AN INFOCERT COMPANY

PERFILES DE CERTIFICADOS

AC CAMERFIRMA 2021 V1.1

31/03/2023

PUB-2022-18-05

INDICE

1 INTRODUCCIÓN

El presente documento especifica los perfiles de certificados que AC Camerfirma SA emite bajo la jerarquía CAMERFIRMA ROOT 2021.

Los perfiles de certificado se especifican mediante tablas con la siguiente leyenda:

O = Obligatorio	
√	Obligatorio
X	Opcional
-	No presente

C = Extensión Crítica	
√	Sí
-	No

2 CERTIFICADOS DE CA

2.1 CAMERFIRMA ROOT 2021

Campo	Contenido	O	C	Observaciones
1. TBSCertificate				
1.1 Version	V3	√	-	[RFC5280]
1.2 Serial number	34612ca9b6c37a12fe6550a06b28eeeceebaf3e4	√	-	[20 bytes]
1.3 Signature Algorithm	sha384WithRSAEncryption	√	-	OID 1.2.840.113549.1.1.12
1.4 Issuer		√	-	
1.4.1 countryName (C)	ES	√	-	OID 2.5.4.6 [PRINTABLE STRING]
1.4.2 stateOrProvinceName	MADRID	√	-	OID 2.5.4.8 [UTF8 STRING]
1.4.3 localityName (L)	MADRID	√	-	OID 2.5.4.7 [UTF8 STRING]
1.4.4 serialNumber	A82743287	√	-	OID 2.5.4.5 [PRINTABLE STRING]
1.4.5 organizationName (O)	AC CAMERFIRMA S.A.	√	-	OID 2.5.4.10 [UTF8 STRING]
1.4.6 commonName (CN)	CAMERFIRMA ROOT 2021	√	-	OID 2.5.4.3 [UTF8 STRING]
1.5 Validity		√	-	
1.5.1 notBefore	19/10/2021 12:26:35 (Hora UTC)	√	-	UTC Time
1.5.2 notAfter	13/10/2045 12:26:35 (Hora UTC)	√	-	UTC Time
1.6 Subject		√	-	
1.6.1 countryName (C)	ES	√	-	OID 2.5.4.6 [PRINTABLE STRING]
1.6.2 stateOrProvinceName	MADRID	√	-	OID 2.5.4.8 [UTF8 STRING]

1.6.3 localityName (L)	MADRID	√	-	OID 2.5.4.7 [UTF8 STRING]
1.6.4 serialNumber	A82743287	√	-	OID 2.5.4.5 [PRINTABLE STRING]
1.6.5 organizationName (O)	AC CAMERFIRMA S.A.	√	-	OID 2.5.4.10 [UTF8 STRING]
1.6.6 commonName (CN)	CAMERFIRMA ROOT 2021	√	-	OID 2.5.4.3 [UTF8 STRING]
1.7 Subject Public Key Info	rsaEncryption	√	-	Clave pública de 4.096 bits [RFC3279] OID 1.2.840.113549.1.1.1
1.8 Extensions				
1.8.1 Standard Extensions				
1.8.1.1 Authority Key Identifier	No está presente	-	-	OID 2.5.29.35
1.8.1.2 Subject Key Identifier	5111327a10d0d88c4c098497b1a93eb254ba87c9	√	-	OID 2.5.29.14
1.8.1.3 Key Usage		√	√	OID 2.5.29.15
1.8.1.3.1 digitalSignature	No seleccionado “0”	-	-	
1.8.1.3.2 contentCommitment	No seleccionado “0”	-	-	
1.8.1.3.3 keyEncipherment	No Seleccionado “0”	-	-	
1.8.1.3.4 dataEncipherment	No seleccionado “0”	-	-	
1.8.1.3.5 keyAgreement	No seleccionado “0”	-	-	
1.8.1.3.6 keyCertSign	Seleccionado “1”	√	-	
1.8.1.3.7 cRLSign	Seleccionado “1”	√	-	
1.8.1.3.8 encipherOnly	No seleccionado “0”	-	-	
1.8.1.3.9	No seleccionado “0”	-	-	

decipherOnly				
1.8.1.4 Certificate Policies	No está presente	-	-	OID 2.5.29.32
1.8.1.5 Policy Mappings	No está presente	-	-	OID 2.5.29.33
1.8.1.6 Subject Alternative Name	No está presente	-	-	OID 2.5.29.17
1.8.1.7 Issuer Alternative Name	No está presente	-	-	OID 2.5.29.18
1.8.1.8 Subject Directory Attributes	No está presente	-	-	OID 2.5.29.9
1.8.1.9 Basic Constraints		√	√	OID 2.5.29.19
1.8.1.9.1 cA	TRUE	√	-	
1.8.1.9.2 pathLenConstraint	No está presente	-	-	
1.8.1.10 Name Constraints	No está presente	-	-	OID 2.5.29.30
1.8.1.11 Policy Constraints	No está presente	-	-	OID 2.5.29.36
1.8.1.12 Extended Key Usage	No está presente	-	-	OID 2.5.29.37
1.8.1.13 CRL Distribution Points	No está presente	-	-	OID 2.5.29.31
1.8.1.14 Inhibit Any-Policy	No está presente	-	-	
1.8.1.15 Freshest CRL	No está presente	-	-	
1.8.2 Internet Certificate Extensions				
1.8.2.1.1 Authority Information Access	No está presente	-	-	OID 1.3.6.1.5.5.7.1.1
1.8.2.2 Subject Information Access	No está presente	-	-	

2.2 AC CAMERFIRMA QUALIFIED CERTIFICATES - 2021

Campo	Contenido	O	C	Observaciones
1. TBSCertificate				
1.1 Version	V3	√	-	[RFC5280]
1.2 Serial number	1c200d921123b898380fc2b92419bba99b94c2c2	√	-	[20 bytes]
1.3 Signature Algorithm	sha384WithRSAEncryption	√	-	OID 1.2.840.113549.1.1 .12
1.4 Issuer		√	-	
1.4.1 countryName (C)	ES	√	-	OID 2.5.4.6 [PRINTABLE STRING]
1.4.2 stateOrProvinceName	MADRID	√	-	OID 2.5.4.8 [UTF8 STRING]
1.4.3 localityName (L)	MADRID	√	-	OID 2.5.4.7 [UTF8 STRING]
1.4.4 serialNumber	A82743287	√	-	OID 2.5.4.5 [PRINTABLE STRING]
1.4.5 organizationName (O)	AC CAMERFIRMA S.A.	√	-	OID 2.5.4.10 [UTF8 STRING]
1.4.6 commonName (CN)	CAMERFIRMA ROOT 2021	√	-	OID 2.5.4.3 [UTF8 STRING]
1.5 Validity		√	-	
1.5.1 notBefore	20 de octubre de 2021 15:12:16 (Hora UTC)	√	-	UTC Time
1.5.2 notAfter	16 de octubre de 2037 15:12:16 (Hora UTC)	√	-	UTC Time
1.6 Subject		√	-	
1.6.1 countryName (C)	ES	√	-	OID 2.5.4.6 [PRINTABLE STRING]
1.6.2 stateOrProvinceName	MADRID	√	-	OID 2.5.4.8 [UTF8 STRING]

