# Política de Certificados da EC do Cartão de Cidadão

## Políticas (POL#22)

**Estado do documento**

Este documento é controlado e aprovado pelo Instituto dos Registos e do Notariado, I.P. (IRN). Embora possa ser impresso, **a versão eletrónica assinada digitalmente pelo(s) membro(s) do Grupo de Gestão constitui a única cópia controlada**. Qualquer cópia impressa deste documento é considerada **não controlada**.

Por se tratar de um documento controlado e de acesso público, poderá ser arquivado em unidades locais ou de rede, bem como consultado diretamente no repositório da PKI do Cartão de Cidadão, disponível em: http://pki.cartaodecidadao.pt/ e/ou http://pki2.cartaodecidadao.pt/



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

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

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

**Data:** Fev 2026

**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)<br>- 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 |
| 5.0 | Set 2025 | Alteração do campo *Organization* do Certificado da EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão |
| **6.0** | **Fev 2026** | **Atualização para eIDAS 2 e ETSI (EN 319 401 v3.1.1; EN 319 411-2 v2.5.1; EN 319 412-1 v1.6.1; EN 319 102-1 v1.4.1; TS 119 312 v1.5.1** |

### 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.<br>Disponível em https://pki2.cartaodecidadao.pt/publico/politica-certificados |
| **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.<br>Disponível em https://pki2.cartaodecidadao.pt/publico/politica-certificados |

# Índice

# 1 Introdução

A Entidade de Certificação do Cartão de Cidadão (EC CC) é uma Entidade Certificadora Sub-Raiz do Sistema de Certificação Eletrónica do Estado (SCEE), integrada na hierarquia de confiança do Estado Português e responsável pela emissão de certificados para:

- Entidades Certificadoras subordinadas do Cartão de Cidadão (EC AsC, EC AuC, EC CMD);
- Serviços associados ao Cartão de Cidadão, incluindo certificados para Entidade Certificadora de Documentos (ECD) e validação online (VA/OCSP);
- Infraestrutura criptográfica necessária ao funcionamento do Cartão de Cidadão.

A EC CC fornece a base de confiança para todos os certificados emitidos na infraestrutura do Cartão de Cidadão, assegurando:

- a autenticidade e integridade das chaves públicas emitidas;
- o correto encadeamento da hierarquia de certificação do SCEE;
- os mecanismos de validação do estado dos certificados (LCR e OCSP);
- o suporte técnico-normativo à utilização de certificados qualificados de pessoa singular e certificados operacionais.

A presente Política de Certificados (POL#22) define os perfis X.509, extensões, campos, OIDs, requisitos de identificação e estrutura dos certificados emitidos pela EC CC, bem como os perfis da Lista de Certificados Revogados (LCR) e das respostas OCSP emitidas pela EC CC.

Esta Política assegura conformidade integral com:

- o Regulamento (UE) n.º 910/2014, com as alterações introduzidas pelo Regulamento (UE) 2024/1183 (eIDAS 2);
- o Decreto-Lei n.º 12/2021, que executa o regime eIDAS na ordem jurídica nacional;
- os referenciais técnicos ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2 e ETSI EN 319 412 (partes 1, 2 e 5);
- a Política de Certificados do SCEE e Requisitos Mínimos de Segurança;
- a Declaração de Práticas de Certificação da EC CC (POL#27), a qual prevalece em caso de conflito.

Esta Política é complementada pela Declaração de Divulgação de Princípios da EC CC (POL#20) e pelas Políticas de Certificados das EC subordinadas (POL#23, POL#24, etc.), assegurando uniformidade na hierarquia de certificação do Cartão de Cidadão.

