Política de Certificados da EC de Assinatura Digital Qualificada do Cartão de Cidadão

Políticas (POL#23)

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

Título: Política de Certificados da EC de Assinatura Digital Qualificada do Cartão de Cidadão

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

Data: Abr 2026

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

Histórico de Versões

Versão	Data	Detalhes
1.0	Jan 2022	Versão uniformizada que inclui todos os certificados emitidos pela EC de Assinatura, em substituição das Políticas de Certificados de assinatura qualificada, validação cronológica e validação on-line documento anterior.
2.0	Mar 2024	Alteração dos algoritmos de assinatura dos certificados emitidos pela EC de Assinatura Qualificada do Cartão de Cidadão
3.0	Julho 2024	Correção da validade do certificado de assinatura (inclusão da preposição "até") e inclusão do URL do site de testes da pki do Cartão de Cidadão no campo da política de divulgação de princípios
4.0	Jan 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)
5.0	**Abr 2026**	**Correção do KU dos perfis de certificados de VA e VC**

Documentos Relacionados

Documento	Autor	Descrição
Declaração de Práticas de Certificação da EC de Assinatura Digital Qualificada do Cartão de Cidadão (POL#28)	IRN	Descreve os procedimentos e práticas utilizados pela EC de Assinatura Digital Qualificada do Cartão de Cidadão para suportar a sua atividade de emissão de certificados qualificados. Disponível em https://pki2.cartaodecidadao.pt/publico/politica-certificados

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 (*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 EC CC integra-se na estrutura do Sistema de Certificação Eletrónica do Estado Português[1] (SCEE) – Infraestrutura de Chaves Públicas do Estado -, cumprindo os requisitos da Política de Certificados do SCEE e Requisitos Mínimos de Segurança[2] e alinhando-se com o Regulamento (UE) n.º 910/2014 relativo à Identificação Eletrónica e aos Serviços de Confiança para as Transações Eletrónicas no Mercado Interno (eIDAS), o qual estabelece as bases jurídicas para a identificação eletrónica, os serviços de confiança, e o seu reconhecimento transfronteiriço na União Europeia.

O presente documento - *Política de Certificados da EC de Assinatura Digital Qualificada do Cartão de Cidadão* - descreve os perfis dos certificados e lista de certificados revogados (LCR), emitidos pela EC de Assinatura Digital Qualificada do Cartão de Cidadão (EC AsC) que integra a hierarquia de confiança da EC CC, em conformidade com os requisitos estabelecidos no Regulamento eIDAS para serviços de confiança qualificados, incluindo assinaturas eletrónicas qualificadas, selos eletrónicos, carimbos temporais e outros serviços regulados.

1.1 Público-Alvo

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

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 Assinatura Digital Qualificada 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 no repositório da PKI do Cartão de Cidadão, em http://pki2.cartaodecidadao.pt.

2 Contexto Geral

O presente documento define um conjunto de parâmetros dos perfis dos certificados e lista de certificados revogados (LCR), emitidos pela EC de Assinatura Digital Qualificada do Cartão de Cidadão (EC AsC). Não se pretende nomear regras legais ou obrigações formais, mas antes disponibilizar informação clara, direta e compreensível.

Os Certificados emitidos pela EC AsC contêm uma referência à respetiva Política de Certificados (PC), permitindo que partes confiantes e outras pessoas interessadas possam aceder à informação sobre o certificado e as políticas adotadas pela entidade emissora.

A EC AsC adota, como políticas de certificado base aplicáveis aos **certificados qualificados**, as políticas com os seguintes OID:

- 0.4.0.2042.1.2 – NCP+: *Normalized Certificate Policy requiring a secure cryptographic device* (cf. ETSI EN 319 411-1[4]);
- 0.4.0.194112.1.2 – QCP-n-qscd: *Policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD* (cf. ETSI EN 319 411-2[5])
- 0.4.0.19422.1.1 - *id-etsi-tsts-EuQCompliance: By inclusion of this statement the issuer claims that this time-stamp token is issued as a qualified electronic time-stamp according to the* REGULATION (EU) No 910/2014"

Os certificados emitidos pela EC AsC estão em conformidade com a as políticas identificadas pelos OID presente no campo "*policyIdentifier*" do próprio certificado (cf. perfis de certificado na secção 4.1.8).

