Sectigo eIDAS Qualified Certificate profiles

Sectigo (Europe) SL
Versión 2.2
Rambla Catalunya, 86 3 1,
08008 Barcelona, España

SECTIGO

Contents

INTRODUCTION 3

LOCAL DEVICE 4

Natural person 4

- Citizen 4
- Citizen (QSCD) 5
- Employee 6
- Employee (QSCD) 8
- QWAC-n 9

Legal person 11

- Seal 11
- Seal (QSCD) 12
- QWAC-l 13
- QWAC-l for PSD2 15
- Seal for PSD2 16
- Seal for PSD2 (QSCD) 18

Notes 20

- qcCompliance 20
- qcRetentionPeriod 20
- qcPDS 20

Sectigo OIDs 20

INTRODUCTION

Sectigo can only issue qualified certificates according to this document and the profiles defined. All certificate profiles within the qualified hierarchy of Sectigo are detailed below.

Additionally, specific certificate policies and Sectigo liability arrangements that are not described in the qualified CP/CPS may be drawn up under contract for individual subscribers.

Different certificate profiles may be issued with different key usages.

LOCAL DEVICE

These certificates are issued locally, either in a QSCD for those issuing qualified signatures/seals that is securely delivered to the subscribers or in a non-QSCD for those issuing advanced signatures/seals which do not use any qualified device and the issuance process can be done online entirely.

Natural person

OID: 1.3.6.1.4.1.6449.1.2.1.7 eIDAS Natural person

Citizen

Field/Extension		**Content**	**Optional/Critical**
Version		3 (0x2)	
Serial Number	containing at least 64 bits of output from a CSPRNG	XXX	
Signature Algorithm		Sha256WithRSAEncryption or ecdsa-with-SHA256	
Issuer	commonName	Sectigo Qualified Natural Person CA R/E35	
	organizationName	Sectigo (Europe) SL	
	countryName	ES	
Validity		1,2,3,4,5 years	
Subject	commonName (CN)	XXXX	
	serialNumber	As per ETSI EN 319 412-1 Semantics Identifier for natural persons	
	Surname (SN)	XXXX	
	Name (G)	XXXX	
	countryName (C)	XXXX	
Subject Public Key Info	id-ecPublicKey and EcpkParameters or rsaEncryption and RSAPublicKey	RSA 2048 bits or P-256 minimum	
Authority Key Identifier	keyID: based on the subject key identifier in the issuer's certificate		
Subject Key Identifier	SHA-1 hash of the value of the subjectPublicKey (excluding the tag, length, and number of unused bits)		
Key Usage		digitalSignature, nonRepudiation	Critical
Basic Constraints		CA:FALSE	Critical
Extended Key Usage		Client Authentication, email protection	

Certificate Policies	policyIdentifier	1.3.6.1.4.1.6449.1.2.1.7.1	
	cpsURI	https://sectigo.com/eIDAS CPS	
	policyIdentifier	0.4.0.194112.1.0 (QCP-n)	
CRL Distribution Points		http://crl.sectigo.com/SectigoQualifiedNaturalPersonCAR35.crl http://crl.sectigo.com/SectigoQualifiedNaturalPersonCAE35.crl	
Authority Information Access	CA Issuers	http://crt.sectigo.com/SectigoQualifiedNaturalPersonCAR35.crt http://crt.sectigo.com/SectigoQualifiedNaturalPersonCAE35.crt	
	OCSP	http://ocsp.sectigo.com	
Subject Alternative Name	Rfc822Name	Subscriber email	Optional
qcStatements	qcCompliance	Present	
	qcType	id-etsi-qct-esign	
	qcRententionPeriod	15 years	
	qcPDS	https://sectigo.com/pds/	
	qcStatement-2	0.4.0.194121.1.1 (id-etsi-qcs-SemanticsId-Natural)	Optional

Citizen (QSCD)

