

Política de Certificados da EC de Autenticação do Cartão de Cidadão

Políticas (POL#24)

Nível de Acesso: Público

Versão: 3.0

Data: Julho 2024

Identificador do Documento: POL#24

Palavras-chave: PKI CC, Cartão de Cidadão, Política de Certificado

Tipologia Documental: Políticas

Título: Política de Certificados da EC de Autenticação do Cartão de Cidadão

Nível de acesso: Público

Autor: IRN - Instituto dos Registos e Notariado, I.P.

Data: Julho 2024

Versão atual: 3.0

Validade do Documento: 2 (dois) anos após a sua aprovação.

Histórico de Versões

Versão	Data	Detalhes
1.0	Fev 2022	Versão que incorpora todos os certificados emitidos pela EC de Autenticação.
2.0	Mar 2024	Alteração dos algoritmos de assinatura dos certificados emitidos pela EC de Autenticação do Cartão de Cidadão
3.0	Julho 2024	Inclusão da preposição “até” na validade do certificado de autenticação.

Documentos Relacionados

Documento	Autor	Descrição
Declaração de Práticas de Certificação da EC de Autenticação do Cartão de Cidadão (POL#29)	IRN	Descreve os procedimentos e práticas utilizados pela EC de Autenticação do Cartão de Cidadão para suportar a sua atividade de emissão de certificados.

Estado do documento

Este é um documento controlado e aprovado pelo IRN.

Embora este documento possa ser impresso, a versão eletrónica assinada digitalmente pelo(s) elemento(s) do Grupo de Gestão, é a cópia controlada. Qualquer cópia impressa deste documento não é controlada.

Sendo um documento **controlado** e de **acesso público**, este documento pode ser arquivado em unidades locais ou de rede, assim como ser acedido diretamente no repositório da PKI do Cartão de Cidadão em <http://pki.cartaodecidadao.pt/> e <http://pki2.cartaodecidadao.pt/>.

Índice

Política de Certificados da EC de Autenticação do Cartão de Cidadão	1
Índice	3
1 Introdução.....	4
1.1 Público-Alvo	4
2 Contexto Geral	5
2.1 Visão Geral	5
2.2 Designação e Identificação do Documento.....	5
3 Identificação e Autenticação	6
3.1 Atribuição de Nomes.....	6
3.1.1 Tipo de Nomes	6
3.2 Uso do certificado e par de chaves pelo titular	7
4 Perfis de Certificado, LCR e OCSP	8
4.1 Perfil de Certificado	8
4.1.1 Número da Versão.....	9
4.1.2 OID do Algoritmo de assinatura.....	9
4.1.3 Formato dos Nomes (<i>Distinguished Name</i>)	9
4.1.4 Condicionamento dos Nomes (<i>Distinguished Name</i>).....	9
4.1.5 Sintaxe e semântica do qualificador da Política de Certificado.....	9
4.1.6 Utilização da extensão <i>Policy Constraints</i>	9
4.1.7 Semântica de processamento para a extensão crítica <i>Certificate Policies</i>	9
4.1.8 Campos e extensões do certificado	10
4.1.8.1 Perfil de certificado de Autenticação	11
4.1.8.2 Perfil de certificado “espécimen” de Autenticação	15
4.1.8.3 Perfil de certificado de VA.....	15
4.2 Perfil da lista de certificados revogados (LCR).....	20
4.2.1 Número da Versão.....	20
4.2.2 Campos e extensões da LCR	20
4.2.2.1 LCR da EC AuC.....	21
4.2.2.2 Delta-LCR da EC AuC	23
4.3 Perfil de resposta OCSP.....	26
Aprovação	27

I Introdução

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 eletrónico (*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 eletrónicas indispensáveis aos processos de desmaterialização que têm vindo a ser disponibilizados pelo Estado.

A infraestrutura da Entidade de Certificação do Cartão de Cidadão (ou EC CC) fornece uma hierarquia de confiança, que promove a segurança eletrónica do Cidadão no seu relacionamento com o Estado. A EC CC 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 hierarquia de confiança da Entidade de Certificação do Cartão de Cidadão encontra-se englobada na hierarquia do Sistema de Certificação Eletrónica do Estado Português¹ (SCEE) – Infraestrutura de Chaves Públicas do Estado, de acordo com os requisitos da "Política de Certificados do SCEE e Requisitos Mínimos de Segurança"².

Este documento (Política de Certificados da EC de Autenticação do Cartão de Cidadão) descreve os perfis dos certificados, lista de certificados revogados (LCR) e OCSP (*Online Certificate Status Protocol*) emitidos pela EC de Autenticação do Cartão de Cidadão (EC AuC) que faz parte integrante da hierarquia de confiança da Entidade de Certificação do Cartão de Cidadão.

