Sectigo eIDAS Qualified Certificate profiles

Sectigo (Europe) SL
Versión 2.8
Rambla Catalunya, 33 3º
08007 Barcelona

Contents

INTRODUCTION 4

LOCAL DEVICE 5

Natural person 5

Citizen 5

Citizen (QSCD) 6

Employee 7

Employee (QSCD) 9

QWAC-n 10

Legal person 12

Seal 12

Seal (QSCD) 14

QWAC-l 15

QWAC-l for PSD2 (QEVCP-w) 17

Seal for PSD2 19

Seal for PSD2 (QSCD) 20

Subject fields 22

QcCompliance 22

QcEuRetentionPeriod 22

QcEuPDS 22

Validity period on TLS certificates 23

Sectigo OIDs 23

Annex A: Root CAs 24

USERTrust ECC CA 24

USERTrust RSA CA 24

Sectigo Qualified Legal Person Root E45 25

Sectigo Qualified Legal Person Root R45 25

Sectigo Qualified Natural Person Root E45 26

Sectigo Qualified Natural Person Root R45 26

Sectigo Qualified Time Stamping Root R45 27

Sectigo Public Server Authentication Root R46 28

Sectigo Public Server Authentication Root E46 28

Annex B: Issuing CAs 30

Sectigo Qualified Website Authentication CA E35 30

Sectigo Qualified Website Authentication CA Natural E35 30

Sectigo Qualified Website Authentication CA R35 31
Sectigo Qualified Website Authentication CA Natural R35 31
Sectigo Qualified Legal Person CA E35 32
Sectigo Qualified Legal Person CA R35 33
Sectigo Qualified Natural Person CA E35 33
Sectigo Qualified Natural Person CA R35 34
Sectigo Qualified Time Stamping CA R35 34
Sectigo Qualified Website Authentication CA E39 35
Sectigo Qualified Website Authentication CA Natural E39 35
Sectigo Qualified Website Authentication CA R39 36
Sectigo Qualified Website Authentication CA Natural R39 37
Annex C: Changelog 38

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 (optional), 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/eIDASCPS	
	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	
	QcEuRetentionPeriod	15 years	
	QcEuPDS	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 (optional), 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	
QCStatements	QcCompliance	Present	
	QcType	id-etsi-qct-esign	
	QcEuRetentionPeriod	15 years	
	QcEuPDS	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 as per ETSI EN 319 412-1 , semantics identifier for legal persons.	
	Title	XXXX	Optional
	OrganizationName (O)	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 (optional), 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	
	QcEuRetentionPeriod	15 years	
	QcEuPDS	https://sectigo.com/pds/	
	QcStatement-2	0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)	

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 v1.4.4, section 5.1.3, Semantics Identifier for natural persons	
	Surname (SN)	XXXX	
	Name (G)	XXXX	
	organizationIdentifier	3 characters+Country ID+ - Identifier as per ETSI EN 319 412-1 v1.4.4, section 5.1.4, semantics identifier for legal person.	
	Title	XXXX	Optional
	OrganizationName (O)	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 (optional), 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	
	QcEuRetentionPeriod	15 years	
	QcEuPDS	https://sectigo.com/pds/	
	QcStatement-2	0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)	
	QcSSCD	present	

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 or R/E39	
	organizationName	Sectigo (Europe) SL	
	countryName	ES	
Validity		XXX	
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, keyEnchiperment (RSA)	Critical
Basic Constraints		CA:FALSE	Critical
Extended Key Usage		Server Authentication, Client Authentication (optional)	
Certificate Policies	policyIdentifier	1.3.6.1.4.1.6449.1.2.1.7.5	
	cpsURI	https://sectigo.com/eIDAS CPS	
	policyIdentifier	0.4.0.194112.1.5 (QNCP-w)	
	policyIdentifier	2.23.140.1.2.3	
CRL Distribution Points		The URL of the issuing CAs CRL file Example: http://crl.sectigo.com/SectigoQualifiedWebsiteAuthenticationCANaturalR35.crl http://crl.sectigo.com/SectigoQualifiedWebsiteAuthenticationCANaturalE35.crl http://crl.sectigo.com/SectigoQualifiedWebsiteAuthe	

		nticationCANaturalR39.crl http://crl.sectigo.com/SectigoQualifiedWebsiteAuthenticationCANaturalE39.crl	
Authority Information Access	CA Issuers	The URL of the issuing CAs CA-issuers file Example: http://crt.sectigo.com/SectigoQualifiedWebsiteAuthenticationCANaturalR35.crt http://crt.sectigo.com/SectigoQualifiedWebsiteAuthenticationCANaturalE35.crt http://crt.sectigo.com/SectigoQualifiedWebsiteAuthenticationCANaturalR39.crt http://crt.sectigo.com/SectigoQualifiedWebsiteAuthenticationCANaturalE39.crt	
	OCSP	http://ocsp.sectigo.com	
Subject Alternative Name	dNSName	To follow CAB Forum BRs	
QCStatements	QcCompliance	Present	
	QcType	id-etsi-qct-web	
	QcEuRetentionPeriod	15 years	
	QcEuPDS	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/E35	
	organizationName	Sectigo (Europe) SL	
	countryName	ES	
Validity		1,2,3,4,5 years	