2.1 Visão Geral

Esta Política observa o Regulamento (UE) n.º 910/2014, alterado pelo Regulamento (UE) 2024/1183, doravante 'eIDAS', e as normas ETSI aplicáveis aos prestadores de serviços de confiança qualificados que emitem certificados qualificados para assinatura eletrónica.

2.2 Designação e Identificação do Documento (OIDs)

Este documento é a "Política de Certificados da EC de Assinatura Digital Qualificada do Cartão de Cidadão". É identificada no certificado através de um OID próprio, específico para cada perfil de certificado, conforme tabela seguinte e secção 4.1).

Os OIDs próprios da EC AsC referem-se explicitamente a políticas conformes com o Regulamento (UE) 2024/1183 e normas ETSI EN 319 411-1/2 e TS 119 412. Mantêm-se os OIDs: 0.4.0.2042.1.2 (NCP+) e 0.4.0.194112.1.2 (QCP-n-qscd), com a descrição atualizada para o contexto do eIDAS 2.

[4] ETSI EN 319 411-1 v1.5.1 *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements*
[5] ETSI EN 319 411-2 *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates*

Este documento é identificado pelos dados constantes na seguinte tabela:

INFORMAÇÃO DO DOCUMENTO

Nome	Política de Certificados da EC de Assinatura Digital Qualificada do Cartão de Cidadão
Versão	5.0
Estado	Aprovado
OID	De acordo com o perfil de certificado emitido: • 2.16.620.1.1.1.2.4.1.0.1.1– Certificado de Assinatura Digital Qualificada, emitido em conformidade com o Regulamento (UE) n.º 910/2014[6], alterado pelo Regulamento (UE) 2024/1183, e com as normas de referência estabelecidas pelo Regulamento de Execução (UE) 2025/1943. A chave privada encontra-se num dispositivo QSCD (*Qualified Signature Creation Device*) • 2.16.620.1.1.1.2.4.1.0.1.2 – Certificado de Validação on-line OCSP (VA), Certificado de Assinatura de Respostas OCSP, emitido exclusivamente para a assinatura criptográfica de respostas OCSP, em conformidade com o perfil definido na RFC 6960 e com os requisitos aplicáveis da ETSI EN 319 411-1; • 2.16.620.1.1.1.2.4.0.1.7 – Certificado de Validação Cronológica (VC), emitido como certificado qualificado de acordo com o Regulamento (UE) n.º 910/2014.
Data	Abr 2026
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

[6] Regulamento (UE) nº 910/2014 do Parlamento Europeu e do Conselho de 23 de julho de 2014 relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE.

3 Identificação e Autenticação

Os processos de verificação de identidade (presencial ou remota) cumprem a ETSI EN 319 411-2 v2.5.1: recolha e verificação de evidências, prova de vida (quando aplicável), conservação de registos, medidas anti-fraude, trilhos de auditoria, segregação de funções e revisões periódicas. As modalidades remotas admitem apenas métodos e garantias reconhecidos pela norma e exigidos pela autoridade de supervisão.

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 Assinatura Digital Qualificada do Cartão de Cidadão"[3].

3.1.1 Tipo de Nomes

Todos os 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[7], atualizados pelos RFCs 6818[8], 8398[9] e 8399[10], em que:

a) O DN contém 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):

3.1.1.1 Certificados emitidos para o Cidadão

Atributo (Código)	**Certificado de Assinatura Digital Qualificada**
*Country (**C**)*	PT
*Organization (**O**)*	Cartão de Cidadão
*Organization Unit (**OU**)*	Cidadão Português
*Organization Unit (**OU**)*	Assinatura Qualificada do Cidadão

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

Atributo (Código)	**Certificado de Assinatura Digital Qualificada**
*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<número de identificação civil>

3.1.1.2 Certificados para serviços do Cartão de Cidadão

Atributo (Código)	**Certificado de VA**	**Certificado de VC**
*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**)*	Validação on-line	Validação Cronológica
*Common Name (**CN**)*	Serviço de Validação on-line do Cartão de Cidadão <nnnnnn>[11] - EC de Assinatura Qualificada do Cidadão	Serviço de Validação Cronológica do Cartão de Cidadão <nnnnnn>[11]

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 certificado emitido (cf. secção 4.1):

Perfil de certificado	*Titular*	*Uso do certificado e par de chaves*
Certificado de Assinatura Digital Qualificada	Cidadão identificado no DN do "Subject" (cf. secção 3.1.1)	Utilizado para assinatura digital qualificada, de acordo com o Regulamento (UE) n.º 910/2014, alterado pelo Regulamento (UE) 2024/1183, e com as normas de referência estabelecidas pelo Regulamento de Execução (UE) 2025/1943, em que a chave privada se encontra num dispositivo criptográfico QSCD (*Qualified Signature Creation Device*), garantindo o não repúdio.