I.1 Público-Alvo

O público-alvo deste documento são os titulares, e terceiras partes de confiança, de certificados eletrónicos emitidos pela EC AuC.

Assume-se que o leitor deste documento 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 nesses tópicos antes de prosseguir com a leitura do documento.

Este documento complementa a "Declaração de Práticas de Certificação da EC de Autenticação do Cartão de Cidadão"³, presumindo-se que o leitor leu integralmente o seu conteúdo antes de iniciar a leitura deste documento.

¹ <https://www.scee.gov.pt/>

² Documento identificado pelo OID 2.16.620.1.1.1.2.1.4.0, disponível em <https://www.scee.gov.pt/rep/>

³ Documento identificado pelo OID 2.16.620.1.1.1.2.4.1.0.7, disponível nos repositórios da PKI do Cartão de Cidadão, em <http://pki2.cartaodecidadao.pt>.

2 Contexto Geral

O presente documento é um documento que tem como objetivo a definição de um conjunto de parâmetros que definem os perfis dos certificados, lista de certificados revogados (LCR) e OCSP (*Online Certificate Status Protocol*) emitidos pela EC de Autenticação do Cartão de Cidadão (EC AuC). 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.

Os Certificados emitidos pela EC AuC contêm uma referência à Política de Certificados (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.

Os certificados emitidos pela EC AuC estão conforme as várias políticas identificadas pelos OID indicados no campo “*policyIdentifier*” do certificado (cf. perfis de certificado na secção 4.1.8).

2.1 Visão Geral

Este documento satisfaz e complementa os requisitos impostos pela “Declaração de Práticas de Certificação da EC de Autenticação do Cartão de Cidadão”³ e a “Política de Certificados do SCEE e Requisitos Mínimos de Segurança”² pela qual a EC AuC se rege.

2.2 Designação e Identificação do Documento

Este documento é a “Política de Certificados da EC de Autenticação do Cartão de Cidadão”. É representada no certificado eletrónico através de um número único designado de “identificador de objeto” (OID), sendo o valor do mesmo dependente do perfil de certificado emitido (cf. próxima tabela e secção 4.1).

Este documento é identificado pelos dados constantes na seguinte tabela:

INFORMAÇÃO DO DOCUMENTO	
Nome	Política de Certificados da EC de Autenticação do Cartão de Cidadão
Versão	3.0
Estado	Aprovado
OID	De acordo com o perfil de certificado emitido: <ul style="list-style-type: none">2.16.620.1.1.1.2.4.2.0.1.1 – certificado de Autenticação.2.16.620.1.1.1.2.4.2.0.1.2 – certificado de Validação on-line OCSP (VA).
Data	Julho 2024
Validade	Até 2 (dois) anos após a sua aprovação, ou até que seja substituído por uma nova versão (o que ocorrer primeiro)
Localização	http://pki2.cartaodecidadao.pt/publico/politica-certificados

3 Identificação e Autenticação

3.1 Atribuição de Nomes

A atribuição de nomes (DN - *Distinguished Name*) segue a convenção determinada na "Política de Certificados do SCEE) e Requisitos Mínimos de Segurança"² e "Declaração de Práticas de Certificação da EC de Autenticação do Cartão de Cidadão"³.

3.1.1 Tipo de Nomes

Todos os de certificados requerem um nome único (DN - *Distinguished Name*) de acordo com o standard X.500.

Os certificados emitidos pela EC AuC contêm no campo "Subject", um DN, para utilização como identificador único de cada entidade, de acordo com o preconizado no IETF RFC 5280⁴, atualizados pelos IETF RFCs 6818⁵, 8398⁶ e 8399⁷, em que:

- Nos certificados emitidos a pessoas, o DN identifica univocamente o titular do certificado;
- Nos certificados atribuídos a equipamentos, no DN é inscrito o nome da organização (ou um nome que permita determinar qual a organização) responsável pela sua operação (patrocinador);
- O DN tem de ser sempre preenchido.

O DN do campo "Subject" é construído com os atributos indicados nas tabelas seguintes, de acordo com o perfil de certificado emitido (cf. secção 4.1):

- Certificados emitidos para o Cidadão

Atributo (Código)	Certificado de Autenticação
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)	BI<identificador único do Cidadão>

⁴ IETF RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

⁵ IETF RFC 6818 - Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

⁶ IETF RFC 8398 - Internationalized Email Addresses in X.509 Certificates

⁷ IETF RFC 8399 - Internationalization Updates to RFC 5280

- Certificados para serviços do Cartão de Cidadão

Atributo (Código)	Certificado de VA
Country (C)	PT
Organization (O)	Cartão de Cidadão
Organization Unit (OU)	Serviços do Cartão de Cidadão
Organization Unit (OU)	Validação on-line
Common Name (CN)	Serviço de Validação on-line do Cartão de Cidadão <nnnnnn> ⁸ - EC de Autenticação do Cidadão