Field/Extension		**Content**	**Optional/Critical**
Version		3 (0x2)	
Serial Number	containing at least 64 bits of output from a CSPRNG	XXX	
Signature Algorithm		Sha256WithRSAEncryption or ecdsa-with-SHA256	
Issuer	commonName	Sectigo Qualified Natural Person CA R/E35	
	organizationName	Sectigo (Europe) SL	
	countryName	ES	
Validity		1,2,3,4,5 years	
Subject	commonName (CN)	XXXX	
	serialNumber	As per ETSI EN 319 412-1 Semantics Identifier for natural persons	
	Surname (SN)	XXXX	
	Name (G)	XXXX	
	countryName (C)	XXXX	
Subject Public Key Info	id-ecPublicKey and EcpkParameters or rsaEncryption and RSAPublicKey	RSA 2048 bits or P-256 minimum	

Authority Key Identifier	keyID: based on the subject key identifier in the issuer's certificate		
Subject Key Identifier	SHA-1 hash of the value of the subjectPublicKey (excluding the tag, length, and number of unused bits)		
Key Usage		digitalSignature, nonRepudiation	Critical
Basic Constraints		CA:FALSE	Critical
Extended Key Usage		Client Authentication, email protection,	
Certificate Policies	policyIdentifier	1.3.6.1.4.1.6449.1.2.1.7.2	
	cpsURI	https://sectigo.com/eIDAS CPS	
	policyIdentifier	0.4.0.194112.1.2 (QCP-n-qscd)	
CRL Distribution Points		http://crl.sectigo.com/SectigoQualifiedNaturalPersonCAR35.crl http://crl.sectigo.com/SectigoQualifiedNaturalPersonCAE35.crl	
Authority Information Access	CA Issuers	http://crt.sectigo.com/SectigoQualifiedNaturalPersonCAR35.crt http://crt.sectigo.com/SectigoQualifiedNaturalPersonCAE35.crt	
	OCSP	http://ocsp.sectigo.com	
Subject Alternative Name	Rfc822Name	Subscriber email	Optional
qcStatements	qcCompliance	Present	
	qcType	id-etsi-qct-esign	
	qcRententionPeriod	15 years	
	qcPDS	https://sectigo.com/pds/	
	qcSSCD	present	
	qcStatement-2	0.4.0.194121.1.1 (id-etsi-qcs-SemanticsId-Natural)	Optional

Employee

Field/Extension		**Content**	**Optional/Critical**
Version		3 (0x2)	
Serial Number	containing at least 64 bits of output from a CSPRNG	XXX	
Signature Algorithm		Sha256WithRSAEncryption or ecdsa-with-SHA256	

Issuer	commonName	Sectigo Qualified Natural Person CA R/E35	
	organizationName	Sectigo (Europe) SL	
	countryName	ES	
Validity		1,2,3,4,5 years	
Subject	commonName (CN)	XXXX	
	serialNumber	As per ETSI EN 319 412-1 Semantics Identifier for natural persons	
	Surname (SN)	XXXX	
	Name (G)	XXXX	
	organizationIdentifier	3 characters+Country ID+ - Identifier Example: VATUK-04058690 or VATES-A29394909 as per ETSI EN 319 412-1.	
	Title	XXXX	Optional
	OrganizationName (O)	XXXX	
	Department (OU)	XXXX	Optional
	Locality	XXXX	Optional
	StateorProvince	XXXX	Optional
	countryName (C)	XXXX	
Subject Public Key Info	id-ecPublicKey and EcpkParameters or rsaEncryption and RSAPublicKey	RSA 2048 bits or P-256 minimum	
Authority Key Identifier	keyID: based on the subject key identifier in the issuer's certificate		
Subject Key Identifier	SHA-1 hash of the value of the subjectPublicKey (excluding the tag, length, and number of unused bits)		
Key Usage		digitalSignature, nonRepudiation	Critical
Basic Constraints		CA:FALSE	Critical
Extended Key Usage		Client Authentication, emailProtection	
Certificate Policies	policyIdentifier	1.3.6.1.4.1.6449.1.2.1.7.3	
	cpsURI	https://sectigo.com/eIDAS CPS	
	policyIdentifier	0.4.0.194112.1.0 (QCP-n)	
CRL Distribution Points		http://crl.sectigo.com/SectigoQualifiedNaturalPersonCAR35.crl http://crl.sectigo.com/SectigoQualifiedNaturalPersonCAE35.crl	
Authority Information Access	CA Issuers	http://crt.sectigo.com/SectigoQualifiedNaturalPersonCAR35.crt http://crt.sectigo.com/SectigoQualifiedNaturalPersonCAE35.crt	
	OCSP	http://ocsp.sectigo.com	