## 1.1 Público-Alvo

Este documento destina-se a:

- Entidades Certificadoras subordinadas da EC CC;
- Entidades que validam certificados da hierarquia do Cartão de Cidadão;
- Autoridades de Supervisão e Organismos de Avaliação de Conformidade;

- Implementadores e operadores de sistemas que utilizam certificados do SCEE;
- Fabricantes e integradores do Cartão de Cidadão;
- Partes confiantes e utilizadores avançados que necessitam compreender o perfil técnico dos certificados emitidos pela EC CC.

Recomenda-se que o leitor esteja familiarizado com infraestruturas de chave pública (PKI), certificados digitais X.509 e mecanismos de validação (LCR/OCSP).

A leitura desta Política deve ser complementada com a Declaração de Práticas de Certificação da EC CC (POL#27) e com a Política de Certificados do SCEE, pelas quais a EC CC se rege e que estabelecem a base normativa e organizacional aplicável.

# 2 Contexto Geral

Este O presente documento estabelece os parâmetros aplicáveis aos perfis de certificados, à Lista de Certificados Revogados (LCR) e às respostas OCSP emitidas pela Entidade de Certificação do Cartão de Cidadão (EC CC). O seu objetivo consiste em definir, de forma estruturada e tecnicamente rigorosa, os elementos essenciais que caracterizam a política de certificados da EC CC, assegurando a sua conformidade com os referenciais nacionais e europeus aplicáveis.

Este documento deve ser interpretado em articulação com a Declaração de Práticas de Certificação da EC do Cartão de Cidadão (POL#27), que estabelece as práticas operacionais, organizacionais, técnicas e de segurança que suportam a emissão e gestão dos certificados descritos na presente política. A POL#27 constitui o documento normativo que define o enquadramento procedimental e os controlos aplicáveis à infraestrutura de certificação, regulando, entre outros, o ciclo de vida dos certificados, a gestão de chaves, a segurança física e lógica, a auditoria, o controlo de acessos e os mecanismos de registo e arquivo.

A Política de Certificados (POL#22) descreve, assim, os requisitos e características dos perfis de certificados, enquanto a Declaração de Práticas de Certificação (POL#27) define os processos e práticas que garantem o cumprimento destes requisitos. Os dois documentos devem ser lidos como complementares e coerentes entre si, formando o quadro normativo completo da atividade da EC CC.

Os certificados emitidos pela EC CC incluem uma referência explícita à presente política, permitindo que partes confiantes acedam diretamente ao seu conteúdo através dos qualificadores de política incluídos nos certificados, conforme previsto nas normas X.509 e RFC 5280.

## 2.1 Visão Geral

A presente política assegura a conformidade com os requisitos estabelecidos na Declaração de Práticas de Certificação da EC CC (POL#27) e na Política de Certificados do Sistema de Certificação Eletrónica do Estado (SCEE), pela qual a EC CC se rege.

Adicionalmente, o documento cumpre os requisitos aplicáveis previstos no Regulamento (UE) n.º 910/2014 (eIDAS) e no Regulamento (UE) 2024/1183 (eIDAS 2), que atualiza o quadro europeu relativo aos serviços de confiança e à identidade digital. Conforme definido pelo regulador europeu, o eIDAS 2 mantém o enquadramento relativo a certificados eletrónicos qualificados, reforça os requisitos de atuação dos prestadores de serviços de confiança e introduz o novo *European Digital Identity Wallet* (EUDI *Wallet*) como mecanismo interoperável para armazenamento e utilização de credenciais digitais, incluindo certificados eletrónicos.

O alinhamento com estes referenciais garante que os certificados emitidos pela EC CC são interoperáveis, auditáveis e conformes às práticas europeias aplicáveis à prestação de serviços de confiança qualificados, incluindo requisitos de segurança, supervisão, certificação e interoperabilidade.

## 2.2 Designação e Identificação do Documento

A Política de Certificados da EC do Cartão de Cidadão (POL#22) é identificada nos certificados eletrónicos através de identificadores de objeto (OID) específicos, distintos conforme o perfil de certificado emitido. Estes OIDs permitem às aplicações confiantes determinar automaticamente a política aplicável a cada certificado e aceder ao respetivo documento através do URI incluído no qualificador de política.

