Política de Certificados da EC do Cartão de Cidadão

Políticas (POL#22)

Nível de Acesso: Público

Versão: 4.0

Data: Mar 2024

IRN – Instituto dos Registos e Notariado, I.P.
Av. D. João II, Lote 1.08.01, Edifício H, Parque das Nações 1990-097 Lisboa, Portugal
Telefone: +351 217 985 500 e-mail: geral@irn.mj.pt

Identificador do Documento: POL#22

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

Tipologia Documental: Políticas

Título: Política de Certificados da EC do Cartão de Cidadão

Nível de acesso: Público

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

Data: Mar 2024

Versão atual: 4.0

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

Histórico de Versões

Versão	Data	Detalhes
1.0	10/01/2007	Versão inicial.
1.1	10/03/2010	Atualização do ID do Documento e Logótipo;
1.2-1.3	01/05/2014	Atualização do algoritmo de assinatura para SHA256
1.4	01/10/2017	- Atualização de referenciais inerentes ao regulamento (EU nº 910/2014) - Alteração da validade do certificado para 14 anos
1.5	10/11/2019	Atualização do link da localização documento
2.0	**Jan 2020**	**Revisão sem alterações relevantes**
3.0	**Jan 2023**	**Integração de todos os perfis de certificados emitidos pela EC CC no documento.**
4.0	Mar 2024	Alteração de Algoritmos Criptográficos e localização da documentação pública

Documentos Relacionados

Documento	Autor	Descrição
Declaração de Práticas de Certificação da Entidade de Certificação do Cartão de Cidadão (POL#27)	IRN	Descreve a Política de Certificados da EC do Cartão de Cidadão, identificando os perfis de certificado e LCR emitidos, assim como a resposta OCSP.
Declaração de Divulgação de Princípios da EC CC (POL#20)	IRN	Resume, de forma simples e acessível, as características descritas nas Políticas de Certificado e Declaração de Políticas de Certificação da Infraestrutura de chave pública da Entidade de Certificação do Cartão de Cidadão.

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 https://pki.cartaodecidadao.pt/ e http://pki2.cartaodecidadao.pt.

Índice

1 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 (e*Government*), 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 Português[1] (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 CC) descreve os perfis dos certificados, lista de certificados revogados (LCR) e OCSP (*Online Certificate Status Protocol*) emitidos pela EC CC.

1.1 Público-Alvo

O público-alvo deste documento são os titulares, e terceiras partes de confiança, de certificados eletrónicos emitidos na hierarquia de confiança da Entidade de Certificação do Cartão de Cidadão.

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 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 2.16.620.1.1.1.2.4.0.7, disponível no repositório 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 CC. 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 CC 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.

2.1 Visão Geral

Este documento satisfaz e complementa os requisitos impostos pela "Declaração de Práticas de Certificação da EC do Cartão de Cidadão"[3] e a "Política de Certificados do SCEE e Requisitos Mínimos de Segurança"[2] pela qual a EC CC se rege.

2.2 Designação e Identificação do Documento

Este documento é a "Política de Certificados da EC 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 do Cartão de Cidadão
Versão	4.0
Estado	Aprovado
OID	De acordo com o perfil de certificado emitido: • 2.16.620.1.1.1.2.4.0.1.2 – certificado da EC de Assinatura Digital Qualificada do Cartão de Cidadão (EC AsC); • 2.16.620.1.1.1.2.4.0.1.3 – certificado da EC de Autenticação do Cartão de Cidadão (EC AuC); • 2.16.620.1.1.1.2.4.0.1.5 – certificado para Entidade Certificadora de Documentos (ECD); • 2.16.620.1.1.1.2.4.0.1.6 – certificado de Validação on-line OCSP (VA); • 2.16.620.1.1.1.2.4.0.1.9 – certificado da EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão (EC CMD).
Data	Mar 2024

Validade	Até 2 (dois) anos após a sua aprovação, ou até que seja substituído por uma nova versão (o que ocorrer primeiro)
Localização	https:// pki2.cartaodecidadao.pt/publico/praticas-certificacao

