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

Políticas (POL#23)

Nível de Acesso: Público

Versão: 3.0

Data: Julho 2024

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

Identificador do Documento: POL#23

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

Tipologia Documental: Políticas

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

Nível de acesso: Público

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

Data: Julho 2024

Versão atual: 3.0

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

Histórico de Versões

Versão	Data	Detalhes
1.0	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.**

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.

Estado do documento

Este é um documento controlado e aprovado pelo IRN.

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

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

Índice

1 Introdução

Decorrente da implementação de vários programas públicos para a promoção das tecnologias de informação e comunicação e a introdução de novos processos de relacionamento em sociedade, entre cidadãos, empresas, organizações não-governamentais e o Estado, com vista ao fortalecimento da sociedade de informação e do governo eletrónico (*eGovernment*), o Cartão de Cidadão fornece os mecanismos necessários para a autenticação digital forte da identidade do Cidadão perante os serviços da Administração Pública, assim como as assinaturas eletrónicas indispensáveis aos processos de desmaterialização que têm vindo a ser disponibilizados pelo Estado.

A infraestrutura da Entidade de Certificação do Cartão de Cidadão (ou EC CC) fornece uma hierarquia de confiança, que promove a segurança eletrónica do Cidadão no seu relacionamento com o Estado. A EC CC estabelece uma estrutura de confiança eletrónica que proporciona a realização de transações eletrónicas seguras, a autenticação forte, um meio de assinar eletronicamente transações ou informações e documentos eletrónicos, assegurando a sua autoria, integridade e não repúdio, e assegurando a confidencialidade das transações ou informação.

A hierarquia de confiança da Entidade de Certificação do Cartão de Cidadão encontra-se englobada na hierarquia do Sistema de Certificação Eletrónica do Estado Português[1] (SCEE) – Infraestrutura de Chaves Públicas do Estado, de acordo com os requisitos da "Política de Certificados do SCEE e Requisitos Mínimos de Segurança"[2].

Este documento (Política de Certificados da EC 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 faz parte integrante da hierarquia de confiança da Entidade de Certificação do Cartão de Cidadão.

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, mas antes informar, pelo que se pretende que este documento seja simples, direto e entendido por um público alargado.

Os Certificados emitidos pela EC AsC contêm uma referência à Política de Certificados (PC) de modo a permitir que partes confiantes e outras pessoas interessadas possam encontrar informação sobre o certificado e sobre as políticas seguidas pela entidade que o emitiu.

A EC AsC adota como políticas de certificado base (para os 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 conforme as várias políticas identificadas pelos OID indicados no campo "*policyIdentifier*" do certificado (cf. perfis de certificado na secção 4.1.8).

2.1 Visão Geral

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

2.2 Designação e Identificação do Documento

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

Este documento é identificado pelos dados constantes na seguinte tabela:

INFORMAÇÃO DO DOCUMENTO	
Nome	Política de Certificados da EC de Assinatura Digital Qualificada do Cartão de Cidadão

[4] ETSI EN 319 411-1 *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*

Versão	3.0
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, de acordo com Regulamento (UE) nº 910/2014[6], e em que a chave privada se encontra num dispositivo criptográfico QSCD (*Qualified Signature Creation Device*) • 2.16.620.1.1.1.2.4.1.0.1.2 – certificado de Validação on-line OCSP (VA); • 2.16.620.1.1.1.2.4.0.1.7 – certificado de Validação Cronológica (VC).
Data	Julho 2024
Validade	Até 2 (dois) anos após a sua aprovação, ou até que seja substituído por uma nova versão (o que ocorrer primeiro)
Localização	http://pki2.cartaodecidadao.pt/publico/politica-certificados

[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

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 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[7], atualizados pelos RFCs 6818[8], 8398[9] e 8399[10], 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):

- 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
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>

[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*

- 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 Regulamento (UE) nº 910/2014[6], em que a chave privada se encontra num dispositivo criptográfico QSCD.
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 integridade e não-repúdio 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 integridade e não-repúdio dessas mesmas respostas.

