PÚBLICO

CENTRO TECNOLÓGICO DEL NOTARIADO

Perfiles de certificados

Certificados cualificados

Control documental

Título del documento:	Perfiles de certificados
Nombre del fichero:	Perfiles certificados CA G3 v1.0 REV.docx
Versión:	1.0
Estado:	Aprobado
Confidencialidad:	Público
Fecha:	15/02/2024
Autor:	Oficina de Seguridad

Revisión, Aprobación		
Revisado por:	Responsable de Seguridad	Fecha: 24/03/2025
Aprobado por:	Comité de Seguridad	Fecha: 28/03/2025

Historial de cambios			
Versión	**Fecha**	**Descripción de la acción**	**Páginas**
1.0	15/02/2024	Creación del documento	

Índice

1. Introducción

El presente documento recoge los perfiles de certificados de la jerarquía de entidades de certificación para la emisión de certificados cualificados del Centro Tecnológico del Notariado que dependen jerárquicamente de la CA raíz "Centro Tecnológico del Notariado RootCA-QC".

1.1. Referencias

Los perfiles de certificados detallados en este documento son conformes a la versión vigente de las siguientes normas técnicas:

- ETSI EN 319 411-2
- ETSI EN 319 412.1
- ETSI EN 319 412.2
- ETSI EN 319 412.3
- ETSI EN 319 412.5
- ETSI EN 319 422

1.2. Términos

DCF: Dispositivo de Creación de Firma[1].

DCS: Dispositivo de Creación de Sellos electrónicos.

SCD: Signature Creation Device / Seal Creation Device.

QSCD: Qualified Signature Creation Device.

QSCD on behalf: QSCD gestionado por el Prestador de Servicios de Confianza.

2. Taxonomía de certificados

2.1. Criterios

En el diseño del catálogo de perfiles de certificado se han tenido en cuenta los siguientes criterios:

Comunidad a la que se dirige el servicio:

- Público general
- Consejo General del Notariado

Tipo de certificado:

- Persona física
- Sello electrónico

Mecanismo de custodia de la clave privada:

- Dispositivo seguro de creación QSCD.

[1] Equivalente al término inglés SCD.

- Dispositivos criptográficos hardware no certificados como QSCD[2].
- Sin dispositivo criptográfico[3].

Usos de la clave privada:

- No repudio
- Generación de firma electrónica
- (Cifrado de datos)

Usos de claves extendidos:

- Autenticación de cliente mTLS
- Correo S/MIME

3. Catálogo de certificados

3.1. Certificados Corporativos

Certificados para el colectivo notarial:

- **Certificados FEREN**: Certificados cualificados expedidos a personas físicas en calidad de Notario activos (con notaría).
- **Certificados de Cargo**: Certificados cualificados expedidos a personas físicas en calidad de titulares de un cargo en el CGN o en un colegio notarial.
- **Certificados de Empleados**: Certificados cualificados expedidos a personas físicas en calidad de empleados de una notaría, un colegio notarial, el Consejo General del Notariado o una organización dependiente de éste.

3.1.1. Certificados FEREN

Certificado cualificado de firma avanzada:

- En tarjeta criptográfica.

Certificado cualificado de firma en dispositivo seguro de creación de firma:

- En tarjeta criptográfica (QSCD).
- En dispositivo seguro de creación de firma remoto.

3.1.2. Certificados de Cargo

Certificado cualificado de firma avanzada:

- En tarjeta criptográfica.
- Sin dispositivo criptográfico (software)

Certificado cualificado de firma en dispositivo seguro de creación de firma:

- En tarjeta criptográfica (QSCD).

---

[2] O en un modo de funcionamiento fuera del modo operacional del dispositivo como QSCD. Por ejemplo, claves dentro del chip de una tarjeta criptográfica pero que no son gestionadas por la aplicación certificada como QSCD.

[3] Por ejemplo, claves almacenadas en contenedores PKCS#12, PKCS#8 o almacenes de claves de sistemas operativos o aplicaciones.

- En dispositivo seguro de creación de firma remoto.

3.1.3. Certificados de Empleados

Certificado cualificado de firma avanzada:

- En tarjeta criptográfica.
- Sin dispositivo criptográfico (software).

Certificado cualificado de firma en dispositivo seguro de creación de firma:

- En tarjeta criptográfica (QSCD).

3.2. Certificados No Corporativos

3.2.1. Certificados personales de propósito general

Certificado personal con representación de entidades jurídicas:

- Certificado de firma avanzada (software).
- Certificado de firma en dispositivo seguro de creación de firma (QSCD).

3.2.2. Certificados personales emitidos para su uso en la Sede Electrónica Notarial

- Certificado persona física SEN.
- Certificado persona física con representación SEN.