Subject	commonName (CN)	XXXX. Usually, the organization name	
	organizationIdentifier	3 characters+Country ID+ - Identifier as per ETSI EN 319 412-1, semantics identifier for legal person.	
	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 (optional), nonRepudiation	Critical
Basic Constraints		CA:FALSE	Critical
Extended Key Usage		Client Authentication, Adobe Authentic Document Trust, id-kp-documentSigning (1.3.6.1.5.5.7.3.36)	
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	
	QcEuRetentionPeriod	15 years	
	QcEuPDS	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. Usually, the organization name	
	organizationIdentifier	3 characters+Country ID+ - Identifier as per ETSI EN 319 412-1, semantics identifier for legal person.	
	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 (optional), nonRepudiation	Critical
Basic Constraints		CA:FALSE	Critical
Extended Key Usage		Client Authentication, Adobe Authentic Document Trust, id-kp-documentSigning (1.3.6.1.5.5.7.3.36)	
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/SectigoQualifiedLegalPersonCA	

		R35.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	
	QcEuRetentionPeriod	15 years	
	QcEuPDS	https://sectigo.com/pds/	
	qcStatement-2	0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)	
	QcSSCD	Present	

QWAC-I

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 or R/E39	
	organizationName	Sectigo (Europe) SL	
	countryName	ES	
Validity		XXX	
Subject	commonName (CN)	Domain name	Optional
	serialNumber	As generated for the EV SSL	
	OrganizationName (O)	XXXX	
	organizationIdentifier	3 characters+Country ID+ - Identifier as per ETSI EN 319 412-1, semantics identifier for legal person.	
	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 encipherment (RSA)	Critical
Basic Constraints		CA:FALSE	Critical
Extended Key Usage		Server Authentication, Client Authentication (optional)	
Certificate Policies	policyIdentifier	1.3.6.1.4.1.6449.1.2.1.8.3	
	cpsURI	https://sectigo.com/eIDASCPS	
	policyIdentifier	0.4.0.194112.1.4 (QEVCP-w)	
	policyIdentifier	2.23.140.1.1	
	policyIdentifier	1.3.6.1.4.1.6449.1.2.1.5.1	
CRL Distribution Points		The URL of the issuing CAs CRL file Example: http://crl.sectigo.com/SectigoQualifiedWebsiteAuthenticationCAR35.crl http://crl.sectigo.com/SectigoQualifiedWebsiteAuthenticationCAE35.crl http://crl.sectigo.com/SectigoQualifiedWebsiteAuthenticationCAR39.crl http://crl.sectigo.com/SectigoQualifiedWebsiteAuthenticationCAE39.crl	
Authority Information Access	CA Issuers	The URL of the issuing CAs CA-issuers file Example: http://crt.sectigo.com/SectigoQualifiedWebsiteAuthenticationCAR35.crt http://crt.sectigo.com/SectigoQualifiedWebsiteAuthenticationCAE35.crt	

		http://crt.sectigo.com/SectigoQualifiedWebsiteAuthenticationCAR39.crt http://crt.sectigo.com/SectigoQualifiedWebsiteAuthenticationCAE39.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	
	QcEuRetentionPeriod	15 years	
	QcEuPDS	https://sectigo.com/pds/	

QWAC-l for PSD2 (QEVCP-w)