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

Perfil de certificado	*Titular*	*Uso do certificado e par de chaves*
Certificado de VA	EC de Assinatura Qualificada do Cartão de Cidadão	Utilizada para assinar as respostas a pedidos de validação on-line OCSP[12] (consulta do estado atual de certificados digitais), garantindo e permitindo verificar a autenticidade e integridade dessas mesmas respostas.
Certificado de VC	EC de Assinatura Qualificada do Cartão de Cidadão	Utilizada para assinar as respostas a pedidos de validações cronológicas[13] (aposição de selos temporais), garantindo e permitindo verificar a autenticidade e integridade dessas mesmas respostas.

3.3 Conformidade Regulamentar e Interoperabilidade

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

- as políticas e práticas consignadas nesta política e na POL#28;
- 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.

[12] IETF RFC 6960, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*
[13] IETF RFC 3161 (*Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*), com as alterações introduzidas pelo RFC 5816 (*ESSCertIDv2 Update for RFC 3161*).

4 Perfis de Certificado, LCR e OCSP

4.1 Perfil de Certificado

Os certificados emitidos pela EC AsC seguem o modelo X.509 v3 e estabelecem a associação entre uma chave pública e o seu titular. Esta associação garantida pela assinatura digital do certificado por uma Entidade de Certificação (EC) de confiança, permitindo que qualquer aplicação valide autonomamente a autenticidade, integridade e período de validade do certificado de acordo com o RFC 5280.

A validade de um certificado é limitada e definida no próprio objeto X.509, podendo ser distribuído por canais públicos, ou armazenado em qualquer tipo de unidades de armazenamento[14], a sua verificação é sempre efetuada através da cadeia de certificação e das listas de revogação (LCR) ou OCSP. Caso uma aplicação não disponha da chave pública da EC emissora, poderá ser necessário construir uma cadeia de certificação completa, incluindo certificados adicionais de EC intermédias.

Os certificados qualificados emitidos pela EC AsC estão conformes com:

- **ETSI EN 319 412-1 v1.6.1** (*Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures*),
- **ETSI EN 319 412-5 v2.4.1** (*Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements*), no que respeita aos *QCStatements* exigidos para certificados qualificados, incluindo id-etsi-qcs-QcCompliance, id-etsi-qcs-QcType, id-etsi-qcs-QcSSCD e id-etsi-qcs-QcPDS;
- **ETSI EN 319 412-2 (Perfil Type A)**, aplicável aos certificados qualificados de assinatura eletrónica, nomeadamente na obrigatoriedade de incluir apenas o *KeyUsage = nonRepudiation (contentCommitment)*;
- **TSI TS 119 312 v1.5.1**, no que respeita às *Cryptographic Suites* obrigatórias, tamanhos mínimos de chave, funções de hash e datas-limite de aceitação. A EC AsC utiliza algoritmos e parâmetros aprovados, incluindo RSA ≥ 3072 bits, ECC ≥ P-256 e SHA-256 ou superior, de acordo com o *eIDAS Cryptographic Requirements*.

A extensão **qcStatements** utiliza os OIDs definidos na ETSI EN 319 412-5, assegurando que cada certificado qualificado contém a declaração legal e técnica exigida pelo eIDAS, incluindo a indicação de que a chave privada reside num dispositivo QSCD quando aplicável.

A EC AsC emite certificados exclusivamente nos perfis e finalidades identificadas na secção 3.2, sendo que a especificação completa de cada perfil (campos, extensões, valores e requisitos críticos) se encontra descrita nas secções seguintes (4.1.8.x).

[14] IETF RFC 5280, atualizados pelos RFCs 6818, 8398 e 8399.

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 AsC, 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 AsC contêm o OID do algoritmo criptográfico utilizado para assinar os certificados: 1.2.840.10045.4.3.2 (ecdsa-with-SHA256[15]).

Até à EC AsC 0009 (inclusive), estes campos continham o OID 1.2.840.113549.1.1.5 (sha1WithRSAEncryptin[16]). Da EC AsC 010 até à EC AsC 0018 contêm o valor 1.2.840.113549.1.1.11 (sha-256WithRSAEncryption[17]).