3.2 Uso do certificado e par de chaves pelo titular

A tabela seguinte identifica o titular do certificado e uso do certificado e par de chaves, por cada perfil de certificado emitido (cf. secção 4.1):

Perfil de certificado	Titular	Uso do certificado e par de chaves
Certificado de Autenticação	Cidadão identificado no DN do "Subject" (cf. secção 3.1.1)	Utilizado para efeitos de autenticação do Cidadão.
Certificado de VA	EC de Autenticação do Cidadão	Utilizada para assinar as respostas a pedidos de validação on-line OCSP ⁹ (consulta do estado atual de certificados digitais), garantindo e permitindo verificar a integridade e não-repúdio dessas mesmas respostas.

⁸ <nnnnnn> (ou <nnnn>) é um valor sequencial iniciado em "000001" (ou "0001") na emissão do primeiro certificado deste tipo.

⁹ IETF RFC 6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP

4 Perfis de Certificado, LCR e OCSP

4.1 Perfil de Certificado

Os utilizadores de uma chave pública têm de ter confiança que a chave privada associada é detida pelo titular (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 Entidade de Certificação (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 armazenamento¹⁰.

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 ECs¹⁰.

O perfil dos certificados emitidos pela EC AuC seguem os seguintes standards:

- Recomendação ITU.T X.509¹¹ | ISO/IEC 9594-8¹²,
- IETF RFC 5280¹⁰,
- Política de Certificados do SCEE e Requisitos Mínimos de Segurança²,
- IETF RFC 3739 (*Internet X.509 Public Key Infrastructure: Qualified Certificates Profile*),
- ETSI TS 119 412-1 (*Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures*),
- ETSI TS 119 412-2 (*Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons*)

A EC AuC emite certificados com os perfis e finalidades identificadas na secção 3.2.

¹⁰ IETF RFC 5280, atualizados pelos IETF RFCs 6818, 8398 e 8399.

¹¹ ITU-T Recommendation X.509. 2019: Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks

¹² ISO/IEC 9594-8:2017 Information technology — Open Systems Interconnection — The Directory — Part 8: Public-key and attribute certificate frameworks

4.1.1 Número da Versão

O campo “*version*” do certificado descreve a versão utilizada na codificação do certificado. Nos perfis dos certificados emitidos pela EC AuC, é utilizado o valor 0x2, de forma a identificar a codificação de certificados ITU-T X.509 versão 3.

4.1.2 OID do Algoritmo de assinatura

Os campos “*signature*” e “*signatureAlgorithm*” do certificado da EC AuC contêm o OID do algoritmo criptográfico utilizado para assinar os certificados: 1.2.840.10045.4.3.2 (ecdsa-with-SHA256¹³).

Até à EC AuC 0009 (inclusive), estes campos continham o OID 1.2.840.113549.1.1.5 (sha1WithRSAEncryption¹⁴). Da EC AuC 010 até à EC AuC 0018 contêm o valor 1.2.840.113549.1.1.11 (sha-256WithRSAEncryption¹⁵).

4.1.3 Formato dos Nomes (*Distinguished Name*)

Tal como definido na secção 3.1.

4.1.4 Condicionamento dos Nomes (*Distinguished Name*)

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 formato UTF8.

4.1.5 Sintaxe e semântica do qualificador da Política de Certificado

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

Os qualificadores opcionais “*policyQualifiers*” (“*policyQualifierID*: 1.3.6.1.5.5.7.2.1” e “*cPSuri*”) identificam o URI onde pode ser encontrado o documento de política de certificado com o OID identificado pelo “*policyIdentifier*”.

4.1.6 Utilização da extensão *Policy Constraints*

A extensão “*policy constraints*” não é utilizada nos certificados emitidos pela EC AuC.

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

A sintaxe e semântica da extensão crítica “*certificate policies*” é descrita na secção 4.1.5.

¹³ ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2 }

¹⁴ sha-1WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsads(113549) pkcs(1) pkcs-1(1) 5 }

¹⁵ sha-256WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsads(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11) }

As extensões marcadas como críticas têm de ser processadas pelas aplicações que utilizam os certificados, devendo ser tido em conta que:

- A extensão “*certificate policies*” identifica as várias políticas de certificado que são cumpridas na emissão do certificado;
- Para que possa ser processado automaticamente, cada política de certificado é identificada pelo respetivo OID no campo “*policyIdentifier*”;
- O documento da política de certificado encontra-se disponível no URI identificado no “*policyQualifiers*” (“*cPSuri*”), sendo utilizada a política válida à data de emissão do certificado;
- O certificado só deve ser aceite, se a aplicação que o processar tiver algum dos OID identificados no campo “*policyIdentifier*” na sua lista de políticas confiáveis, e após verificar se o certificado é válido (através da LCR e/ou OCSP identificada no certificado) e está dentro do seu período de validade;
- A aceitação do certificado é da responsabilidade exclusiva da aplicação que o processa.