1.6.3 localityName (L)	MADRID	√	-	OID 2.5.4.7 [UTF8 STRING]
1.6.4 organizationName (O)	AC CAMERFIRMA S.A.	√	-	OID 2.5.4.10 [UTF8 STRING]
1.6.5 organizationalUnitName (OU)	PKI SERVICES	√	-	OID 2.5.4.11 [UTF8 STRING]
1.6.6 serialNumber	A82743287	√	-	OID 2.5.4.5 [PRINTABLE STRING]
1.6.7 organizationIdentifier	VATES-A82743287	√	-	[ETSI EN 319 412-1] OID 2.5.4.97 [UTF8 STRING]
1.6.8 commonName (CN)	AC CAMERFIRMA QUALIFIED CERTIFICATES - 2021	√	-	OID 2.5.4.3 [UTF8 STRING] [Tamaño máx. 64]
1.7 Subject Public Key Info	rsaEncryption	√	-	Clave pública de 4.096 bits [RFC3279] OID 1.2.840.113549.1.1.1
1.8 Extensions				
1.8.1 Standard Extensions				
1.8.1.1 Authority Key Identifier		√	-	OID 2.5.29.35
1.8.1.1.1 keyIdentifier	5111327a10d0d88c4c098497b1a93eb254ba87c9	√	-	
1.8.1.1.2 authorityCertIssuer	No está presente	-	-	
1.8.1.1.3 authorityCertSerialNumber	No está presente	-	-	
1.8.1.2 Subject Key Identifier	c76f2dc4108a6eddf3116569c64a437bc30f6814	√	-	OID 2.5.29.14
1.8.1.3 Key Usage		√	√	OID 2.5.29.15

1.8.1.3.1 digitalSignature	No seleccionado “0”	-	-	
1.8.1.3.2 contentCommitment	No seleccionado “0”	-	-	
1.8.1.3.3 keyEncipherment	No Seleccionado “0”	-	-	
1.8.1.3.4 dataEncipherment	No seleccionado “0”	-	-	
1.8.1.3.5 keyAgreement	No seleccionado “0”	-	-	
1.8.1.3.6 keyCertSign	Seleccionado “1”	√	-	
1.8.1.3.7 cRLSign	Seleccionado “1”	√	-	
1.8.1.3.8 encipherOnly	No seleccionado “0”	-	-	
1.8.1.3.9 decipherOnly	No seleccionado “0”	-	-	
1.8.1.4 Certificate Policies		√	-	OID 2.5.29.32
1.8.1.4.1 Policy Identifier	anyPolicy	√	-	OID 2.5.29.32.0
1.8.1.4.1.1 Policy Qualifier ID		√	-	
1.8.1.4.1.1.1 CPS Pointer	URI: https://policy2021.camerfirma.com	√	-	OID 1.3.6.1.5.5.7.2.1
1.8.1.4.1.1.2 User Notice	No está presente	-	-	OID 1.3.6.1.5.5.7.2.2
1.8.1.5 Policy Mappings	No está presente	-	-	OID 2.5.29.33
1.8.1.6 Subject Alternative Name	No está presente	-	-	OID 2.5.29.17
1.8.1.7 Issuer Alternative Name	No está presente	-	-	OID 2.5.29.18
1.8.1.8 Subject Directory Attributes	No está presente	-	-	OID 2.5.29.9
1.8.1.9 Basic Constraints		√	√	OID 2.5.29.19
1.8.1.9.1 cA	TRUE	√	-	
1.8.1.9.2 pathLenConstraint	0	√	-	
1.8.1.10 Name Constraints	No está presente	-	-	OID 2.5.29.30

1.8.1.11 Policy Constraints	No está presente	-	-	OID 2.5.29.36
1.8.1.12 Extended Key Usage		√	-	OID 2.5.29.37
1.8.1.12.1 serverAuth	No está presente	-	-	OID 1.3.6.1.5.5.7.3.1
1.8.1.12.2 clientAuth	Presente	√	-	OID 1.3.6.1.5.5.7.3.2
1.8.1.12.3 codeSigning	No está presente	-	-	OID 1.3.6.1.5.5.7.3.3
1.8.1.12.4 emailProtection	Presente	√	-	OID 1.3.6.1.5.5.7.3.4
1.8.1.12.5 timeStamping	No está presente	-	-	OID 1.3.6.1.5.5.7.3.8
1.8.1.12.6 OCSPSigning	No está presente	-	-	OID 1.3.6.1.5.5.7.3.9
1.8.1.12.7 Microsoft Smart Card Logon for Windows	No está presente	-	-	OID 1.3.6.1.4.1.311.20.2.2
1.8.1.13 CRL Distribution Points		√	-	OID 2.5.29.31
1.8.1.13.1 CRL Distribution Point 1	http://crl.ca.camerfirma.com/camerfirmaroot2021.crl	√	-	
1.8.1.13.2 CRL Distribution Point 2	http://crl1.ca.camerfirma.com/camerfirmaroot2021.crl	√		
1.8.1.14 Inhibit Any-Policy	No está presente	-	-	
1.8.1.15 Freshest CRL	No está presente	-	-	
1.8.2 Internet Certificate Extensions				
1.8.2.1.1 Authority Information Access		√	-	OID 1.3.6.1.5.5.7.1.1
1.8.2.1.1.1 accessMethod	id-ad-ocsp	√	-	OID 1.3.6.1.5.5.7.48.1
1.8.2.1.1.2 accessLocation	URI: http://ocsp2021.camerfirma.com	√	-	
1.8.2.1.2.1 accessMethod	id-ad-calssuers	√		OID 1.3.6.1.5.5.7.48.2

1.8.2.1.2.2 accessLocation	URI: http://ca.camerfirma.com/certs/camerfirmaroot2021.crt	√	-	
1.8.2.2 Subject Information Access	No está presente	-	-	