Os algoritmos, tamanhos de chave e funções *hash* cumprem o eIDAS *Cryptographic Requirements* v1.4.1 (2024), incluindo: RSA ≥ 3072 bits; ECC ≥ P-256; SHA-256 ou superior; e parâmetros autorizados pelos atos de execução

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*".

4.1.6 Utilização da extensão *Policy Constraints*

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

[15] ecdsa-with-SHA256 OBJECT IDENTIFIER::= { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2 }
[16] sha-1WithRSAEncryption OBJECT IDENTIFIER::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 }
[17] 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 extensão crítica "*certificate policies*" define os identificadores de política (*policyIdentifier*) aplicáveis ao certificado e os respetivos qualificadores. A sintaxe e semântica encontram-se descritas na secção 4.1.5. Sendo uma extensão marcada como crítica, todas as aplicações que validam certificados devem processá-la obrigatoriamente, conforme RFC 5280.

No processamento destas extensões devem ser observados os seguintes princípios:

- A extensão "*certificate policies*" identifica as várias políticas seguidas na emissão do certificado, cada uma identificada de forma única através do seu OID;
- O processamento automático exige que cada política seja reconhecida pelo OID presente 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 sempre da responsabilidade da aplicação que o processa, devendo esta cumprir as regras de validação definidas no RFC 5280 e nas políticas de confiança aplicáveis.

4.1.8 Campos e extensões do certificado

Os certificados X.509 v3 utilizam um conjunto estruturado de campos e extensões que permitem associar atributos ao titular e à respetiva chave pública, bem como suportar a validação da cadeia de certificação, a verificação do estado do certificado e o cumprimento das políticas aplicáveis. Os perfis de certificado emitidos pela EC AsC utilizam os campos e extensões definidos no RFC 5280[14], complementados pelos requisitos específicos das normas ETSI EN 319 412-1/2/5, aplicáveis a certificados qualificados.

As secções seguintes especificam de forma detalhada cada campo e extensão utilizados nos perfis de certificado da EC AsC, incluindo os valores obrigatórios, críticos e opcionais, bem como os elementos exigidos para certificados qualificados (por exemplo *QCStatements*, *KeyUsage* restrito, políticas qualificadas e constrangimentos técnicos).

4.1.8.1 Perfil de certificado de Assinatura Digital Qualificada

RFC 5280		Valor	Tipo[18]	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 AsC 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 Assinatura Digital Qualificada do Cartão de Cidadão <nnnn>[11]	m	
5.	***Validity***		m	Até 10 (dez) anos e 1 mês.
	not Before	<data de emissão>		
	not After	<data de emissão +/- 10 anos e 1 mês>		

[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
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 AsC 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***	Não Repúdio	mc	Uso do certificado e par de chaves, de acordo com secção 3.2. Nota: Conforme ETSI EN 319 412-2 (Perfil Type A), o certificado qualificado de assinatura eletrónica deve ter exclusivamente KeyUsage = nonRepudiation (contentCommitment).
4.	***Certificate Policies***		m	
	policyIdentifier ***policyQualifiers***	2.16.620.1.1.1.2.10 (scee-assinatura) *policyQualiflierID*: 1.3.6.1.5.5.7.2.1 *cPSuri*: 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 assinatura, indicando o URL do repositório onde se encontra esse documento.
	policyIdentifier	2.16.620.1.1.1.2.4.1.0.7		Significa que o certificado emitido está de acordo com a "Declaração de Práticas de Certificação da EC de Assinatura Digital Qualificada do

