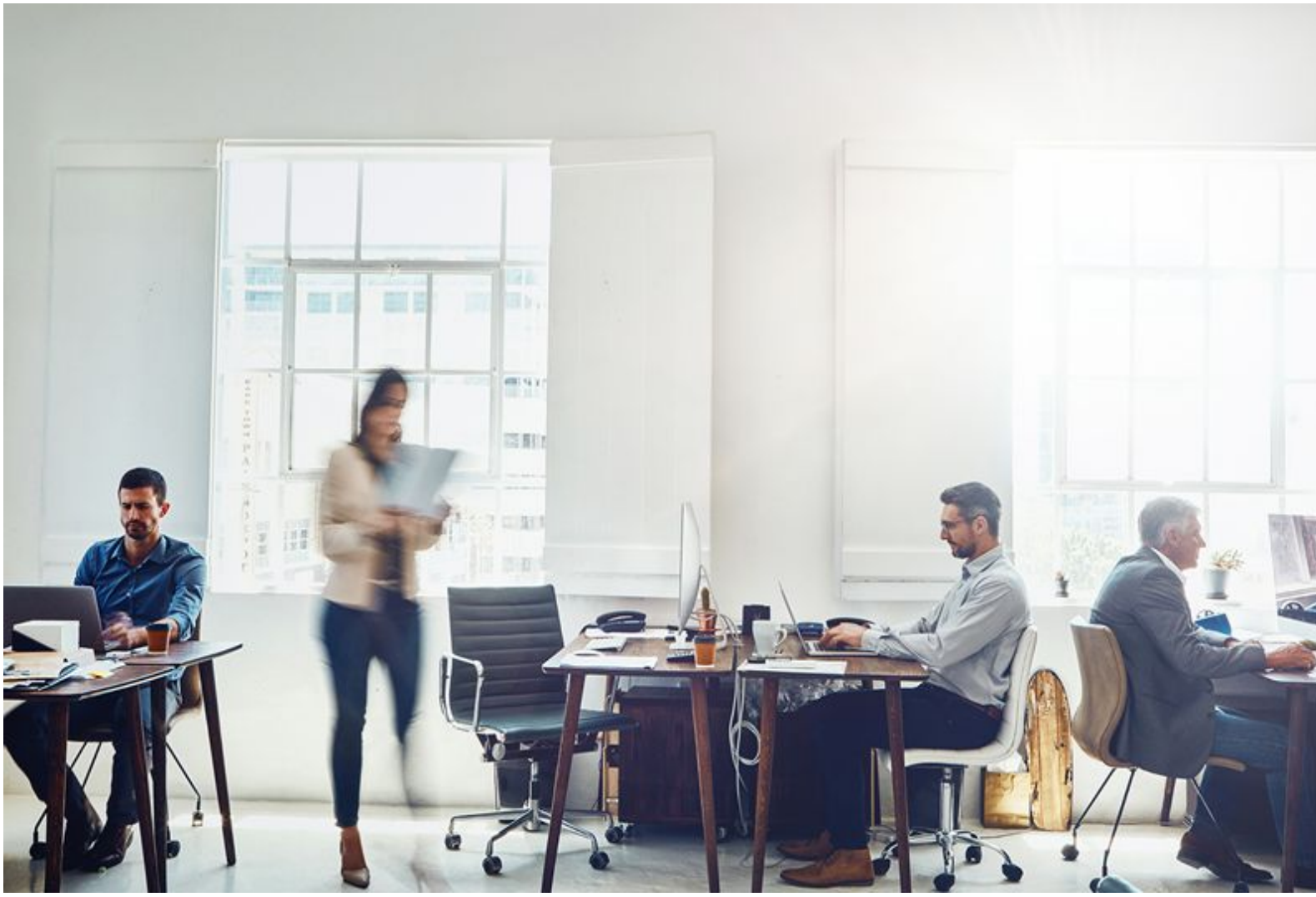
Documento Perfiles de los Certificados de Firmaprofesional