[11] <nnnnnn> (ou <nnnn>) é um valor sequencial iniciado em "000001" (ou "0001") na emissão do primeiro certificado deste tipo.
[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 utilizadores de uma chave pública confiam que a chave privada associada é detida pelo titular (pessoa ou sistema) com o qual irão utilizar mecanismos de cifra ou assinatura digital. Esta confiança é obtida através do uso de certificados digitais X.509 v3, que são estrutura de dados que fazem a ligação entre a chave pública e o seu titular. Esta ligação é afirmada através da assinatura digital de cada certificado, por uma Entidade de Certificação (EC) de confiança. A EC pode basear esta afirmação em meios técnicos (por exemplo, prova de posse da chave privada através de um protocolo desafio-resposta), na apresentação da chave privada, ou no registo efetuado pelo titular.

Um certificado tem um período limitado de validade, indicado no seu conteúdo e assinado pela EC. Como a assinatura do certificado e a sua validade podem ser verificadas independentemente por qualquer software que utilize certificados, estes podem ser distribuídos através de linhas de comunicação e sistemas públicos, assim como podem ser guardados em qualquer tipo de unidades de armazenamento[14].

O utilizador de um serviço de segurança que requeira o conhecimento da chave pública do utilizador necessita, normalmente, de obter e validar o certificado que contém essa chave. Se o serviço não dispuser de uma cópia fidedigna da chave pública da EC que assinou o certificado, assim como do nome da EC e informação relacionada (tal como o período de validade), então poderá necessitar um certificado adicional para obter a chave pública da EC e validar a chave pública do utilizador. Em geral, para validar a chave pública de um utilizador, pode ser necessária uma cadeia de múltiplos certificados, incluindo o certificado da chave pública do utilizador assinado por uma EC e, zero ou mais certificados adicionais de ECs assinados por outras ECs[14].

Os perfis dos certificados emitidos pela EC AsC estão conformes com:

- Recomendação ITU.T X.509[15] | ISO/IEC 9594-8[16],
- RFC 5280[14],
- Política de Certificados do SCEE e Requisitos Mínimos de Segurança[2],
- RFC 3739 (*Internet X.509 Public Key Infrastructure: Qualified Certificates Profile*),
- ETSI TS 119 412-1 (*Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures*),
- ETSI TS 119 412-2 (*Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons*), e
- ETSI TS 119 412-5 (*Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements*).

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

[14] IETF RFC 5280, atualizados pelos RFCs 6818, 8398 e 8399.
[15] *ITU-T Recommendation X.509. 2019: Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*
[16] ISO/IEC 9594-8:2017 *Information technology — Open Systems Interconnection — The Directory — Part 8: Public-key and attribute certificate frameworks*

4.1.1 Número da Versão

O campo "*version*" do certificado descreve a versão utilizada na codificação do certificado. Nos perfis dos certificados emitidos pela EC 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[17]).

Até à EC AsC 0009 (inclusive), estes campos continham o OID 1.2.840.113549.1.1.5 (sha1WithRSAEncryptino [18]). Da EC AsC 010 até à EC AsC 0018 contêm o valor 1.2.840.113549.1.1.11 (sha-256WithRSAEncryption[19]).

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.

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.

---

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

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

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

4.1.8 Campos e extensões do certificado

Os campos e as extensões definidas para os certificados X.509 v3 fornecem métodos para associar atributos a titulares ou chaves públicas, assim como para gerir a hierarquia de certificação. Nos perfis dos certificados emitidos pela EC AsC podem ser utilizados os campos e extensões identificadas no RFC 5280[14].

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

4.1.8.1 Perfil de certificado de Assinatura Digital Qualificada

RFC 5280		Valor	Tipo[20]	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 ***not After***	<data de emissão> <data de emissão + 10 anos e 1 mês>		

[20] 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[20]	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***	*Non Repudiation*	mc	Uso do certificado e par de chaves, de acordo com secção 3.2.
4.	***Certificate Policies***		m	
	policyIdentifier ***policyQualifiers***	2.16.620.1.1.1.2.10 (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 ***policyQualifiers***	2.16.620.1.1.1.2.4.1.0.7 *policyQualiflierID*: 1.3.6.1.5.5.7.2.1		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",

RFC 5280		Valor	Tipo[20]	Comentários
		cPSuri: http://pki2.cartaodecidadao.pt/publico/praticas-certificacao		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 *policyQualiflierID*: 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