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 or R/E39	
	organizationName	Sectigo (Europe) SL	
	countryName	ES	
Validity		XXX	
Subject	commonName (CN)	Domain name	Optional
	serialNumber	As generated for the EV SSL	
	OrganizationName (O)	XXXX	
	organizationIdentifier	PSD2 authorization number according to an NCA. See ETSI TS 119 495	
	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, keyEncipherment (RSA)	Critical
Basic Constraints		CA:FALSE	Critical
Extended Key Usage		Server Authentication, Client Authentication (optional)	
Certificate Policies	policyIdentifier	1.3.6.1.4.1.6449.1.2.1.8.4	
	cpsURI	https://sectigo.com/eIDASCPS	
	policyIdentifier	0.4.0.194112.1.4 (QEVCP-w)	
	policyIdentifier	2.23.140.1.1	
	policyIdentifier	0.4.0.19495.3.1 (QCP-w-psd2)	Optional
	policyIdentifier	1.3.6.1.4.1.6449.1.2.1.5.1	
CRL Distribution Points		The URL of the issuing CAs CRL file Example: http://crl.sectigo.com/SectigoQualifiedWebsiteAuthenticationCAR35.crl http://crl.sectigo.com/SectigoQualifiedWebsiteAuthenticationCAE35.crl http://crl.sectigo.com/SectigoQualifiedWebsiteAuthenticationCAR39.crl http://crl.sectigo.com/SectigoQualifiedWebsiteAuthenticationCAE39.crl	
Authority Information Access	CA Issuers	The URL of the issuing CAs CA-issuers file Example: http://crt.sectigo.com/SectigoQualifiedWebsiteAuthenticationCAR35.crt http://crt.sectigo.com/Sect	

		igoQualifiedWebsiteAuthenticationCAE35.crt http://crt.sectigo.com/SectigoQualifiedWebsiteAuthenticationCAR39.crt http://crt.sectigo.com/SectigoQualifiedWebsiteAuthenticationCAE39.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	
	QcEuRetentionPeriod	15 years	
	QcEuPDS	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		1,2,3,4,5 years	
Subject	commonName (CN)	XXXX. Usually, the organization name	
	organizationIdentifier	PSD2 authorization number according to an NCA. See ETSI TS 119 495	
	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 (optional), nonRepudiation	Critical
Basic Constraints		CA:FALSE	Critical
Extended Key Usage		Client Authentication, Adobe Authentic Document Trust, id-kp-documentSigning (1.3.6.1.5.5.7.3.36)	
Certificate Policies	policyIdentifier	1.3.6.1.4.1.6449.1.2.1.8.5	
	cpsURI	https://sectigo.com/eIDASCPS	
	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	
	QcEuRetentionPeriod	15 years	
	QcEuPDS	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		1,2,3,4,5 years	
Subject	commonName (CN)	XXXX. Usually, the organization name	
	organizationIdentifier	PSD2 authorization number according to an NCA. See ETSI TS 119 495	
	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 (optional), nonRepudiation	Critical
Basic Constraints		CA:FALSE	Critical
Extended Key Usage		Client Authentication, Adobe Authentic Document Trust, id-kp-documentSigning (1.3.6.1.5.5.7.3.36)	
Certificate Policies	policyIdentifier	1.3.6.1.4.1.6449.1.2.1.8.6	
	cpsURI	https://sectigo.com/eIDASCPS	
	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/Sect	

		igoQualifiedLegalPersonCAE35.crt	
	OCSP	http://ocsp.sectigo.com	
QCStatements	QcCompliance	Present	
	QcType	id-etsi-qct-eseal	
	QcEuRetentionPeriod	15 years	
	QcEuPDS	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

Subject fields

One of either subject:locality (L) or subject:stateOrProvince (S) is required.
subject:stateOrProvince is preferred to be included.

QcCompliance

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

QcEuRetentionPeriod

- 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 QcStatement that **may** be used with any applicable regulatory framework as indicated in ETSI EN 319 412-5

QcEuPDS

- 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.

Validity period on TLS certificates

The validity period of those certificates with EKU serverAuth will depend on the hierarchy where they are issued from.

- Hierarchy included in the browsers root stores, the validity period will be as indicated in the TLS CP/CPS, section 6.3.2 (indicated as well in the eIDAS CP/CPS same section).
- Hierarchy that is not included in the browsers root stores, the maximum validity period of the certificates will be 398 days.

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
1.3.6.1.4.1.6449.1.2.1.5.1	QWAC-l and QWAC-l for PSD2 (based on QEVCP-w)
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

Annex A: Root CAs

USERTrust ECC CA

crt.sh | 2841410

Field/Extension		Content	Optional/Critical
Version	3 (0x2)		
Serial Number	containing at least 64 bits of output from a CSPRNG	5c8b99c55a94c5d27156decd8980cc26	
Signature Algorithm		sha384ECDSA	
Issuer	commonName	USERTrust ECC Certification Authority	
	organizationName	The USERTRUST Network	
	locality	Jersey City	
	stateOrProvince	New Jersey	
	countryName	US	
Validity	Not before	Feb 1 00:00:00 2010 GMT	
	Not after	Jan 18 23:59:59 2038 GMT	
Subject	commonName	USERTrust ECC Certification Authority	
	organizationName	The USERTRUST Network	
	locality	Jersey City	
	stateOrProvince	New Jersey	
	countryName	US	
Subject Public Key Info	Public Key Algorithm and RSAPublicKey	ECC (384 bits)	
Key Usage		Certificate Sign, CRL Sign	Critical
Basic Constraints		CA:TRUE	Critical