3 CERTIFICADOS DE OCSP RESPONDER

3.1 OCSP RESPONDER CAMERFIRMA ROOT 2021

Campo	Contenido	O	C	Observaciones
1. TBSCertificate				
1.1 Version	V3	√	-	[RFC5280]
1.2 Serial number	<proviene de la CA>	√	-	Establecido automáticamente por la CA [20 bytes]
1.3 Signature Algorithm	sha256WithRSAEncryption	√	-	OID 1.2.840.113549.1.1.11
1.4 Issuer		√	-	
1.4.1 countryName (C)	ES	√	-	OID 2.5.4.6 [PRINTABLE STRING]
1.4.2 stateOrProvinceName	MADRID	√	-	OID 2.5.4.8 [UTF8 STRING]
1.4.3 localityName (L)	MADRID	√	-	OID 2.5.4.7 [UTF8 STRING]
1.4.4 serialNumber	A82743287	√	-	OID 2.5.4.5 [PRINTABLE STRING]
1.4.5 organizationName (O)	AC CAMERFIRMA S.A.	√	-	OID 2.5.4.10 [UTF8 STRING]
1.4.6 commonName (CN)	CAMERFIRMA ROOT 2021	√	-	OID 2.5.4.3 [UTF8 STRING]
1.5 Validity	365 días	√	-	
1.5.1 notBefore	<a incorporar cuando se emita el certificado>	√	-	UTC Time
1.5.2 notAfter	<a incorporar cuando se emita el certificado>	√	-	UTC Time
1.6 Subject		√	-	
1.6.1 countryName (C)	ES	√	-	OID 2.5.4.6 [PRINTABLE STRING]
1.6.2 stateOrProvinceName	MADRID	√	-	OID 2.5.4.8 [UTF8 STRING]
1.6.3 localityName (L)	MADRID	√	-	OID 2.5.4.7 [UTF8 STRING]
1.6.4 serialNumber	A82743287	√	-	OID 2.5.4.5 [PRINTABLE STRING]
1.6.5 organizationName (O)	AC CAMERFIRMA S.A.	√	-	OID 2.5.4.10 [UTF8 STRING]
1.6.6 commonName (CN)	OCSP RESPONDER CAMERFIRMA ROOT 2021	√	-	OID 2.5.4.3 [UTF8 STRING]
1.7 Subject Public Key Info	rsaEncryption	√	-	Clave pública de 2.048 bits [RFC3279]

				OID 1.2.840.113549.1.1.1
1.8 Extensions				
1.8.1 Standard Extensions				
1.8.1.1 Authority Key Identifier		√	-	OID 2.5.29.35
1.8.1.1.1 keyIdentifier	5111327a10d0d88c4c098497b1a93eb254ba87c9	√	-	
1.8.1.1.2 authorityCertIssuer	No está presente	-	-	
1.8.1.1.3 authorityCertSerialNumber	No está presente	-	-	
1.8.1.2 Subject Key Identifier	<a incorporar cuando se emita el certificado>	√	-	OID 2.5.29.14
1.8.1.3 Key Usage		√	√	OID 2.5.29.15
1.8.1.3.1 digitalSignature	Seleccionado “1”	√	-	
1.8.1.3.2 contentCommitment	Seleccionado “1”	√	-	
1.8.1.3.3 keyEncipherment	No Seleccionado “0”	-	-	
1.8.1.3.4 dataEncipherment	No seleccionado “0”	-	-	
1.8.1.3.5 keyAgreement	No seleccionado “0”	-	-	
1.8.1.3.6 keyCertSign	No seleccionado “0”	-	-	
1.8.1.3.7 cRLSign	No seleccionado “0”	-	-	
1.8.1.3.8 encipherOnly	No seleccionado “0”	-	-	
1.8.1.3.9 decipherOnly	No seleccionado “0”	-	-	
1.8.1.4 Certificate Policies		√	-	OID 2.5.29.32
1.8.1.4.1 Policy Identifier	OID de la política [Camerfirma]	√	-	OID 1.3.6.1.4.1.17326.10.21.0.1
1.8.1.4.1.1 Policy Qualifier ID		√	-	
1.8.1.4.1.1.1 CPS Pointer	URI: https://policy2021.camerfirma.com	√	-	OID 1.3.6.1.5.5.7.2.1
1.8.1.4.1.1.2 User Notice	No está presente	-	-	OID 1.3.6.1.5.5.7.2.2
1.8.1.5 Policy Mappings	No está presente	-	-	OID 2.5.29.33
1.8.1.6 Subject Alternative Name	No está presente	-	-	OID 2.5.29.17

1.8.1.7 Issuer Alternative Name		√	-	OID 2.5.29.18
1.8.1.7.1 rfc822Name	ca@camerfirma.com	√	-	
1.8.1.8 Subject Directory Attributes	No está presente	-	-	OID 2.5.29.9
1.8.1.9 Basic Constraints		√	√	OID 2.5.29.19
1.8.1.9.1 cA	FALSE	√	-	
1.8.1.9.2 pathLenConstraint	No está presente	-	-	
1.8.1.10 Name Constraints	No está presente	-	-	OID 2.5.29.30
1.8.1.11 Policy Constraints	No está presente	-	-	OID 2.5.29.36
1.8.1.12 Extended Key Usage		√	√	OID 2.5.29.37
1.8.1.12.1 serverAuth	No está presente	-	-	OID 1.3.6.1.5.5.7.3.1
1.8.1.12.2 clientAuth	No está presente	-	-	OID 1.3.6.1.5.5.7.3.2
1.8.1.12.3 codeSigning	No está presente	-	-	OID 1.3.6.1.5.5.7.3.3
1.8.1.12.4 emailProtection	No está presente	-	-	OID 1.3.6.1.5.5.7.3.4
1.8.1.12.5 timeStamping	No está presente	-	-	OID 1.3.6.1.5.5.7.3.8
1.8.1.12.6 OCSPSigning	Presente	√	-	OID 1.3.6.1.5.5.7.3.9
1.8.1.12.7 Microsoft Smart Card Logon for Windows	No está presente	-	-	OID 1.3.6.1.4.1.311.20.2.2
1.8.1.13 CRL Distribution Points		√	-	OID 2.5.29.31
1.8.1.13.1 CRL Distribution Point 1	http://crl.ca.camerfirma.com/camerfirmaroot2021.crl	√	-	
1.8.1.13.2 CRL Distribution Point 2	http://crl1.ca.camerfirma.com/camerfirmaroot2021.crl	√		
1.8.1.14 Inhibit Any-Policy	No está presente	-	-	
1.8.1.15 Freshest CRL	No está presente	-	-	
1.8.2 Internet Certificate Extensions				
1.8.2.1.1 Authority Information Access		√	-	OID 1.3.6.1.5.5.7.1.1
1.8.2.1.2.1 accessMethod	id-ad-caIssuers	√	-	OID 1.3.6.1.5.5.7.48.2
1.8.2.1.2.2 accessLocation	http://ca.camerfirma.com/certs/camerfirmaroot2021.crt	√	-	
1.8.2.2 Subject Information Access	No está presente	-	-	

