Política de Certificado de Autenticação

Políticas

PJ.CC_24.1.2_0011_pt_AuC.pdf

Identificação do Projecto: Cartão de Cidadão

Identificação da CA: AuC

Nível de Acesso: Público

Versão: 1.2

Data: 28/06/2012

Identificador do documento: PJ.CC_24.1.2_0011_pt_AuC.pdf

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

Tipologia documental: Políticas

Título: Política de Certificado de Autenticação

Língua original: Português

Língua de publicação: Português

Nível de acesso: Público

Data:28/06/2012

Versão actual: 1.2

Identificação do Projecto: Cartão de Cidadão

Identificação da CA: AuC

Cliente: Ministério da Justiça

Documentos Relacionados

ID Documento	Detalhes	Autor(es)
PJ.CC_24.1.1_0003_pt_AuC.pdf	Declaração de Práticas de Certificação da EC de Autenticação do Cartão de Cidadão	MULTICERT S.A.

Apêndices

ID Documento	Detalhes	Autor(es)
PJ.CC_53.2.1_0006_pt_AuC.doc	Formulário de emissão de certificado "espécimen" de Autenticação	MULTICERT S.A.

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 de Cidadão (ou Entidade de Certificação de 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 de Cidadão encontra-se englobada na hierarquia do Sistema de Certificação Electrónica do Estado Português[1] (SCEE) – Infra-Estrutura de Chaves Públicas do Estado.

Assim, a EC AuC não é detentora de uma Política de Certificados, sendo que a emissão de certificados segue as orientações constantes na Política de Certificados do SCEE.

É ainda apresentado neste documento o perfil de Certificado de Autenticação do Cartão de Cidadão emitidos pela EC AuC, em complemento das secções 3 e 7 da Política de Certificados do SCEE.

[1] *cf.* SCEE 2.16.620.1.1.1.2.1.1.0. 2006, Política de Certificados da SCEE e Requisitos mínimos de Segurança.

Sumário

Introdução

Objectivos

O objectivo deste documento apresentar o perfil do certificado de Autenticação emitido pela Entidade de Certificação de Autenticação do Cartão de Cidadão (EC AuC).

Público-Alvo

Este documento deve ser lido por:

– Recursos humanos atribuídos aos grupos de trabalho da EC AuC;

– Terceiras partes, encarregues de auditar a EC AuC;

– 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 de Autenticação do Cartão de Cidadão[2].

[2] *cf.* PJ.CC_24.1.1_0003_pt_AuC.doc. 2007, Declaração de Práticas de Certificação da EC de Autenticação do Cartão de Cidadão.

1 Contexto Geral

O presente documento tem como objectivo a definição de um conjunto parâmetros que definem o perfil dos Certificados de Autenticação emitidos pela Entidade de Certificação de Autenticação do Cartão de Cidadão (EC AuC), permitindo assim garantir a fiabilidade dos mesmos. 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.

Os certificados emitidos pela EC AuC contêm uma referência ao PC de modo a permitir que partes confiantes e outras entidades ou 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 de Autenticação do Cartão de Cidadão[2].

1.2 Designação e Identificação do Documento

Este documento é a Política de Certificados do certificado de Autenticação. 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 "2.16.620.1.1.1.2.4.2.0.1.1".

Este documento é identificado pelos dados constantes na seguinte tabela:

INFORMAÇÃO DO DOCUMENTO	
Versão do Documento	Versão 1.2
Estado do Documento	Aprovado
OID	2.16.620.1.1.1.2.4.2.0.1.1
Data de Emissão	28/Jun/2012
Validade	Não aplicável
Localização	http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_sub-ec_cidadao_autenticacao_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 de Autenticação do Cartão de Cidadão[2].

2.1.1 Tipos de nomes

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

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

Atributo	Código	Valor
Country	C	PT
Organization	O	Cartão de Cidadão
Organization Unit	OU	Cidadão Português
Organization Unit	OU	Autenticação do Cidadão
Common Name	CN	<concatenação do *givenName* e *SN* do Cidadão>
Surname	SN	<nome de família do Cidadão>
Given Name	givenName	<parte do nome do Cidadão que não é o nome de família nem os nomes intermédios>
Serial Number	serialNumber	<identificador único do Cidadão>

2.2 Uso do certificado e par de chaves pelo titular

O Cidadão (pessoa singular) identificado pelo *Distinguished Name* é o titular do Certificado de Autenticação. O certificado emitido segundo esta política é utilizado em qualquer aplicação para efeitos de autenticação do Cidadão.

