

Política de Certificados de Autenticação

Políticas

MULTICERT_PJ.CC_24.1.2_0011_pt_AuC.doc

Identificação do Projecto: Cartão de Cidadão

Identificação da CA: AuC

Nível de Acesso: Público

Versão: 1.0

Data: 17/08/2007

Aviso Legal Copyright © 2007 MULTICERT — Serviços de Certificação Electrónica, S.A. (MULTICERT)

Todos os direitos reservados: a MULTICERT detém todos os direitos de propriedade intelectual sobre o conteúdo do presente documento ou foi devidamente autorizada a utilizá-los. As marcas constantes deste documento são utilizadas apenas para identificar produtos e serviços e encontram-se sujeitas às regras de protecção legalmente previstas. Nenhuma parte deste documento poderá ser fotocopiada, reproduzida, guardada, traduzida ou transmitida a terceiros, seja por que meio, sem o consentimento prévio por escrito da MULTICERT. Igualmente, o Cliente deverá garantir que não utilizará fora do âmbito Cartão de Cidadão ou transmitirá a terceiras entidades o "know-how" e as metodologias de trabalho apresentadas pela MULTICERT.

Confidencialidade

As informações contidas em todas as páginas deste documento, incluindo conceitos organizacionais, constituem informações sigilosas comerciais ou financeiras e confidenciais ou privilegiadas e são propriedade da MULTICERT. São fornecidas ao Cliente de forma fiduciária, com o conhecimento de que não serão utilizadas nem divulgadas, sem autorização da MULTICERT, para outros fins que não os Cartão de Cidadão e nos termos que venham a ser definidos nos projecto final. O cliente poderá permitir a determinados colaboradores, consultores e agentes que tenham necessidade de conhecer o conteúdo deste documento, ter acesso a este conteúdo, mas tomará as devidas providências para garantir que as referidas pessoas e entidades se encontram obrigados pela obrigação do cliente a mantê-lo confidencial.

As referidas restrições não limitam o direito de utilização ou divulgação das informações constantes do presente documento por parte do Ministério da Justiça, quando obtidos por outra fonte não sujeita a reservas ou que previamente ao seu fornecimento, já tenha sido legitimamente divulgada por terceiros.

Identificador do documento: MULTICERT_PJ.CC_24.1.2_0011_pt_AuC.doc

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

Tipologia documental: Políticas

Título: Política de Certificados de Autenticação

Língua original: Português

Língua de publicação: Português

Nível de acesso: Público

Data: 17/08/2007

Versão actual: 1.0

Identificação do Projecto: Cartão de Cidadão

Identificação da CA: AuC

Cliente: Ministério da Justiça

Histórico de Versões

N.º de Versão	Data	Detalhes	Autor(es)
<u>1.0</u>	<u>17/08/2007</u>	<u>Versão inicial</u>	<u>José Pina Miranda</u>

Documentos Relacionados

ID Documento	Detalhes	Autor(es)
MULTICERT_PJ.CC_24.1.1_0003_pt_AuC.doc	Declaração de Práticas de Certificação da EC de Autenticação do Cartão de Cidadão	José Pina Miranda

Apêndices

ID Documento	Detalhes	Autor(es)
MULTICERT_PJ.CC_53.2.1_0006_pt_AuC.doc	Formulário de emissão de certificado "espécimen" de Autenticação	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 Português¹ (SCEE) – Infra-Estrutura de Chaves Públicas do Estado.

Este documento define a Política de certificados utilizada na emissão do certificado de Autenticação, que complementa e está de acordo com a Declaração de Práticas de Certificação da EC de Autenticação do Cartão de Cidadão², presumindo-se que o leitor leu integralmente o seu conteúdo antes de iniciar a leitura deste documento.

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_0003_pt_AuC.doc. 2007, Declaração de Práticas de Certificação da EC de Autenticação do Cartão de Cidadão.

Sumário

Resumo Executivo	3
Sumário.....	4
Introdução.....	5
I Contexto Geral	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 Perfis de Certificado e LRC.....	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.....	15
3.1.4 Formato dos Nomes.....	15
3.1.5 Condicionamento nos Nomes.....	15
3.1.6 OID da Política de Certificados.....	15
3.1.7 Utilização da extensão Policy Constraints	15
3.1.8 Sintaxe e semântica do qualificador de política.....	15
3.1.9 Semântica de processamento para a extensão crítica Certificate Policies.....	15
3.2 Certificado “espécimen”	16
3.3 Perfil da lista de revogação de certificados	16
3.3.1 Número da Versão.....	16
3.3.2 Extensões da LRC Base da EC AuC.....	17
3.3.3 Extensões da Delta LRC da EC AuC	20
Conclusão.....	23
Referências Bibliográficas.....	24

Introdução

Objectivos

O objectivo deste documento é definir as políticas utilizadas na emissão do certificado de Autenticação, 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.

I Contexto Geral

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 Autenticação, emitido pela Entidade de Certificação de Autenticação do Cartão de Cidadão (EC AuC).

Os Certificados emitidos pela EC AuC 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.