3.2.3. Certificados de sello electrónico

- En dispositivo seguro de creación de sellos electrónicos (QSCD).
- Sin dispositivo criptográfico (software).

4. Uso de identificadores

4.1. OID

4.1.1. Base

La Agencia Notarial de Certificación S.L. Unipersonal tiene asignado por la IANA el Private Enterprise Number (PEN) número 18920, con lo que el OID base para todos los identificadores es el **1.3.6.1.4.1.18920**.

4.1.2. Reglas de asignación de OID para los perfiles de certificados

El OID para identificar a las políticas de certificación aplicables a cada perfil de certificado se asignará según la siguiente regla:

1.3.6.1.4.1.18920.<R>.<S>.<T>.<V>.<K>

<R>: Identificador asignado a la CA raíz de la jerarquía, ver Tabla 1.

<S>: Identificador asignado a la CA emisora dentro de su jerarquía, ver Tabla 1.

<T>: Identificador asignado a la clase de certificado.

<V>: Identificador asignado a la versión del perfil de certificado, por defecto tomará el valor 1.

<K>: Identificador asignado al soporte de la clave privada, ver Tabla 2.

OID	Autoridad de Certificación	Nombre corto
1.3.6.1.4.1.18920.5	Centro Tecnológico del Notariado RootCA-QC	CTNotariadoRootCA-QC
1.3.6.1.4.1.18920.5.1	Centro Tecnológico del Notariado CA-QC Corporativos	CTNotariadoIntCA-QC
1.3.6.1.4.1.18920.5.2	Centro Tecnológico del Notariado CA-QC No Corporativos	CTNotariadoExtCA-QC
1.3.6.1.4.1.18920.5.3	Centro Tecnológico del Notariado CA QTSA	CTNotariadoTsaCA

Tabla 1 - Asignación de OID por CA

Valor <K>	Propósito
1	Clave en dispositivo cualificado de creación de firma o sello (QSCD/QECD)
2	Clave en dispositivo hardware no cualificado o que no es utilizado según su perfil QSCD/QECD.
3	Sin garantía de dispositivo y el PSC guarda copia de la clave privada[4]
4	Sin garantía de dispositivo.
5	Clave en dispositivo cualificado de creación de firma o sello remoto gestionado por el PSC (rQSCD)
6	Clave en dispositivo de creación de firma o sello remoto gestionado por el PSC (rSCD). El dispositivo no es cualificado o bien no es utilizado según su perfil QSCD/QECD.

Tabla 2 - Identificadores según el soporte de la clave privada

4.2. URL

4.2.1. Dominios

Primario: **tsp.ctnotariado.com**

Secundario: **tsp2.ctnotariado.com**

4.2.2. Recursos

Recurso	HTTPS	Descripción
/crl	MAY	Punto de distribución de CRL
/ocsp	MAY	Servicio de OCSP
/tsa	MAY	Autoridad de sellado de tiempo
/cacerts	MAY	Puntos de descarga de los certificados de las CA (referenciados en la extensión AIA)
/cps	MUST	Repositorio de documentación del que descargar la CPS y el resto de documentación legal del servicio

4.3. Longitud de los nombres

Los componentes de los Nombres de los certificados de entidad final podrán superar las longitudes máximas definidas en el RFC 5280, en especial los componentes CN, GN, SN, O, OU, Description, podrán tener una longitud ilimitada de acuerdo con la norma ITU-T X.509.

[4] Se utiliza para claves de cifrado con servicio de KeyRecovery.

4.4. Uso de mayúsculas y minúsculas en los nombres

Sin estipulación.

4.5. Abreviaturas

Siempre se utilizará la abreviatura CTNotariado para “Centro Tecnológico del Notariado”

4.6. Entornos previos

4.6.1. Dominios

Desarrollo: **des-tsp.ctnotariado.com**

Integración: **int-tsp.ctnotariado.com**

Preproducción: **pre-tsp.ctnotariado.com**

4.6.2. Nombres

Se añadirá un literal que identificará el entorno al final del CN de los certificados.