USERTrust RSA CA

crt.sh | 1199354

Field/Extension		Content	Optional/Critical
Version	3 (0x2)		
Serial Number	containing at least 64 bits of output from a CSPRNG	01fd6d30fca3ca51a81bbc640e35032d	
Signature Algorithm		sha384RSA	
Issuer	commonName	USERTrust RSA Certification Authority	
	organizationName	The USERTRUST Network	
	locality	Jersey City	
	stateOrProvince	New Jersey	
	countryName	US	
Validity	Not before	Feb 1 00:00:00 2010 GMT	
	Not after	Jan 18 23:59:59 2038 GMT	

Subject	commonName	USERTrust RSA Certification Authority	
	organizationName	The USERTRUST Network	
	locality	Jersey City	
	stateOrProvince	New Jersey	
	countryName	US	
Subject Public Key Info	Public Key Algorithm and RSAPublicKey	RSA (4096 bits)	
Key Usage		Certificate Sign, CRL Sign	Critical
Basic Constraints		CA:TRUE	Critical

Sectigo Qualified Legal Person Root E45

crt.sh | 3547980734

Field/Extension		**Content**	**Optional/Critical**
Version	3 (0x2)		
Serial Number	containing at least 64 bits of output from a CSPRNG	18ba1a9ac0ee669ffc9c703d032dc189	
Signature Algorithm		sha384ECDSA	
Issuer	commonName	Sectigo Qualified Legal Person Root E45	
	organizationName	Sectigo (Europe) SL	
	countryName	ES	
Validity	Not before	Oct 5 00:00:00 2020 GMT	
	Not after	Oct 4 23:59:59 2045 GMT	
Subject	commonName	Sectigo Qualified Legal Person Root E45	
	organizationName	Sectigo (Europe) SL	
	countryName	ES	
Subject Public Key Info	Public Key Algorithm and RSAPublicKey	ECC (384 bits)	
Key Usage		Certificate Sign, CRL Sign, digital signature	Critical
Basic Constraints		CA:TRUE	Critical

Sectigo Qualified Legal Person Root R45

crt.sh | 3547980733

Field/Extension		**Content**	**Optional/Critical**
Version	3 (0x2)		
Serial Number	containing at least 64 bits of output from a CSPRNG	20655a1b3ef150d79171ce6d8034ddbd	
Signature Algorithm		sha384RSA	

Issuer	commonName	Sectigo Qualified Legal Person Root R45	
	organizationName	Sectigo (Europe) SL	
	countryName	ES	
Validity	Not before	Oct 5 00:00:00 2020 GMT	
	Not after	Oct 4 23:59:59 2045 GMT	
Subject	commonName	Sectigo Qualified Legal Person Root R45	
	organizationName	Sectigo (Europe) SL	
	countryName	ES	
Subject Public Key Info	Public Key Algorithm and RSAPublicKey	RSA (4096 bits)	
Key Usage		Certificate Sign, CRL Sign, digital signature	Critical
Basic Constraints		CA:TRUE	Critical

Sectigo Qualified Natural Person Root E45

crt.sh | 3547980727

Field/Extension		**Content**	**Optional/Critical**
Version	3 (0x2)		
Serial Number	containing at least 64 bits of output from a CSPRNG	7e0aa94f2cbb01ea668b51e9e9423f57	
Signature Algorithm		sha384ECDSA	
Issuer	commonName	Sectigo Qualified Natural Person Root E45	
	organizationName	Sectigo (Europe) SL	
	countryName	ES	
Validity	Not before	Oct 5 00:00:00 2020 GMT	
	Not after	Oct 4 23:59:59 2045 GMT	
Subject	commonName	Sectigo Qualified Natural Person Root E45	
	organizationName	Sectigo (Europe) SL	
	countryName	ES	
Subject Public Key Info	Public Key Algorithm and RSAPublicKey	ECC (384 bits)	
Key Usage		Certificate Sign, CRL Sign, digital signature	Critical
Basic Constraints		CA:TRUE	Critical