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 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 CC contêm no campo "*Subject*", um DN, para utilização como identificador único de cada entidade, de acordo com o preconizado no RFC 5280[4], atualizados pelos RFCs 6818[5], 8398[6] e 8399[7], em que:

a) Nos certificados emitidos a pessoas, o DN identifica univocamente o titular do certificado;

b) 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);

c) 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):

3.1.1.1 Certificados de ECEstado

Atributo (Código)	***Certificado auto assinado da EC CC***
Country (C)	PT
Organization (O)	SCEE – Sistema de Certificação Electrónica do Estado
Organization Unit (OU)	ECEstado
Common Name (CN)	Cartão de Cidadão <nnn>[8]

[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*
[8] <nnn> é um valor sequencial iniciado em "001" na emissão do primeiro certificado deste perfil.

3.1.1.2 Certificados de subECEstado

Atributo (Código)	*Certificado da EC AsC*	*Certificado da EC AuC*	*Certificado da EC CMD*
Country (C)	PT	PT	PT
Organization (O)	Instituto dos Registos e do Notariado I.P	Instituto dos Registos e do Notariado I.P	AMA – Agência para a Modernização Administrativa I.P.
Organization Unit (OU)	Cartão de Cidadão	Cartão de Cidadão	Cartão de Cidadão
Organization Unit (OU)	subECEstado	subECEstado	subECEstado
Common Name (CN)	EC de Assinatura Digital Qualificada do Cartão de Cidadão <nnnn>[8]	EC de Autenticação do Cartão de Cidadão <nnnn>[8]	EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão <nnnn>[8]

3.1.1.3 Certificados para serviços do Cartão de Cidadão

Atributo (Código)	*Certificado para ECD*	*Certificado de VA*
Country (C)	PT	PT
Organization (O)	Cartão de Cidadão	Cartão de Cidadão
Organization Unit (OU)	Serviços do Cartão de Cidadão	Serviços do Cartão de Cidadão
Organization Unit (OU)	Entidade Certificadora de Documentos	Validação on-line
Common Name (CN)	Entidade Certificadora de Documentos do Cartão de Cidadão <nnn>[8]	Serviço de Validação on-line do Cartão de Cidadão <nnn>[8] - EC do Cartão de 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 auto assinado da EC CC	Entidade de Certificação do Cartão de Cidadão	Utilizado para a assinatura de certificados de EC subordinada, certificados de operação e serviços, assim como para a assinatura da

		respetiva Lista de Certificados Revogados (LCR).
Certificado da EC AsC	Instituto dos Registos e do Notariado I.P	Utilizado para a assinatura de certificados de Assinatura Digital Qualificada do Cidadão, certificados de operação e serviços, assim como para a assinatura da respetiva Lista de Certificados Revogados (LCR).
Certificado da EC AuC	Instituto dos Registos e do Notariado I.P	Utilizado para a assinatura de certificados de Autenticação do Cidadão, certificados de operação e serviços, assim como para a assinatura da respetiva Lista de Certificados Revogados (LCR).
Certificado da EC CMD	AMA – Agência para a Modernização Administrativa I.P.	Utilizado para a assinatura de certificados de Chave Móvel Digital de Assinatura Qualificada do Cidadão, certificados de operação e serviços, assim como para a assinatura da respetiva Lista de Certificados Revogados (LCR).
Certificado para ECD	Entidade de Certificação do Cartão de Cidadão	Utilizado para a assinatura de dados a colocar no *chip* do Cartão de Cidadão, garantindo e permitindo verificar a integridade dos mesmos.
Certificado de VA	Entidade de Certificação do Cartão de 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.

[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 que 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 armazenamento[10].

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[10].

O perfil dos certificados emitidos pela EC CC, e na hierarquia da EC CC, estão em conformidade com:

- Recomendação ITU.T X.509[11] | ISO/IEC 9594-8[12],
- RFC 5280[10],
- Política de Certificados do SCEE e Requisitos Mínimos de Segurança[2],
- 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*), e
- ETSI TS 119 412-5 (*Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements*).

A EC CC emite certificados com os perfis e finalidades identificadas na secção 0.

[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 CC, 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 CC contêm o OID do algoritmo criptográfico utilizado para assinar os certificados: 1.2.840.10045.4.3.2 (ecdsa-with-SHA256[13]).