1.8.3 Certificate Extensions NO RFC 5280				
1.8.3.3 OCSP No Check	Presente	√	-	OID 1.3.6.1.5.5.7.48.1.5

3.2 OCSP RESPONDER AC CAMERFIRMA QUALIFIED CERTIFICATES - 2021

Campo	Contenido	O	C	Observaciones
1. TBSCertificate				
1.1 Version	V3	√	-	[RFC5280]
1.2 Serial number	<proviene de la CA>	√	-	Establecido automáticamente por la CA [20 bytes]
1.3 Signature Algorithm	sha256WithRSAEncryption	√	-	OID 1.2.840.113549.1.1.11
1.4 Issuer		√	-	
1.4.1 countryName (C)	ES	√	-	OID 2.5.4.6 [PRINTABLE STRING]
1.4.2 stateOrProvinceName	MADRID	√	-	OID 2.5.4.8 [UTF8 STRING]
1.4.3 localityName (L)	MADRID	√	-	OID 2.5.4.7 [UTF8 STRING]
1.4.4 organizationName (O)	AC CAMERFIRMA S.A.	√	-	OID 2.5.4.10 [UTF8 STRING]
1.4.5 organizationalUnitName (OU)	PKI SERVICES	√	-	OID 2.5.4.11 [UTF8 STRING]
1.4.6 serialNumber	A82743287	√	-	OID 2.5.4.5 [PRINTABLE STRING]
1.4.7 organizationIdentifier	VATES-A82743287	√	-	[ETSI EN 319 412-1] OID 2.5.4.97 [UTF8 STRING]
1.4.8 commonName (CN)	AC CAMERFIRMA QUALIFIED CERTIFICATES - 2021	√	-	OID 2.5.4.3 [UTF8 STRING]
1.5 Validity	365 días	√	-	
1.5.1 notBefore	<a incorporar cuando se emita el certificado>	√	-	UTC Time
1.5.2 notAfter	<a incorporar cuando se emita el certificado>	√	-	UTC Time
1.6 Subject		√	-	
1.6.1 countryName (C)	ES	√	-	OID 2.5.4.6 [PRINTABLE STRING]
1.6.2 stateOrProvinceName	MADRID	√	-	OID 2.5.4.8 [UTF8 STRING]

1.6.3 localityName (L)	MADRID	√	-	OID 2.5.4.7 [UTF8 STRING]
1.6.4 organizationName (O)	AC CAMERFIRMA S.A.	√	-	OID 2.5.4.10 [UTF8 STRING]
1.6.5 organizationalUnitName (OU)	PKI SERVICES	√	-	OID 2.5.4.11 [UTF8 STRING]
1.6.6 serialNumber	A82743287	√	-	OID 2.5.4.5 [PRINTABLE STRING]
1.6.7 organizationIdentifier	VATES-A82743287	√	-	[ETSI EN 319 412-1] OID 2.5.4.97 [UTF8 STRING]
1.6.8 commonName (CN)	OCSP RESPONDER AC CAMERFIRMA QUALIFIED CERTIFICATES - 2021	√	-	OID 2.5.4.3 [UTF8 STRING]
1.7 Subject Public Key Info	rsaEncryption	√	-	Clave pública de 2.048 bits [RFC3279] OID 1.2.840.113549.1.1.1
1.8 Extensions				
1.8.1 Standard Extensions				
1.8.1.1 Authority Key Identifier		√	-	OID 2.5.29.35
1.8.1.1.1 keyIdentifier	c76f2dc4108a6eddf3116569c64a437bc30f6814	√	-	
1.8.1.1.2 authorityCertIssuer	No está presente	-	-	
1.8.1.1.3 authorityCertSerialNumber	No está presente	-	-	
1.8.1.2 Subject Key Identifier	<a incorporar cuando se emita el certificado>	√	-	OID 2.5.29.14
1.8.1.3 Key Usage		√	√	OID 2.5.29.15
1.8.1.3.1 digitalSignature	Seleccionado “1”	√	-	
1.8.1.3.2 contentCommitment	Seleccionado “1”	√	-	
1.8.1.3.3 keyEncipherment	No Seleccionado “0”	-	-	
1.8.1.3.4 dataEncipherment	No seleccionado “0”	-	-	
1.8.1.3.5 keyAgreement	No seleccionado “0”	-	-	
1.8.1.3.6 keyCertSign	No seleccionado “0”	-	-	
1.8.1.3.7 cRLSign	No seleccionado “0”	-	-	

1.8.1.3.8 encipherOnly	No seleccionado “0”	-	-	
1.8.1.3.9 decipherOnly	No seleccionado “0”	-	-	
1.8.1.4 Certificate Policies		√	-	OID 2.5.29.32
1.8.1.4.1 Policy Identifier	OID de la política [Camerfirma]	√	-	OID 1.3.6.1.4.1.17326.10.21.0.1
1.8.1.4.1.1 Policy Qualifier ID		√	-	
1.8.1.4.1.1.1 CPS Pointer	URI: https://policy2021.camerfirma.com	√	-	OID 1.3.6.1.5.5.7.2.1
1.8.1.4.1.1.2 User Notice	No está presente	-	-	OID 1.3.6.1.5.5.7.2.2
1.8.1.5 Policy Mappings	No está presente	-	-	OID 2.5.29.33
1.8.1.6 Subject Alternative Name	No está presente	-	-	OID 2.5.29.17
1.8.1.7 Issuer Alternative Name		√	-	OID 2.5.29.18
1.8.1.7.1 rfc822Name	ca@camerfirma.com	√	-	
1.8.1.8 Subject Directory Attributes	No está presente	-	-	OID 2.5.29.9
1.8.1.9 Basic Constraints		√	√	OID 2.5.29.19
1.8.1.9.1 cA	FALSE	√	-	
1.8.1.9.2 pathLenConstraint	No está presente	-	-	
1.8.1.10 Name Constraints	No está presente	-	-	OID 2.5.29.30
1.8.1.11 Policy Constraints	No está presente	-	-	OID 2.5.29.36
1.8.1.12 Extended Key Usage		√	√	OID 2.5.29.37
1.8.1.12.1 serverAuth	No está presente	-	-	OID 1.3.6.1.5.5.7.3.1
1.8.1.12.2 clientAuth	No está presente	-	-	OID 1.3.6.1.5.5.7.3.2
1.8.1.12.3 codeSigning	No está presente	-	-	OID 1.3.6.1.5.5.7.3.3
1.8.1.12.4 emailProtection	No está presente	-	-	OID 1.3.6.1.5.5.7.3.4
1.8.1.12.5 timeStamping	No está presente	-	-	OID 1.3.6.1.5.5.7.3.8
1.8.1.12.6 OCSPSigning	Presente	√	-	OID 1.3.6.1.5.5.7.3.9
1.8.1.12.7 Microsoft Smart Card Logon for Windows	No está presente	-	-	OID 1.3.6.1.4.1.311.20.2.2
1.8.1.13 CRL Distribution Points		√	-	OID 2.5.29.31