RFC 5280		Valor	Tipo[20]	Comentários
14.	***Freshest CRL***	--	-	URI para a delta-LCR onde pode ser verificado o estado do certificado. 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[21]	Valor	Tipo[20]	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[22].
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

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

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 0000001);

4.1.8.3 Perfil de certificado de VA

RFC 5280		Valor	Tipo[20]	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

RFC 5280		Valor	Tipo[20]	Comentários
	not Before ***not After***	<data de emissão> <data de emissão + 1.900 dias>		respostas OCSP.
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 Até à EC AsC 0018 (inclusive)
4.2 Certificate Extension				
4.2.1 Standard Extensions			m	
1.	***Authority Key Identifier***	<Composto pela hash de 160-bit SHA-1 do valor da BIT STRING da chave pública correspondente à chave privada utilizada para assinar o certificado>	m	
2.	***Subject Key Identifier***	<Composto pela hash de 160-bit SHA-1 do valor da BIT STRING da chave pública do certificado>	m	
3.	***Key Usage***	*Digital Signature* *Non Repudiation*	mc	Uso do certificado e par de chaves, de acordo com secção 3.2.
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.

RFC 5280		Valor	Tipo[20]	Comentários
				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> *policyQualiflierID*: 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. **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

RFC 5280		Valor	Tipo[20]	Comentários
4.2.2. Private Internet Extensions				
1.	***Authority Information Access***		m	
	accessMethod	1.3.6.1.5.5.7.48.1		URI para serviço de validação OCSP onde pode ser verificado o estado do certificado.
	accessLocation	http://ocsp.asc.pki2.cartaodecidadao.pt/ocsp		**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				
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[23]		**Valor**	**Tipo[20]**	**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				

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

RFC 5280		Valor	Tipo[20]	Comentários
	id-pkix-ocsp-nocheck	**OCSPNocheck**: NULL	o	Não é uma extensão definida no RFC 5280, mas encontra-se definida no RFC 6960 (id-pkix-ocsp-nocheck). Esta extensão indica ao cliente OCSP que este certificado é confiável, mesmo sem o validar junto do servidor OCSP ou LCR.

4.1.8.4 Perfil de certificado de VC

RFC 5280		Valor	Tipo[20]	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	

RFC 5280		Valor	Tipo[20]	Comentários
5.	***Validity***		m	Até aproximadamente 6 anos e seis meses. Utilizado para assinar respostas a pedidos de validações cronológicas durante o primeiro ano de validade, 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 ***publicKey***	1.2.840.113549.1.1.1 3072 bit		rsaEncryption (RSA) 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* *Non Repudiation*	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 *policyQualiflierID*: 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

RFC 5280		Valor	Tipo[20]	Comentários
				documento.
	policyIdentifier ***policyQualifiers***	<OID do perfil de certificado emitido, cf. secção 2.2> *policyQualiflierID*: 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.
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.

RFC 5280		Valor	Tipo[20]	Comentários
	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[24].
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.
RFC 3739[21]		**Valor**	**Tipo[20]**	**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[25].
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-

[24] ETSI EN 319 421 *Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps*
[25] ETSI EN 319 412-5 *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements*

RFC 5280	Valor	Tipo[20]	Comentários
			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.

4.2 Perfil da lista de certificados revogados (LCR)

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

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

O perfil da LCR está conforme com:

- Recomendação ITU.T X.509[15] | ISO/IEC 9594-8[16],
- RFC 5280[14],
- Política de Certificados do SCEE e Requisitos Mínimos de Segurança[2].

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

4.2.1 Número da Versão

O campo "*version*" da LCR descreve a versão utilizada na codificação da LCR. Nos perfis das LCR emitidos pela EC 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[20]	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	

RFC 5280		Valor	Tipo[20]	Comentários
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. 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.

RFC 5280		Valor	Tipo[20]	Comentários
	distributionPoint			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 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 que 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*

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[20]	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	
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
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*[26], 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.

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

Aprovação

Aprovado pelo Grupo de Gestão.

Assinado por: **DIOGO DE CAMPOS MONTEIRO BRÁS**
Num. de Identificação: 10295504
Data: 2024.08.22 16:25:54+01'00'

CARTÃO DE CIDADÃO