Sectigo Qualified Natural Person Root R45

crt.sh | 3547980725

Field/Extension		**Content**	**Optional/Critical**

Version	3 (0x2)		
Serial Number	containing at least 64 bits of output from a CSPRNG	29c39ebe521f1d39cf0bcad43ba5f33f	
Signature Algorithm		sha384RSA	
Issuer	commonName	Sectigo Qualified Natural Person Root R45	
	organizationName	Sectigo (Europe) SL	
	countryName	ES	
Validity	Not before	Oct 5 00:00:00 2020 GMT	
	Not after	Oct 4 23:59:59 2045 GMT	
Subject	commonName	Sectigo Qualified Natural Person Root R45	
	organizationName	Sectigo (Europe) SL	
	countryName	ES	
Subject Public Key Info	Public Key Algorithm and RSAPublicKey	RSA (4096 bits)	
Key Usage		Certificate Sign, CRL Sign, digital signature	Critical
Basic Constraints		CA:TRUE	Critical

Sectigo Qualified Time Stamping Root R45

crt.sh | 3547980726

Field/Extension		**Content**	**Optional/Critical**
Version	3 (0x2)		
Serial Number	containing at least 64 bits of output from a CSPRNG	7b24e01933c796dfc404ce01161f5373	
Signature Algorithm		sha384RSA	
Issuer	commonName	Sectigo Qualified Time Stamping Root R45	
	organizationName	Sectigo (Europe) SL	
	countryName	ES	
Validity	Not before	Oct 5 00:00:00 2020 GMT	
	Not after	Oct 4 23:59:59 2045 GMT	
Subject	commonName	Sectigo Qualified Time Stamping Root R45	
	organizationName	Sectigo (Europe) SL	
	countryName	ES	
Subject Public Key Info	Public Key Algorithm and RSAPublicKey	RSA (4096 bits)	
Key Usage		Certificate Sign, CRL Sign, digital signature	Critical
Basic Constraints		CA:TRUE	Critical

Sectigo Public Server Authentication Root R46

crt.sh | 4256644734

Field/Extension		Content	Optional/Critical
Version	3 (0x2)		
Serial Number	containing at least 64 bits of output from a CSPRNG	758dfd8bae7c0700faa925a7e1c7ad14	
Signature Algorithm		sha384RSA	
Issuer	commonName	Sectigo Public Server Authentication Root R46	
	organizationName	Sectigo Limited	
	countryName	GB	
Validity	Not before	Mar 22 00:00:00 2021 GMT	
	Not after	Mar 21 23:59:59 2046 GMT	
Subject	commonName	Sectigo Public Server Authentication Root R46	
	organizationName	Sectigo Limited	
	countryName	GB	
Subject Public Key Info	Public Key Algorithm and RSAPublicKey	RSA (4096 bits)	
Key Usage		Certificate Sign, CRL Sign, digital signature	Critical
Basic Constraints		CA:TRUE	Critical

Sectigo Public Server Authentication Root E46

crt.sh | 4256644603

Field/Extension		Content	Optional/Critical
Version	3 (0x2)		
Serial Number	containing at least 64 bits of output from a CSPRNG	42f2ccda1b6937445f15fe752810b8f4	
Signature Algorithm		sha384ECDSA	
Issuer	commonName	Sectigo Public Server Authentication Root E46	
	organizationName	Sectigo Limited	
	countryName	GB	
Validity	Not before	Mar 22 00:00:00 2021 GMT	
	Not after	Mar 21 23:59:59 2046 GMT	
Subject	commonName	Sectigo Public Server Authentication Root E46	
	organizationName	Sectigo Limited	
	countryName	GB	

Subject Public Key Info	Public Key Algorithm and RSAPublicKey	ECC (384 bits)	
Key Usage		Certificate Sign, CRL Sign, digital signature	Critical
Basic Constraints		CA:TRUE	Critical

Annex B: Issuing CAs

Sectigo Qualified Website Authentication CA E35

crt.sh | 3504044090

Field/Extension		Content	Optional/Critical
Version	3 (0x2)		
Serial Number	containing at least 64 bits of output from a CSPRNG	9e568d21ded89307c34080ff2d995901	
Signature Algorithm		sha384ECDSA	
Issuer	commonName	USERTrust ECC Certification Authority	
	organizationName	The USERTRUST Network	
	locality	Jersey City	
	stateOrProvince	New Jersey	
	countryName	US	
Validity	Not before	Oct 5 00:00:00 2020 GMT	
	Not after	Oct 4 23:59:59 2035 GMT	
Subject	commonName	Sectigo Qualified Website Authentication CA E35	
	organizationName	Sectigo (Europe) SL	
	countryName	ES	
Subject Public Key Info	Public Key Algorithm and RSAPublicKey	ECC (256 bits)	
Key Usage		Certificate Sign, CRL Sign, digital signature	Critical
Extended Key Usage		Server authentication, client authentication	
Basic Constraints		CA:TRUE	Critical