Até à EC CC 002 (inclusive), estes campos continham o OID 1.2.840.113549.1.1.5 (sha1WithRSAEncryptino [14]). Da EC CC 003 até à EC CC 007 contêm o valor 1.2.840.113549.1.1.11 (sha-256WithRSAEncryption[15]).

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*".

Até à EC do Cidadão 002 (inclusive), foi utilizado o "userNotice explicitText" para identificar o URI desta política.

4.1.6 Utilização da extensão *Policy Constraints*

A extensão "*policy constraints*" não é utilizada nos certificados emitidos pela EC CC.

[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) rsadsi(113549) pkcs(1) pkcs-1(1) 5 }
[15] sha-256WithRSAEncryption OBJECT IDENTIFIER::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}

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.

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 CC podem ser utilizados os campos e extensões identificadas no RFC 5280[10].

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

4.1.8.1 Perfil de certificado da Sub-EC's da EC CC: EC AsC, EC AuC e EC CMD

Campo	Valor	Tipo[Erro! Marcador não definido.]	Comentários
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 CC 007 (inclusive) este campo assume o valor sha256withRSA
4. Issuer Distinguished Name	C = PT O = SCEE – Sistema de Certificação Electrónica do Estado OU = ECEstado CN = Cartão de Cidadão <nnn>[8]	m	--
5. Validity		m	Validade de doze anos e seis meses. Renovado (com geração de novo par de chaves) após 2 anos dois anos de validade.
not Before ***not After***	<data de emissão> <data de emissão + 12 anos + 6 meses>		
6. Subject Distinguished Name	<cf. indicado na secção 3.1.1>	m	--
7. Subject Public Key Info		m	--
algorithm ***publicKey***	1.2.840.10045.4.3.21 ECC (384 bits)		Sha256ECDSA Prime384v1/P-384

			Nota: Até à EC CC 007 (inclusive) a chave pública destas Sub-EC's é rsaEncryption (RSA) com 4096 bits
8. *X.509v3 Extensions*		m	--
8.1 *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	--
8.2 *Subject Key Identifier*	<Composto pela hash de 160-bit SHA-1 do valor da BIT STRING da chave pública do certificado>	m	--
8.3 *Key Usage*	*Key Certificate Signature* *CRL Signature*	mc	Uso do certificado e par de chaves, de acordo com secção 3.2.
8.4 *Certificate Policies*		m	--
policyIdentifier ***policyQualifiers***	2.5.29.32.0 *policyQualiflierID*: 1.3.6.1.5.5.7.2.1 *cPSuri*: https://www.scee.gov.pt/rep		Identificador de política, conforme indicado na "Declaração de Práticas de Certificação do SCEE", indicando o URL do repositório onde se encontra esse documento.
policyIdentifier ***policyQualifiers***	2.16.620.1.1.1.2.4.0.7 *policyQualiflierID*: 1.3.6.1.5.5.7.2.1 *cPSuri*: //pki2.cartaodecidadao.pt/publico/praticas-certificacao		Significa que o certificado emitido está de acordo com a "Declaração de Práticas de Certificação da EC CC", indicando o URL do repositório onde se encontra esse documento. **Nota:** Para EC's emitidas por ECs CC anteriores à EC CC 008, o URL é https://pki.cartaodecidadao.pt/publico/politicas/cps.html
policyIdentifier ***policyQualifiers***	<OID do perfil de certificado emitido, cf. secção 2.2> *policyQualiflierID*: 1.3.6.1.5.5.7.2.1 *cPSuri*: pki2.cartaodecidadao.pt/publico/politica-certificados		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.