1.8.1.13.1 CRL Distribution Point 1	http://crls.ca.camerfirma.com/qc2021/CRL$$.crl	√	-	$$ será 01, 02, 03 etc cada 50.000 certificados emitidos
1.8.1.14 Inhibit Any-Policy	No está presente	-	-	
1.8.1.15 Freshest CRL	No está presente	-	-	
1.8.2 Internet Certificate Extensions				
1.8.2.1.1 Authority Information Access		√	-	OID 1.3.6.1.5.5.7.1.1
1.8.2.1.2.1 accessMethod	id-ad-caIssuers	√	-	OID 1.3.6.1.5.5.7.48.2
1.8.2.1.2.2 accessLocation	http://ca.camerfirma.com/certs/camerfirmaqc2021.crt	√	-	
1.8.2.2 Subject Information Access	No está presente	-	-	
1.8.3 Certificate Extensions NO RFC 5280				
1.8.3.3 OCSP No Check	Presente	√	-	OID 1.3.6.1.5.5.7.48.1.5

4 CERTIFICADOS DE ENTIDAD FINAL

4.1 AC CAMERFIRMA QUALIFIED CERTIFICATES - 2021

1000 CiQT = Certificado Cualificado de Ciudadano - QSCD Tarjeta/Token

1002 CiQN = Certificado Cualificado de Ciudadano - QSCD Nube

1010 CQT = Certificado Cualificado Corporativo - QSCD Tarjeta/Token

1012 CQN = Certificado Cualificado Corporativo - QSCD Nube

1200 RLECPJQT = Certificado Cualificado de Representante Legal de Entidad Con Personalidad Jurídica - QSCD Tarjeta/Token

1202 RLECPJQN = Certificado Cualificado de Representante Legal de Entidad Con Personalidad Jurídica - QSCD Nube

1210 RLESPJQT = Certificado Cualificado de Representante Legal de Entidad Sin Personalidad Jurídica - QSCD Tarjeta/Token

1212 RLESPJQN = Certificado Cualificado de Representante Legal de Entidad Sin Personalidad Jurídica - QSCD Nube

1300 RVECPJQT = Certificado Cualificado de Representante Voluntario de Entidad Con Personalidad Jurídica ante las AAPP - QSCD Tarjeta/Token

1302 RVECPJQN = Certificado Cualificado de Representante Voluntario de Entidad Con Personalidad Jurídica ante las AAPP - QSCD Nube

1310 RVESPJQT = Certificado Cualificado de Representante Voluntario de Entidad Sin Personalidad Jurídica ante las AAPP - QSCD Tarjeta/Token

1312 RVESPJQN = Certificado Cualificado de Representante Voluntario de Entidad Sin Personalidad Jurídica ante las AAPP - QSCD Nube

1400 AECPJQT = Certificado Cualificado de Apoderado de Entidad Con Personalidad Jurídica - QSCD Tarjeta/Token

1402 AECPJQN = Certificado Cualificado de Apoderado de Entidad Con Personalidad Jurídica - QSCD Nube

1410 AESPJQT = Certificado Cualificado de Apoderado de Entidad Sin Personalidad Jurídica - QSCD Tarjeta/Token

1412 AESPJQN = Certificado Cualificado de Apoderado de Entidad Sin Personalidad Jurídica - QSCD Nube

Campo	Contenido	O	C	Observaciones	
1. TBSCertificate					
1.1 Version	V3	√	-	[RFC5280]	
1.2 Serial number	<proviene de la CA>	√	-	Establecido automáticamente por la CA [20 bytes]	
1.3 Signature Algorithm	sha256WithRSAEncryption	√	-	OID 1.2.840.113549.1.1.11	
1.4 Issuer		√	-		
1.4.1 countryName (C)	ES	√	-	OID 2.5.4.6 [PRINTABLE STRING]	
1.4.2 stateOrProvinceName	MADRID	√	-	OID 2.5.4.8 [UTF8 STRING]	
1.4.3 localityName (L)	MADRID	√	-	OID 2.5.4.7 [UTF8 STRING]	
1.4.4 organizationName (O)	AC CAMERFIRMA S.A.	√	-	OID 2.5.4.10 [UTF8 STRING]	
1.4.5 organizationalUnitName (OU)	PKI SERVICES	√	-	OID 2.5.4.11 [UTF8 STRING]	
1.4.6 serialNumber	A82743287	√	-	OID 2.5.4.5 [PRINTABLE STRING]	
1.4.7 organizationIdentifier	VATES-A82743287	√	-	[ETSI EN 319 412-1] OID 2.5.4.97 [UTF8 STRING]	
1.4.8 commonName (CN)	AC CAMERFIRMA QUALIFIED CERTIFICATES - 2021	√	-	OID 2.5.4.3 [UTF8 STRING]	
1.5 Validity	730 días	√	-		
1.5.1 notBefore	<a incorporar cuando se emita el certificado>	√	-	UTC Time	
1.5.2 notAfter	<a incorporar cuando se emita el certificado>	√	-	UTC Time	
1.6 Subject		√	-		
1.6.1 countryName (C)	Estado cuya ley rige el valor del atributo serialNumber	√	-	Por defecto “ES” [ISO 3166-1 alpha-2] OID 2.5.4.6 [PRINTABLE STRING] [Tamaño máx. 2]	
1.6.2 organizationName (O)	Razón social, tal y como figura en los registros oficiales	-	-	CiQT CiQN	En mayúsculas, con tildes

		√		CQT CQN AECPJQT AECPJQN AESPJQT AESPJQN RLECPJQT RLECPJQN RLESPJQT RLESPJQN RVECPJQT RVECPJQN RVESPJQT RVESPJQN	[Tamaño máx. 128] OID 2.5.4.10 [UTF8 STRING]
1.6.3 organizationalUnit Name (OU)	Departamento 1 en la organización al que pertenece el responsable del certificado	-	-	CiQT CiQN	Área / Departamento / Unidad de trabajo OID 2.5.4.11 [UTF8 STRING] En mayúsculas, con tildes [Tamaño máx. 128]
		√		CQT CQN AECPJQT AECPJQN AESPJQT AESPJQN	
		X		RLECPJQT RLECPJQN RLESPJQT RLESPJQN RVECPJQT RVECPJQN RVESPJQT RVESPJQN	
1.6.4 organizationalUnit Name (OU)	Departamento 2 en la organización al que pertenece el responsable del certificado	-	-	CiQT CiQN	Área / Departamento / Unidad de trabajo OID 2.5.4.11 [UTF8 STRING] En mayúsculas, con tildes [Tamaño máx. 128]
		X		CQT CQN AECPJQT AECPJQN AESPJQT AESPJQN RLECPJQT RLECPJQN RLESPJQT RLESPJQN RVECPJQT RVECPJQN RVESPJQT RVESPJQN	