RFC 5280		Valor	Tipo[18]	Comentários
	policyQualifiers	*policyQualifierID*: 1.3.6.1.5.5.7.2.1 *cPSuri*: http://pki2.cartaodecidadao.pt/publico/praticas-certificacao		Cartão de Cidadão", indicando o URL do repositório onde se encontra esse documento. Até à EC AsC 0018 (inclusive), o URL é http://pki.cartaodecidadao.pt/publico/politicas/dpc/cc_sub-ec_cidadao_assinatura_dpc.html
	policyIdentifier ***policyQualifiers***	2.16.620.1.1.1.2.4.1.0.1.1 *policyQualifierID*: 1.3.6.1.5.5.7.2.1 *cPSuri*: http://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. Até à EC AsC 0018 (inclusive), o URL é http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_sub-ec_cidadao_assinatura_pc.html
	policyIdentifier	0.4.0.2042.1.2		NCP+: *Normalized Certificate Policy requiring a secure cryptographic device* (cf. ETSI EN 319 411-1[4])
	policyIdentifier	0.4.0.194112.1.2		QCP-n-qscd: *Policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD* (cf. ETSI EN 319 411-2[5])
8.	***Subject Directory Attributes***		m	
	dateOfBirth	<data de nascimento do cidadão>		
9.	***Basic Constraints***		mc	
	CA	FALSE		
13.	***CRLDistributionPoints***	http://pki2.cartaodecidadao.pt/entidade-certificacao-assinatura/lista-revogacao/CC_Asc <Id_EC>_partition<num_seq>.crl	m	URI para a LCR onde pode ser verificado o estado do certificado. Até à EC AsC 0018 (inclusive), o URL é: http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_assinatura_crl<ID_EC>_p<num_seq>.crl
14.	***Freshest CRL***	--	-	URI para a delta-LCR onde pode ser verificado o estado do certificado.

RFC 5280		Valor	Tipo[18]	Comentários
				Deixa de ser usado na EC AsC 0019. Até à EC AsC 0018, o URL é http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_assinatura_crl<ID_EC>_p<num_seq>.crl
4.2.2 Private Internet Extensions				
1.	***Authority Information Access***		m	
	CA Issuer	URL=http://pki2.cartaodecidadao.pt/entidade-certificacao-assinatura/certificados/CC_Asc<Id_EC>.crt		URI para o certificado da EC emissora Passou a ser usado na EC AsC 0019
	accessMethod ***accessLocation***	1.3.6.1.5.5.7.48.1 http://ocsp.asc.pki2.cartaodecidadao.pt/ocsp		URI para serviço de validação OCSP onde pode ser verificado o estado do certificado. Até à EC AsC 0018 (inclusive), o URL é: http://ocsp.asc.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 AsC>	m	Ao gerar esta assinatura, a EC certifica a ligação entre a chave pública e o titular (*subject*) do certificado.
RFC 3739[19]		**Valor**	**Tipo**[18]	**Comentários**
Qualified Certificate Statement			m	Não é uma extensão definida no RFC 5280, mas encontra-se definida no RFC 3739 e no ETSI EN 319 412-5[20].

[19] RFC 3739 *Internet X.509 Public Key Infrastructure: Qualified Certificates Profile*
[20] ETSI EN 319 412-5 *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements*

RFC 5280	Valor	Tipo[18]	Comentários
id-qcs-pkixQCSyntax-v2	*esi4-qcStatement-1: id-etsi-qcs-QcCompliance*		*QCStatement claiming that the certificate is an EU qualified certificate, or a certificate being qualified within a defined legal framework from an identified country or set of countries*. (cf. ETSI EN 319 412-5)
id-qcs-pkixQCSyntax-v2	*esi4-qcStatement-4: id-etsi-qcs-QcSSCD*		*QCStatement claiming that the private key related to the certified public key resides in a QSCD.* (cf. ETSI EN 319 412-5)
id-qcs-pkixQCSyntax-v2	*esi4-qcStatement-6*: *id-etsi-qct-esign* *Text*: "*Certificate for electronic signatures as defined in Regulation (EU) No 910/2014*"		*QCStatement states that an EU qualified certificate is issued only with the purpose of electronic signature, according to the Regulation (EU) No 910/2014.* (cf. ETSI EN 319 412-5)
id-qcs-pkixQCSyntax-v2	*esi4-qcStatement-5: id-etsi-qcs-QcPDS* *url:* https://pki2.cartaodecidadao.pt/publico/praticas-certificacao *language:* PT		Localização da "Declaração de Divulgação de Princípios da EC CC". Notas: - Até à EC AsC 0018 (inclusive) está em https://pki.cartaodecidadao.pt/publico/politicas/cps.html. - os certificados emitidos de 11/06/2024, até 25/06/2024 contêm neste campo o URL https://pki2.teste.cartaodecidadao.pt/publico/praticas-certificacao, tendo passado após esta data, a assumir o valor indicado, https://pki2.cartaodecidadao.pt/publico/praticas-certificacao

4.1.8.2 Perfil de certificado "espécimen" de Assinatura Digital Qualificada

O certificado "espécimen" de Assinatura Digital Qualificada 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 Assinatura Digital Qualificada (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 001);