			Nota: Para EC's emitidas por ECs CC anteriores à EC CC 008, o URL é https://pki.cartaodecidadao.pt/publico/politicas/cp.html
8.5 *Basic Constraints*	--	mc	--
CA ***PathLenConstraint***	TRUE 0		Certificado emitido para Entidade de Certificação.
8.6 *CRLDistributionPoints*	http://pki2.cartaodecidadao.pt/entidade-certificacao-cc/lista-revogacao/CC_Root<ID_CA>.crl	m	URI para a LCR onde pode ser verificado a validade do certificado. **Nota:** Para EC's emitidas por ECs CC anteriores à EC CC 008, o URL é http://pki.cartaodecidadao.pt/publico/lrc/cc_ec_cidadao_crl<ID_CA>_crl.crl
8.7 *Authority Information Access*	--	m	--
accessMethod ***accessLocation***	1.3.6.1.5.5.7.48.1 http://ocsp.root.pki2.cartaodecidadao.pt/ocsp		OCSP URI para serviço de validação OCSP onde pode ser verificado a validade do certificado. **Nota:** Para EC's emitidas por ECs CC anteriores à EC CC 008, o URL é http://ocsp.root.cartaodecidadao.pt/publico/ocsp
9. *Signature Algorithm*	1.2.840.10045.4.3.2	m	sha256ECDSA **Nota**: Até à EC CC 007 (inclusive) este campo assume o valor sha256withRSA
10. *Signature Value*	<contém a assinatura digital do certificado, efetuada pela chave privada da EC CC>	m	Ao gerar esta assinatura, a EC certifica a ligação entre a chave pública e o titular (*subject*) do certificado.

4.1.8.2 Perfil de certificado para ECD

Campo	Valor	Tipo[Erro! Marcador não definido.]	Comentários
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 CC 007 (inclusive) este campo assume o valor sha256withRSA
4. *Issuer Distinguished Name*	C = PT O = SCEE – Sistema de Certificação Electrónica do Estado OU = ECEstado CN = Cartão de Cidadão <nnn>[8]	m	--
5. *Validity*		m	Validade de dez anos e um mês. Utilizado para assinar estruturas de informação durante o primeiro mês de validade e renovado (com geração de novo par de chaves) antes de perfazer o primeiro mês de validade.
not Before ***not After***	<data de emissão> <data de emissão + 10 anos e um mês>		
6. *Subject Distinguished Name*	<cf. indicado na secção 3.1.1>	m	--
7. *Subject Public Key Info*		m	--
algorithm ***publicKey***	1.2.840.10045.4.3.21 ECC (256 bits)		Sha256ECDSA Prime256v1/P-256 **Nota**: Até à EC CC 007 (inclusive) a chave pública é rsaEncryption (RSA) com 4096 bits

Campo	Valor	Tipo[Erro! Marcador não definido.]	Comentários
8. *X.509v3 Extensions*		m	--
8.1 *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	--
8.2 *Subject Key Identifier*	<Composto pela hash de 160-bit SHA-1 do valor da BIT STRING da chave pública do certificado>	m	--
8.3 *Key Usage*	*Digital Signature*	mc	--
8.4 *Certificate Policies*		**m**	**--**
policyIdentifier *policyQualifiers*	2.16.620.1.1.1.2.4.0.7 *policyQualifierID*: 1.3.6.1.5.5.7.2.1 *cPSuri*: //pki2.cartaodecidadao.pt/publico/praticas-certificacao		Significa que o certificado emitido está de acordo com a "Declaração de Práticas de Certificação da EC CC", indicando o URL do repositório onde se encontra esse documento. **Nota:** Para EC's emitidas por ECs CC anteriores à EC CC 008, o URL é https://pki.cartaodecidadao.pt/publico/politicas/cps.html
policyIdentifier *policyQualifiers*	<OID do perfil de certificado emitido, cf. secção 2.2> *policyQualifierID*: 1.3.6.1.5.5.7.2.1 *cPSuri*: pki2.cartaodecidadao.pt/publico/politica-certificados		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. **Nota:** Para EC's emitidas por ECs CC anteriores à EC CC 008, o URL é https://pki.cartaodecidadao.pt/publico/politicas/cp.html
8.5 *Basic Constraints*		mc	
CA	FALSE		--

