Política de Certificados de Validação Cronológica

Políticas

MULTICERT_PJ.CC_24.1.2_0007_pt_Root.doc

Identificação do Projecto: Cartão de Cidadão

Identificação da CA: Root

Nível de Acesso: Público

Versão: 1.0

Data: 07/09/2007

MULTICERT, Serviços de Certificação Electrónica, S.A.,
Polo Tecnológico de Lisboa, Sala 101, CID - Lote 1, 1600-546 Lisboa, Portugal
Telefone: +351 217 123 010 Facsimile: +351 217 123 011

Identificador do documento: MULTICERT_PJ.CC_24.1.2_0007_pt_Root.doc

Palavras-chave: Cartão de Cidadão, Política de Certificados, EC do Cidadão

Tipologia documental: Políticas

Título: Política de Certificados de Validação Cronológica

Língua original: Português

Língua de publicação: Português

Nível de acesso: Público

Data: 07/09/2007

Versão actual: 1.0

Identificação do Projecto: Cartão de Cidadão

Identificação da CA: Root

Cliente: Ministério da Justiça

Histórico de Versões

N.º de Versão	Data	Detalhes	Autor(es)
1.0	07/09/2007	Política de Certificados de Validação Cronológica	José Pina Miranda

Documentos Relacionados

ID Documento	Detalhes	Autor(es)
MULTICERT_PJ.CC_24.1.1_0001_pt_Root.doc	Declaração de Práticas de Certificação da EC do Cidadão	José Pina Miranda

Resumo Executivo

Decorrente da implementação de vários programas públicos 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 e do governo electrónico (*eGovernment*), o Cartão de Cidadão fornece os mecanismos necessários para a autenticação digital forte da identidade do Cidadão perante os serviços da Administração Pública, assim como as assinaturas electrónicas indispensáveis aos processos de desmaterialização que estão a ser disponibilizados pelo Estado.

A infra-estrutura da Entidade de Certificação do Cartão do Cidadão (ou Entidade de Certificação do Cidadão) fornece uma hierarquia de confiança, que promoverá a segurança electrónica do Cidadão no seu relacionamento com o Estado. A Entidade de Certificação do Cidadão 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 hierarquia de confiança da Entidade de Certificação do Cartão do Cidadão encontra-se englobada na hierarquia do Sistema de Certificação Electrónica do Estado Português[1] (SCEE) – Infra-Estrutura de Chaves Públicas do Estado.

Este documento define a Política de certificados utilizada na emissão do certificado de Validação Cronológica, que complementa e está de acordo com a Declaração de Práticas de Certificação da EC do Cidadão.[2]

[1] *cf.* SCEE 2.16.620.1.1.1.2.1.1.0. 2006, Política de Certificados da SCEE e Requisitos mínimos de Segurança.
[2] *cf.* MULTICERT_PJ.CC_24.1.1_0001_pt_Root.doc. 2007, Declaração de Práticas de Certificação da EC do Cidadão.

Sumário

Resumo Executivo 3

Sumário 4

Introdução 5

1 Introdução 6

1.1 Visão Geral 6
1.2 Designação e Identificação do Documento 6
2 Identificação e Autenticação 7

2.1 Atribuição de Nomes 7
2.1.1 Tipos de nomes 7
2.2 Uso do certificado e par de chaves pelo titular 7
3 Perfil de Certificado 8

3.1 Perfil de Certificado 8
3.1.1 Número da Versão 8
3.1.2 Extensões do Certificado 8
3.1.3 OID do Algoritmo 13
3.1.4 Formato dos Nomes 13
3.1.5 Condicionamento nos Nomes 13
3.1.6 OID da Política de Certificados 13
3.1.7 Utilização da extensão Policy Constraints 13
3.1.8 Sintaxe e semântica do qualificador de política 13
3.1.9 Semântica de processamento para a extensão crítica Certificate Policies 13
Conclusão 14

Referências Bibliográficas 15

Introdução

Objectivos

O objectivo deste documento é definir as políticas utilizadas na emissão do certificado de Validação Cronológica, pela Entidade de Certificação do Cartão do Cidadão (EC do Cidadão).

Público-Alvo

Este documento deve ser lido por:

- Recursos humanos atribuídos aos grupos de trabalho da EC do Cidadão,
- Terceiras partes encarregues de auditar a EC do Cidadão,
- 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 do Cidadão[2], presumindo-se que o leitor leu integralmente o seu conteúdo antes de iniciar a leitura deste documento.

1 Introdução

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

Este documento descreve a política de certificados para a emissão e gestão do certificado de Validação Cronológica, emitido pela EC do Cidadão.

Os Certificados emitidos pela EC CC 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 do Cidadão[2].

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 o 2.16.620.1.1.1.2.4.0.1.7.

Este documento é identificado pelos dados constantes na seguinte tabela:

INFORMAÇÃO DO DOCUMENTO	
Versão do Documento	Versão 1.0
Estado do Documento	Aprovado
OID	2.16.620.1.1.1.2.4.0.1.7
Data de Emissão	26-Jan-2007
Validade	Não aplicável
Localização	http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_timestamp_pc.html

2 Identificação e Autenticação

2.1 Atribuição de Nomes

A atribuição de nomes segue a convenção determinada pelo SCEE[1] e pela DPC da EC do Cidadão[2].