4.1.8.3 Perfil de certificado de VA

	RFC 5280	Valor	Tipo[1] [8]	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 AsC 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 CN = EC de Assinatura Digital Qualificada do Cartão de Cidadão <nnnn>[11]	m	
5.	***Validity***		m	Até 5 anos e dois meses. Utilizado para assinar respostas OCSP.
	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	

RFC 5280		Valor	Tipo[1] 8	Comentários
	algorithm ***publicKey***	1.2.840.10045.4.3.2 ECC (256 bits)		Sha256ECDSA - prime256v1/P-256 - Até à EC AsC 0018 (inclusive) Sha256RSA
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*	mc	Uso do certificado e par de chaves, de acordo com secção 3.2.
4.	***Certificate Policies***		m	
	policyIdentifier ***policyQualifiers***	2.16.620.1.1.1.2.4.1.0.7 *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 de Assinatura Digital Qualificada do Cartão de Cidadão", indicando o URL do repositório onde se encontra esse documento. **Nota**: Até à EC AsC 0018 (inclusive) está em http://pki.cartaodecidadao.pt/publico/politicas/dpc/cc_sub-ec_cidadao_assinatura_dpc.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.cartaodecidadao.pt/publico/politica-certificados		Significa que o certificado emitido está de acordo com a "Política de Certificados da EC de Assinatura Digital Qualificada 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.

RFC 5280		Valor	Tipo[1] [8]	Comentários
				Nota: Até à EC AsC 0018 (inclusive) está em http://pki.cartaodecidadao.pt/publico/politicas/pc/cc_sub-ec_cidadao_assinatura_pc.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***	http://pki2.cartaodecidadao.pt/entidade-certificacao-assinatura/lista-revogacao/CC_Asc <Id_EC>_partition<num_seq>.crl	m	URI para a LCR onde pode ser verificado o estado do certificado. **Nota**: Até à EC AsC 0018 (inclusive) está em http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_assinatura_crl<ID_CA>_p<num_seq>.crl
14.	**Freshest CRL**	--	m	Não é usado a partir da EC AsC 0018. URI para a delta-LCR onde pode ser verificado o estado do certificado. **Nota**: Até à EC AsC 0018 (inclusive) está em: http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_assinatura_crl<ID_CA>_delta_p<num_seq>.crl
4.2.2. Private Internet Extensions				
	Authority Information Access		m	
1.	***accessMethod*** ***accessLocation***	1.3.6.1.5.5.7.48.1 http://ocsp.asc.pki2.cartaodecidadao.pt/ocsp		URI para serviço de validação OCSP onde pode ser verificado o estado do certificado. **Nota:** Até à EC AsC 0018 (inclusive), o URL é: http://ocsp.asc.cartaodecidadao.pt/publico/ocsp
5. CRL and CRL Extensions Profile				
5.1. CRL Fields				

RFC 5280		Valor	Tipo[18]	Comentários
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 AsC>	m	Ao gerar esta assinatura, a EC certifica a ligação entre a chave pública e o titular (*subject*) do certificado.
RFC 6960[21]		**Valor**	**Tipo[18]**	**Comentários**
4. Details of the Protocol				
4.2. Response Syntax				
4.2.2. Notes on OCSP Responses				
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.

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

4.1.8.4 Perfil de certificado de VC

RFC 5280		Valor	Tipo[18]	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***	1.2.840.113549.1.1.11	m	sha256WithRSAEncryption
4.	***Issuer Distinguished Name***	C = PT O = Instituto dos Registos e do Notariado I. P. OU = Cartão de Cidadão OU = subECEstado CN = EC de Assinatura Digital Qualificada do Cartão de Cidadão <nnnn>[11]	m	
5.	***Validity***		m	Até aproximadamente 6 anos e seis meses. Utilizado para assinar respostas a pedidos de validações cronológicas, sendo renovado (com geração de novo par de chaves) após o primeiro ano de validade.
	not Before ***not After***	<data de emissão> <data de emissão + 6 anos e 6 meses>		
6.	***Subject Distinguished Name***	<cf. indicado na secção 3.1.1>	m	
7.	***Subject Public Key Info***		m	
	algorithm	1.2.840.113549.1.1.1		rsaEncryption (RSA)