O documento é caracterizado pelos seguintes elementos formais:

***INFORMAÇÃO DO DOCUMENTO***

| | |
|---|---|
| ***NOME*** | Política de Certificados da EC do Cartão de Cidadão |
| ***VERSÃO*** | 6.0 |
| ***ESTADO*** | Aprovado |
| ***OID*** | De acordo com o perfil de certificado emitido:<br>• 2.16.620.1.1.1.2.4.0.1.2 – Certificado da EC de Assinatura Digital Qualificada do Cartão de Cidadão (EC AsC);<br>• 2.16.620.1.1.1.2.4.0.1.3 – Certificado da EC de Autenticação do Cartão de Cidadão (EC AuC);<br>• 2.16.620.1.1.1.2.4.0.1.5 – Certificado para Entidade Certificadora de Documentos (ECD);<br>• 2.16.620.1.1.1.2.4.0.1.6 – Certificado de Validação on-line OCSP (VA);<br>• 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*** | Fev 2026 |
| ***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 |

Os OIDs associados aos perfis de certificados obedecem à estrutura definida na hierarquia da EC CC e garantem conformidade com a estrutura regulamentar e técnica definida pela política do SCEE, pela POL#27 e pelas normas europeias aplicáveis, incluindo o enquadramento de eIDAS e eIDAS 2. Esta estrutura assegura ainda a interoperabilidade com o ecossistema europeu de identidade digital, incluindo a futura integração com o EUDI *Wallet*, conforme previsto pelos atos de implementação do eIDAS 2 publicados entre 2024 e 2025).

# 3 Identificação e Autenticação

O processo de identificação e autenticação adotado pela Entidade de Certificação do Cartão de Cidadão (EC CC) assegura que cada certificado emitido corresponde inequivocamente à entidade titular da chave pública nele contida. Este processo fundamenta-se em critérios técnicos e procedimentais definidos na Política de Certificados (POL#22), na Declaração de Práticas de Certificação (POL#27) e nos requisitos estabelecidos pelo Regulamento (UE) n.º 910/2014 (eIDAS) e pelo Regulamento (UE) 2024/1183 (eIDAS 2).

A identificação rigorosa do titular do certificado e a garantia de que este detém o controlo da respetiva chave privada constituem pilares essenciais da confiança depositada no ecossistema de certificação eletrónica do Estado Português. Os mecanismos adotados garantem autenticidade, integridade e não repúdio, assegurando que a ligação entre o certificado e o seu titular é tecnicamente robusta e juridicamente válida.

## 3.1 Atribuição de Nomes

A atribuição de nomes segue modelo X.500 e cumpre as normas internacionais aplicáveis ao formato de certificados X.509. Cada certificado contém um ***Distinguished Name*** **(DN)** que identifica univocamente o respetivo titular, garantindo consistência, unicidade e alinhamento com os referenciais técnicos do SCEE.

O DN é composto por atributos normalizados (tais como *Country*, *Organization*, *Organizational Unit e Common Name*), cuja utilização é definida de acordo com o perfil de certificado. A construção do DN observa princípios de interoperabilidade e compatibilidade, permitindo que sistemas confiantes processem automaticamente o conteúdo do certificado e determinem o contexto da sua emissão.

### 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 AsC contêm no campo "*Subject*", um DN, para utilização como identificador único de cada entidade, de acordo com o RFC 5280[1], atualizados pelos RFCs 6818[2], 8398[3] e 8399[4], em que:

a) O DN contem sempre valor, não pode ser nulo.