Subject Alternative Name	Rfc822Name	Subscriber email	
qcStatements	qcCompliance	Present	
	qcType	id-etsi-qct-esign	
	qcRententionPeriod	15 years	
	qcPDS	https://sectigo.com/pds/	
	qcStatement-2	0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)	
	qcStatement-2	0.4.0.194121.1.1 (id-etsi-qcs-SemanticsId-Natural)	Optional

Employee (QSCD)

Field/Extension		**Content**	**Optional/Critical**
Version		3 (0x2)	
Serial Number	containing at least 64 bits of output from a CSPRNG	XXX	
Signature Algorithm		Sha256WithRSAEncryption or ecdsa-with-SHA256	
Issuer	commonName	Sectigo Qualified Natural Person CA R/E35	
	organizationName	Sectigo (Europe) SL	
	countryName	ES	
Validity		1,2,3,4,5 years	
Subject	commonName (CN)	XXXX	
	serialNumber	As per ETSI EN 319 412-1 Semantics Identifier for natural persons	
	Surname (SN)	XXXX	
	Name (G)	XXXX	
	organizationIdentifier	3 characters+Country ID+ - Identifier Example: VATUK-04058690 or VATES-A29394909 as per ETSI EN 319 412-1.	
	Title	XXXX	Optional
	OrganizationName (O)	XXXX	
	Department (OU)	XXXX	Optional
	Locality	XXXX	Optional
	StateorProvince	XXXX	Optional
	countryName (C)	XXXX	
Subject Public Key Info	id-ecPublicKey and EcpkParameters or rsaEncryption and RSAPublicKey	RSA 2048 bits or P-256 minimum	
Authority Key Identifier	keyID: based on the subject key identifier in the issuer's certificate		
Subject Key Identifier	SHA-1 hash of the value of the subjectPublicKey (excluding the		

	tag, length, and number of unused bits)		
Key Usage		digitalSignature, nonRepudiation	Critical
Basic Constraints		CA:FALSE	Critical
Extended Key Usage		Client Authentication, emailProtection, smartcardlogon	
Certificate Policies	policyIdentifier	1.3.6.1.4.1.6449.1.2.1.7.4	
	cpsURI	https://sectigo.com/eIDAS CPS	
	policyIdentifier	0.4.0.194112.1.2 (QCP-n-qscd)	
CRL Distribution Points		http://crl.sectigo.com/SectigoQualifiedNaturalPersonCAR35.crl http://crl.sectigo.com/SectigoQualifiedNaturalPersonCAE35.crl	
Authority Information Access	CA Issuers	http://crt.sectigo.com/SectigoQualifiedNaturalPersonCAR35.crt http://crt.sectigo.com/SectigoQualifiedNaturalPersonCAE35.crt	
	OCSP	http://ocsp.sectigo.com	
Subject Alternative Name	Rfc822Name	Subscriber email	
qcStatements	qcCompliance	Present	
	qcType	id-etsi-qct-esign	
	qcRententionPeriod	15 years	
	qcPDS	https://sectigo.com/pds/	
	qcStatement-2	0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)	
	qcSSCD	present	
	qcStatement-2	0.4.0.194121.1.1 (id-etsi-qcs-SemanticsId-Natural)	Optional