Perfiles de los Certificados

Versión: 190507

Clasificación: Público



BARCELONA
EDIF. ESADECREAPOLIS
AV. TORRE BLANCA, 57 - LOCAL M2
08173 SANT CUGAT DEL VALLÈS
+34 934 774 245

MADRID
VELÁZQUEZ 59, 1º CTRO.-IZDA.
28001 MADRID
+34 915 762 181

WWW.FIRMAPROFESIONAL.COM

Histórico de versiones

Versión	Sección y cambios	Fecha de publicación
181221	Creación de un documento específico de perfiles de certificados. Integra los perfiles que previamente se encontraban incluidos dentro de sus correspondientes Políticas de Certificación, que pueden ser consultadas en http://www.firmaprofesional.com/cps	21/12/2018
190227	"*2.8. Perfil de los certificados de empleado público con seudónimo*": ● En "*2.8.3.1. Extensiones de los certificados*", dentro del Subject Alternative Name, se han cambiado los OIDs del Directory Name. "*5.2. Perfiles de los certificados de VA*": ● Se añade como opcional la extensión noCheck en los *certificados* de VA no cualificada, y como obligatoria en los certificados de VA cualificada	27/02/2019
190507	"2.7. Perfil de los certificados de empleado público": ● Eliminado "1.3.6.1.4.1.13177.10.1.22.3.1:DCCF centralizado autenticación" por no ser cualificado. ● "1.3.6.1.4.1.13177.10.1.22.3.2: DCCF centralizado seudónimo" por información duplicada. "2.8. Perfil de los certificados de empleado público con seudónimo": ● Eliminado el campo opcional de mail del Subject Alternative Name. ● Cambiada la descripción del tercer campo OU. ● Añadido OID para el campo "pseudonym". Todos los perfiles: ● Eliminada la extensión que indica la ruta de la PDS, por haber pasado a ser opcional en la normativa.	07/05/2019

Índice

1. Introducción

En el presente documento se describen los perfiles de los certificados emitidos por Firmaprofesional como Prestador de Servicios de Certificación.

Para la elaboración de los Perfiles de los Certificados se ha tenido en cuenta las siguientes disposiciones:

- Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (de ahora en adelante, eIDAS)
- Política de Firma y de Certificados de la Administración General del Estado:. Anexo 2: Perfiles de certificados electrónicos.
- ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI); Certificate Profiles
- "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" publicada en https://wwww.cabforum.org/

Los perfiles de los diferentes certificados emitidos por Firmaprofesional se agrupan de la siguiente forma, en función de las Políticas a las que van asociados:

A. Certificados de Firma Electrónica, agrupados en :

1. Corporativos. Divididos a su vez en:
    - Certificados Corporativos de Colegiado
    - Certificados Corporativos de Persona Física
    - Certificados de Representación, que pueden ser de tres tipos:
        - Certificados de Representante de entidad sin personalidad jurídica
        - Certificados de Representante legal
        - Certificados de Representante voluntario
2. Personales
3. Empleado Público, divididos a su vez en:
    - Certificados de empleado público
    - Certificados de Empleado público con seudónimo

B. Certificados de Sello Electrónico

1. Certificados de Sello de Órgano, Administración o Entidad de Derecho Público
2. Certificados de Sello de Empresa

C. Certificados de Autenticación Web

1. Certificados de Sede Electrónica
2. Certificados de Servidor Seguro

D. Certificados de Servicio Seguro

1. Certificados de CA
2. Certificados de VA
3. Certificados de TSA

Las Políticas de Certificación a las que se asocian estos certificados están publicadas y accesibles en www.firmaprofesional.com/cps

2. Descripción de perfiles de los Certificados de Firma Electrónica

2.1. Perfil de los certificados corporativos de colegiado

2.1.1. Nombre Distinguido (DN)

Campo del DN	Nombre	Descripción
CN, Common Name	Nombre	Nombre y Apellidos del firmante Adicionalmente se puede incluir el número de colegiado precedido de la palabra "num:" y separado por el carácter "/". *Ej: CN = NOMBRE APELL1 APELL2 / num:4444*
E, E-mail	E-mail	Correo electrónico del firmante.
O, Organization	Organización	Nombre del Colegio Oficial que actúa como RA Adicionalmente se puede incluir el código y el número de la RA que gestionó la emisión del certificado, separados por el carácter "/".
OU, Organization Unit	Unidad en la organización	Contendrá el estatus colegial del firmante En general, "Colegiado".
T, Title	Título	Título o especialidad del firmante
ST, State	Ubicación Geográfica	Ámbito geográfico del firmante
C, Country	País	Código de país de dos dígitos según ISO 3166-1. Por defecto "ES".
serialNumber	Número de identificación	NIF o NIE del firmante
SN, surName	Apellidos	Apellidos del firmante tal y como aparecen en el documento de identidad utilizado
GN, givenName	Nombre de Pila	Nombre de pila del firmante tal y como aparece en el documento de identidad utilizado

En caso de que el firmante no disponga de NIF o NIE, se indicará el Número de Pasaporte en el formato indicado en el apartado 7.1.4 de la CPS.