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

c) Nos certificados atribuídos a serviços, no DN é inscrito o nome da organização (ou um nome que permita determinar qual a organização) responsável pela sua operação (patrocinador);

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):

[1] IETF RFC 5280 - *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*
[2] IETF RFC 6818 - *Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*
[3] IETF RFC 8398 - *Internationalized Email Addresses in X.509 Certificates*
[4] IETF RFC 8399 - *Internationalization Updates to RFC 5280*

#### 3.1.1.1 Certificado da EC CC

O DN da EC Raiz do CC:

| *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>[5] |

#### 3.1.1.2 EC's subordinadas da EC CC

A EC CC emite certificados para as:

| *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 | Agência para a Reforma Tecnológica do Estado, 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>[5] | EC de Autenticação do Cartão de Cidadão <nnnn>[5] | EC de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão <nnnn>[5] |

#### 3.1.1.3 Certificados de Serviços

O DN identifica os serviços do Cartão de Cidadão que atuam como titulares dos certificados destinados a funções operacionais (ex.: validação online, certificadora de documentos).

A EC emite os certificados para os serviços seguinte com o DN:

| *ATRIBUTO (CÓDIGO)* | *CERTIFICADO PARA ASSINATURA DE DOCUMENTOS* | *CERTIFICADO DE VA* |
|---|---|---|
| ***COUNTRY (C)*** | PT | PT |

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

| *ATRIBUTO (CÓDIGO)* | *CERTIFICADO PARA ASSINATURA DE DOCUMENTOS* | *CERTIFICADO DE VA* |
|---|---|---|
| ***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>[5] | Serviço de Validação on-line do Cartão de Cidadão <nnn>[5] - EC do Cartão de Cidadão |

#### 3.1.1.4 Certificados de Pessoas Singulares

Esta EC não emite certificados para pessoas singulares.

## 3.2 Uso do certificado e par de chaves pelo titular

Os certificados emitidos pela EC CC devem ser utilizados em conformidade com a finalidade definida no respetivo perfil. Cada certificado estabelece:

- o titular autorizado,
- o conjunto de usos permitidos (ex.: assinatura digital, autenticação, validação, assinatura de OCSP),
- restrições aplicáveis,
- requisitos de proteção da chave privada.

O titular tem responsabilidade exclusiva pela guarda da chave privada, devendo assegurar a sua utilização segura e reportar imediatamente qualquer suspeita de compromisso.

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 |

| *Perfil de certificado* | *Titular* | *Uso do certificado e par de chaves* |
|---|---|---|
| | | serviços, assim como para a assinatura da respetiva Lista de Certificados Revogados (LCR). |
| ***Certificado da EC CMD*** | ARTE – Agência para a Reforma Tecnológica do Estado, 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*** Assinatura de Documentos | 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[6] (consulta do estado atual de certificados digitais), garantindo e permitindo verificar a integridade e não-repúdio dessas mesmas respostas. |

## 3.3 Conformidade Regulamentar e Interoperabilidadade

O modelo de identificação e autenticação adotado pela EC CC assegura conformidade com:

- as políticas e práticas consignadas nesta política e na POL#27;
- os requisitos técnicos das normas X.509 e RFC aplicáveis;
- o quadro regulamentar europeu eIDAS e eIDAS 2, incluindo a futura integração com o **EUDI Wallet**, onde certificados qualificados podem ser armazenados e utilizados.

A adoção destes referenciais garante interoperabilidade europeia, confiança jurídica e alinhamento com os mecanismos de supervisão previstos no quadro regulamentar europeu.

[6] IETF RFC 6960, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*

# 4 Perfis de Certificado, LCR e OCSP

A Entidade de Certificação do Cartão de Cidadão (EC CC) emite certificados digitais X.509 v3 que estabelecem uma relação verificável entre uma chave pública e a entidade titular. Estes certificados obedecem aos referenciais técnicos e regulamentares aplicáveis, assegurando a autenticidade, integridade, validade temporal e conformidade legal das transações eletrónicas realizadas no contexto do Cartão de Cidadão.

