempo baseada no segundo, como definido na *ITU-R Recommendation TF.460-5* [10].
UTC(k)	Escala de tempo fornecida pelo laboratório "k" que garante ±100 ns em relação ao UTC (conforme *ITU-R Recommendation TF.536-1* [11])
Validação cronológica	Declaração de uma EVC que atesta a data e hora da criação, expedição ou receção de um documento eletrónico.

Acrónimos

ANSI	*American National Standards Institute*
C	*Country*
CA	*Certification Authority* (o mesmo que EC)
CN	*Common Name*
CRL	Ver LRC
DL	Decreto Lei
DN	*Distinguished Name*
DPC	Declaração de Práticas de Certificação
DR	Decreto Regulamentar
EC	Entidade de Certificação
ECD	Entidade Certificadora de Documentos
ER	Entidade de Registo
GMT	Tempo Médio de Greenwich (*Greenwich Mean Time*)

GNS	*Gabinete Nacional de Segurança*
LRC	Lista de Revogação de Certificados
MAC	*Message Authentication Codes*
O	*Organization*
OCSP	*Online Certificate Status Protocol*
OID	Identificador de Objecto
PC	Política de Certificado
PKCS	*Public-Key Cryptography Standards*
PKI	*Public Key Infrastructure* (Infra-estrutura de Chave Pública)
SHA	*Secure Hash Algorithm*
SGCVC	*Sistema de Gestão de Ciclo de Vida de Certificados*
SSCD	*Secure Signature-Creation Device*
TSA	*Time-Stamping Authority* (o mesmo que EVC)

7 Aprovação

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

Digitally signed by [Assinatura Qualificada] MULTICERT - SERVIÇOS DE CERTIFICAÇÃO ELECTRÓNICA S.A.
DN: c=PT, o=MULTICERT - SERVIÇOS DE CERTIFICAÇÃO ELECTRÓNICA S.A., ou=Certificado para pessoa colectiva - Assinatura Qualificada, title=Procurador com os poderes indicados na procuração emitida em 16/10/2013 - Informação confirmada pela Entidade de Certificação apenas na data de emissão e que não foi confirmada posteriormente a essa data, serialNumber=505767457, cn=[Assinatura Qualificada] MULTICERT - SERVIÇOS DE CERTIFICAÇÃO ELECTRÓNICA S.A.
Date: 2016.11.24 09:53:36 Z