1.6.5 organizationIdentifier	Identificación de la entidad suscriptora del certificado	-	-	CiQT CiQN	"VAT" + "<cod país>" + "-" + <NIF de la entidad suscriptora> [ETSI EN 319 412-1] P.Ej.: "VATES-A99999999" OID 2.5.4.97 [UTF8 STRING] [Tamaño máx. 64]
		√		CQT CQN AECPJQT AECPJQN AESPJQT AESPJQN RLECPJQT RLECPJQN RLESPJQT RLESPJQN RVECPJQT RVECPJQN RVESPJQT RVESPJQN	
1.6.6 title (T)	Puesto o cargo del responsable del certificado que lo vincula con la entidad suscriptora del certificado	-	-	CiQT CiQN	OID 2.5.4.12 [UTF8 STRING]
		X		CQT CQN AECPJQT AECPJQN AESPJQT AESPJQN RLECPJQT RLECPJQN RLESPJQT RLESPJQN RVECPJQT RVECPJQN RVESPJQT RVESPJQN	
1.6.7 serialNumber	DNI o NIE del responsable del certificado	√	-	"IDC" + "<cod país>" + "-" + <DNI> / "PNO" + "<cod país>" + "-" + <NIE u otro NIF distinto de DNI> [ETSI EN 319 412-1] P.Ej.: IDCES-99999999A OID 2.5.4.5 [PRINTABLE STRING] [Tamaño máx. 64]	
1.6.8 Surname	Apellidos del responsable del certificado	√	-	Apellidos conformes al documento de identificación presentado. P.Ej.: "DE LA CAMARA ESPAÑOL" OID 2.5.4.4 [UTF8 STRING]	

				En mayúsculas, con tildes [Tamaño máx. 80]	
1.6.9 Given Name	Nombre del responsable del certificado	√	-	Nombre conforme al documento de identificación presentado OID 2.5.4.42 [UTF8 STRING] En mayúsculas, con tildes [Tamaño máx. 40]	
1.6.10 commonName (CN)	DNI o NIE, nombre y primer apellido del responsable del certificado (truncando el apellido si el CN excede el tamaño máximo), identificación del tipo de certificado y NIF de la entidad a la que está vinculado el titular del certificado	√	-	CiQT CiQN	<DNI/NIE del responsable del certificado> + " " + <Nombre y primer apellido del responsable del certificado> P.Ej.: "99999999A JUAN ANTONIO DE LA CAMARA" OID 2.5.4.3 [UTF8 STRING] En mayúsculas, con tildes [Tamaño máx. 64]
				CQT CQN	<DNI/NIE del responsable del certificado> + " " + <Nombre y primer apellido del responsable del certificado> + " (**C**:" + <NIF de la entidad suscriptora> + ")" P.Ej.: "99999999A JUAN ANTONIO DE LA CAMARA (**C**:A99999999)" OID 2.5.4.3 [UTF8 STRING] En mayúsculas, con tildes [Tamaño máx. 64]
				RLECPJQT RLECPJQN RLESPJQT RLESPJQN RVECPJQT	<DNI/NIE del responsable del certificado> + " " + <Nombre y primer apellido del

				RVECPJQN RVESPJQT RVESPJQN	responsable del certificado> + " (**R**:" + <NIF de la entidad suscriptora> + ")" P.Ej.: "99999999A JUAN ANTONIO DE LA CAMARA (**R**:A99999999)" OID 2.5.4.3 [UTF8 STRING] En mayúsculas, con tildes [Tamaño máx. 64]
				AECPJQT AECPJQN AESPJQT AESPJQN	<DNI/NIE del responsable del certificado> + " " + <Nombre y primer apellido del responsable del certificado> + " (**A**:" + <NIF de la entidad suscriptora> + ")" P.Ej.: "99999999A JUAN ANTONIO DE LA CAMARA (**A**:A99999999)" OID 2.5.4.3 [UTF8 STRING] En mayúsculas, con tildes [Tamaño máx. 64]
1.6.11 description	Codificación del documento público que acredita las facultades del firmante o los datos registrales	-	-	CiQT CiQN	No está presente
		-		CQT CQN	No está presente

		√		RLECPJQT RLECPJQN RLESPJQT RLESPJQN RVECPJQT RVECPJQN RVESPJQT RVESPJQN AECPJQT AECPJQN AESPJQT AESPJQN	En el Registro Mercantil: “Reg: “ + <Registro Mercantil> + “ /Hoja: “ + <Hoja> + “/Tomo: “ + <Tomo> “/Sección: “ + <Sección> + “/Libro: “ + <Libro> + “/Folio: “ + <Folio> + “/Fecha: “ + <fecha dd-mm-yyyy> + “/Inscripción: “ + <Inscripción> Ej.: “Reg: MADRID /Hoja: M-99999 /Tomo: 99999 /Sección: 99 /Libro: 9999 /Folio: 999 /Fecha: 30-02-2050 /Inscripción: 9” Poder Notarial: “Notario: “ + <Nombre notario> + “ ” <Apellido 1 notario> + “ ” <Apellido 2 notario> + “/Núm Protocolo: “ + <Número de protocolo> + “/Fecha Otorgamiento: “ + <fecha otorgamiento dd-mm-yyyy> Ej: “Notario: NOMBRE APELLIDO1 APELLIDO2/Núm Protocolo: 99999/Fecha Otorgamiento: 30-02-2050” Boletín Oficial: “Boletín: “ + <Boletín Oficial> + “/Fecha: “ + <fecha Boletín Oficial dd-mm-yyyy> + “/Número

					resolución: “ + <nº de resolución> Ej: “Boletín: BOE/Fecha: 30-02-2050/Número resolución: 9999” Contrato privado: “Contrato Privado: Fecha contrato: “+ <fecha contrato dd-mm-aaaa>+” /Fecha autorización: “ + <Fecha autorización dd-mm-aaaa> Ej: “Contrato Privado: Fecha contrato: 30-02-2050 /Fecha autorización: 31-02-2050“ OID 2.5.4.13 [UTF8 STRING]
1.6.12 dnQualifier	Universally Unique IDentifier	√	-	[PrintableString] OID 2.5.4.46 Ej: “2ec6f5b4-15a2-49d8-9c92-1ca824f0ee83” [Tamaño máx. 36]	
1.7 Subject Public Key Info	rsaEncryption	√	-	Clave pública de 2.048 bits [RFC3279] OID 1.2.840.113549.1.1.1	
1.8 Extensions					
1.8.1 Standard Extensions					
1.8.1.1 Authority Key Identifier		√	-	OID 2.5.29.35	
1.8.1.1.1 keyIdentifier	c76f2dc4108a6eddf3116569c64a437bc30f6814	√	-		
1.8.1.1.2 authorityCertIssuer	No está presente	-	-		
1.8.1.1.3 authorityCertSerialNumber	No está presente	-	-		
1.8.1.2 Subject Key Identifier	<a incorporar cuando se emita el certificado>	√	-	OID 2.5.29.14	
1.8.1.3 Key Usage		√	√	OID 2.5.29.15	