QWAC-n

Field/Extension		**Content**	**Optional/Critical**
Version		3 (0x2)	
Serial Number	containing at least 64 bits of output from a CSPRNG	XXX	
Signature Algorithm		Sha256WithRSAEncryption or ecdsa-with-SHA256	
Issuer	commonName	Sectigo Qualified Website Authentication CA Natural R/E35	

	organizationName	Sectigo (Europe) SL	
	countryName	ES	
Validity		1 year	
Subject	commonName (CN)	Domain name	Optional
	serialNumber	As per ETSI EN 319 412-1 Semantics Identifier for natural persons	
	Name (G)	XXXX	
	Surname (SN)	XXXX	
	Locality	XXXX	Optional
	StateorProvince	XXXX	Optional
	countryName (C)	XXXX	
Subject Public Key Info	id-ecPublicKey and EcpkParameters or rsaEncryption and RSAPublicKey	RSA 2048 bits or P-256 minimum	
Authority Key Identifier	keyID: based on the subject key identifier in the issuer's certificate		
Subject Key Identifier	SHA-1 hash of the value of the subjectPublicKey (excluding the tag, length, and number of unused bits)		
Key Usage		digitalSignature	Critical
Basic Constraints		CA:FALSE	Critical
Extended Key Usage		Server Authentication, Client Authentication	
Certificate Policies	policyIdentifier	1.3.6.1.4.1.6449.1.2.1.7.5	
	cpsURI	https://sectigo.com/eIDAS CPS	
	policyIdentifier	0.4.0.194112.1.4 (QCP-w)	
	policyIdentifier	2.23.140.1.2.3	
CRL Distribution Points		http://crl.sectigo.com/SectigoQualifiedWebsiteAuthenticationCANaturalR35.crl http://crl.sectigo.com/SectigoQualifiedWebsiteAuthenticationCANaturalE35.crl	
Authority Information Access	CA Issuers	http://crt.sectigo.com/SectigoQualifiedWebsiteAuthenticationCANaturalR35.crt http://crt.sectigo.com/SectigoQualifiedWebsiteAuthenticationCANaturalE35.crt	
	OCSP	http://ocsp.sectigo.com	
Subject Alternative Name	dNSName	To follow CAB Forum BRs	
qcStatements	qcCompliance	Present	
	qcType	id-etsi-qct-web	
	qcRententionPeriod	15 years	
	qcPDS	https://sectigo.com/pds/	
	qcStatement-2	0.4.0.194121.1.1 (id-etsi-qcs-SemanticsId-Natural)	Optional

Legal person

OID: 1.3.6.1.4.1.6449.1.2.1.8 eIDAS Legal person

Seal

Field/Extension		Content	Optional/Critical
Version		3 (0x2)	
Serial Number	containing at least 64 bits of output from a CSPRNG	XXX	
Signature Algorithm		Sha256WithRSAEncryption or ecdsa-with-SHA256	
Issuer	commonName	Sectigo Qualified Legal Person CA R/E35L	
	organizationName	Sectigo (Europe) SL	
	countryName	ES	
Validity		1,2,3,4,5 years	
Subject	commonName (CN)	XXXX Example: this could be the system name or the automatic process application name	
	organizationIdentifier	3 characters+Country ID+ - Identifier Example: VATUK-04058690 or VATES-A29394909 as per ETSI EN 319 412-1.	
	OrganizationName (O)	XXXX	
	countryName (C)	XXXX	
Subject Public Key Info	id-ecPublicKey and EcpkParameters or rsaEncryption and RSAPublicKey	RSA 2048 bits or P-256 minimum	
Authority Key Identifier	keyID: based on the subject key identifier in the issuer's certificate		
Subject Key Identifier	SHA-1 hash of the value of the subjectPublicKey (excluding the tag, length, and number of unused bits)		
Key Usage		digitalSignature, nonRepudiation	Critical
Basic Constraints		CA:FALSE	Critical
Extended Key Usage		Client Authentication, codeSigning	
Certificate Policies	policyIdentifier	1.3.6.1.4.1.6449.1.2.1.8.1	
	cpsURI	https://sectigo.com/eIDAS CPS	