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 da EC do Cidadão é identificado pelos seguintes componentes:

Atributo	Código	Valor
Country	C	PT
Organization	O	Cartão de Cidadão
Organization Unit	OU	Serviços do Cartão de Cidadão
Organization Unit	OU	Validação Cronológica
Common Name	CN	Serviço de Validação Cronológica do Cartão de Cidadão <nnnnnn>[3]

2.2 Uso do certificado e par de chaves pelo titular

A EC do Cidadão é a titular do certificado de Validação cronológica, sendo o mesmo emitido para o servidor de validação cronológica da EC do Cidadão. A chave privada associada a este tipo de certificados é utilizada para assinar as respostas a pedidos de validações cronológicas[4], garantindo e permitindo verificar a integridade e não-repúdio dessas mesmas respostas.

[3] <nnnnnn> é um valor sequencial iniciado em "000001" na emissão do primeiro certificado deste tipo.
[4] *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 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 em qualquer tipo de unidades de armazenamento.[5]

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.[5]

O perfil do certificado de Validação Cronológica está de acordo com:

- Recomendação ITU.T X.509[6],
- RFC 3280[5], e
- Política de Certificados da SCEE[1].

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.

[5] cf. RFC 3280. 2002, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
[6] cf. ITU-T Recommendation X.509. 1997, (1997 E): Information Technology - Open Systems Interconnection – The Directory: Authentication Framework.

Cerificate Component		Section in RFC 3280	Value	Field Type	Comments
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)		"SCEE – Sistema de Certificação Electrónica do Estado"		
	Organization Unit (OU)		" ECEstado"		
	Common Name (CN)		"Cartão de Cidadão <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 + 1.900 dias>		Validade de aproximadamente 5 anos e dois meses. Utilizado para assinar objectos 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	
	Country (C)		"PT"		
	Organization (O)		"Cartão de Cidadão"		
	Organization Unit (OU)		"Serviços do Cartão de Cidadão"		

	Organization Unit (OU)		"Validação Cronológica"		
	Common Name (CN)		"Serviço de Validação Cronológica do Cartão de Cidadão <nnnnnn>"		
	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.[7]
	subjectPublicKey		<Chave Pública com modulus n de 2048 bits>		
	X.509v3 Extensions	4.1.2.9		m	
	Authority Key Identifier	4.2.1.1		o	
	keyIdentifier		<O key Identifier é composto pela hash de 160-bit SHA-1 do valor da BIT STRING do subject key identifier 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.

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

	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		
	Decipher Only		"0" seleccionado		
	Certificate Policies	4.2.1.5		o	
	policyIdentifier		2.16.620.1.1.1.2.4.0.7	m	Identificador da Declaração de Práticas de Certificação da EC CC.
	policyQualifiers		policyQualiflierID: 1.3.6.1.5.5.7.2.1 cPSuri: http://pki.cartaodecidadao.pt/publico/politicas/dpc/cc_ec_cidadao_dpc.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		2.16.620.1.1.1.2.4.0.1.7	m	Identificador da Política de Certificados de Validação Cronológica.
	policyQualifiers		policyQualiflierID: 1.3.6.1.5.5.7.2.2 userNotice explicitText: "http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_timestamp_pc.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	4.2.1.10		c	Esta extensão é marcada CRÍTICA.
	CA		FALSE		
	PathLenConstraint		0		
	Extended Key Usage	4.2.1.13	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 objecto a uma hora e data obtida de uma fonte fiável de tempo. Esta extensão TEM de ser crítica[4].
	CRLDistributionPoints	4.2.1.14		o	
	distributionPoint		http://pki.cartaodecidadao.pt /publico/lrc/cc_ec_cidadao_crl<ID_CA>_crl.crl	o	
	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.root.cartaodecidadao.pt/publico/ocsp	o	
	Signature Algorithm	4.1.1.2	1.2.840.113549.1.1.5	m	TEM que conter o mesmo OID do identificador do algoritmo do campo signature no campo da sequência tbsCertificate. sha-1WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 }[7]
	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: 1.2.840.113549.1.1.5 (sha-1WithRSAEncryption[8])[7].

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 Directório 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*". 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).

3.1.7 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, o "*userNotice explicitText*" que contém um apontador, na forma de URI, para a Politica de Certificados.

3.1.9 Semântica de processamento para a extensão crítica Certificate Policies

Nada a assinalar.

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

Conclusão

Este documento define as Políticas de Certificados do certificado de Validação Cronológica, utilizada pela Entidade de Certificação do Cartão do Cidadão no suporte à sua actividade de certificação digital. A hierarquia de confiança da Entidade de Certificação do Cartão do Cidadão encontra-se englobada na hierarquia do Sistema de Certificação Electrónica do Estado Português (SCEE) – Infra-Estrutura de Chaves Públicas do Estado:

- fornecendo uma hierarquia de confiança, que promoverá a segurança electrónica do Cidadão no seu relacionamento com o Estado
- proporcionando 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 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 3280. 2002, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

SCEE 2.16.620.1.1.1.2.1.1.0. 2006, Política de Certificados da SCEE e Requisitos mínimos de Segurança.