1.8.1.3.1 digitalSignature	Seleccionado “1”	√	-		
1.8.1.3.2 contentCommitment	Seleccionado “1”	√	-		
1.8.1.3.3 keyEncipherment	Seleccionado “1”	√	-		
1.8.1.3.4 dataEncipherment	No seleccionado “0”	-	-		
1.8.1.3.5 keyAgreement	No seleccionado “0”	-	-		
1.8.1.3.6 keyCertSign	No seleccionado “0”	-	-		
1.8.1.3.7 cRLSign	No seleccionado “0”	-	-		
1.8.1.3.8 encipherOnly	No seleccionado “0”	-	-		
1.8.1.3.9 decipherOnly	No seleccionado “0”	-	-		
1.8.1.4 Certificate Policies		√	-	OID 2.5.29.32	
1.8.1.4.1 Policy Identifier 1	OID de la política [Camerfirma]	√	-	CiQT	OID 1.3.6.1.4.1.17326.10.21.1.1.1
				CiQN	OID 1.3.6.1.4.1.17326.10.21.1.1.3
				CQT	OID 1.3.6.1.4.1.17326.10.21.1.2.1
				CQN	OID 1.3.6.1.4.1.17326.10.21.1.2.3
				RLECPJQT	OID 1.3.6.1.4.1.17326.10.21.1.3.1
				RLECPJQN	OID 1.3.6.1.4.1.17326.10.21.1.3.3
				RLESPJQT	OID 1.3.6.1.4.1.17326.10.21.1.4.1
				RLESPJQN	OID 1.3.6.1.4.1.17326.10.21.1.4.3
				RVECPJQT	OID 1.3.6.1.4.1.17326.10.21.1.5.1

				RVECPJQN	OID 1.3.6.1.4.1.17326.10.21.1.5.3
				RVESPJQT	OID 1.3.6.1.4.1.17326.10.21.1.6.1
				RVESPJQN	OID 1.3.6.1.4.1.17326.10.21.1.6.3
				AECPJQT	OID 1.3.6.1.4.1.17326.10.21.1.7.1
				AECPJQN	OID 1.3.6.1.4.1.17326.10.21.1.7.3
				AESPJQT	OID 1.3.6.1.4.1.17326.10.21.1.8.1
				AESPJQN	OID 1.3.6.1.4.1.17326.10.21.1.8.3
1.8.1.4.1.1 Policy Qualifier ID		√	-		
1.8.1.4.1.1.1 CPS Pointer	URI: https://policy2021.camerfirma.com	√	-	OID 1.3.6.1.5.5.7.2.1	
1.8.1.4.1.1.2 User Notice	Presente	√	-	OID 1.3.6.1.5.5.7.2.2 [UTF8 STRING]	
				CiQT CiQN	Certificado Cualificado de Ciudadano en dispositivo cualificado (QSCD). Consulte las condiciones de uso en https://policy2021.camerfirma.com
				CQT CQN	Certificado Cualificado Corporativo en dispositivo cualificado (QSCD). Consulte las condiciones de uso en https://policy2021.camerfirma.com

				RLECPJQT RLECPJQN	Certificado Cualificado de Representante Legal de Entidad con Personalidad Jurídica en dispositivo cualificado (QSCD). Consulte las condiciones de uso en https://policy2021.camerfirma.com
				RLESPJQT RLESPJQN	Certificado Cualificado de Representante Legal de Entidad sin Personalidad Jurídica en dispositivo cualificado (QSCD). Consulte las condiciones de uso en https://policy2021.camerfirma.com
				RVECPJQT RVECPJQN	Certificado Cualificado de Representante Voluntario de Entidad con Pers. Jurídica ante las AAPP en dispositivo cualificado (QSCD). Consulte las condiciones de uso en https://policy2021.camerfirma.com
				RVESPJQT RVESPJQN	Certificado Cualificado de Representante Voluntario de Entidad sin Pers. Jurídica ante las AAPP en dispositivo cualificado (QSCD). Consulte las condiciones de uso en

					https://policy2021.camerfirma.com
				AECPJQT AECPJQN	Certificado Cualificado de Apoderado de Entidad con Personalidad Jurídica en dispositivo cualificado (QSCD). Consulte las condiciones de uso en https://policy2021.camerfirma.com
				AESPJQT AESPJQN	Certificado Cualificado de Apoderado de Entidad sin Personalidad Jurídica en dispositivo cualificado (QSCD). Consulte las condiciones de uso en https://policy2021.camerfirma.com
1.8.1.4.2 Policy Identifier 2	OID de la política [política para Representante de Entidad Con/Sin Personalidad Jurídica según normativa nacional]	-	-	CiQT CiQN CQT CQN AECPJQT AECPJQN AESPJQT AESPJQN	No está presente
		√		RLECPJQT RLECPJQN RVECPJQT RVECPJQN	OID 2.16.724.1.3.5.8
		√		RLESPJQT RLESPJQN RVESPJQT RVESPJQN	OID 2.16.724.1.3.5.9
1.8.1.4.3 Policy Identifier 3	OID de la política [QCP-n-qscd]	√	-	OID 0.4.0.194112.1.2	
1.8.1.5 Policy Mappings	No está presente	-	-	OID 2.5.29.33	
1.8.1.6 Subject Alternative Name		√	-	OID 2.5.29.17	

1.8.1.6.1 rfc822Name	Correo electrónico del responsable del certificado	√	-		
1.8.1.6.2 Directory Name		√	-		
1.8.1.6.2.1 Nombre	Nombre del responsable del certificado	√	-	OID 1.3.6.1.4.1.17326.30.7 [UTF8 STRING] En mayúsculas, con tildes [Tamaño máx. 40]	
1.8.1.6.2.2 Primer Apellido	Primer apellido del responsable del certificado	√	-	OID 1.3.6.1.4.1.17326.30.8 [UTF8 STRING] En mayúsculas, con tildes [Tamaño máx. 40]	
1.8.1.6.2.3 Segundo Apellido	Segundo apellido del responsable del certificado	√	-	En caso de no existir se dejará este campo en blanco OID 1.3.6.1.4.1.17326.30.9 [UTF8 STRING] En mayúsculas, con tildes [Tamaño máx. 40]	
1.8.1.6.2.4 Tipo de certificado	Descripción del tipo de certificado	√	-	OID 1.3.6.1.4.1.17326.30.10 [UTF8 STRING]	
				CiQT CiQN	CERTIFICADO ELECTRONICO CUALIFICADO DE CIUDADANO EN DISPOSITIVO CUALIFICADO (QSCD)
				CQT CQN	CERTIFICADO ELECTRONICO CUALIFICADO CORPORATIVO EN DISPOSITIVO CUALIFICADO (QSCD)
				RLECPJQT RLECPJQN	CERTIFICADO ELECTRONICO CUALIFICADO DE REPRESENTANTE LEGAL DE ENTIDAD CON PERSONALIDAD JURIDICA EN DISPOSITIVO CUALIFICADO (QSCD)
				RLESPJQT RLESPJQN	CERTIFICADO ELECTRONICO CUALIFICADO DE REPRESENTANTE LEGAL DE ENTIDAD SIN PERSONALIDAD