	policyIdentifier	0.4.0.194112.1.1 (QCP-l)	
CRL Distribution Points		http://crl.sectigo.com/SectigoQualifiedLegalPersonCAR35.crl http://crl.sectigo.com/SectigoQualifiedLegalPersonCAE35.crl	
Authority Information Access	CA Issuers	http://crt.sectigo.com/SectigoQualifiedLegalPersonCAR35.crt http://crt.sectigo.com/SectigoQualifiedLegalPersonCAE35.crt	
	OCSP	http://ocsp.sectigo.com	
qcStatements	qcCompliance	Present	
	qcType	id-etsi-qct-eseal	
	qcRententionPeriod	15 years	
	qcPDS	https://sectigo.com/pds/	
	qcStatement-2	0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)	

Seal (QSCD)

Field/Extension		**Content**	**Optional/Critical**
Version		3 (0x2)	
Serial Number	containing at least 64 bits of output from a CSPRNG	XXX	
Signature Algorithm		Sha256WithRSAEncryption or ecdsa-with-SHA256	
Issuer	commonName	Sectigo Qualified Legal Person CA R/E35	
	organizationName	Sectigo (Europe) SL	
	countryName	ES	
Validity		1,2,3,4,5 years	
Subject	commonName (CN)	XXXX Example: this could be the system name or the automatic process application name	
	organizationIdentifier	3 characters+Country ID+ -Identifier Example: VATUK-04058690 or VATES-A29394909 as per ETSI EN 319 412-1.	
	OrganizationName (O)	XXXX	
	countryName (C)	XXXX	
Subject Public Key Info	id-ecPublicKey and EcpkParameters or rsaEncryption and RSAPublicKey	RSA 2048 bits or P-256 minimum	
Authority Key Identifier	keyID: based on the subject key identifier in the issuer's certificate		

Subject Key Identifier	SHA-1 hash of the value of the subjectPublicKey (excluding the tag, length, and number of unused bits)		
Key Usage		digitalSignature, nonRepudiation	Critical
Basic Constraints		CA:FALSE	Critical
Extended Key Usage		Client Authentication, codeSigning	
Certificate Policies	policyIdentifier	1.3.6.1.4.1.6449.1.2.1.8.2	
	cpsURI	https://sectigo.com/eIDAS CPS	
	policyIdentifier	0.4.0.194112.1.3 (QCP-l-qscd)	
CRL Distribution Points		http://crl.sectigo.com/SectigoQualifiedLegalPersonCAR35.crl http://crl.sectigo.com/SectigoQualifiedLegalPersonCAE35.crl	
Authority Information Access	CA Issuers	http://crt.sectigo.com/SectigoQualifiedLegalPersonCAR35.crt http://crt.sectigo.com/SectigoQualifiedLegalPersonCAE35.crt	
	OCSP	http://ocsp.sectigo.com	
qcStatements	qcCompliance	Present	
	qcType	id-etsi-qct-eseal	
	qcRententionPeriod	15 years	
	qcPDS	https://sectigo.com/pds/	
	qcStatement-2	0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)	
	qcSSCD	Present	

QWAC-l

Field/Extension		**Content**	**Optional/Critical**
Version		3 (0x2)	
Serial Number	containing at least 64 bits of output from a CSPRNG	XXX	
Signature Algorithm		Sha256WithRSAEncryption or ecdsa-with-SHA256	
Issuer	commonName	Sectigo Qualified Website Authentication CA R/E35	
	organizationName	Sectigo (Europe) SL	
	countryName	ES	
Validity		1 year	
Subject	commonName (CN)	Domain name	Optional