Sectigo Qualified Website Authentication CA Natural E35

crt.sh | 3696575834

Field/Extension		Content	Optional/Critical
Version	3 (0x2)		
Serial Number	containing at least 64 bits of output from a CSPRNG	6866d57377f27657da8268a09e3faeb5	
Signature Algorithm		sha384ECDSA	
Issuer	commonName	USERTrust ECC Certification Authority	
	organizationName	The USERTRUST Network	
	locality	Jersey City	
	stateOrProvince	New Jersey	
	countryName	US	
Validity	Not before	Nov 17 00:00:00 2020 GMT	
	Not after	Nov 16 23:59:59 2035 GMT	

Subject	commonName	Sectigo Qualified Website Authentication CA Natural E35	
	organizationName	Sectigo (Europe) SL	
	countryName	ES	
Subject Public Key Info	Public Key Algorithm and RSAPublicKey	ECC (256 bits)	
Key Usage		Certificate Sign, CRL Sign, digital signature	Critical
Extended Key Usage		Server authentication, client authentication	
Basic Constraints		CA:TRUE	Critical

Sectigo Qualified Website Authentication CA R35

crt.sh | 3504044089

Field/Extension		**Content**	**Optional/Critical**
Version	3 (0x2)		
Serial Number	containing at least 64 bits of output from a CSPRNG	2762378048a1b3628d507e29220de220	
Signature Algorithm		sha384RSA	
Issuer	commonName	USERTrust RSA Certification Authority	
	organizationName	The USERTRUST Network	
	locality	Jersey City	
	stateOrProvince	New Jersey	
	countryName	US	
Validity	Not before	Oct 5 00:00:00 2020 GMT	
	Not after	Oct 4 23:59:59 2035 GMT	
Subject	commonName	Sectigo Qualified Website Authentication CA R35	
	organizationName	Sectigo (Europe) SL	
	countryName	ES	
Subject Public Key Info	Public Key Algorithm and RSAPublicKey	RSA (3072 bits)	
Key Usage		Certificate Sign, CRL Sign, digital signature	Critical
Extended Key Usage		Server authentication, client authentication	
Basic Constraints		CA:TRUE	Critical

Sectigo Qualified Website Authentication CA Natural R35

crt.sh | 3696575835

Field/Extension		**Content**	**Optional/Critical**

Version	3 (0x2)		
Serial Number	containing at least 64 bits of output from a CSPRNG	86380b2d3e65b9801030481e0e74362e	
Signature Algorithm		sha384RSA	
Issuer	commonName	USERTrust RSA Certification Authority	
	organizationName	The USERTRUST Network	
	locality	Jersey City	
	stateOrProvince	New Jersey	
	countryName	US	
Validity	Not before	Nov 17 00:00:00 2020 GMT	
	Not after	Nov 16 23:59:59 2035 GMT	
Subject	commonName	Sectigo Qualified Website Authentication CA Natural R35	
	organizationName	Sectigo (Europe) SL	
	countryName	ES	
Subject Public Key Info	Public Key Algorithm and RSAPublicKey	RSA (3072 bits)	
Key Usage		Certificate Sign, CRL Sign, digital signature	Critical
Extended Key Usage		Server authentication, client authentication	
Basic Constraints		CA:TRUE	Critical

Sectigo Qualified Legal Person CA E35

crt.sh | 3547998111

Field/Extension		**Content**	**Optional/Critical**
Version	3 (0x2)		
Serial Number	containing at least 64 bits of output from a CSPRNG	bf55b3b08ba28abad271e2ef2492b3c8	
Signature Algorithm		sha384ECDSA	
Issuer	commonName	Sectigo Qualified Legal Person Root E45	
	organizationName	Sectigo (Europe) SL	
	countryName	ES	
Validity	Not before	Oct 5 00:00:00 2020 GMT	
	Not after	Oct 4 23:59:59 2035 GMT	
Subject	commonName	Sectigo Qualified Legal Person CA E35	
	organizationName	Sectigo (Europe) SL	
	countryName	ES	
Subject Public Key Info	Public Key Algorithm and RSAPublicKey	ECC (256 bits)	
Key Usage		Certificate Sign, CRL Sign, digital signature	Critical
Extended Key Usage		Client authentication, email protection	