3 Perfis 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. 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 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.[3]

O utilizador de um serviço de segurança que requeira o conhecimento da chave pública do utilizador necessita, normalmente, de obter e validar o certificado que contém essa chave. Se o serviço não dispuser de uma cópia fidedigna da chave pública da EC que assinou o certificado, assim como do nome da EC e informação relacionada (tal como o período de validade), então poderá necessitar um certificado adicional para obter a chave pública da EC e validar a chave pública do utilizador. Em geral, para validar a chave pública de um utilizador pode ser necessária uma cadeia de múltiplos certificados, incluindo o certificado da chave pública do utilizador assinado por uma EC e, zero ou mais certificados adicionais de ECs assinados por outras ECs.[3]

O perfil do certificado de Autenticação está de acordo com:

- Recomendação ITU.T X.509[4];
- RFC 5280[3] 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] cf. RFC 5280. 2008, Internet X.509 *Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.
[4] cf. ITU-T *Recommendation* X.509. 1997, (1997 E): *Information Technology - Open Systems Interconnection – The Directory: Authentication Framework*.

3.1.2 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.

Componente do Certificado		Secção no RFC 3280	Valor	Tipo[5]	Comentários
tbsCertificate	**Version**	4.1.2.1	v3	m	
	Serial Number	4.1.2.2	<atribuído pela EC a cada certificado>	m	
	Signature	4.1.2.3	1.2.840.113549.1.1.5	m	Valor TEM que ser igual ao OID no *signatureAlgorithm* (abaixo)
	Issuer	4.1.2.4		m	
	Country (C)		"PT"		
	Organization (O)		"Cartão de Cidadão"		
	Organization Unit (OU)		"subECEstado"		
	Common Name (CN)		"EC de Autenticação do Cartão de Cidadão <nnnn>"		
	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 + 5 anos>		
	Subject	4.1.2.6		m	
	Country (C)		"PT"		
	Organization (O)		"Cartão de Cidadão"		

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

	Organization Unit (OU)		"Cidadão Português"		
	Organization Unit (OU)		" Autenticação do Cidadão "		
	Common Name (CN)		<concatenação do *givenName* e SN do cidadão>		
	Surname (SN)		<nome de familia do cidadão>		
	Given Name (givenName)		<nome(s) próprio do cidadão>		
	Serial Number (serialNumber)		<ID do cidadão>		
	Subject Public Key Info	4.1.2.7		m	Utilizado para conter a chave pública e identificar o algoritmo com o qual a chave é utilizada (e.g., RSA, DSA ou Diffie-Hellman)
	algorithm		1.2.840.113549.1.1.1		O OID rsaEncryption identifica chaves públicas RSA. pkcs-1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 1 } rsaEncryption OBJECT IDENTIFIER ::= { pkcs-1 1} O OID rsaEncryption deve ser utilizado no campo algorithm com um valor do tipo AlgorithmIdentifier. Os parâmetros do campo TÊM que ter o tipo ASN.1 a NULL para o identificador deste algoritmo.[6]
	subjectPublicKey		<Chave Pública com modulus n de 1024 bits>		
	X.509v3 Extensions	4.1.2.9		m	
	Authority Key Identifier	4.2.1.1		o	

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

	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.
	Digital Signature		"1" seleccionado		
	Non Repudiation		"0" seleccionado		
	Key Encipherment		"0" seleccionado		
	Data Encipherment		"0" seleccionado		
	Key Agreement		"1" 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		2.16.620.1.1.1.2.20	m	scee-autenticacao[1]

	policyQualifiers		policyQualiflierID: 1.3.6.1.5.5.7.2.1 cPSuri: http://www.scee.gov.pt/pcert		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)
	policyQualifiers		policyQualiflierID: 1.3.6.1.5.5.7.2.2 userNotice explicitText: "O certificado emitido segundo esta política é utilizado para autenticação do Cidadão"		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)
	policyIdentifier		2.16.620.1.1.1.2.4.2.0.7	m	Identificador da Declaração de Práticas de Certificação da EC AuC.
	policyQualifiers		policyQualiflierID: 1.3.6.1.5.5.7.2.1 cPSuri: http://pki.cartaodecidadao.pt/publico/politicas/dpc/cc_sub-ec_cidadao_autenticacao_dpc.html	o	
	policyIdentifier		2.16.620.1.1.1.2.4.2.0.1.1	m	Identificador da Política de Certificados de Autenticação.
	policyQualifiers		policyQualiflierID: 1.3.6.1.5.5.7.2.1 cPSuri: "http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_sub-ec_cidadao_autenticacao_pc.html"	o	
	Basic Constraints	4.2.1.10		c	Esta extensão é marcada CRÍTICA.
	CA		FALSE		
	PathLenConstraint		0		