	serialNumber	As generated for the EV SSL	
	OrganizationName (O)	XXXX	
	Department (OU)	XXXX	Optional
	organizationIdentifier	3 characters+Country ID+ - Identifier Example: VATUK-04058690 or VATES-A29394909 as per ETSI EN 319 412-1.	
	Locality	XXXX	Optional
	StateorProvince	XXXX	Optional
	countryName (C)	XXXX	
	BusinessCategory	According to CAB Forum EV guidelines	
	jurisdictionOfIncorporationLocalityName	XXXX	Optional
	jurisdictionOfIncorporationStateOrProvinceName	XXXX	Optional
	jurisdictionOfIncorporationCountryName	XXXX	
Subject Public Key Info	id-ecPublicKey and EcpkParameters or rsaEncryption and RSAPublicKey	RSA 2048 bits or P-256 minimum	
Authority Key Identifier	keyID: based on the subject key identifier in the issuer's certificate		
Subject Key Identifier	SHA-1 hash of the value of the subjectPublicKey (excluding the tag, length, and number of unused bits)		
Key Usage		digitalSignature, key encirphement	Critical
Basic Constraints		CA:FALSE	Critical
Extended Key Usage		Server Authentication, Client Authentication	
Certificate Policies	policyIdentifier	1.3.6.1.4.1.6449.1.2.1.8.3	
	cpsURI	https://sectigo.com/eIDAS CPS	
	policyIdentifier	0.4.0.194112.1.4 (QCP-w)	
	policyIdentifier	2.23.140.1.1	
	policyIdentifier	1.3.6.1.4.1.6449.1.2.1.5.1	
CRL Distribution Points		http://crl.sectigo.com/SectigoQualifiedWebsiteAuthenticationCAR35.crl http://crl.sectigo.com/SectigoQualifiedWebsiteAuthenticationCAE35.crl	
Authority Information Access	CA Issuers	http://crt.sectigo.com/SectigoQualifiedWebsiteAuthenticationCAR35.crt http://crt.sectigo.com/SectigoQualifiedWebsiteAuthenticationCAE35.crt	
	OCSP	http://ocsp.sectigo.com	

Subject Alternative Name	dNSName	To follow CAB Forum BRs	
cabfOrganizationIdentifier	OID: 2.23.140.3.1	Registration scheme as per ETSI EN 319 412-1 Authorization Number formatted according to EV Guidelines	
qcStatements	qcCompliance	Present	
	qcType	id-etsi-qct-web	
	qcRententionPeriod	15 years	
	qcPDS	https://sectigo.com/pds/	

QWAC-I for PSD2

Field/Extension		**Content**	**Optional/Critical**
Version		3 (0x2)	
Serial Number	containing at least 64 bits of output from a CSPRNG	XXX	
Signature Algorithm		Sha256WithRSAEncryption or ecdsa-with-SHA256	
Issuer	commonName	Sectigo Qualified Website Authentication CA R/E35	
	organizationName	Sectigo (Europe) SL	
	countryName	ES	
Validity		1 year	
Subject	commonName (CN)	Domain name	Optional
	serialNumber	As generated for the EV SSL	
	OrganizationName (O)	XXXX	
	Department (OU)	XXXX	Optional
	organizationIdentifier	PSD2 authorization number according to an NCA	
	Locality	XXXX	Optional
	StateorProvince	XXXX	Optional
	countryName (C)	XXXX	
	BusinessCategory	According to CAB Forum EV guidelines	
	jurisdictionOfIncorporationLocalityName	XXXX	Optional
	jurisdictionOfIncorporationStateOrProvinceName	XXXX	Optional
	jurisdictionOfIncorporationCountryName	XXXX	
Subject Public Key Info	id-ecPublicKey and EcpkParameters or rsaEncryption and RSAPublicKey	RSA 2048 bits or P-256 minimum	
Authority Key Identifier	keyID: based on the subject key identifier in the issuer's certificate		