I.1 Visão Geral

Esta PC satisfaz e complementa os requisitos impostos pela Declaração de Práticas de Certificação da EC de Autenticação do Cartão de Cidadão².

I.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 1.0
Estado do Documento	Aprovado
OID	2.16.620.1.1.1.2.4.2.0.1.1
Data de Emissão	26-Jan-2007
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 SCEE¹ e pela DPC da EC de Autenticação do Cartão de Cidadão².

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 <i>givenName</i> e <i>SN</i> do Cidadão>
Surname	SN	<nome de família do Cidadão>
Given Name	<i>givenName</i>	<parte do nome do Cidadão que não é o nome de família nem os nomes intermédios>
Serial Number	<i>serialNumber</i>	<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 e LRC

3.1 Perfil de Certificado

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

Um certificado tem um período limitado de validade, indicado no seu conteúdo e assinado pela EC. Como a assinatura do certificado e a sua validade podem ser verificadas independentemente por qualquer software que utilize certificados, os certificados podem ser distribuídos através de linhas de comunicação e sistemas públicos, assim como podem ser guardados 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.509⁴,
- RFC 3280³, e
- Política de Certificados da SCEE¹.

3.1.1 Número da Versão

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

3.1.2 Extensões do Certificado

As componentes e as extensões definidas para os certificados X.509 v3 fornecem métodos para associar atributos a utilizadores ou chaves públicas, assim como para gerir a hierarquia de certificação.

³ cf. RFC 3280. 2002, 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.

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 <i>signatureAlgorithm</i> (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"		

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 (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)		<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		policyQualifierID: 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		policyQualifierID: 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		policyQualifierID: 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		policyQualifierID: 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>.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.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) rsads(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: 1.2.840.1.13549.1.1.5 (sha-1WithRSAEncryption⁷).

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 (“*policyQualifierID*: 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 (“*policyQualifierID*: 1.3.6.1.5.5.7.2.2” e “*userNotice explicitText*”) apontam para o URI onde pode ser encontrados a Política 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 Política de Certificados, assim como a indicação explícita dos fins para os quais este certificado deverá ser utilizado.

3.1.9 Semântica de processamento para a extensão crítica Certificate Policies

Nada a assinalar.

⁷ sha-1WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsdsi(1.13549) pkcs(1) pkcs-1(1) 5

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 específico⁸;
- Revogação do certificado: o certificado é revogado imediatamente após a sua emissão⁸.

3.3 Perfil da lista de revogação de certificados

Quando um certificado é emitido, espera-se que seja utilizado durante todo o seu período de validade. Contudo, várias circunstâncias podem causar que um certificado se torne inválido antes da expiração do seu período de validade. Tais circunstâncias incluem a mudança de nome, mudança de associação entre o titular e os dados do certificado (por exemplo, um trabalhador que termina o emprego) e, o compromisso ou suspeita de compromisso da chave privada correspondente. Sob tais circunstâncias, a EC tem que revogar o certificado.³

O protocolo X.509 define um método de revogação do certificado, que envolve a emissão periódica, pela EC, de uma estrutura de dados assinada, a que se dá o nome de Lista de Revogação de Certificados (LRC). A LRC é uma lista com identificação temporal dos certificados revogados, assinada pela EC e disponibilizada livremente num repositório público. Cada certificado revogado é identificado na LRC pelo seu número de série. Quando uma aplicação utiliza um certificado (por exemplo, para verificar a assinatura digital de um utilizador remoto), a aplicação verifica a assinatura e validade do certificado, assim como obtém a LRC mais recente e verifica se o número de série do certificado não faz parte da mesma. Note-se que uma EC emite uma nova LRC numa base regular periódica.³

O perfil da LRC está de acordo com:

- Recomendação ITU.T X.509⁴,
- RFC 3280³, e
- Política de Certificados da SCEE¹.

3.3.1 Número da Versão

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

⁸ cf. MULTICERT_PJ.CC_53.2.1_0006_pt_AuC.doc. 2007, Formulário de emissão de certificado “espécimen” de Autenticação.

3.3.2 Extensões da LRC Base da EC AuC

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

Componente da Lista de Revogação de Certificados	Secção no RFC 3280	Valor	Tipo	Comentários	
tbsCertList	Version	5.1.2.1	1	m	Versão v2 (o valor inteiro é 1)
	Signature	5.1.2.2	1.2.840.113549.1.1.5	m	Contém o identificador do algoritmo utilizado para assinar a LRC. O valor TEM que ser igual ao OID no campo signatureAlgorithm (abaixo)
	Issuer	5.1.2.3		m	
	Country (C)		"PT"		
	Organization (O)		"Cartão de Cidadão"		
	Organization Unit (OU)		"subECEstado"		
	Common Name (CN)		"EC de Autenticação do Cartão de Cidadão <nnnn>"		
	thisUpdate	5.1.2.4	<data de emissão da LRC>	m	Implementações TÊM que utilizar o tempo UTC até 2049, e a partir dessa data devem utilizar o GeneralisedTime.
	nextUpdate	5.1.2.5	<data da próxima emissão da LRC = <i>thisUpdate</i> + N>	m	Este campo indica a data em que a próxima LRC vai ser emitida. A próxima LRC pode ser emitida antes da data indicada, mas não será emitida depois dessa data. Os emissores da CRL DEVEM emitir CRL com o tempo de nextUpdate maior ou igual a todas as LRC anteriores. Implementações TÊM que utilizar o tempo UTC até 2049, e a partir dessa data devem utilizar o GeneralisedTime. N será no máximo 1 semana ¹ .
	revokedCertificates	5.1.2.6	<lista de certificados revogados>	m	

