multicert
Engineering for digital security

Política de Certificado de Validação Cronológica

Políticas

MULTICERT_PJ.CA3_24.1.2_0004_pt.doc

Identificação do Projeto: PKI MULTICERT

Identificação da CA: MC TS CA

Nível de Acesso: Público

Versão: 3.0

Data: 28/08/2017

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

Identificador do documento: MULTICERT_PJ.CA3_24.1.2_0004_pt.doc

Palavras-chave: Política de Certificados, Trust Services, Validação Cronológica

Tipologia documental: Políticas

Título: Política de Certificado de Validação Cronológica

Língua original: Português

Língua de publicação: Português

Nível de acesso: Público

Data: 28/08/2017

Versão atual: 3.0

Identificação do Projeto: PKI MULTICERT

Identificação da CA: MC TS CA

Cliente: ---

Documentos Relacionados

ID Documento	Detalhes	Autor(es)
MULTICERT_PJ.CA3_24.1.1_0002_pt.doc	Declaração de Práticas de Validação Cronológica	MULTICERT S.A.
MULTICERT_PJ.CA3_24.1.13_0001_pt.doc	Declaração de Divulgação de Princípios de Validação Cronológica	MULTICERT S.A.
MULTICERT_PJ.ECRAIZ_127.doc	Declaração de Práticas de Certificação da MC TS CA	MULTICERT S.A.

Resumo Executivo

Decorrente da implementação de vários programas públicos e privados para a promoção das tecnologias de informação e comunicação e a introdução de novos processos de relacionamento em sociedade, entre cidadãos, empresas, organizações não-governamentais e o Estado, com vista ao fortalecimento da sociedade de informação, do governo eletrónico (*eGovernment*) e do comércio eletrónico, os certificados digitais emitidos na PKI da MULTICERT, cujas Entidades de Certificação são credenciadas pela Autoridade Credenciadora (conforme previsto na legislação europeia e nacional), fornecem os mecanismos necessários para a autenticação digital forte da identidade do titular do certificado eletrónico, assim como as assinaturas eletrónicas (equivalente legal das assinaturas manuscritas) indispensáveis aos processos de desmaterialização.

A infra-estrutura da PKI da MULTICERT fornece uma hierarquia de confiança, que promove a segurança eletrónica do titular de certificados digitais. A Entidade de Certificação MULTICERT estabelece uma estrutura de confiança eletrónica que proporciona a realização de transações eletrónicas seguras, a autenticação forte, um meio de assinar eletronicamente transações ou informações e documentos eletrónicos, assegurando a sua autoria, integridade e não repúdio, e assegurando a confidencialidade das transações ou informação.

A PKI da MULTICERT está devidamente credenciada pela Autoridade Nacional de Segurança (http://www.gns.gov.pt/trusted-lists.aspx), com credenciação número ANS-ECC-7/2014, à data de 20/06/2014, conforme previsto na legislação portuguesa e europeia, estando deste modo habilitada legalmente a emitir todo o tipo de certificados digitais, incluindo os certificados digitais qualificados (certificados digitais de mais elevado grau de segurança previsto na legislação) bem como selos temporais qualificados.

Este documento define a Política de certificados utilizada na emissão do certificado responsável pela assinatura dos selos temporais emitidos pela Entidade de Validação Cronológica, que complementa e está de acordo com a Declaração de Práticas de Certificação da MULTICERT TS CA bem como a Declaração de Praticas de Certificação de Validação Cronológica.

Sumário

Introdução

Objetivos

O objetivo deste documento é apresentar o perfil dos Certificado de Validação Cronológica emitido pela MULTICERT *Trust Services Certification Authority* (MC TS CA).

Público-Alvo

Este documento deve ser lido por:

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

Estrutura do Documento

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

Este documento complementa a Declaração de Práticas de Validação Cronológica bem como a Declaração de Práticas de Certificação da MULTICERT TS CA, presumindo-se que o leitor leu integralmente o seu conteúdo antes de iniciar a leitura deste documento.

1 Contexto Geral

O presente documento tem como objetivo a definição de um conjunto de parâmetros que definem o perfil dos Certificados de Validação Cronológica emitidos na PKI da MULTICERT, permitindo assim garantir a fiabilidade do serviço de Validação Cronológica disponível também na PKI da MULTICERT. 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.

1.1 Visão Geral

Esta Política satisfaz e complementa os requisitos impostos pela Declaração de Práticas de Certificação da MC TS CA.

1.2 Designação e Identificação do Documento

Este documento é a Política de Certificados do Certificado de Validação Cronológica. 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 é o "1.3.6.1.4.1.25070.1.1.1.2.0.1.1".

Este documento é identificado pelos dados constantes na seguinte tabela:

INFORMAÇÃO DO DOCUMENTO	
Versão do Documento	Versão 3.0
Estado do Documento	Aprovado
OID	1.3.6.1.4.1.25070.1.1.1.2.0.1.1
Data de Emissão	28/08/2017
Validade	1 Ano
Localização	https://pki.multicert.com/index.html

2 Identificação e Autenticação

2.1 Atribuição de Nomes

A atribuição de nomes segue a convenção determinada pela DPC.