Subject Key Identifier	SHA-1 hash of the value of the subjectPublicKey (excluding the tag, length, and number of unused bits)		
Key Usage		digitalSignature	Critical
Basic Constraints		CA:FALSE	Critical
Extended Key Usage		Server Authentication, Client Authentication	
Certificate Policies	policyIdentifier	1.3.6.1.4.1.6449.1.2.1.8.4	
	cpsURI	https://sectigo.com/eIDAS CPS	
	policyIdentifier	0.4.0.194112.1.4 (QCP-w)	
	policyIdentifier	2.23.140.1.1	
	policyIdentifier	0.4.0.19495.3.1 (QCP-w-psd2)	Optional
CRL Distribution Points		http://crl.sectigo.com/SectigoQualifiedWebsiteAuthenticationCAR35.crl http://crl.sectigo.com/SectigoQualifiedWebsiteAuthenticationCAE35.crl	
Authority Information Access	CA Issuers	http://crt.sectigo.com/SectigoQualifiedWebsiteAuthenticationCAR35.crt http://crt.sectigo.com/SectigoQualifiedWebsiteAuthenticationCAE35.crt	
	OCSP	http://ocsp.sectigo.com	
Subject Alternative Name	dNSName	To follow CAB Forum BRs	
cabfOrganizationIdentifier	OID: 2.23.140.3.1	PSD2 Authorization Number as per ETSI TS 119 495, formatted according to EV Guidelines	
qcStatements	qcCompliance	Present	
	qcType	id-etsi-qct-web	
	qcRententionPeriod	15 years	
	qcPDS	https://sectigo.com/pds/	

	qcPSD2	PSD2QcType ::= SEQUENCE
		{
		rolesOfPSP RolesOfPSP,
		nCAName NCAName,
		nCAId NCAId
		}	

Seal for PSD2

Field/Extension		**Content**	**Optional/Critical**
Version		3 (0x2)	
Serial Number	containing at least 64 bits of output from a CSPRNG	XXX	

Signature Algorithm		Sha256WithRSAEncryption or ecdsa-with-SHA256	
Issuer	commonName	Sectigo Qualified Legal Person CA R/E35	
	organizationName	Sectigo (Europe) SL	
	countryName	ES	
Validity		1,2,3 years	
Subject	commonName (CN)	XXXX Example: this could be the system name or the automatic process application name	
	organizationIdentifier	PSD2 authorization number according to an NCA	
	OrganizationName (O)	XXXX	
	countryName (C)	XXXX	
Subject Public Key Info	id-ecPublicKey and EcpkParameters or rsaEncryption and RSAPublicKey	RSA 2048 bits or P-256 minimum	
Authority Key Identifier	keyID: based on the subject key identifier in the issuer's certificate		
Subject Key Identifier	SHA-1 hash of the value of the subjectPublicKey (excluding the tag, length, and number of unused bits)		
Key Usage		digitalSignature, nonRepudiation	Critical
Basic Constraints		CA:FALSE	Critical
Extended Key Usage		Client Authentication, code signing	
Certificate Policies	policyIdentifier	1.3.6.1.4.1.6449.1.2.1.8.5	
	cpsURI	https://sectigo.com/eIDAS CPS	
	policyIdentifier	0.4.0.194112.1.1 (QCP-l)	
CRL Distribution Points		http://crl.sectigo.com/SectigoQualifiedLegalPersonCAR35.crl http://crl.sectigo.com/SectigoQualifiedLegalPersonCAE35.crl	
Authority Information Access	CA Issuers	http://crt.sectigo.com/SectigoQualifiedLegalPersonCAR35.crt http://crt.sectigo.com/SectigoQualifiedLegalPersonCAE35.crt	
	OCSP	http://ocsp.sectigo.com	
qcStatements	qcCompliance	Present	
	qcType	id-etsi-qct-eseal	
	qcRententionPeriod	15 years	
	qcPDS	https://sectigo.com/pds/	

	qcStatement-2	0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)	

	qcPSD2	PSD2QcType ::= SEQUENCE
		{
		rolesOfPSP RolesOfPSP,
		nCAName NCAName,
		nCAId NCAId
		}	

Seal for PSD2 (QSCD)