O presente capítulo descreve os perfis de certificado, bem como os perfis das Listas de Certificados Revogados (LCR) e das respostas OCSP emitidas pela EC CC. As características aqui definidas seguem as normas técnicas aplicáveis, nomeadamente ITU-T X.509, RFC 5280 e RFC 6960, e estão alinhadas com os requisitos da POL#27 e do Regulamento eIDAS/eIDAS2.

## 4.1 Perfil de Certificado

Os utilizadores de uma chave pública devem poder confiar que a chave privada correspondente é detida exclusivamente pelo titular (pessoa singular, pessoa coletiva ou sistema) com o qual irão estabelecer operações criptográficas, nomeadamente mecanismos de cifra, assinatura digital ou autenticação forte. Esta confiança é assegurada através da utilização de **certificados digitais X.509 v3**, que constituem estruturas de dados normalizadas destinadas a associar, de forma autenticada, uma chave pública ao respetivo titular.

A relação entre o titular e a chave pública é garantida pela **assinatura digital do certificado** por uma Entidade de Certificação (EC) reconhecida na hierarquia de confiança. A EC fundamenta esta afirmação com base em procedimentos técnicos e operacionais adequados, incluindo, entre outros:

- verificação da **prova de posse da chave privada**, através de protocolos de desafio-resposta;
- validação de processos seguros de geração e custódia das chaves;
- processos formais de registo e identificação do titular, conforme definidos na POL#27.

Os certificados possuem um **período de validade limitado**, indicado no próprio certificado e protegido pela assinatura da EC. Como a assinatura e o período de validade podem ser verificados independentemente por qualquer aplicação confiável, os certificados podem ser distribuídos por redes públicas e armazenados em diversos tipos de suportes sem comprometer a sua integridade.

Sempre que um serviço de segurança exige a utilização de uma chave pública, o utilizador deve obter e validar o certificado que contém essa chave. Caso o serviço não detenha previamente uma cópia autêntica da chave pública da EC que assinou o certificado, ou não disponha das informações necessárias (como o nome da EC ou o respetivo período de validade), poderá ser necessária a obtenção e validação de certificados adicionais. Em muitos casos, a validação completa de um certificado implica a verificação de **toda a cadeia de certificação**, incluindo:

- o certificado do titular,
- zero ou mais certificados de ECs subordinadas,
- o certificado da EC emissora até à EC Raiz.

Esta cadeia deve permitir estabelecer uma linha ininterrupta de confiança até à entidade certificadora de topo.

Os perfis de certificado emitidos pela EC CC — tanto no âmbito da EC Raiz como das EC subordinadas — cumprem integralmente os referenciais técnicos aplicáveis, nomeadamente:

- **ITU-T X.509 / ISO/IEC 9594-8**,

- **RFC 5280** (Internet X.509 Public Key Infrastructure Certificate and CRL Profile),
- **Política de Certificados do SCEE e Requisitos Mínimos de Segurança**,
- **RFC 3739** (Qualified Certificates Profile),
- **ETSI TS 119 412-1** (estrutura comum de dados para perfis de certificados),
- **ETSI TS 119 412-2** (perfis de certificados emitidos a pessoas singulares),
- **ETSI TS 119 412-5** (declarações QCStatements aplicáveis a certificados qualificados).

A EC CC emite certificados com os perfis e finalidades definidos na secção 3, assegurando a interoperabilidade, a conformidade regulamentar e a adequada aplicação a serviços de identificação, autenticação, assinatura digital qualificada, validação e certificação de dados no ecossistema do Cartão de Cidadão.

### 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[7]).

Até à EC CC 002 (inclusive), estes campos continham o OID 1.2.840.113549.1.1.5 (sha1WithRSAEncryptino[8]). Da EC CC 003 até à EC CC 007 contêm o valor 1.2.840.113549.1.1.11 (sha-256WithRSAEncryption[9]).