*Ejemplo: “CN=Centro Tecnológico del Notariado RootCA-QC **DES**” o “CN=Centro Tecnológico del Notariado RootCA-QC **PRE**”*

5. Jerarquía de entidades de certificación

5.1. Diagrama

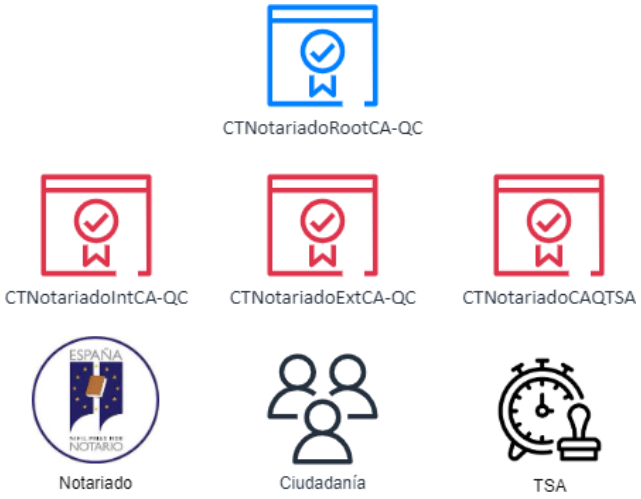

Tabla 3 - Jerarquía de autoridades de certificación

6. Perfil CA raíz

6.1. Requisitos generales

6.1.1. Atributos comunes

Atributo	Valor
version	*MUST be v3(2)*
serialNumber	*MUST be a non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.*
keySize	*4096 bits*
signatureAlgorithm	*RSA with SHA-256*

6.2. Issuer DN

Atributo	Valor
commonName	*Centro Tecnológico del Notariado RootCA-QC*
organizationIdentifier	*VATES-B83395988*
organizationName	*Agencia Notarial de Certificación S.L. Unipersonal*
countryName	*ES*

6.3. Subject DN

El mismo valor que el de la sección 6.2.

6.4. Validez del certificado

10 años

6.5. Extensiones

Extensión	Presencia[5]	Critical	Valor
authorityKeyIdentifier	RECOMMENDED	*N*	***keyIdentifier*** *MUST be present. MUST be identical to the subjectKeyIdentifier field.*
basicConstraints	MUST	*Y*	***cA*** *MUST be set TRUE* ***pathLenConstraint*** *NOT RECOMMENDED*
keyUsage	MUST	*Y*	***digitalSignature, keyCertSign, cRLSign***
subjectKeyIdentifier	MUST	*N*	*keyIdentifier*

7. Perfiles CA emisoras

7.1. Issuer DN

El mismo valor que el de la sección 6.2.

[5] Se debe interpretar según la definición RFC 2119

7.2. Subject DN

Atributo	Valor
commonName	*Ver sección 7.2.1*
organizationIdentifier	*VATES-B83395988*
organizationName	*Agencia Notarial de Certificación S.L. Unipersonal*
countryName	*ES*

7.2.1. CA commonName

CA	commonName
Corporativos	*Centro Tecnológico del Notariado CA-QC Corporativos*
No Corporativos	*Centro Tecnológico del Notariado CA-QC No Corporativos*
TSA	*Centro Tecnológico del Notariado CA QTSA*

7.3. Validez del certificado

10 años

7.4. Extensiones

Extensión	Critical	Valor
authorityKeyIdentifier	*N*	***keyIdentifier*** *MUST be present. MUST be identical to the Root CA subjectKeyIdentifier field.*
basicConstraints	*Y*	***cA*** *MUST be set TRUE* ***pathLenConstraint*** *= 0*
keyUsage	*Y*	***keyCertSign, cRLSign***
extKeyUsage	*N*	*Ver sección 7.4.1*
subjectKeyIdentifier	*N*	***keyIdentifier***
certificatePolicies	*N*	***policyIdentifier*** *= anyPolicy* ***policyQualifiers****:* *id-qt-cps = https://tsp.ctnotariado.com/cps*
cRLDistributionPoints	*N*	*http://tsp.ctnotariado.com/crl/CTNotariadoRootCA-QC.crl* *http://tsp2.ctnotariado.com/crl/CTNotariadoRootCA-QC.crl*
authorityInformationAccess	*N*	*accessMethod = 1.3.6.1.5.5.7.48.2 (id-ad-caIssuers)* *http://tsp.ctnotariado.com/cacerts/CTNotariadoRootCA-QC.cer*

7.4.1. Extensión extKeyUsage

CA	extKeyUsage
Corporativos	*id-kp-emailProtection, id-kp-clientAuth*
No Corporativos	*id-kp-emailProtection, id-kp-clientAuth*
TSA	*id-kp-timeStamping*

8. Perfiles entidades finales

8.1. Requisitos generales

8.1.1. Atributos comunes

Atributo	Valor
version	*MUST be v3(2)*
serialNumber	*MUST be a non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.*
keySize	*4096 bits*
signatureAlgorithm	*RSA with SHA-256*

8.1.2. Identificadores comunes

8.1.2.1. Codificación del tipo de certificado en el Common Name

Los siguientes literales podrán ser utilizados en el Common Name del certificado para ayudar al subscriptor a identificar su certificado en caso de contar con más de uno.