Campo	Valor	Tipo[Erro! Marcador não definido.]	Comentários
8.6 *CRLDistributionPoints*	http://pki2.cartaodecidadao.pt/entidade-certificacao-cc/lista-revogacao/CC_Root<ID_CA>.crl	m	URI para a LCR onde pode ser verificado a validade do certificado. **Nota:** Para EC's emitidas por ECs CC anteriores à EC CC 008, o URL é http://pki.cartaodecidadao.pt /publico/lrc/cc_ec_cidadao_crl<ID_CA>_crl.crl
8.7 *Authority Information Access*		m	--
accessMethod *accessLocation*	1.3.6.1.5.5.7.48.1 http://ocsp.root.pki2.cartaodecidadao.pt/ocsp		OCSP URI para serviço de validação OCSP onde pode ser verificado a validade do certificado. **Nota:** Para EC's emitidas por ECs CC anteriores à EC CC 008, o URL é http://ocsp.root.cartaodecidadao.pt/publico/ocsp
9. *Signature Algorithm*	1.2.840.10045.4.3.2	m	sha256ECDSA **Nota**: Até à EC CC 007 (inclusive) este campo assume o valor sha256withRSA
10. *Signature Value*	<contém a assinatura digital do certificado, efetuada pela chave privada da EC CC>	m	Ao gerar esta assinatura, a EC certifica a ligação entre a chave pública e o titular (*subject*) do certificado.

4.1.8.3 Perfil de certificado de VA

Campo	Valor	Tipo[Erro! Marcador não definido.]	Comentários
1. Version	3 (0x2)	m	----

Campo	Valor	Tipo[Erro! Marcador não definido.]	Comentários
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 CC 007 (inclusive) este campo assume o valor sha256withRSA
4. Issuer Distinguished Name	C = PT O = SCEE – Sistema de Certificação Electrónica do Estado OU = ECEstado CN = Cartão de Cidadão <nnn>[8]	m	--
5. Validity		m	Validade de 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 primeiro mês de validade.
not Before ***not After***	<data de emissão> <data de emissão + 1.900 dias>		
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 CC 007 (inclusive) a chave pública é rsaEncryption (RSA) com 2048 bits de tamanho
8. X.509v3 Extensions		m	--

Campo	Valor	Tipo[Erro! Marcador não definido.]	Comentários
8.1 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	--
8.2 Subject Key Identifier	<Composto pela hash de 160-bit SHA-1 do valor da BIT STRING da chave pública do certificado>	m	--
8.3 Key Usage	*Digital Signature* *Non Repudiation*	mc	Uso do certificado e par de chaves, de acordo com secção 3.2.
8.4 Extended Key Usage	1.3.6.1.5.5.7.3.9 (OCSP Signing)	m	
8.5 Certificate Policies		m	--
policyIdentifier ***policyQualifiers***	2.16.620.1.1.1.2.4.0.7 *policyQualifierID*: 1.3.6.1.5.5.7.2.1 *cPSuri*: http://pki2.cartaodecidadao.pt/publico/praticas-certificacao		Significa que o certificado emitido está de acordo com a "Declaração de Práticas de Certificação da EC CC", indicando o URL do repositório onde se encontra esse documento. **Nota:** Para EC's emitidas por ECs CC anteriores à EC CC 008, o URL é https://pki.cartaodecidadao.pt/publico/politicas/cps.html
policyIdentifier ***policyQualifiers***	<OID do perfil de certificado emitido, cf. secção 2.2> *policyQualifierID*: 1.3.6.1.5.5.7.2.1 *cPSuri*: http://pki2.teste.cartaodecidadao.pt/publico/politica-certificados		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. **Nota:** Para EC's emitidas por ECs CC anteriores à EC CC 008, o URL é https://pki.cartaodecidadao.pt/publico/politicas/cp.html
8.6 Basic Constraints		mc	--
CA	FALSE		--