2.1.2. Extensiones de los certificados

Extensión	Crítica	Valores
X509v3 Subject Alternative Name	-	RFC822:<email del firmante> directoryName: • 1.3.6.1.4.1.13177.0.1: Nombre de pila de la persona física tal y como aparece en su documento de identidad. • 1.3.6.1.4.1.13177.0.2: Primer apellido de la persona física tal y como aparece en su documento de identidad • 1.3.6.1.4.1.13177.0.3: Segundo apellido de la persona física tal y como aparece en su documento de identidad (este campo puede estar vacío)
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Key Usage	Sí	Digital Signature Content Commitment Key Encipherment
X509v3 Extended Key Usage	-	TLS Web Client Authentication E-mail Protection
X509v3 Subject Key Identifier	-	<id de la clave pública del certificado, obtenido a partir del hash de la misma>
X509v3 Authority Key Identifier	-	<id de la clave pública del certificado de la CA, obtenido a partir del hash de la misma>
X509v3 CRL Distribution Points	-	<URI de la CRL>
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI de acceso al servicio OCSP> Access Method: Id-ad-calssuers Access Location: <URI de acceso al certificado de la CA emisora>

2.1.3. Extensiones de los certificados sin DCCF

Extensión	Crítica	Valores
X509v3 Certificate Policies	-	<OID de la política de certificación correspondiente al certificado> 1.3.6.1.4.1.13177.10.1.1.2 <URI de la CPS> User Notice: "Éste es un Certificado Corporativo de Colegiado cualificado, para su uso sin DCCF. Dirección del prestador de servicios de confianza: Paseo de la Bonanova, 47. 08017 Barcelona" <OID de la política de certificación europea: 0.4.0.194112.1.0> (Corresponde a la política para certificados EU cualificados emitidos a personas físicas "QCP-n", sin uso de un DCCF)
QcStatements	-	Id-etsi-qcs-QcCompliance: 0.4.0.1862.1.1 (indicando que el certificado cualificado) Id-etsi-qcs-QcRetentionPeriod: 0.4.0.1862.1.3 (con un valor de 15 años) Id-etsi-qcs-QcType: 0.4.0.1862.1.6.1 (qct-esign, indica que es un certificado para crear firmas electrónicas).

2.1.4. Extensiones de los certificados con DCCF

Extensión	Crítica	Valores
X509v3 Certificate Policies	-	<OID de la política de certificación correspondiente al certificado> 1.3.6.1.4.1.13177.10.1.1.1: DCCF portable 1.3.6.1.4.1.13177.10.1.1.3: DCCF centralizado <URI de la CPS> User Notice: "Éste es un Certificado Corporativo de Colegiado cualificado, para su uso con DCCF. Dirección del prestador de servicios de confianza: Paseo de la Bonanova, 47. 08017 Barcelona" <OID de la política de certificación europea: 0.4.0.194112.1.2> (Corresponde a la política para certificados EU cualificados emitidos a personas físicas "QCP-n-qscd", con uso de un DCCF)

QcStatements	-	Id-etsi-qcs-QcCompliance: 0.4.0.1862.1.1 (indicando que el certificado cualificado) Id-etsi-qcs-QcRetentionPeriod: 0.4.0.1862.1.3 (con un valor de 15 años) Id-etsi-qcs-QcType: 0.4.0.1862.1.6.1 (qct-esign, indica que es un certificado para crear firmas electrónicas). Id-etsi-qcs-QcSSCD: 0.4.0.1862.1.4 (indica que la clave privada se custodia en un DCCF)

2.2. Perfil de los certificados corporativos de persona física

2.2.1. Nombre Distinguido (DN)

Campo del DN	Nombre	Descripción
CN, Common Name	Nombre	Nombre y apellidos del firmante
E, E-mail (Opcional)	E-mail	Correo electrónico del firmante
O, Organization	Organización	Nombre del suscriptor (empresa o entidad privada o pública) con la que existe una vinculación con el firmante En caso que el suscriptor sea un autónomo, se puede incluir el nombre comercial de su establecimiento, su CNAE o IAE
1.3.6.1.4.1.4710.1.3.2(*)	CIF de la Organización	CIF correspondiente a la persona o entidad a la que está vinculado el firmante.
OrganizationIdentifier	CIF de la Organización	NIF, tal como figura en los registros oficiales. Codificado según la Norma Europea ETSI EN 319 412-1 (Ej: VATES-B0085974Z)
OU, Organization Unit	Unidad en la organización	Contendrá uno de los siguientes valores: • El Departamento al que pertenezca el firmante • Tipo de vinculación con la organización.
T, Title	Título	Cargo, título o rol del firmante en la organización.
ST, State	Ubicación Geográfica	Ámbito geográfico de vinculación del firmante.