Identificador	Descripción
Firma	Certificado de firma electrónica cualificada (uso exclusivo de clave) en tarjeta criptográfica.
Cifrado	Certificado de cifrado (uso exclusivo de clave)
Autenticación	Certificado de firma avanzada, autenticación web cliente y correo electrónico seguro (S/MIME) en tarjeta criptográfica.

Tabla 4 - Identificadores del de uso de claves en el Common Name

8.2. Certificados Corporativos

8.2.1. Listado de perfiles

Nombre del Perfil	Política[6]	OID	Nombre corto
FEREN firma cualificada	QCP-n-qscd	1.3.6.1.4.1.18920.5.1.1.1.1	INT FEREN QSCD
FEREN firma avanzada	QCP-n	1.3.6.1.4.1.18920.5.1.1.1.2	INT FEREN SCD
FEREN firma cualificada remota	QCP-n-qscd	1.3.6.1.4.1.18920.5.1.1.1.5	INT FEREN RQSCD
Cargo firma cualificada	QCP-n-qscd	1.3.6.1.4.1.18920.5.1.2.1.1	INT CARGO QSCD
Cargo firma avanzada	QCP-n	1.3.6.1.4.1.18920.5.1.2.1.2	INT CARGO SCD
Cargo firma avanzada sin DCF	QCP-n	1.3.6.1.4.1.18920.5.1.2.1.4	INT CARGO SW
Cargo firma cualificada remota	QCP-n-qscd	1.3.6.1.4.1.18920.5.1.2.1.5	INT CARGO RQSCD
Empleado firma cualificada	QCP-n-qscd	1.3.6.1.4.1.18920.5.1.3.1.1	INT EMP QSCD
Empleado firma avanzada	QCP-n	1.3.6.1.4.1.18920.5.1.3.1.2	INT EMP SCD
Empleado firma avanzada sin DCF	QCP-n	1.3.6.1.4.1.18920.5.1.3.1.4	INT EMP SW

[6] De acuerdo con ETSI EN 319 411-2

Tabla 5 - Perfiles de Certificados Corporativos

8.2.2. Issuer DN

Atributo	Valor
commonName	*Centro Tecnológico del Notariado CA-QC Corporativos*
organizationIdentifier	*VATES-B83395988*
organizationName	*Agencia Notarial de Certificación S.L. Unipersonal*
countryName	*ES*

8.2.3. Subject DN

8.2.3.1. Certificados FEREN

Atributo	Presencia	Valor
commonName	MUST	*Nombre Apellido1 (<Tipo Certificado>, ver sección 8.1.2.1)*
clientSerialNumber	MUST	*IDCES-<Número DNI>*
givenName	MUST	*Nombre*
surname	MUST	*Apellidos*
title	MUST	*Notario*
organizationalUnitName	MUST	*Código de notaría, 8 dígitos*
organizationalUnitName	MUST	*Colegio Notarial de <Nombre del Colegio>*
organizationName	MUST	*Consejo General del Notariado*
locality	MUST	*Localidad de la notaría*
state	MUST	*Provincia de la notaría*
countryName	MUST	*ES*

8.2.3.2. Certificados de Cargo

Atributo	Presencia	Valor
commonName	MUST	*Nombre Apellido1 (<Tipo Certificado>, ver sección 8.1.2.1)*
clientSerialNumber	MUST	*IDCES-<Número DNI>*
givenName	MUST	*Nombre*
surname	MUST	*Apellidos*
title	MUST	*Cargo*
organizationalUnitName	MUST	*IDCN<Código del cargo>*
organizationalUnitName	MAY	*Unidad organizativa*
organizationalUnitName	MAY	*Unidad organizativa*
organizationName	MUST	*Consejo General del Notariado*
locality	MUST	*Localidad de la notaría*
state	MUST	*Provincia de la notaría*
countryName	MUST	*ES*

8.2.3.3. Certificados de Empleado

Atributo	Presencia	Valor

commonName	MUST	*Nombre Apellido1 (<Tipo Certificado>, ver sección 8.1.2.1)*
clientSerialNumber	MUST	*IDCES-<Número DNI>*
givenName	MUST	*Nombre*
surname	MUST	*Apellidos*
title	MAY	*Cargo*
organizationalUnitName	MAY	*Unidad organizativa*
organizationalUnitName	MAY	*Unidad organizativa*
organizationalUnitName	MAY	*Unidad organizativa*
organizationName	MUST	*Consejo General del Notariado*
countryName	MUST	*ES*

8.2.3.3.1. Personal de notaría

Atributo	**Presencia**	**Valor**
organizationalUnitName	MUST	*Personal de Notaría*
organizationName	MUST	*Consejo General del Notariado*