Campo	Valor	Tipo[Erro! Marcador não definido.]	Comentários
8.7 CRLDistributionPoints	http://pki2.cartaodecidadao.pt/entidade-certificacao-assinatura/lista-revogacao/CC_<EC><Id_EC>_partition<num_seq>.crl	m	URI para a LCR onde pode ser verificado a validade do certificado. **Nota:** Para EC's emitidas por ECs CC anteriores à EC CC 008, o URL é http://pki.cartaodecidadao.pt /publico/lrc/cc_ec_cidadao_crl<ID_CA>_crl.crl
8.8 Authority Information Access		m	--
accessMethod ***accessLocation***	1.3.6.1.5.5.7.48.1 http://ocsp.root.pki2.cartaodecidadao.pt/ocsp		OCSP URI para serviço de validação OCSP onde pode ser verificado a validade do certificado. **Nota:** Para EC's emitidas por ECs CC anteriores à EC CC 008, o URL é http://ocsp.root.cartaodecidadao.pt/publico/ocsp
8.9 OCSPNocheck	NULL	o	Não é uma extensão definida no RFC 5280, mas encontra-se definida no RFC 6960 (id-pkix-ocsp-nocheck) e em https://www.alvestrand.no/objectid/1.3.6.1.5.5.7.48.1.5.html. Esta extensão indica ao cliente OCSP que este certificado é confiável, mesmo sem o validar junto do servidor OCSP ou LCR.
9. Signature Algorithm	1.2.840.10045.4.3.2	m	sha256ECDSA **Nota**: Até à EC CC 007 (inclusive) este campo assume o valor sha256withRSA
10. Signature Value	<contém a assinatura digital do certificado, efetuada pela chave privada da EC CC>	m	Ao gerar esta assinatura, a EC certifica a ligação entre a chave pública e o titular (*subject*) do certificado.

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 que 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.509[11] | ISO/IEC 9594-8[12],
- RFC 5280[10],
- Política de Certificados do SCEE e Requisitos Mínimos de Segurança[2].

A EC CC emite a LCR completa com uma periodicidade semanal, e não emite delta-LCR. 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 CC, 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 CC são utilizadas as seguintes extensões obrigatórias, não críticas:

- *CRLNumber*, implementado de acordo com as recomendações do RFC 5280[10];
- *AuthorityKeyIdentifier*: contém o *hash* (SHA-1) da chave pública da EC que assinou a LCR.

4.2.2.1 LCR da EC CC

Campo	Valor	Tipo[Erro! Marcador não definido.]	Comentários
1. *Version*	2 (0x1)	m	--
2. *Signature*	1.2.840.10045.4.3.2	m	sha256ECDSA **Nota**: Até à EC CC 007 (inclusive) este campo assume o valor sha256withRSA
3. *Issuer Distinguished Name*	C = PT O = SCEE – Sistema de Certificação Electrónica do Estado OU = ECEstado CN = Cartão de Cidadão <nnn>[8]	m	--
4. *thisUpdate*	<data de emissão da LCR>	m	--
5. *nextUpdate*	<data da próxima emissão da LCR = *thisUpdate* + 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 mês.
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	--

Campo	Valor	Tipo[Erro! Marcador não definido.]	Comentários
6.2 *CRL Number*	<número sequencial único da LCR>	m	--
7. *Revoked Certificates*		m	Estrutura com os certificados revogados, constituída por uma sequência de estruturas *Serial Number* (uma estrutura *Serial Number*, 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> *Reason Code*: <motivo de revogação do certificado>	m o	Valor tem de ser um dos seguintes (cf. RFC 5280[10]): 0 – *unspecified* 1 – *keyCompromise* 2 – *cACompromise* 3 – *affiliationChanged* 4 – *superseded* 5 – *cessationOfOperation* 6 – *certificateHold* 8 – *removeFromCRL* 9 – *privilegeWithdrawn* 10 – *aACompromise*
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 CC>	m	--

4.3 Perfil de resposta OCSP

O serviço de validação OCSP[9] dos certificados emitidos pela EC do Cartão de Cidadão encontra-se disponível em http://ocsp.root.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 RFC 6960[9].

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*[16], 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 do Cartão de Cidadão e que não se encontrem revogados (embora possam já não estar dentro do seu período de validade);
- "*revoked*" para certificado emitidos pela EC do Cartão de Cidadão e que se encontrem revogados;
- "*unknown*", para certificados que não tenham sido emitidos pela EC do Cartão de Cidadão.

[16] 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.

Assinado por: **DIOGO DE CAMPOS MONTEIRO BRÁS**
Num. de Identificação: 10295504
Data: 2024.03.01 13:40:35+00'00'

CARTÃO DE CIDADÃO

Assinado por: **RICARDO JOÃO CORREIA VIEIRA**
Num. de Identificação: 13004962
Data: 2024.05.06 15:13:58+01'00'

CARTÃO DE CIDADÃO