Basic Constraints		CA:TRUE	Critical

Sectigo Qualified Legal Person CA R35

crt.sh | 3547998110

Field/Extension		Content	Optional/Critical
Version	3 (0x2)		
Serial Number	containing at least 64 bits of output from a CSPRNG	d40b1204c9e4513275768b644f7a9df5	
Signature Algorithm		sha384RSA	
Issuer	commonName	Sectigo Qualified Legal Person Root R45	
	organizationName	Sectigo (Europe) SL	
	countryName	ES	
Validity	Not before	Oct 5 00:00:00 2020 GMT	
	Not after	Oct 4 23:59:59 2035 GMT	
Subject	commonName	Sectigo Qualified Legal Person CA R35	
	organizationName	Sectigo (Europe) SL	
	countryName	ES	
Subject Public Key Info	Public Key Algorithm and RSAPublicKey	RSA (3072 bits)	
Key Usage		Certificate Sign, CRL Sign, digital signature	Critical
Extended Key Usage		Client authentication, email protection	
Basic Constraints		CA:TRUE	Critical

Sectigo Qualified Natural Person CA E35

crt.sh | 3547998109

Field/Extension		Content	Optional/Critical
Version	3 (0x2)		
Serial Number	containing at least 64 bits of output from a CSPRNG	c0721eeb06ad9b21780fa4db48c9db25	
Signature Algorithm		sha384ECDSA	
Issuer	commonName	Sectigo Qualified Natural Person Root E45	
	organizationName	Sectigo (Europe) SL	
	countryName	ES	
Validity	Not before	Oct 5 00:00:00 2020 GMT	
	Not after	Oct 4 23:59:59 2035 GMT	
Subject	commonName	Sectigo Qualified Natural Person CA E35	

	organizationName	Sectigo (Europe) SL	
	countryName	ES	
Subject Public Key Info	Public Key Algorithm and RSAPublicKey	ECC (256 bits)	
Key Usage		Certificate Sign, CRL Sign, digital signature	Critical
Extended Key Usage		Client authentication, email protection	
Basic Constraints		CA:TRUE	Critical

Sectigo Qualified Natural Person CA R35

crt.sh | 3547998113

Field/Extension		**Content**	**Optional/Critical**
Version	3 (0x2)		
Serial Number	containing at least 64 bits of output from a CSPRNG	42211ba7e8e10a81d25da9bd8fd8120a	
Signature Algorithm		sha384RSA	
Issuer	commonName	Sectigo Qualified Natural Person Root R45	
	organizationName	Sectigo (Europe) SL	
	countryName	ES	
Validity	Not before	Oct 5 00:00:00 2020 GMT	
	Not after	Oct 4 23:59:59 2035 GMT	
Subject	commonName	Sectigo Qualified Natural Person CA R35	
	organizationName	Sectigo (Europe) SL	
	countryName	ES	
Subject Public Key Info	Public Key Algorithm and RSAPublicKey	RSA (3072 bits)	
Key Usage		Certificate Sign, CRL Sign, digital signature	Critical
Extended Key Usage		Client authentication, email protection	
Basic Constraints		CA:TRUE	Critical

Sectigo Qualified Time Stamping CA R35

crt.sh | 3547998112

Field/Extension		**Content**	**Optional/Critical**
Version	3 (0x2)		
Serial Number	containing at least 64 bits of output from a CSPRNG	0cda8301d3f3280e71cdb028a352c65b	
Signature Algorithm		sha384RSA	
Issuer	commonName	Sectigo Qualified Time Stamping Root R45	
	organizationName	Sectigo (Europe) SL	

	countryName	ES	
Validity	Not before	Oct 5 00:00:00 2020 GMT	
	Not after	Oct 4 23:59:59 2035 GMT	
Subject	commonName	Sectigo Qualified Time Stamping CA R35	
	organizationName	Sectigo (Europe) SL	
	countryName	ES	
Subject Public Key Info	Public Key Algorithm and RSAPublicKey	RSA (3072 bits)	
Key Usage		Certificate Sign, CRL Sign, digital signature	Critical
Extended Key Usage		Time stamping	
Basic Constraints		CA:TRUE	Critical

Sectigo Qualified Website Authentication CA E39

crt.sh | 14599514167

Field/Extension		**Content**	**Optional/Critical**
Version	3 (0x2)		
Serial Number	containing at least 64 bits of output from a CSPRNG	42cf38ec30d857fb9ce9dd5a5fc8f38f	
Signature Algorithm		sha384ECDSA	
Issuer	commonName	Sectigo Public Server Authentication Root E46	
	organizationName	Sectigo Limited	
	countryName	GB	
Validity	Not before	Sep 18 00:00:00 2024 GMT	
	Not after	Sep 17 23:59:59 2039 GMT	
Subject	commonName	Sectigo Qualified Website Authentication CA E39	
	organizationName	Sectigo (Europe) SL	
	countryName	ES	
Subject Public Key Info	Public Key Algorithm and RSAPublicKey	ECC (256 bits)	
Key Usage		Certificate Sign, CRL Sign, digital signature	Critical
Extended Key Usage		Server authentication, client authentication	
Basic Constraints		CA:TRUE	Critical