4.1.8 Campos e extensões do certificado

Os campos e as extensões definidas para os certificados X.509 v3 fornecem métodos para associar atributos a titulares ou chaves públicas, assim como para gerir a hierarquia de certificação. Nos perfis dos certificados emitidos pela EC AuC podem ser utilizados os campos e extensões identificadas no IETF RFC 5280¹⁰.

De seguida identificam-se os campos e extensões dos perfis de certificados emitidos pela EC AuC.

4.1.8.1 Perfil de certificado de Autenticação

RFC 5280	Valor	Tipo ¹⁶	Comentários
4. Certificate and Certificate Extensions Profile			
4.1. Basic Certificate Fields			
4.1.2. TBSCertificate			
1.	Version	3 (0x2)	m
2.	Serial Number	<valor aleatório, atribuído pela EC a cada certificado>	m
3.	Signature	1.2.840.10045.4.3.2	m sha256ECDSA Nota: Até à EC AuC 0018 (inclusive) a assinatura era sha256RSA
4.	Issuer Distinguished Name	C = PT O = Instituto dos Registos e do Notariado I. P. OU = Cartão de Cidadão OU = subECEstado CN = EC de Autenticação do Cartão de Cidadão <nnnn> ⁸	m
5.	Validity		m Até 10 (dez) anos e 1 (um) mês.
	not Before	<data de emissão>	
	not After	<data de emissão + 10 anos e 1 mês>	

¹⁶ A terminologia utilizada para cada um dos tipos de campo no formato X.509, significa o seguinte:

- 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).

RFC 5280		Valor	Tipo ¹⁶	Comentários
6.	Subject Distinguished Name	<cf. indicado na secção 3.1.1.>	m	
7.	Subject Public Key Info		m	
	<i>algorithm</i> <i>publicKey</i>	1.2.840.10045.4.3.2 ECC (256 bits)		Sha256ECDSA prime256v1/P-256 Nota: Até à EC AuC 0018 (inclusive) a chave pública é rsaEncryption (RSA) com 3072 bits de tamanho
4.2 Certificate Extension				
4.2.1 Standard Extensions				
1.	Authority Key Identifier	<Composto pela hash de 160-bit SHA-1 do valor da BIT STRING da chave pública correspondente à chave privada utilizada para assinar o certificado>	m	
2.	Subject Key Identifier	<Composto pela hash de 160-bit SHA-1 do valor da BIT STRING da chave pública do certificado>	m	
3.	Key Usage	<i>Digital Signature</i> <i>Key Agreement</i>	mc	Uso do certificado e par de chaves, de acordo com secção 3.2.
4.	Certificate Policies		m	
	<i>policyIdentifier</i> <i>policyQualifiers</i>	2.16.620.1.1.1.2.20 (scee-autenticacao) <i>policyQualifierID</i> : 1.3.6.1.5.5.7.2.1 <i>cPSuri</i> : https://www.scee.gov.pt/rep		Significa que o certificado emitido está de acordo com a “Política de Certificados do SCEE e Requisitos Mínimos de Segurança” para certificados de digitais, indicando o URL do repositório onde se encontra esse documento.

RFC 5280		Valor	Tipo ¹⁶	Comentários
		<p><i>policyQualifierID</i>: 1.3.6.1.5.5.7.2.2</p> <p><i>userNotice explicitText</i>: “O certificado emitido segundo esta política é utilizado para autenticação do Cidadão”</p>		
		<p>2.16.620.1.1.1.2.4.2.0.7</p> <p><i>policyQualifierID</i>: 1.3.6.1.5.5.7.2.1</p> <p><i>cPSuri</i>: http://pki2.cartaodecidadao.pt/publico/praticas-certificacao</p>		<p>Significa que o certificado emitido está de acordo com a “Declaração de Práticas de Certificação da EC de Autenticação do Cartão de Cidadão”, indicando o URL do repositório onde se encontra esse documento.</p> <p>Até à EC AuC 0018 (inclusive), o URL é https://pki.cartaodecidadao.pt/publico/politicas/cps.html</p>
		<p>2.16.620.1.1.1.2.4.2.0.1.1</p> <p><i>policyQualifierID</i>: 1.3.6.1.5.5.7.2.1</p> <p><i>cPSuri</i>: http://pki2.cartaodecidadao.pt/publico/politica-certificados</p>		<p>Significa que o certificado emitido está de acordo com este documento de políticas, para o perfil de certificado emitido (cf. secção 2.2), indicando o URL do repositório onde se encontra o documento.</p> <p>Até à EC AuC 0018 (inclusive), o URL é https://pki.cartaodecidadao.pt/publico/politicas/cp.html</p>
8.	Subject Directory Attributes			
	dateOfBirth	<data de nascimento do cidadão>	m	
9.	Basic Constraints		mc	
	CA	FALSE		
13.	CRLDistributionPoints	<p>http://pki2.cartaodecidadao.pt/entidade-certificacao-autenticacao/lista-revogacao/CC_Auc</p> <p><Id_EC>_partition<num_seq>.crl</p>	m	<p>URI para a LCR onde pode ser verificado o estado do certificado.</p> <p>Até à EC AuC 0018 (inclusive), o URL é: <a href="http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_autenticacao_crl<ID_CA>_p<num_seq>.crl">http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_autenticacao_crl<ID_CA>_p<num_seq>.crl</p>