### 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*" ("*policyQualiflierID*: 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*".

[7] ecdsa-with-SHA256 OBJECT IDENTIFIER::= { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2 }
[8] sha-1WithRSAEncryption OBJECT IDENTIFIER::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 }
[9] sha-256WithRSAEncryption OBJECT IDENTIFIER::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}

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.

### 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 certificados X.509 v3 emitidos pela Entidade de Certificação do Cartão de Cidadão (EC CC) incluem um conjunto de campos obrigatórios e extensões críticas e não críticas que asseguram a identificação do titular, a validação da cadeia de certificação, a definição da política aplicável e a determinação das finalidades autorizadas para o uso da chave pública. Os campos e extensões implementados seguem as especificações do **RFC 5280** e das normas ETSI aplicáveis ao perfil de certificados qualificados.

As subseções seguintes descrevem, de forma estruturada e normativa, os elementos que constituem o perfil de certificado utilizado na hierarquia da 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 | 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<br>**Nota**: Até à EC CC 007 (inclusive) este campo assume o valor sha256withRSA |
| **4.** ***Issuer Distinguished Name*** | C = PT<br>O = SCEE – Sistema de Certificação Electrónica do Estado<br>OU = ECEstado<br>CN = Cartão de Cidadão <nnn>[5] | 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***<br>***not After*** | <data de emissão><br><data de emissão + 12 anos + 6 meses> | | |
| **6.** ***Subject Distinguished Name*** | <cf. indicado na secção 3> | m | -- |
| **7.** ***Subject Public Key Info*** | | m | -- |
| ***algorithm***<br>***publicKey*** | 1.2.840.10045.4.3.21<br>ECC (384 bits) | | Sha256ECDSA<br>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*<br>*CRL Signature* | mc | Uso do certificado e par de chaves, de acordo com secção 3.2. |
| **8.4** ***Certificate Policies*** | | m | -- |
| ***policyIdentifier***<br>***policyQualifiers*** | 2.5.29.32.0<br>*policyQualifierID*: 1.3.6.1.5.5.7.2.1<br>*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***<br>***policyQualifiers*** | 2.16.620.1.1.1.2.4.0.7<br>*policyQualifierID*: 1.3.6.1.5.5.7.2.1<br>*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.<br>**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***<br>***policyQualifiers*** | <OID do perfil de certificado emitido, cf. secção 2.2><br>*policyQualifierID*: 1.3.6.1.5.5.7.2.1<br>*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***<br>***PathLenConstraint*** | TRUE<br>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.<br>**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***<br>***accessLocation*** | 1.3.6.1.5.5.7.48.1<br>http://ocsp.root.pki2.cartaodecidadao.pt/ocsp | | OCSP<br>URI para serviço de validação OCSP onde pode ser verificado a validade do certificado.<br>**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<br>**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 Servido de assinatura de dados (ECD)

| Campo | Valor | Tipo | 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<br>**Nota**: Até à EC CC 007 (inclusive) este campo assume o valor sha256withRSA |
| **4. *Issuer Distinguished Name*** | C = PT<br>O = SCEE – Sistema de Certificação Electrónica do Estado<br>OU = ECEstado<br>CN = Cartão de Cidadão <nnn>[5] | 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***<br>***not After*** | <data de emissão><br><data de emissão + 10 anos e um mês> | | |
| **6. *Subject Distinguished Name*** | <cf. indicado na secção 3> | m | -- |
| **7. *Subject Public Key Info*** | | m | -- |
| ***algorithm***<br>***publicKey*** | 1.2.840.10045.4.3.21<br>ECC (256 bits) | | Sha256ECDSA<br>Prime256v1/P-256<br>**Nota**: Até à EC CC 007 (inclusive) a chave pública é rsaEncryption (RSA) com 4096 bits |