2.1.1 Tipos de nomes

O Certificado de Validação Cronológica é identificado por um nome único (DN – *Distinguished Name*) de acordo com *standard* X.500.

O nome único do certificado de Validação Cronológica é identificado pelos seguintes componentes:

Atributo	Código	Valor
Country	C	PT
Organization	O	MULTICERT - Serviços de Certificação Electrónica S.A.
Organization Unit	OU	Time Stamping Services
Serial Number	Serial Number	'nnnnnn'
Common Name	CN	MULTICERT Qualified Time Stamping Authority

2.2 Uso do certificado e par de chaves pelo titular

A MULTICERT é a titular do Certificado de Validação Cronológica, sendo o mesmo emitido para a Entidade de Validação Cronológica (EVC) da PKI da MULTICERT. A chave privada associada a este tipo de certificados é utilizada para assinar as respostas a pedidos de validações cronológicas[1] (aposição de selos temporais), garantindo e permitindo verificar a integridade e não-repúdio dessas mesmas respostas.

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

3 Perfil de Certificado

3.1 Perfil de Certificado

Os utilizadores de uma chave pública têm que ter confiança que a chave privada associada é detida pelo titular remoto correto (pessoa ou sistema) com o qual irão utilizar mecanismos de cifra ou assinatura digital. Essa confiança é dada através do uso de certificados digitais X.509 v3, que são 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.[2]

O utilizador de um serviço de segurança que requeira o conhecimento da chave pública do utilizador necessita, normalmente, de obter e validar o certificado que contém essa chave. Se o serviço não dispuser de uma cópia fidedigna da chave pública da EC que assinou o certificado, assim como do nome da EC e informação relacionada (tal como o período de validade), então poderá necessitar um certificado adicional para obter a chave pública da EC e validar a chave pública do utilizador. Em geral, para validar a chave pública de um utilizador pode ser necessária uma cadeia de múltiplos certificados, incluindo o certificado da chave pública do utilizador assinado por uma EC e, zero ou mais certificados adicionais de ECs assinados por outras ECs.[2]

O perfil dos Certificados de Validação Cronológica está de acordo com os standards referidos na secção "Referências Bibliográficas"

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 a 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.

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

Componente de Certificado		Secção na RFC 5280	Valor	Tipo	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
	Organization Unit (OU)		" MULTICERT Trust Services Provider"		Outra designação da organização do titular
	Common Name (CN)		"MULTICERT Trust Services Certification Authority <nnn>"		Nome da CA
	Validity	4.1.2.5		m	Validade do certificado TEM que utilizar tempo UTC até 2049, passando a partir daí a utilizar ***GeneralisedTime***
	Not Before		<data de emissão>		
	Not After		<data de emissão + 2375 dias>		Validade de aproximadamente 6 anos e meio. Utilizado para assinar objetos de tempo durante o primeiro mês de validade, sendo renovado (com geração de novo par de chaves) após o primeiro mês de validade.
	Subject	4.1.2.6		m	

Componente de Certificado		Secção na RFC 5280	Valor	Tipo	Comentários
	Country (C)		"PT"		
	Organization (O)		"MULTICERT - Serviços de Certificação Electrónica S.A."		
	Organization Unit (OU)		"Time Stamping Services"		Designação do tipo de certificado
	SerialNumber		"<nnnnnn>"		
	Common Name (CN)		"MULTICERT Qualified Time Stamping Authority"		
	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 ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(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.[3]
	subjectPublicKey		<Chave Pública com modulus n de 2048 bits>		

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

Componente de Certificado		Secção na RFC 5280	Valor	Tipo	Comentários
	X.509v3 Extensions	4.1.2.9		m	
	Authority Key Identifier	4.2.1.1		o	
	keyIdentifier		<O *key Identifier* é composto pela hash de 160-bit SHA-1 do valor da BIT STRING do *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 160-bit SHA-1 do valor da BIT STRING do *subjectPublicKey* (excluindo a tag, length, e número de bits não usado)>	m	
	Key Usage	4.2.1.3		mc	Esta extensão é marcada CRÍTICA. Confere o tipo de utilização do certificado.
	Digital Signature		"1" seleccionado		
	Non Repudiation		"1" seleccionado		
	Key Encipherment		"0" seleccionado		
	Data Encipherment		"0" seleccionado		
	Key Agreement		"0" seleccionado		
	Key Certificate Signature		"0" seleccionado		
	CRL Signature		"0" seleccionado		
	Encipher Only		"0" seleccionado		