RFC 5280		Valor	Tipo ¹⁶	Comentários
14.	Freshest CRL	--	-	URI para a delta-LCR onde pode ser verificado o estado do certificado. Deixa de ser usado na EC AuC 0019. Até à EC AuC 0018, o URL é: <a href="http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_autenticacao_crl<ID_CA>_delta_p<num_seq>.crl">http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_autenticacao_crl<ID_CA>_delta_p<num_seq>.crl
4.2.2 Private Internet Extensions				
1.	Authority Information Access		m	
	CA Issuer	URL= <a href="http://pki2.cartaodecidadao.pt/entidade-certificacao-autenticacao/certificados/CC_Auc<Id_EC>.crt">http://pki2.cartaodecidadao.pt/entidade-certificacao-autenticacao/certificados/CC_Auc<Id_EC>.crt		URI para o certificado da EC emissora Passou a ser usado na EC AuC 0019
	accessMethod accessLocation	1.3.6.1.5.5.7.48.1 http://ocsp.auc.pki2.cartaodecidadao.pt/ocsp		OCSP URI para serviço de validação OCSP onde pode ser verificado o estado do certificado. Até à EC AuC 0018 (inclusive), o URL é: http://ocsp.auc.cartaodecidadao.pt/publico/ocsp
5. CRL and CRL Extensions Profile				
5.1. CRL Fields				
5.1.1. Certificate List Fields				
2.	Signature Algorithm	1.2.840.10045.4.3.2	m	sha256ECDSA
3.	Signature Value	<contém a assinatura digital do certificado, efetuada pela chave privada da EC AuC>	m	Ao gerar esta assinatura, a EC certifica a ligação entre a chave pública e o titular (<i>subject</i>) do certificado.

4.1.8.2 Perfil de certificado “espécimen” de Autenticação

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 perfil de certificado de Autenticação (descrito na secção 4.1.8.1):

- O *CommonName* (CN) tem “Espécimen”;
- O atributo *serialNumber* do DN contém “especimen” seguido de um número sequencial único (que começa em 0000001);

4.1.8.3 Perfil de certificado de VA

RFC 5280	Valor	Tipo ¹⁶	Comentários
4. Certificate and Certificate Extensions Profile			
4.1. Basic Certificate Fields			
4.1.2. TBSCertificate			
1.	Version	3 (0x2)	m
2.	Serial Number	<valor aleatório, atribuído pela EC a cada certificado>	m
3.	Signature	1.2.840.10045.4.3.2	m sha256ECDSA Nota: Até à EC AuC 0018 (inclusive) é sha256WithRSAEncryption
4.	Issuer Distinguished Name	C = PT O = Instituto dos Registos e do Notariado I. P. OU = Cartão de Cidadão OU = subECEstado	m

RFC 5280		Valor	Tipo ¹⁶	Comentários
		CN = EC de Autenticação do Cartão de Cidadão <nnnn> ⁸		
5.	Validity		m	
	not Before not After	<data de emissão> <data de emissão + 1.900 dias>		Até aproximadamente 5 anos e dois meses. Utilizado para assinar respostas OCSP durante o primeiro mês de validade e renovado (com geração de novo par de chaves) antes de perfazer o segundo mês de validade.
6.	Subject Distinguished Name	<cf. indicado na secção 3.1.1>	m	
7.	Subject Public Key Info		m	
	algorithm publicKey	1.2.840.10045.4.3.2 ECC (256 bits)		Sha256ECDSA prime256v1/P-256 Nota: Até à EC AuC 0018 (inclusive) 2048 bits
4.2 Certificate Extension				
4.2.1 Standard Extensions			m	
1.	Authority Key Identifier	<Composto pela hash de 160-bit SHA-1 do valor da BIT STRING da chave pública correspondente à chave privada utilizada para assinar o certificado>	m	
2.	Subject Key Identifier	<Composto pela hash de 160-bit SHA-1 do valor da BIT STRING da chave pública do certificado>	m	
3.	Key Usage	Digital Signature Non Repudiation	mc	Uso do certificado e par de chaves, de acordo com secção 3.2.