8.2.3.3.2. Personal de colegio notarial

Atributo	**Presencia**	**Valor**
title	MUST	*Oficial de colegio | Empleado de colegio*
organizationalUnitName	MUST	*Colegio Notarial de <Comunidad Autónoma>*
organizationName	MUST	*Consejo General del Notariado*

8.2.3.3.3. Personal del CGN

Atributo	**Presencia**	**Valor**
title	MAY	*<Cargo>*
organizationalUnitName	MUST	*<Unidad organizativa, e.g. "Órgano Centralizado de Prevención del Blanqueo de Capitales", "Centro Tecnológico del Notariado", etc.>*
organizationName	MUST	*Consejo General del Notariado*

8.2.4. Validez del certificado

Periodo de validez máximo de 5 años, se permiten duraciones inferiores.

8.2.5. Extensiones

Extensión	**Presencia**	**Critical**	**Valor**
authorityKeyIdentifier	RECOMMENDED	*N*	***keyIdentifier*** *MUST be present. MUST be identical to the issuing CA subjectKeyIdentifier field.*
basicConstraints	MUST	*Y*	***cA*** *MUST be set FALSE*
keyUsage	MUST	*Y*	*Ver sección 8.2.5.1*
extKeyUsage	MAY	*N*	*Ver sección 8.2.5.2*
subjectKeyIdentifier	MUST	*N*	*keyIdentifier*
subjectAltNames	RECOMMENDED	*N*	*rfc822Name = <dirección de correo>*

certificatePolicies	MUST	*N*	*policyIdentifier = ver sección 8.2.5.3* *policyQualifiers:* *id-qt-cps = https://tsp.ctnotariado.com/cps*
cRLDistributionPoints	MUST	*N*	*http://tsp.ctnotariado.com/crl/CTNotariadoIntCA-QC.crl* *http://tsp2.ctnotariado.com/crl/CTNotariadoIntCA-QC.crl*
authorityInformationAccess	MUST	*N*	*accessMethod = 1.3.6.1.5.5.7.48.2 (id-ad-caIssuers)* *http://tsp.ctnotariado.com/cacerts/CTNotariadoIntCA-QC.cer* *accessMethod = 1.3.6.1.5.5.7.48.1 (id-ad-ocsp)* *http://tsp.ctnotariado.com/ocsp*
qcStatements	MUST		*Ver sección 8.3.6.4*

8.2.5.1. KeyUsage

Tipo	**KeyUsgae**
Firma cualificada	*contentCommitment*
Firma avanzada	*digitalSignature, key encipherment*
Firma avanzada sin DCF	*contentCommitment, digitalSignature, key encipherment*
Firma cualificada remota	*contentCommitment*

8.2.5.2. ExtKeyUsage

Tipo	**ExtKeyUsage**
Firma cualificada	<sin uso>
Firma avanzada	*id-kp-emailProtection, d-kp-clientAuth*
Firma avanzada sin DCF	*id-kp-emailProtection, d-kp-clientAuth*
Firma cualificada remota	<sin uso>

8.2.5.3. PolicyIdentifier

Perfil	**OID**
FEREN firma cualificada	1.3.6.1.4.1.18920.5.1.1.1.1, 0.4.0.194112.1.2
FEREN firma avanzada	1.3.6.1.4.1.18920.5.1.1.1.2, 0.4.0.194112.1.0
FEREN firma cualificada remota	1.3.6.1.4.1.18920.5.1.1.1.5, 0.4.0.194112.1.2
Cargo firma cualificada	1.3.6.1.4.1.18920.5.1.2.1.1, 0.4.0.194112.1.2
Cargo firma avanzada	1.3.6.1.4.1.18920.5.1.2.1.2, 0.4.0.194112.1.0
Cargo firma avanzada sin DCF	1.3.6.1.4.1.18920.5.1.2.1.4, 0.4.0.194112.1.0
Cargo firma cualificada remota	1.3.6.1.4.1.18920.5.1.2.1.5, 0.4.0.194112.1.2
Empleado firma cualificada	1.3.6.1.4.1.18920.5.1.3.1.1, 0.4.0.194112.1.2
Empleado firma avanzada	1.3.6.1.4.1.18920.5.1.3.1.2, 0.4.0.194112.1.0

Empleado firma avanzada sin DCF	1.3.6.1.4.1.18920.5.1.3.1.4, 0.4.0.194112.1.0

8.2.5.4. QcStatements

Declaraciones comunes a todos los perfiles:

Perfil	Value
Todos los perfiles	id-etsi-qcs-QcCompliance : presente id-etsi-qcs-QcType : id-etsi-qct-esign id-qcs-pkixQCSyntax-v2 : id-etsi-qcs-semanticsId-eIDASNatural

Declaraciones adicionales según perfil:

Perfil	Value
FEREN firma cualificada	id-etsi-qcs-QcSSCD : presente
FEREN firma avanzada	<sin QC adicionales>
FEREN firma cualificada remota	id-etsi-qcs-QcSSCD : presente
Cargo firma cualificada	id-etsi-qcs-QcSSCD : presente
Cargo firma avanzada	<sin QcStatements adicionales>
Cargo firma avanzada sin DCF	<sin QC adicionales>
Cargo firma cualificada remota	id-etsi-qcs-QcSSCD : presente
Empleado firma cualificada	id-etsi-qcs-QcSSCD : presente
Empleado firma avanzada	<sin QC adicionales>
Empleado firma avanzada sin DCF	<sin QC adicionales>

8.3. Certificados No Corporativos

8.3.1. Listado de perfiles

Perfil	Política	OID	Nombre corto
Sede Electrónica Notarial persona física	QCP-n	1.3.6.1.4.1.18920.5.2.1.1.6	EXT SEN PF RSCD
Sede Electrónica Notarial persona física con representación	QCP-n	1.3.6.1.4.1.18920.5.2.2.1.6	EXT SEN PF REP RSCD
Representante firma cualificada	QCP-n-qscd	1.3.6.1.4.1.18920.5.2.3.1.1	EXT PF REP QSCD
Representante firma avanzada	QCP-n	1.3.6.1.4.1.18920.5.2.3.1.2	EXT PF REP SCD
Representante firma avanzada sin DCF	QCP-n	1.3.6.1.4.1.18920.5.2.3.1.4	EXT PF REP SW
Sello electrónico	QCP-l-qscd	1.3.6.1.4.1.18920.5.2.4.1.1	EXT ESEAL QSCD
Sello electrónico sin DCS	QCP-l	1.3.6.1.4.1.18920.5.2.4.1.4	EXT ESEAL SW

8.3.2. Issuer DN

Atributo	Presencia	Valor
commonName	MUST	*Centro Tecnológico del Notariado CA-QC No Corporativos*
organizationIdentifier	NOT RECOMMENDED	*VATES-B83395988*
organizationName	MUST	*Agencia Notarial de Certificación S.L. Unipersonal*
countryName	MUST	*ES*

8.3.3. Subject DN

8.3.3.1. Certificado de ciudadano de la Sede Electrónica Notarial

Atributo	Presencia	Valor
commonName	MUST	*Nombre Apellido1 Apellido2*
clientSerialNumber	MUST	*IDCES-<Número DNI>*
givenName	MUST	*Nombre*
surname	MUST	*Apellidos*
organizationalUnitName	MUST	*Certificado persona física Sede Electrónica Notarial*
countryName	MUST	*ES*

8.3.3.2. Certificado de ciudadano con representación de la Sede Electrónica Notarial

Atributo	Presencia	Valor
commonName	MUST	*<DNI> Nombre Apellido1 (R:<CIF>)*
clientSerialNumber	MUST	*IDCES-<Número DNI>*
givenName	MUST	*Nombre*
surname	MUST	*Apellidos*
organizationalUnitName	MUST	*Certificado persona física con representación Sede Electrónica Notarial*
organizationIdentifier	MUST	*VATES-<Número CIF>*
organization	MUST	*Razón social*
countryName	MUST	*ES*
description	MUST	*Ver sección 8.3.4*

8.3.3.3. Certificados personales con representación

Atributo	Presencia	Valor
commonName	MUST	*<DNI> Nombre Apellido1 (R:<CIF>)*
clientSerialNumber	MUST	*IDCES-<Número DNI>*
givenName	MUST	*Nombre*
surname	MUST	*Apellidos*
organizationalUnitName	MUST	*Certificado persona física con representación*
organizationIdentifier	MUST	*VATES-<Número CIF>*
organization	MUST	*Razón social*
countryName	MUST	*ES*

description	MUST	*Ver sección 8.3.4*

8.3.3.4. Certificados de Sello Electrónico

Atributo	Presencia	Valor
commonName	MUST	*Nombre para referirse al componente / sistema de firma o marca (no tiene que coincidir con la razón social)*
organizationIdentifier	MUST	*VATES-<Número CIF>*
organizationalUnitName	MUST	*Certificado de sello electrónico*
organizationName	MUST	*Razón social*
countryName	MUST	*ES*

8.3.4. Codificación del documento de representación

La codificación de la representación se realizará de acuerdo con la sección 14.1.3.3 del documento "Perfiles de certificados electrónicos del Ministerio de Hacienda y Administraciones Públicas":

- En el Registro Mercantil: Reg: XXX /Hoja: XXX /Tomo:XXX /Sección:XXX/Libro:XXX /Folio:XXX /Fecha: dd-mm-aaaa /Inscripción: XXX
- Poder Notarial: Notario: Nombre Apellido1 Apellido2 /Núm Protocolo: XXX/Fecha Otorgamiento: dd-mm-aaaa
- En el caso de que las facultades vengan indicadas en Boletines Oficiales: Boletín: XXX/ /Fecha: dd-mm-aaaa /Numero resolución: XXX

8.3.5. Validez del certificado

Para los certificados vinculados a la Sede Electrónica Notarial, el periodo de validez estándar es de 1 mes y se permite una duración máxima de 1 año.