RFC 5280		Valor	Tipo[18]	Comentários
	publicKey	3072 bit		Tamanho da chave
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*	mc	Uso do certificado e par de chaves, de acordo com secção 3.2.
4.	***Certificate Policies***		m	
	policyIdentifier ***policyQualifiers***	2.16.620.1.1.1.2.4.1.0.7 *policyQualifierID*: 1.3.6.1.5.5.7.2.1 *cPSuri*: https://pki.cartaodecidadao.pt/publico/politicas/cps.html		Significa que o certificado emitido está de acordo com a "Declaração de Práticas de Certificação da EC de Assinatura Digital Qualificada do Cartão de Cidadão", indicando o URL do repositório onde se encontra esse documento.
	policyIdentifier ***policyQualifiers***	<OID do perfil de certificado emitido, cf. secção 2.2> *policyQualifierID*: 1.3.6.1.5.5.7.2.1 *cPSuri:* https://pki.cartaodecidadao.pt/publico/politicas/cp.html		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.
9.	***Basic Constraints***		mc	
	CA	FALSE		
12.	**Extended *Key Usage***	1.3.6.1.5.5.7.3.8 (Time Stamping)	mc	
13.	***CRLDistributionPoints***	http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_assinatura_crl<ID_CA>_p<num_seq>.crl	m	URI para a LCR onde pode ser verificado o estado do certificado.

RFC 5280		Valor	Tipo[18]	Comentários
15.	***Freshest CRL***	http://pki.cartaodecidadao.pt/publico/lrc/cc_sub-ec_cidadao_assinatura_crl<ID_CA>_delta_p<num_seq>.crl	m	URI para a delta-LCR onde pode ser verificado o estado do certificado.
4.2.2. Private Internet Extensions				
1.	**8.9 *Authority Information Access***		m	
	accessMethod ***accessLocation***	1.3.6.1.5.5.7.48.1 http://ocsp.asc.cartaodecidadao.pt/publico/ocsp		URI para serviço de validação OCSP onde pode ser verificado o estado do certificado.
	8.10 Qualified Certificate Statement		m	Não é uma extensão definida no RFC 5280, mas encontra-se definida no RFC 3739 e no ETSI EN 319 412-5.
	id-qcs-pkixQCSyntax-v2	*id-etsi-tsts-EuQCompliance* *Text*: "*By inclusion of this statement the issuer claims that this time-stamp token is issued as a qualified electronic time-stamp according to the REGULATION (EU) No 910/2014*"		Conforme secção 8.1 do ETSI 319 421[22].
5. CRL and CRL Extensions Profile				
5.1. CRL Fields				
5.1.1. Certificate List Fields				
2.	***Signature Algorithm***	1.2.840.113549.1.1.11	m	sha256WithRSAEncryption
3.	***Signature Value***	<contém a assinatura digital do certificado, efetuada pela chave privada da EC AsC>	m	Ao gerar esta assinatura, a EC certifica a ligação entre a chave pública e o titular (*subject*) do certificado.

[22] ETSI EN 319 421 *Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps*

RFC 5280	Valor	Tipo[18]	Comentários
RFC 3739[19]	**Valor**	**Tipo[18]**	**Comentários**
Qualified Certificate Statement		m	Não é uma extensão definida no RFC 5280, mas encontra-se definida no RFC 3739 e no ETSI EN 319 412-5[23].
id-qcs-pkixQCSyntax-v2	*esi4-qcStatement-4: id-etsi-qcs-QcSSCD*		*QCStatement claiming that the private key related to the certified public key resides in a QSCD.* (cf. ETSI EN 319 412-5)
id-qcs-pkixQCSyntax-v2	*esi4-qcStatement-6*: *id-etsi-qct-esign* *Text*: "Certificate for electronic signatures as defined in Regulation (EU) No 910/2014"		*QCStatement states that an EU qualified certificate is issued only with the purpose of electronic signature, according to the Regulation (EU) No 910/2014.* (cf. ETSI EN 319 412-5)
id-qcs-pkixQCSyntax-v2	*esi4-qcStatement-5: id-etsi-qcs-QcPDS* *url:* https://pki.cartaodecidadao.pt/publico/politicas/cps.html *language:* PT		Localização da "Declaração de Divulgação de Princípios da EC CC" aplicável.