RFC 5280		Valor	Tipo ¹⁶	Comentários
4.	Certificate Policies		m	
	<i>policyIdentifier</i> <i>policyQualifiers</i>	2.16.620.1.1.1.2.4.2.0.7 <i>policyQualifierID</i> : 1.3.6.1.5.5.7.2.1 <i>cPSuri</i> : http://pki2.cartaodecidadao.pt/publico/praticas-certificacao		Significa que o certificado emitido está de acordo com a “Declaração de Práticas de Certificação da EC de Autenticação do Cartão de Cidadão”, indicando o URL do repositório onde se encontra esse documento. Nota: Até à EC AuC 0018 (inclusive) está em https://pki.cartaodecidadao.pt/publico/politicas/cps.html
	<i>policyIdentifier</i> <i>policyQualifiers</i>	<OID do perfil de certificado emitido, cf. secção 2.2> <i>policyQualifierID</i> : 1.3.6.1.5.5.7.2.1 <i>cPSuri</i> : http://pki2.cartaodecidadao.pt/publico/politica-certificados		Significa que o certificado emitido está de acordo com a “Política de Certificados da EC de Autenticação do Cartão de Cidadão” (este documento), para o perfil de certificado emitido (cf. secção 2.2), indicando o URL do repositório onde se encontra o documento. Nota: Até à EC AuC 0018 (inclusive) está em https://pki.cartaodecidadao.pt/publico/politicas/cp.html
9.	Basic Constraints		mc	
	CA	FALSE		
12.	Extended Key Usage	1.3.6.1.5.5.7.3.9 (OCSP Signing)	m	
13.	CRLDistributionPoints	<a href="http://pki2.cartaodecidadao.pt/entidade-certificacao-autenticacao/lista-revogacao/CC_Auc<Id_EC>_partition<num_seq>.crl">http://pki2.cartaodecidadao.pt/entidade-certificacao-autenticacao/lista-revogacao/CC_Auc<Id_EC>_partition<num_seq>.crl		URI para a LCR onde pode ser verificado o estado do certificado. Nota: Até à EC AuC 0018 (inclusive) está em <a href="http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_autenticacao_crl<ID_CA>_p<num_seq>.crl">http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_autenticacao_crl<ID_CA>_p<num_seq>.crl
14.	Freshest CRL			Não é usado a partir da EC AuC 0018. URI para a delta-LCR onde pode ser verificado o estado do certificado.

RFC 5280		Valor	Tipo ¹⁶	Comentários
				Nota: Até à EC AuC 0018 (inclusive) está em: <a href="http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_autenticacao_crl<ID_CA>_delta_p<num_seq>.crl">http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_autenticacao_crl<ID_CA>_delta_p<num_seq>.crl
4.2.2. Private Internet Extensions				
1.	Authority Information Access		m	URI para serviço de validação OCSP onde pode ser verificado o estado do certificado. Nota: Até à EC AuC 0018 (inclusive), o URL é: http://ocsp.auc.cartaodecidadao.pt/publico/ocsp
	accessMethod accessLocation	1.3.6.1.5.5.7.48.1 http://ocsp.auc.pki2.cartaodecidadao.pt/ocsp		
5. CRL and CRL Extensions Profile				
5.1. CRL Fields				
5.1.1. Certificate List Fields				
2.	Signature Algorithm	1.2.840.10045.4.3.2	m	sha256ECDSA
3.	Signature Value	<contém a assinatura digital do certificado, efetuada pela chave privada da EC AuC>	m	Ao gerar esta assinatura, a EC certifica a ligação entre a chave pública e o titular (<i>subject</i>) do certificado.
RFC 6960 ¹⁷		Valor	Tipo ¹⁶	Comentários
4. Details of the Protocol				
4.2. Response Syntax				
4.2.2. Notes on OCSP Responses				

¹⁷ RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP

RFC 5280	Valor	Tipo ¹⁶	Comentários
4.2.2.2. Authorized Responders			
4.2.2.2.1. Revocation Checking of an Authorized Responder			
	id-pkix-ocsp-nocheck	OCSPNocheck: NULL	o Não é uma extensão definida no RFC 5280, mas encontra-se definida no RFC 6960 (id-pkix-ocsp-nocheck). Esta extensão indica ao cliente OCSP que este certificado é confiável, mesmo sem o validar junto do servidor OCSP ou LCR.

4.2 Perfil da lista de certificados revogados (LCR)

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 de revogar o certificado.

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 Certificados Revogados (LCR). A LCR é uma lista com identificação temporal dos certificados revogados, assinada pela EC e disponibilizada livremente num repositório público. Cada certificado revogado é identificado na LCR 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 LCR mais recente e verifica se o número de série do certificado não faz parte da mesma. Note-se que uma EC emite uma nova LCR numa base regular periódica.