Field/Extension		**Content**	**Optional/Critical**
Version		3 (0x2)	
Serial Number	containing at least 64 bits of output from a CSPRNG	XXX	
Signature Algorithm		Sha256WithRSAEncryption or ecdsa-with-SHA256	
Issuer	commonName	Sectigo Qualified Legal Person CA R/E35	
	organizationName	Sectigo (Europe) SL	
	countryName	ES	
Validity		1,2,3 years	
Subject	commonName (CN)	XXXX Example: this could be the system name or the automatic process application name	
	organizationIdentifier	PSD2 authorization number according to an NCA	
	OrganizationName (O)	XXXX	
	countryName (C)	XXXX	
Subject Public Key Info	id-ecPublicKey and EcpkParameters or rsaEncryption and RSAPublicKey	RSA 2048 bits or P-256 minimum	
Authority Key Identifier	keyID: based on the subject key identifier in the issuer's certificate		
Subject Key Identifier	SHA-1 hash of the value of the subjectPublicKey (excluding the tag, length, and number of unused bits)		
Key Usage		digitalSignature, nonRepudiation	Critical
Basic Constraints		CA:FALSE	Critical
Extended Key Usage		Client Authentication	
Certificate Policies	policyIdentifier	1.3.6.1.4.1.6449.1.2.1.8.6	
	cpsURI	https://sectigo.com/eIDAS CPS	

	policyIdentifier	0.4.0.194112.1.3 (QCP-l-qscd)	
CRL Distribution Points		http://crl.sectigo.com/SectigoQualifiedLegalPersonCAR35.crl http://crl.sectigo.com/SectigoQualifiedLegalPersonCAE35.crl	
Authority Information Access	CA Issuers	http://crt.sectigo.com/SectigoQualifiedLegalPersonCAR35.crt http://crt.sectigo.com/SectigoQualifiedLegalPersonCAE35.crt	
	OCSP	http://ocsp.sectigo.com	
qcStatements	qcCompliance	Present	
	qcType	id-etsi-qct-eseal	
	qcRententionPeriod	15 years	
	qcPDS	https://sectigo.com/pds/	
	qcStatement-2	0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)	

	qcPSD2	PSD2QcType ::= SEQUENCE
		{
		rolesOfPSP RolesOfPSP,
		nCAName NCAName,
		nCAId NCAId
		}	

	qcSSCD	Present	

Notes

qcCompliance

This is the only qcStatement mandatory according to ETSI EN 319 412-5

qcRetentionPeriod

- eIDAS does not impose any specific time, just what is considered valid. Article 24 2h.
- ETSI EN 319 411-1 indicates 7 years in clause 6.4.6
- Spanish signature law indicates 15 years as per Article 20 f.

This is a generic qcStatements that **may** be used with any applicable regulatory framework as indicated in ETSI EN 319 412-5

qcPDS

- eIDAS does not impose the use of this PDS (PKI Disclosure Statement)
- ETSI EN 319 411-1 Annex A shows an example of a PDS. It´s informative. The intention is to help consumers understand the rights, obligations, etc. that may not be easily to find/understand in the CP/CPS. It´s just a short document to explain this information
- Spanish signature law does not say anything about it.

This is a generic qcStatement that **may** be used with any applicable regulatory framework as indicated in ETSI EN 319 412-5.

Sectigo OIDs

1.3.6.1.4.1.6449.1.2.1.7	eIDAS Natural person
1.3.6.1.4.1.6449.1.2.1.7.1	Citizen
1.3.6.1.4.1.6449.1.2.1.7.2	Citizen (QSCD)
1.3.6.1.4.1.6449.1.2.1.7.3	Employee
1.3.6.1.4.1.6449.1.2.1.7.4	Employee (QSCD)
1.3.6.1.4.1.6449.1.2.1.7.5	QWAC-n
1.3.6.1.4.1.6449.1.2.1.8	eIDAS Legal person
1.3.6.1.4.1.6449.1.2.1.8.1	Seal
1.3.6.1.4.1.6449.1.2.1.8.2	Seal (QSCD)
1.3.6.1.4.1.6449.1.2.1.8.3	QWAC-l
1.3.6.1.4.1.6449.1.2.1.8.4	QWAC-l for PSD2
1.3.6.1.4.1.6449.1.2.1.8.5	Seal for PSD2
1.3.6.1.4.1.6449.1.2.1.8.6	Seal for PSD2 (QSCD)
1.3.6.1.4.1.6449.1.2.1.9	eIDAS Timestamping