	CRLDistributionPoints	4.2.1.14		o	
	distributionPoint		http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_autenticacao_crl<ID_CA>_p<num_seq>.crl	o	
	Freshest CRL	4.2.1.16		o	
	distributionPoint		http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_autenticacao_crl<ID_CA>_delta_p<num_seq>.crl	o	
	Netscape Certificate Type	-	SSL Client Authentication = 1 S/MIME = 1	o	Não é uma extensão definida no RFC 3280. Definida em http://www.redhat.com/docs/manuals/cert-system/admin/app_ext.htm.
	Subject Directory Attributes	-		o	
	dateOfBirth		<data de nascimento do cidadão>		Não é uma extensão definida no RFC 3280. Esta extensão PODE conter atributos adicionais associados com o titular do certificado, como complemento à informação presente no campo subject e na extensão subject alternative name. (http://www.alvestrand.no/objectid/submissions/2.5.29.9.html)
	Internet Certificate Extensions				
	Authority Information Access	4.2.2.1		o	
	accessMethod		1.3.6.1.5.5.7.48.1	o	Valor do OID: 1.3.6.1.5.5.7.48.1 (id-ad-ocsp) Descrição do OID: Online Certificate Status Protocol
	accessLocation		http://ocsp.auc.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 }[6]
	Signature Value	4.1.1.3	<contém a assinatura digital emitida pela EC>	m	Ao gerar esta assinatura, a EC certifica a ligação entre a chave pública e o titular (subject) do certificado.

3.1.3 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*[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 ("*policyQualiflierID*: 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 ("*policyQualiflierID*: 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, assim como a indicação explicita dos fins para os quais este certificado deverá ser utilizado.

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

3.1.9 Semântica de processamento para a extensão crítica Certificate Policies

Nada a assinalar.

3.2 Certificado “espécimen”

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

- Perfil de certificado: é adicionado o prefixo “(espécimen) “ ao *CommonName* (CN);
- Perfil de certificado: o atributo serialNumber é formado por “especimen” seguido de um número sequencial (que começa em 0000001);
- Emissão do certificado: de acordo com formulário específico[8];
- Revogação do certificado: o certificado é revogado imediatamente após a sua emissão[8].

[8] *cf.* PJ.CC_53.2.1_0006_pt_AuC.doc. 2007, Formulário de emissão de certificado "espécimen" de Autenticação.

Conclusão

Este documento rege-se pelo definido na Política de Certificados do SCEE especificando o perfil dos certificados de Autenticação, emitidos pela Entidade de Certificação de Autenticação do Cartão de Cidadão no suporte à sua actividade de certificação digital. A hierarquia de confiança da Entidade de Certificação de Autenticação do Cartão de 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 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*.

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

Aprovação do Conselho Gestor

ANTÓNIO MANUEL MARTINS DA CRUZ	Assinado de forma digital por ANTÓNIO MANUEL MARTINS DA CRUZ DN: cn=ANTÓNIO MANUEL MARTINS DA CRUZ, serialNumber=BI103203710, givenName=ANTÓNIO MANUEL, sn=MARTINS DA CRUZ, ou=Assinatura Qualificada do Cidadão, ou=Cidadão Português, o=Cartão de Cidadão, c=PT Dados: 2012.06.28 22:50:49 +01'00'

GONÇALO NUNO MENDES DE ALMEIDA CASEIRO	Assinado de forma digital por GONÇALO NUNO MENDES DE ALMEIDA CASEIRO DN: c=PT, o=Cartão de Cidadão, ou=Cidadão Português, ou=Assinatura Qualificada do Cidadão, sn=MENDES DE ALMEIDA CASEIRO, givenName=GONÇALO NUNO, serialNumber=BI116298120, cn=GONÇALO NUNO MENDES DE ALMEIDA CASEIRO Dados: 2012.07.02 11:57:13 +01'00'

José António Alves Rodrigues	Assinado de forma digital por José António Alves Rodrigues DN: givenName=José António, sn=Alves Rodrigues, title=Especialista de Informática, c=PT, o=MJ, ou=ITIJ, ou=DIEAS, cn=José António Alves Rodrigues Dados: 2012.06.29 17:29:19 +01'00'

João Pedro Monteiro Rodrigues	Assinado de forma digital por João Pedro Monteiro Rodrigues DN: c=PT, o=Ministério da Justiça, ou=Instituto dos Registos e do Notariado IP, cn=João Pedro Monteiro Rodrigues Dados: 2012.07.02 14:48:05 +01'00'