O perfil da LCR está conforme com:

- Recomendação ITU.T X.509¹¹ | ISO/IEC 9594-8¹²,
- IETF RFC 5280¹⁰,
- Política de Certificados do SCEE e Requisitos Mínimos de Segurança².

A EC AuC emite a LCR completa com uma periodicidade semanal e a delta-LCR com uma periodicidade diária. A delta-LCR contém a identificação dos certificados que foram revogados desde a emissão da última LCR completa.

4.2.1 Número da Versão

O campo “*version*” da LCR descreve a versão utilizada na codificação da LCR. Nos perfis das LCR emitidos pela EC AuC, é utilizado o valor 0x1, de forma a identificar a codificação ITU-T X.509 versão 1.

4.2.2 Campos e extensões da LCR

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

Nas LCR emitidas pela EC AuC são utilizadas as seguintes extensões obrigatórias, não críticas:

- *CRLNumber*, implementado de acordo com as recomendações do IETF RFC 5280¹⁰;
- *AuthorityKeyIdentifier*: contém o *hash* (SHA-1) da chave pública da EC que assinou a LCR.

4.2.2.1 LCR da EC AuC

RFC 5280		Valor	Tipo ¹⁸	Comentários
5. CRL and CRL Extensions Profile				
5.1. CRL Fields				
5.1.1. CertificateList Fields				
2.	Signature Algorithm	1.2.840.10045.4.3.2	m	sha256ECDSA Até à EC Auc 0018 o valor deste campo é: 1.2.840.113549.1.1.11 referente sha256WithRSAEncryption
3.	Signature Value	<contém a assinatura digital da LCR, efetuada pela chave privada da EC AuC>	m	
5.1.2. Certificate List "To Be Signed"				
1.	Version	2 (0x1)	m	
2.	Signature	1.2.840.10045.4.3.2	m	sha256ECDSA Até à EC Auc 0018 o valor deste campo é: 1.2.840.113549.1.1.11 referente sha256WithRSAEncryption

¹⁸ A terminologia utilizada para cada um dos tipos de campo no formato X.509, significa o seguinte:

- 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).

RFC 5280		Valor	Tipo ¹⁸	Comentários
3.	Issuer Distinguished Name	C = PT O = Instituto dos Registos e do Notariado I. P. OU = Cartão de Cidadão OU = subECEstado CN = EC de Autenticação do Cartão de Cidadão <nnnn> ⁸	m	
4.	thisUpdate	<data de emissão da LCR>	m	
5.	nextUpdate	<data da próxima emissão da LCR = <i>thisUpdate</i> + N>	m	Este campo indica a data em que a próxima LCR vai ser emitida. A próxima LCR pode ser emitida antes da data indicada, mas não será emitida depois dessa data. Até à EC AuC 0018, N é no máximo 1 semana. Após a EC AuC 0018 o N é no máximo 1 dia.
6.	Revoked Certificates		m	Estrutura com os certificados revogados, constituída por uma sequência de estruturas <i>Serial Number</i> (uma estrutura <i>Serial Number</i> , por cada certificado revogado).
	Serial Number	<número de série do certificado revogado>	m	
	Revocation Date	<data de revogação do certificado>	m	
5.2. CRL Extensions				
1.	Authority Key Identifier	<Composto pela hash de 160-bit SHA-1 do valor da BIT STRING da chave pública correspondente à chave privada utilizada para assinar a LCR>	m	
3.	CRL Number	<número sequencial único da LCR>	m	

RFC 5280		Valor	Tipo ¹⁸	Comentários
5.	Issuing Distribution Point		mc	URI da localização da LCR. Até à EC Auc 0018 o URL é: <code>http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_autenticacao_crl<ID_CA>_p<num_seq>.crl</code>
	distributionPoint	<code>http://pki2.cartaodecidadao.pt/entidade-certificacao-autenticacao/lista-revogacao/CC_Auc<Id_EC>_partition<num_seq>.crl</code>		
6.	Freshest CRL		m	URI da localização da delta-LCR. Este campo é utilizado nas CRL's emitidas pelas EC AuC até à 0018 (inclusive), com o URL <code>/publico/lrc/cc_sub-ec_cidadao_autenticacao_crl<ID_CA>_delta_p<num_seq>.crl</code> A partir da EC AuC 0019 (inclusive) este campo não é usado.
	distributionPoint			
5.3. CRL Entry Extensions				
	CRL entry extensions	<i>Reason Code:</i> <motivo de revogação do certificado>	o	Valor tem de ser um dos seguintes (cf. RFC 5280 ¹⁰): 0 – <i>unspecified</i> 1 – <i>keyCompromise</i> 2 – <i>cACompromise</i> 3 – <i>affiliationChanged</i> 4 – <i>superseded</i> 5 – <i>cessationOfOperation</i> 6 – <i>certificateHold</i> 8 – <i>removeFromCRL</i> 9 – <i>privilegeWithdrawn</i> 10 – <i>aACompromise</i>

4.2.2.2 Delta-LCR da EC AuC

As Delta-LCRs são emitidas pelas EC AuC até à 0018 (inclusive). Após a EC AuC as deltas-LCRs não são usadas.