[23] ETSI EN 319 412-5 *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements*

4.2 Perfil da lista de certificados revogados (LCR/OCSP e Auditoria)

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**[14], relativamente à sintaxe de LCR v2, extensões obrigatórias e processamento;
- Política de Certificados do SCEE e Requisitos Mínimos de Segurança[2], relativamente aos requisitos nacionais aplicáveis.

Atualmente, as ECs AsC, e desde a EC AsC 019 (inclusive), publicam:

- **LCR completa**, emitidas com uma periodicidade diária, contendo todos os certificados revogados, não são emitidas delta-LRC's

  NOTA: Até à EC AsC018 são emitidas a **LRC's** com periodicidade semanal e em complemento são emitidas diariamente **delta-LCR**, contendo apenas os certificados revogados desde a última LCR completa emitida.

A EC AsC 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 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 AsC, 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 AsC são utilizadas as seguintes extensões obrigatórias, não críticas:

- *CRLNumber*, implementado de acordo com as recomendações do RFC 5280[14];
- *AuthorityKeyIdentifier*: contém o *hash* (SHA-1) da chave pública da EC que assinou a LCR.

4.2.2.1 LCR da EC AsC

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 Asc 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 AsC>	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 Asc 0018 o valor deste campo é: 1.2.840.113549.1.1.11 referente 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 Assinatura Digital Qualificada do Cartão de Cidadão <nnnn>[11]	m	
4.	***thisUpdate***	<data de emissão da LCR>	m	

RFC 5280		Valor	Tipo[18]	Comentários
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. Até à EC AsC 0018, N é no máximo 1 semana. Após a EC AsC 0018 o N é no máximo 1 dia.
6.	***Revoked Certificates***		m	Estrutura com os certificados revogados, constituída por uma sequência de estruturas *Serial Number* (uma estrutura *Serial Number*, 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	
5.	**Issuing Distribution Point**		mc	URI da localização da LCR. Até à EC Asc 0018 o URL é: http://pki.cartaodecidadao.pt /publico/lrc/cc_ sub-ec_cidadao_assinatura_crl<ID_CA>_ p<num_seq>.crl
	distributionPoint	http://pki2.cartaodecidadao.pt/entidade-certificacao-assinatura/lista-revogacao/CC_Asc <Id_EC>_partition<num_seq>.crl		
6.	**Freshest CRL**		m	URI da localização da delta-LCR. Este campo é utilizado nas CRL's emitidas pelas EC AsC até à 0018 (inclusive), com o URL http://pki.cartaodecidadao.pt /publico/lrc/cc_ sub-ec_cidadao_assinatura_crl<ID_CA>_delta_p<num_seq>.crl
	distributionPoint			

RFC 5280		Valor	Tipo[18]	Comentários
				A partir da EC AsC 0019 (inclusive) este campo não é usado.
5.3. CRL Entry Extensions				
	CRL entry extensions	*Reason Code*: <motivo de revogação do certificado>	o	Valor tem de ser um dos seguintes (cf. RFC 5280[14]): 0 – *unspecified;* 1 – *keyCompromise;* 2 – *cACompromise;* 3 – *affiliationChanged;* 4 – *superseded;* 5 – *cessationOfOperation;* 6 – *certificateHold;* 8 – *removeFomCRL;* 9 – *privilegeWithdrawn;* 10 – *aACompromise*

4.2.2.2 Delta-LCR da EC AsC

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

Campo	Valor	Tipo[18]	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 Assinatura Digital Qualificada do Cartão de Cidadão <nnnn>[11]	m	
4. *thisUpdate*	<data de emissão da LCR>	m	

Campo	Valor	Tipo[18]	Comentários
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 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_assinatura_crl<ID_CA>_ p<num_seq>.crl		
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[14]): 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

Campo	Valor	Tipo[18]	Comentários
9. Signature Value	<contém a assinatura digital da LCR, efetuada pela chave privada da EC AsC>	m	

4.3 Perfil de resposta OCSP

O serviço de validação OCSP[12] dos certificados emitidos pela EC AsC encontra-se disponível em http://ocsp.asc.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[12].

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

[24] 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: **DIOGO DE CAMPOS MONTEIRO BRÁS**
Num. de Identificação: 10295504
Data: 2026.04.15 13:00:19+01'00'

Assinado por: **Ricardo João Correia Vieira**
Num. de Identificação: 13004962
Data: 2026.04.17 10:29:25+01'00'

Assinado por: **André Ferreira Ferrão Couto e Vasconcelos**
Data: 2026.04.15 19:27:44+01'00'