| Campo | Valor | Tipo | 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*<br>*policyQualifiers* | 2.16.620.1.1.1.2.4.0.7<br>*policyQualifierID*: 1.3.6.1.5.5.7.2.1<br>*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.<br>**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*<br>*policyQualifiers* | <OID do perfil de certificado emitido, cf. secção 2.2><br>*policyQualifierID*: 1.3.6.1.5.5.7.2.1<br>*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.<br>**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 | 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.<br>**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*<br>*accessLocation* | 1.3.6.1.5.5.7.48.1<br>http://ocsp.root.pki2.cartaodecidadao.pt/ocsp | | OCSP<br>URI para serviço de validação OCSP onde pode ser verificado a validade do certificado.<br>**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<br>**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 | 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 |

| Campo | Valor | Tipo | Comentários |
|---|---|---|---|
| | | | **Nota**: Até à EC CC 007 (inclusive) este campo assume o valor sha256withRSA |
| ***4. Issuer Distinguished Name*** | C = PT<br>O = SCEE – Sistema de Certificação Electrónica do Estado<br>OU = ECEstado<br>CN = Cartão de Cidadão <nnn>[5] | 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***<br>***not After*** | <data de emissão><br><data de emissão + 1.900 dias> | | |
| ***6. Subject Distinguished Name*** | <cf. indicado na secção 3> | m | |
| ***7. Subject Public Key Info*** | | m | -- |
| ***algorithm***<br>***publicKey*** | 1.2.840.10045.4.3.2<br>ECC (256 bits) | | Sha256ECDSA<br>prime256v1/P-256<br>**Nota**: Até à EC CC 007 (inclusive) a chave pública é rsaEncryption (RSA) com 2048 bits de tamanho |
| ***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 | -- |

| Campo | Valor | Tipo | Comentários |
|---|---|---|---|
| ***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*<br>*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***<br>***policyQualifiers*** | 2.16.620.1.1.1.2.4.0.7<br>*policyQualiflierID*: 1.3.6.1.5.5.7.2.1<br>*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.<br>**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***<br>***policyQualifiers*** | <OID do perfil de certificado emitido, cf. secção 2.2><br>*policyQualiflierID*: 1.3.6.1.5.5.7.2.1<br>*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.<br>**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 | | -- |
| ***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.<br>**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 |

| Campo | Valor | Tipo | Comentários |
|---|---|---|---|
| ***8.8 Authority Information Access*** | | m | -- |
| ***accessMethod***<br>***accessLocation*** | 1.3.6.1.5.5.7.48.1<br><br>http://ocsp.root.pki2.cartaodecidadao.pt/ocsp | | OCSP<br>URI para serviço de validação OCSP onde pode ser verificado a validade do certificado.<br>**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<br>**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 permaneça válido. Contudo, determinadas circunstâncias podem exigir que um certificado seja invalidado antes da sua expiração. Tais circunstâncias incluem a alteração de atributos do titular, a cessação da relação entre o titular e a entidade associada ao certificado, ou o comprometimento – real ou suspeito – da chave privada correspondente. Sob tais circunstâncias, a EC deve proceder à sua revogação, quando tenha conhecimento de tais factos.

O modelo X.509 define o mecanismo de revogação do certificado suportado pela emissão periódica, de uma Lista de Certificados Revogados (LCR), uma estrutura assinada digitalmente pela EC que identifica, por número de série, os certificados revogados e o momento da revogação. A LRC é disponibilizada num repositório público e pode ser obtida por qualquer aplicação que necessite de validar um certificado. Durante a validação a aplicação deve verificar:

1. A assinatura e integridade da LRC;
2. O período de validade da LRC (*thisUpdate / nextUpdate*);
3. A presença ou ausência do número de série do certificado consultado.

O perfil da LCR está conforme com as seguintes normas:

- **ITU.T X.509 | ISO/IEC 9594-8**, no que respeita à estrutura e semântica das LCR;
- **RFC 5280**, relativamente à sintaxe de LCR v2, extensões obrigatórias e processamento;
- Política de Certificados do SCEE e Requisitos Mínimos de Segurança, relativamente aos requisitos nacionais aplicáveis.