Campo	Valor	Tipo	Comentários
-------	-------	------	-------------

1. Version	2 (0x1)	m	
2. Signature	1.2.840.113549.1.1.11	m	sha256WithRSAEncryption
3. Issuer Distinguished Name	C = PT O = Instituto dos Registos e do Notariado I. P. OU = Cartão de Cidadão OU = subECEstado CN = EC de Autenticação do Cartão de Cidadão <nnnn> ⁸	m	
4. thisUpdate	<data de emissão da LCR>	m	
5. nextUpdate	<data da próxima emissão da LCR = <i>thisUpdate</i> + N>	m	Este campo indica a data em que a próxima LCR vai ser emitida. A próxima LCR pode ser emitida antes da data indicada, mas não será emitida depois dessa data. N é no máximo 1 dia.
6. CRL Extensions		m	
6.1 Authority Key Identifier	<Composto pela hash de 160-bit SHA-1 do valor da BIT STRING da chave pública correspondente à chave privada utilizada para assinar a LCR>	m	
6.2 CRL Number	<número sequencial único da LCR>	m	
6.3 Delta CRL Indicator	<número único da LCR completa>	mc	Identifica o número da LCR completa, a que esta delta-LCR adiciona novas revogações.
6.3 Issuing Distribution Point		mc	URI da localização da LCR completa.
distributionPoint	http://pki.cartaodecidadao.pt /publico/lrc/cc_sub-ec_cidadao_autenticacao_crl<ID_CA>_p<num_seq>.crl		

7. Revoked Certificates		m	Estrutura com os certificados revogados, constituída por uma sequência de estruturas <i>Serial Number</i> (uma estrutura <i>Serial Number</i> , por cada certificado revogado).
7.1 Serial Number	<número de série do certificado revogado>	m	
Revocation Date CRL entry extensions	<data de revogação do certificado> <i>Reason Code</i> : <motivo de revogação do certificado>	m o	Valor tem que ser um dos seguintes (cf. IETF RFC 5280 ¹⁰): 0 – <i>unspecified</i> 1 – <i>keyCompromise</i> 2 – <i>cACompromise</i> 3 – <i>affiliationChanged</i> 4 – <i>superseded</i> 5 – <i>cessationOfOperation</i> 6 – <i>certificateHold</i> 8 – <i>removeFromCRL</i> 9 – <i>privilegeWithdrawn</i> 10 – <i>aACompromise</i>
8. Signature Algorithm	1.2.840.113549.1.1.11	m	sha256WithRSAEncryption
9. Signature Value	<contém a assinatura digital da LCR, efetuada pela chave privada da EC AuC>	m	

4.3 Perfil de resposta OCSP

O serviço de validação OCSP⁹ dos certificados emitidos pela EC AuC encontra-se disponível em <http://ocsp.auc.cartaodecidadao.pt/publico/ocsp>, conforme identificado no campo “*Authority Information Access*” dos certificados. Este serviço permite obter uma resposta assinada relativamente à consulta do estado de um certificado digital. A resposta do serviço de validação OCSP está conforme o definido no IETF RFC 6960⁹.

O certificado que assina a resposta OCSP (cf. perfil de certificado VA, identificado na secção 4.1.8.3) inclui o campo com a extensão *id-pkix-ocsp-nocheck*¹⁹, o que significa que esse certificado é um certificado confiável, não necessitando de ser validado por OCSP ou LCR. Contudo, caso a aplicação que valida a resposta OCSP não saiba interpretar essa extensão, o certificado que assina a resposta OCSP contém o campo “*CRLDistributionPoints*” que permite validar esse certificado na LCR.

A resposta do serviço de validação OCSP é:

- “*good*” para certificado emitidos pela EC AuC e que não se encontrem revogados (embora possam já não estar dentro do seu período de validade);
- “*revoked*” para certificado emitidos pela EC AuC e que se encontrem revogados;
- “*unknown*”, para certificados que não tenham sido emitidos pela EC AuC.

¹⁹ A extensão *id-pkix-ocsp-nocheck* encontra-se definida no RFC 6960 e em <https://www.alvestrand.no/objectid/1.3.6.1.5.5.7.48.1.5.html>.

Aprovação

Aprovado pelo Grupo de Gestão.