Para el resto de certificados el periodo de validez máximo de 5 años, se permiten duraciones inferiores.

8.3.6. Extensiones

Extensión	Presencia	Critical	Valor
authorityKeyIdentifier	RECOMMENDED	*N*	***keyIdentifier*** *MUST be present. MUST be identical to the issuing CA subjectKeyIdentifier field.*
basicConstraints	MUST	*Y*	***cA*** *MUST be set FALSE*
keyUsage	MUST	*Y*	*Ver sección 8.3.6.1*
extKeyUsage	MAY	*N*	*Ver sección 8.3.6.2*
subjectKeyIdentifier	MUST	*N*	*keyIdentifier*
subjectAltNames	RECOMMENDED	*N*	*rfc822Name = <dirección de correo>*
certificatePolicies	MUST	*N*	*policyIdentifier = ver sección 8.3.6.3* *policyQualifiers:* *id-qt-cps = https://tsp.ctnotariado.com/cps*
cRLDistributionPoints	MUST	*N*	*http://tsp.ctnotariado.com/crl/CTNotariadoExtCA-QC.crl* *http://tsp2.ctnotariado.com/crl/CTNotariadoExtCA-QC.crl*

authorityInformationAccess	MUST	*N*	*accessMethod = 1.3.6.1.5.5.7.48.2 (id-ad-caIssuers)* *http://tsp.ctnotariado.com/cacerts/CTNotariadoExtCA-QC.cer* *accessMethod = 1.3.6.1.5.5.7.48.1 (id-ad-ocsp)* *http://tsp.ctnotariado.com/ocsp*
qcStatements	MUST		*Ver sección 8.3.6.4*

8.3.6.1. KeyUsage

Tipo	**KeyUsage**
Firma / Sello cualificada	*contentCommitment*
Firma avanzada	*digitalSignature, key encipherment*
Firma / Sello avanzado sin DCF / DCS	*contentCommitment, digitalSignature, key encipherment*
Firma remota	*contentCommitment*

8.3.6.2. ExtKeyUsage

Tipo	**ExtKeyUsage**
Firma cualificada	<sin uso>
Firma avanzada	*id-kp-emailProtection, d-kp-clientAuth*
Firma avanzada sin DCF	*id-kp-emailProtection, d-kp-clientAuth*
Firma remota	<sin uso>

8.3.6.3. PolicyIdentifier

Perfil	**OID**
Sede electrónica persona física	1.3.6.1.4.1.18920.5.2.1.1.6, 0.4.0.194112.1.0
Sede electrónica persona física con representación	1.3.6.1.4.1.18920.5.2.2.1.6, 0.4.0.194112.1.0, 2.16.724.1.3.5.8
Representante firma cualificada	1.3.6.1.4.1.18920.5.2.3.1.1, 0.4.0.194112.1.2, 2.16.724.1.3.5.8
Representante firma avanzada	1.3.6.1.4.1.18920.5.2.3.1.2, 0.4.0.194112.1.0, 2.16.724.1.3.5.8
Representante sin dispositivo	1.3.6.1.4.1.18920.5.2.3.1.4, 0.4.0.194112.1.0, 2.16.724.1.3.5.8
Sello cualificado	1.3.6.1.4.1.18920.5.2.4.1.1, 0.4.0.194112.1.3
Sello	1.3.6.1.4.1.18920.5.2.4.1.4, 0.4.0.194112.1.1

8.3.6.4. QcStatements

Declaraciones comunes a todos los perfiles:

Perfil	**Value**
Todos los perfiles	id-etsi-qcs-QcCompliance : presente

Declaraciones adicionales según perfil:

Perfil	**Value**

Sede electrónica persona física	id-etsi-qcs-QcType : id-etsi-qct-esign id-qcs-pkixQCSyntax-v2 : id-etsi-qcs-semanticsId-eIDASNatural
Sede electrónica persona física con representación	id-etsi-qcs-QcType : id-etsi-qct-esign id-qcs-pkixQCSyntax-v2 : id-etsi-qcs-semanticsId-eIDASNatural
Representante firma cualificada	id-etsi-qcs-QcSSCD : presente id-etsi-qcs-QcType : id-etsi-qct-esign id-qcs-pkixQCSyntax-v2 : id-etsi-qcs-semanticsId-eIDASNatural
Representante firma avanzada	id-etsi-qcs-QcType : id-etsi-qct-esign id-qcs-pkixQCSyntax-v2 : id-etsi-qcs-semanticsId-eIDASNatural
Representante sin dispositivo	id-etsi-qcs-QcType : id-etsi-qct-esign id-qcs-pkixQCSyntax-v2 : id-etsi-qcs-semanticsId-eIDASNatural
Sello cualificado	id-etsi-qcs-QcSSCD : presente id-etsi-qcs-QcType : id-etsi-qct-eseal id-qcs-pkixQCSyntax-v2 : id-etsi-qcs-semanticsId-eIDASLegal
Sello	id-etsi-qcs-QcType : id-etsi-qct-eseal id-qcs-pkixQCSyntax-v2 : id-etsi-qcs-semanticsId-eIDASLegal

8.4. Certificados TSU

8.4.1. Requisitos generales

Atributo	**Valor**
version	*MUST be v3(2)*
serialNumber	*MUST be a non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.*
keySize	*3072 bits*
signatureAlgorithm	*RSA with SHA-256*

8.4.2. Issuer DN

Atributo	**Valor**
commonName	*Centro Tecnológico del Notariado CA QTSA*
organizationIdentifier	*VATES-B83395988*
organizationName	*Agencia Notarial de Certificación S.L. Unipersonal*
countryName	*ES*

8.4.3. Subject DN

Atributo	**Presencia**	**Valor**
commonName	MUST	*Centro Tecnológico del Notariado QTSA <Identificador>*
organizationIdentifier	MUST	*VATES-B83395988*
organizationName	MUST	*Agencia Notarial de Certificación S.L. Unipersonal*
countryName	MUST	*ES*

8.4.4. Validez del certificado

6 años

8.4.5. Extensiones

Extensión	Presencia	Critical	Valor
authorityKeyIdentifier	RECOMMENDED	*N*	***keyIdentifier*** *MUST be present. MUST be identical to the issuing CA subjectKeyIdentifier field.*
basicConstraints	MUST	*Y*	***cA*** *MUST be set FALSE*
keyUsage	MUST	*Y*	*digitalSignature*
extKeyUsage	MUST	*Y*	*timeStamping*
privateKeyUsagePeriod	RECOMMENDED	*N*	*5 años*
certificatePolicies	MUST	*N*	*policyIdentifier = 1.3.6.1.4.1.18920.5.3.1.1.1*
cRLDistributionPoints	*MUST*	*N*	*http://tsp.ctnotariado.com/crl/CTNotariadoQTSACA.crl* *http://tsp2.ctnotariado.com/crl/CTNotariadoQTSACA.crl*
authorityInformationAccess	*MUST*	*N*	*accessMethod = 1.3.6.1.5.5.7.48.2 (id-ad-caIssuers)* *http://tsp.ctnotariado.com/cacerts/CTNotariadoQTSACA.cer*

8.5. Perfil certificado OCSP

8.5.1. Requisitos generales

Atributo	Valor
version	*MUST be v3(2)*
serialNumber	*MUST be a non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.*
keySize	*3072 bits*
signatureAlgorithm	*RSA with SHA-256*

8.5.2. Issuer DN

El mismo valor que el de la CA emisora que corresponda según la sección 7.2.

8.5.3. Subject DN

Atributo	Presencia	Valor
commonName	MUST	*OCSP <Nombre CA, ver sección 8.5.3.1>*
organizationIdentifier	NOT RECOMMENDED	*VATES-B83395988*
organizationName	MUST	*Agencia Notarial de Certificación S.L. Unipersonal*
countryName	MUST	*ES*

8.5.3.1. CA commonName

CA	commonName
Corporativos	*Centro Tecnológico del Notariado CA-QC Corporativos*
No Corporativos	*Centro Tecnológico del Notariado CA-QC No Corporativos*

TSA	*Centro Tecnológico del Notariado CA QTSA*

8.5.4. Validez del certificado

1 año

8.5.5. Extensiones

Extensión	**Presencia**	**Critical**	**Valor**
authorityKeyIdentifier	MUST	*N*	***keyIdentifier*** *MUST be present. MUST be identical to the issuing CA subjectKeyIdentifier field.*
basicConstraints	MUST	*Y*	***cA*** *MUST be set FALSE*
keyUsage	MUST	*Y*	*digitalSignature*
extKeyUsage	MUST	*Y*	*ocspSigning*
ocspNoRevocationChecking	MUST	*N*	*Presente*

CONSEJO GENERAL
DEL NOTARIADO