CRL Extensions	5.1.2.7		m	
Authority Key Identifier	5.2.1		o	
keyIdentifier		<O key Identifier é composto pela hash de 160-bit SHA-1 do valor da BIT STRING do subject key identifier do certificado do emissor (excluindo a tag, length, e número de bits não usado)>	m	
CRL Number	5.2.3	<número sequencial único e incrementado>	m	
Freshest CRL	5.2.6		o	
distributionPoint		http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_autenticacao_crl<ID_CA>_delta.crl	o	
CRL Entry Extensions	5.3			
Reason Code	5.3.1		o	Valor tem que ser um dos seguintes: 1 – keyCompromise 2 – cACompromise 3 – affiliationChanged 4 – superseded 5 – cessationOfOperation 6 – certificateHold 8 – removeFromCRL 9 – privilegeWithdrawn 10 - aACompromise

	Signature Algorithm	5.1.1.2	1.2.840.113549.1.1.5	m	TEM que conter o mesmo OID do identificador do algoritmo utilizado no campo signature da sequência tbsCertList. sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 } ⁶
	Signature Value	5.1.1.3	<contém a assinatura digital emitida pela EC>	m	Contém a assinatura digital calculada sobre a tbsCertList.

3.3.3 Extensões da Delta LRC da EC AuC

Certificate Revocation List Component		Section in RFC 3280	Value	Field Type	Comments
tbsCertList	Version	5.1.2.1	1	m	Version V2 (the integer value is 1)
	Signature	5.1.2.2	1.2.840.113549.1.1.5	m	Contains the algorithm identifier for the algorithm used to sign the CRL. Value MUST match the OID in signatureAlgorithm (below)
	Issuer	5.1.2.3		m	
	Country (C)		"PT"		
	Organization (O)		"Cartão de Cidadão"		
	Organization Unit (OU)		"subECEstado"		
	Common Name (CN)		"EC de Autenticação do Cartão de Cidadão <nnnnnnnn>"		
	thisUpdate	5.1.2.4	<update date>	m	Implementations MUST specify using UTC time until 2049, from then on using GeneralisedTime
	nextUpdate	5.1.2.5	<next update date = update date + N>	m	This field indicates the date by which the next CRL will be issued. The next CRL could be issued before the indicated date, but it will not be issued any later than the indicated date. CRL issuers SHOULD issue CRLs with a nextUpdate time equal to or later than all previous CRLs. Implementations MUST specify using UTC time until 2049, from then on using GeneralisedTime. N is at most 1 day.
	revokedCertificates	5.1.2.6	<revoked certificates list>	m	

CRL Extensions	5.1.2.7		m	
Authority Key Identifier	5.2.1		o	
keyIdentifier		<The key Identifier is composed of the 160-bit SHA-1 hash of the value of the BIT STRING subject key identifier in the CRL issuer's certificate (excluding the tag, length, and number of unused bits)>	m	
CRL Number	5.2.3	<increasing sequence number>	m	If a CRL issuer generates delta CRLs in addition to complete CRLs for a given scope, the complete CRLs and delta CRLs MUST share one numbering sequence. Given the requirements above, CRL numbers can be expected to contain long integers. CRL verifiers MUST be able to handle CRLNumber values up to 20 octets. Conforming CRL issuers MUST NOT use CRLNumber values longer than 20 octets.
Delta CRL Indicator	5.2.4	<base CRL number>	c	This CRL number identifies the complete base CRL that was used as the starting point in the generation of this delta CRL.
CRL Entry Extensions	5.3			

	Reason Code	5.3.1		o	Value must be one of the followings: <ul style="list-style-type: none"> 1 – keyCompromise 2 – cACompromise 3 – affiliationChanged 4 – superseded 5 – cessationOfOperation 6 – certificateHold 8 – removeFromCRL 9 – privilegeWithdrawn 10 - aACompromise
	Signature Algorithm	5.1.1.2	1.2.840.113549.1.1.5	m	MUST contain the same OID algorithm identifier as the signature field in the sequence tbsCertificate. sha-1WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsads(113549) pkcs(1) pkcs-1(1) 5 } ⁶
	Signature Value	5.1.1.3	<contains digital signature issued by the CA>	m	Contains a digital signature computed upon the tbsCertList. The CA certificate is used to digitally sign certificates and CRLs.

Conclusão

Este documento define as Políticas de Certificados do certificado de Autenticação, utilizada 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 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.