Sectigo Qualified Website Authentication CA Natural E39

crt.sh | 14599514168

Field/Extension		**Content**	**Optional/Critical**
Version	3 (0x2)		

Serial Number	containing at least 64 bits of output from a CSPRNG	42cf38ec30d857fb9ce9dd5a5fc8f38f	
Signature Algorithm		sha384ECDSA	
Issuer	commonName	Sectigo Public Server Authentication Root E46	
	organizationName	Sectigo Limited	
	countryName	GB	
Validity	Not before	Sep 18 00:00:00 2024 GMT	
	Not after	Sep 17 23:59:59 2039 GMT	
Subject	commonName	Sectigo Qualified Website Authentication CA Natural E39	
	organizationName	Sectigo (Europe) SL	
	countryName	ES	
Subject Public Key Info	Public Key Algorithm and RSAPublicKey	ECC (256 bits)	
Key Usage		Certificate Sign, CRL Sign, digital signature	Critical
Extended Key Usage		Server authentication, client authentication	
Basic Constraints		CA:TRUE	Critical

Sectigo Qualified Website Authentication CA R39

crt.sh | 14599514169

Field/Extension		**Content**	**Optional/Critical**
Version	3 (0x2)		
Serial Number	containing at least 64 bits of output from a CSPRNG	8fa10a69b6a87db1336c32c2153bc319	
Signature Algorithm		sha384RSA	
Issuer	commonName	Sectigo Public Server Authentication Root R46	
	organizationName	Sectigo Limited	
	countryName	GB	
Validity	Not before	Sep 18 00:00:00 2024 GMT	
	Not after	Sep 17 23:59:59 2039 GMT	
Subject	commonName	Sectigo Qualified Website Authentication CA R39	
	organizationName	Sectigo (Europe) SL	
	countryName	ES	

Subject Public Key Info	Public Key Algorithm and RSAPublicKey	RSA (3072 bits)	
Key Usage		Certificate Sign, CRL Sign, digital signature	Critical
Extended Key Usage		Server authentication, client authentication	
Basic Constraints		CA:TRUE	Critical

Sectigo Qualified Website Authentication CA Natural R39

crt.sh | 14599514170

Field/Extension		**Content**	**Optional/Critical**
Version	3 (0x2)		
Serial Number	containing at least 64 bits of output from a CSPRNG	6f62368ac38fc63e62cb6029aeae9e0f	
Signature Algorithm		sha384RSA	
Issuer	commonName	Sectigo Public Server Authentication Root R46	
	organizationName	Sectigo Limited	
	countryName	GB	
Validity	Not before	Sep 18 00:00:00 2024 GMT	
	Not after	Sep 17 23:59:59 2039 GMT	
Subject	commonName	Sectigo Qualified Website Authentication CA Natural R39	
	organizationName	Sectigo (Europe) SL	
	countryName	ES	
Subject Public Key Info	Public Key Algorithm and RSAPublicKey	RSA (3072 bits)	
Key Usage		Certificate Sign, CRL Sign, digital signature	Critical
Extended Key Usage		Server authentication, client authentication	
Basic Constraints		CA:TRUE	Critical

Annex C: Changelog

Version	Change Description	Date
	Draft versions included in CPS document	
2.2	First version	February 5, 2021
2.3	Changes: • Citizen: the field SAN:rfc822 is required • Seal: removal of EKU codeSigning • All (where included): Removal of OU • QWAC-l-PSD2: Added 1.3.6.1.4.1.6449.1.2.1.5.1	March 30, 2022
2.4	Changes: • Added KU keyEncipherment to QWAC-n and QWAC-l-PSD2 • Update the ETSI OIDs for QCP-w (QNCP-w and QEVCP-w) • Added annex A with root CAs cert profiles • Added annex B with subCAs cert profiles • Update the changelog to annex C	November 9, 2022
2.5	Changes: • Clarify the CN value in Seal certificates • Clarify the subject:serialNumber and organizationIdentifier according to the new ETSI EN versions in all cert types • Added the Adobe Authentic Document Trust and the new id-kp-documentSigning (1.3.6.1.5.5.7.3.36) as per RFC 9336 in Seals´ EKUs • Clarify the validity period of the QWACs, to up to 398 days	June 13, 2023
2.6	EKU ClientAuth now optional for the QWAC cert types	March 25, 2025
2.7	Added the new roots (E/R 46) and the new subCAS (E/R 39)	August 4, 2025
2.8	Set the digitalSignature bit KU to optional from signing certs for natural and legal persons. Other minor clarifications with optional values.	September 23, 2026