A EC CC emite e publica, numa periodicidade mensal, a **LCR** contendo todos os certificados revogados.

A EC assegura ainda o serviço OCSP de alta disponibilidade, permitindo obter o estado de um certificado em tempo real. O processo de publicação da LRC e OCSP cumpre os requisitos de rastreabilidade, registo e controlo previstos na **ETSI EN 319 403** e o **Regulamento (UE) 2024/1183** (eIDAS 2), garantindo a integridade, autenticidade, tempestividade e proteção dos registos associados ao processo de revogação.

### 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;
- *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 | Comentários |
|---|---|---|---|
| **1. *Version*** | 2 (0x1) | m | -- |
| **2. *Signature*** | 1.2.840.10045.4.3.2 | m | sha256ECDSA<br>**Nota**: Até à EC CC 007 (inclusive) este campo assume o valor sha256withRSA |
| **3. *Issuer Distinguished Name*** | C = PT<br>O = SCEE – Sistema de Certificação Electrónica do Estado<br>OU = ECEstado<br>CN = Cartão de Cidadão <nnn>[5] | 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.<br>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 | -- |
| **6.2 *CRL Number*** | <número sequencial único da LCR> | m | -- |

| Campo | Valor | Tipo | Comentários |
|---|---|---|---|
| **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*<br>CRL entry extensions | <data de revogação do certificado><br>*Reason Code*: <motivo de revogação do certificado> | m<br>o | Valor tem de ser um dos seguintes (cf. RFC 5280): 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[6] 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[6].

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*[10], 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.

[10] 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.

# 5 Conformidade com o Regulamento (UE) 2024/1183 (eIDAS 2)

A EC implementa controlos proporcionais e documentados em: gestão de ativos, controlo de acessos, gestão de incidentes, segurança da rede/operacional, continuidade e segurança da cadeia de fornecimento, conforme ETSI EN 319 401 v3.1.1. Estes controlos refletem as obrigações de cibersegurança previstas na Diretiva (UE) 2022/2555 (NIS2), conforme integradas na EN 319 401 v3.1.1.

# 6 Referências Normativas

- **eIDAS 2**: **Reg. (UE) 2024/1183** que altera o 910/2014 (OJ L de 30.4.2024).
- **EN 319 401 v3.1.1 (06/2024)** — Requisitos gerais para TSP (inclui alinhamento NIS2).
- **EN 319 411-2 v2.5.1 (10/2023)** — QTSP que emitem certificados qualificados.
- **EN 319 411-1 v1.5.1 (2025/2024)** — Requisitos gerais (inclui mapeamento a CA/B).
- **EN 319 412-1 v1.6.1 (06/2025)** + **EN 319 412-5 v2.4.1 (2023)** — Perfis de certificado e **QCStatements**.
- **EN 319 102-1 v1.4.1 (06/2024)** — Criação e validação de AdES.
- **EN 319 421 v1.2.1 (05/2023)** — TSA (Política e Segurança) e **EN 319 422** — Perfis RFC 3161/5816.
- **TS 119 312 v1.5.1 (12/2024)** — **Cryptographic Suites** (inclui datas-limite para tamanhos de chave; RSA <3000 bits até 2028).
- **TR 119 411-4 v1.3.1 (09/2025)** — Checklist de auditoria para EN 319 411-1/-2

# Aprovação

Aprovado pelo Grupo de Gestão.

Assinado por: **Ricardo João Correia Vieira**
Num. de Identificação: 13004962
Data: 2026.03.04 09:17:33+00'00'

Assinado por: **DIOGO DE CAMPOS MONTEIRO BRÁS**
Num. de Identificação: 10295504
Data: 2026.03.04 13:28:47+00'00'