					JURIDICA EN DISPOSITIVO CUALIFICADO (QSCD)
				RVECPJQT RVECPJQN	CERTIFICADO ELECTRONICO CUALIFICADO DE REPRESENTANTE VOLUNTARIO DE ENTIDAD CON PERSONALIDAD JURIDICA ANTE LAS AAPP EN DISPOSITIVO CUALIFICADO (QSCD)
				RVESPJQT RVESPJQN	CERTIFICADO ELECTRONICO CUALIFICADO DE REPRESENTANTE VOLUNTARIO DE ENTIDAD SIN PERSONALIDAD JURIDICA ANTE LAS AAPP EN DISPOSITIVO CUALIFICADO (QSCD)
				AECPJQT AECPJQN	CERTIFICADO ELECTRONICO CUALIFICADO DE APODERADO DE ENTIDAD CON PERSONALIDAD JURIDICA EN DISPOSITIVO CUALIFICADO (QSCD)
				AESPJQT AESPJQN	CERTIFICADO ELECTRONICO CUALIFICADO DE APODERADO DE ENTIDAD SIN PERSONALIDAD JURIDICA EN DISPOSITIVO CUALIFICADO (QSCD)
1.8.1.7 Issuer Alternative Name		√	-	OID 2.5.29.18	
1.8.1.7.1 rfc822Name	ca@camerfirma.com	√	-		

1.8.1.8 Subject Directory Attributes	No está presente	-	-	OID 2.5.29.9
1.8.1.9 Basic Constraints		√	√	OID 2.5.29.19
1.8.1.9.1 cA	FALSE	√	-	
1.8.1.9.2 pathLenConstraint	No está presente	-	-	
1.8.1.10 Name Constraints	No está presente	-	-	OID 2.5.29.30
1.8.1.11 Policy Constraints	No está presente	-	-	OID 2.5.29.36
1.8.1.12 Extended Key Usage		√	-	OID 2.5.29.37
1.8.1.12.1 serverAuth	No está presente	-	-	OID 1.3.6.1.5.5.7.3.1
1.8.1.12.2 clientAuth	Presente	√	-	OID 1.3.6.1.5.5.7.3.2
1.8.1.12.3 codeSigning	No está presente	-	-	OID 1.3.6.1.5.5.7.3.3
1.8.1.12.4 emailProtection	Presente	√	-	OID 1.3.6.1.5.5.7.3.4
1.8.1.12.5 timeStamping	No está presente	-	-	OID 1.3.6.1.5.5.7.3.8
1.8.1.12.6 OCSPSigning	No está presente	-	-	OID 1.3.6.1.5.5.7.3.9
1.8.1.12.7 Microsoft Smart Card Logon for Windows	No está presente	-	-	OID 1.3.6.1.4.1.311.20.2.2
1.8.1.13 CRL Distribution Points		√	-	OID 2.5.29.31
1.8.1.13.1 CRL Distribution Point 1	http://crls.ca.camerfirma.com/qc2021/CRL$$.crl	√	-	$$ será 01, 02, 03 etc cada 50.000 certificados emitidos
1.8.1.14 Inhibit Any-Policy	No está presente	-	-	OID 2.5.29.54
1.8.1.15 Freshest CRL	No está presente	-	-	OID 2.5.29.46
1.8.2 Internet Certificate Extensions				
1.8.2.1.1 Authority Information Access		√	-	OID 1.3.6.1.5.5.7.1.1
1.8.2.1.1.1 accessMethod	id-ad-ocsp	√	-	OID 1.3.6.1.5.5.7.48.1

1.8.2.1.1.2 accessLocation	URI: http://ocspqc2021.ca.camerfirma.com	√	-	
1.8.2.1.2.1 accessMethod	id-ad-caIssuers	√	-	OID 1.3.6.1.5.5.7.48.2
1.8.2.1.2.2 accessLocation	http://ca.camerfirma.com/certs/camerfirmaqc2021.crt	√	-	
1.8.2.2 Subject Information Access	No está presente	-	-	OID 1.3.6.1.5.5.7.1.11
1.8.3 Certificate Extensions NO RFC 5280				
1.8.3.1 biometricInfo	No está presente	-	-	OID 1.3.6.1.5.5.7.1.2
1.8.3.2 qcStatements	Presente	√	-	OID 1.3.6.1.5.5.7.1.3
1.8.3.2.1 esi4-qcStatement-1	Presente	√	-	[ETSI EN 319 412-5 v2.3.1] id-etsi-qcs-QcCompliance OID 0.4.0.1862.1.1
1.8.3.2.2 esi4-qcStatement-2	No está presente	-	-	[ETSI EN 319 412-5 v2.3.1] id-etsi-qcs-QcLimitValue OID 0.4.0.1862.1.2
1.8.3.2.3 esi4-qcStatement-3	15 años	√	-	[ETSI EN 319 412-5 v2.3.1] id-etsi-qcs-QcRetentionPeriod OID 0.4.0.1862.1.3
1.8.3.2.4 esi4-qcStatement-4	Presente	√	-	[ETSI EN 319 412-5 v2.3.1] id-etsi-qcs-QcSSCD OID 0.4.0.1862.1.4
1.8.3.2.5 esi4-qcStatement-5	No está presente	-	-	[ETSI EN 319 412-5 v2.3.1] id-etsi-qcs-QcPDS OID 0.4.0.1862.1.5
1.8.3.2.6 esi4-qcStatement-6	Presente	√	-	[ETSI EN 319 412-5 v2.3.1] id-etsi-qcs-QcType OID 0.4.0.1862.1.6
1.8.3.2.6.1 id-etsi-qct-esign	Presente	√	-	[ETSI EN 319 412-5 v2.3.1] OID 0.4.0.1862.1.6.1
1.8.3.2.6.2 id-etsi-qct-eseal	No está presente	-	-	[ETSI EN 319 412-5 v2.3.1] OID 0.4.0.1862.1.6.2
1.8.3.2.6.3 id-etsi-qct-web	No está presente	-	-	[ETSI EN 319 412-5 v2.3.1] OID 0.4.0.1862.1.6.3
1.8.3.2.7 esi4-qcStatement-7	No está presente	-	-	[ETSI EN 319 412-5 v2.3.1] id-etsi-qcs-QcCClegislation OID 0.4.0.1862.1.7

ANEXO I: HISTORIA DEL DOCUMENTO

19/01/2022	V1.0	Versión inicial
31/03/2023	V1.1	Inclusión código documento Corrección literal C en el CN de los certificados corporativos. Modificación literal A en el CN de los certificados de apoderados Desglose del CN según perfiles Modificación de TINES a PNOES en el serialNumber de los certificados de entidad final Añadidos perfiles de Ciudadano (CiQT y CiQN)

SELLO JURIDICO

Firmado digitalmente por SELLO JURIDICO
Fecha: 2023.03.31 14:21:44 +02'00'