Componente de Certificado		Secção na RFC 5280	Valor	Tipo	Comentários
	Decipher Only		"0" seleccionado		
	Certificate Policies	4.2.1.5		o	
	policyIdentifier		1.3.6.1.4.1.25070.1.1.1.2.0.7	m	Identificador da Declaração de Práticas de Certificação da MC TS CA.
	policyQualifiers		*policyQualifierID*: 1.3.6.1.5.5.7.2.1 *cPSuri*: http://ts4pki.multicert.com/pol/index.html	o	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." (http://www.alvestrand.no/objectid/submissions/1.3.6.1.5.5.7.2.1.html)
	policyIdentifier		1.3.6.1.4.1.25070.1.1.1.2.0.1.1	m	Identificador da Política de Certificados de Validação Cronológica.
	policyQualifiers		*policyQualifierID*: 1.3.6.1.5.5.7.2.1 *cPSuri*: "http://ts4pki.multicert.com/pol/index.html"	o	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 esta política. (http://www.alvestrand.no/objectid/submissions/1.3.6.1.5.5.7.2.2.html)
	Qualified Certificate Statement		id-pe-qcStatements= "1.3.6.1.5.5.7.1.3"[4]		A extensão QCStatements é uma extensão introduzida pelo PKIX Qualified Certificate Profile e ETSI[5]
	id-qcs-pkixQCSyntax-v2		Id-etsi-tsts-EuQCompliance="0.4.0.19422.1.1" Text= "By inclusion of this statement the issuer claims that		

[4] http://www.alvestrand.no/objectid/1.3.6.1.5.5.7.1.3.html
[5] cf. ETSI EN 319 422 - Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles

Componente de Certificado		Secção na RFC 5280	Valor	Tipo	Comentários
			this time-stamp token is issued as a qualified electronic time-stamp according to the REGULATION (EU) No 910/2014"		
	Basic Constraints	4.2.1.10		c	Esta extensão é marcada CRÍTICA.
	CA		FALSE		
	PathLenConstraint		0		
	Extended Key Usage	4.2.1.13			
	Client Authentication		1.3.6.1.5.5.7.3.8	c	Descrição do OID: *id-kp-timeStamping* indica que o certificado é utilizado para ligar um objeto a uma hora e data obtida de uma fonte fiável de tempo. Esta extensão TEM de ser crítica[1].
	CRLDistributionPoints	4.2.1.14		o	
	distributionPoint		http://pki.multicert.com/crl/crl_mtsca001.crl	o	URL para aceder à CRL
	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 do OCSP 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	URL para aceder ao OCSP

Componente de Certificado		Secção na RFC 5280	Valor	Tipo	Comentários
	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)} [3]
	Signature Value	4.1.1.3	<contains digital signature issued by the CA>	m	Ao gerar esta assinatura, a EC certifica a ligação entre a chave pública e o titular (*subject*) do certificado.

3.1.3 OID do Algoritmo

O campo "*signatureAlgorithm*" do certificado contém o OID do algoritmo criptográfico utilizado pela EC para assinar o certificado: "1.2.840.113549.1.1.11" (*sha-256WithRSAEncryption*[3]).

3.1.4 Formato dos Nomes

Tal como definido na secção 2.1

3.1.5 Condicionamento nos Nomes

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

3.1.6 OID da Política de Certificados

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

Os qualificadores opcionais ("*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*" e para o URI desta política, identificado pelo *policyIdentifier*.

3.1.7 Utilização da extensão *Policy Constraints*

Nada a assinalar.

3.1.8 Sintaxe e semântica do qualificador de política

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

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

Nada a assinalar.

Conclusão

Este documento rege-se pelo definido na Declaração de Praticas de Certificação da MC TS CA especificando o perfil de certificado de Validação Cronológica, emitido pela MULTICERT *Trust Services Certification Authority* (MC TS CA) no suporte à sua atividade de certificação digital. A hierarquia de confiança da MC TS CA encontra-se englobada na hierarquia de confiança da MULTICERT – PKI da MULTICERT:

- Fornece uma hierarquia de confiança, que promoverá a segurança eletrónica do titular do certificado no seu relacionamento com terceiras entidades,
- Proporciona a realização de transações eletrónicas seguras, a autenticação forte, um meio de assinar eletronicamente transações ou informações e documentos eletrónicos, assegurando a sua autoria, integridade e não repúdio, e assegurando a confidencialidade das transações ou informação.

Referências Bibliográficas

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

NIST FIPS PUB 180-2. 2002, *Secure Hash Standard, U. S. Department of Commerce, Technology Administration, National Institute of Standards and Technology*.

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

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

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

ETSI 319 421 - *Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps*

ETSI EN 319 422 - Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles

CWA 14167-1: *Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1: System Security Requirements*.

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

Aprovação

Renato Isaias Rodrigues Portela

Digitally signed by Renato Isaias Rodrigues Portela
Date: 2017.08.29 17:26:36 +01'00'

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

Digitally signed by [Assinatura Qualificada] MULTICERT - SERVIÇOS DE CERTIFICAÇÃO ELECTRÓNICA S.A.
Date: 2017.08.30 17:34:43 +01'00'