C, Country	País	Código de país de dos dígitos según ISO 3166-1. Por defecto "ES".
serialNumber	Número de Serie	NIF, NIE o número de pasaporte del firmante. (**)
SN, surName	Apellidos	Apellidos del firmante tal y como aparecen en el documento de identidad utilizado
GN, givenName	Nombre de Pila	Nombre de pila del firmante tal y como aparece en el documento de identidad utilizado

(*) OID propiedad de la empresa Safelayer Secure Communications SA, dedicado a contener un Número de Identificación Fiscal (NIF) o un Código de Identificación Fiscal (CIF).

(**) En caso de que el firmante no disponga de NIF o NIE, se indicará el Número de Pasaporte en el formato indicado en el apartado correspondiente de la CPS.

2.2.2. Extensiones comunes de los certificados

Extensión	Crítica	Valores
X509v3 Subject Alternative Name	-	(Opcional) RFC822:<email del firmante> directoryName: • 1.3.6.1.4.1.13177.0.1: Nombre de pila de la persona física tal y como aparece en su documento de identidad. • 1.3.6.1.4.1.13177.0.2: Primer apellido de la persona física tal y como aparece en su documento de identidad • 1.3.6.1.4.1.13177.0.3: Segundo apellido de la persona física tal y como aparece en su documento de identidad (este campo puede estar vacío)
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Key Usage	Sí	Digital Signature Content Commitment Key Encipherment
X509v3 Extended Key Usage	-	TLS Web Client Authentication E-mail Protection
X509v3 Subject Key Identifier	-	<id de la clave pública del certificado, obtenido a partir del hash de la misma>

X509v3 Authority Key Identifier	-	<id de la clave pública del certificado de la CA, obtenido a partir del hash de la misma>
X509v3 CRL Distribution Points	-	<URI de la CRL>
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI de acceso al servicio OCSP> Access Method: Id-ad-calssuers Access Location: <URI de acceso al certificado de la CA emisora>
QcStatements	-	Id-etsi-qcs-QcCompliance: 0.4.0.1862.1.1 (indicando que el certificado cualificado) Id-etsi-qcs-QcRetentionPeriod: 0.4.0.1862.1.3 (con un valor de 15 años) Id-etsi-qcs-QcType: 0.4.0.1862.1.6.1 (qct-esign, indica que es un certificado para crear firmas electrónicas)

2.2.3. Extensiones de los certificados sin DCCF

Extensión	Crítica	Valores
X509v3 Certificate Policies	-	<OID de la política de certificación correspondiente al certificado> 1.3.6.1.4.1.13177.10.1.2.2 <URI de la CPS> User Notice: "Éste es un Certificado Corporativo de Persona Física cualificado para su uso sin DCCF. Dirección del prestador de Servicios de Confianza: Paseo de la Bonanova, 47. 08017 Barcelona" <OID de la política de certificación europea: 0.4.0.194112.1.0> (Corresponde a la política para certificados EU cualificados emitidos a personas físicas "QCP-n", sin uso de un DCCF)

2.2.4. Extensiones de los certificados con DCCF

Extensión	Crítica	Valores
X509v3 Certificate Policies	-	<OID de la política de certificación correspondiente al certificado> 1.3.6.1.4.1.13177.10.1.2.1: DCCF portable 1.3.6.1.4.1.13177.10.1.2.3: DCCF centralizado <URI de la CPS> User Notice: "Éste es un Certificado Corporativo de Persona Física cualificado para su uso conjuntamente con un DCCF. Dirección del prestador de Servicios de Confianza: Paseo de la Bonanova, 47. 08017 Barcelona" <OID de la política de certificación europea: 0.4.0.194112.1.2> (Corresponde a la política para certificados EU cualificados emitidos a personas físicas "QCP-n-qscd", con uso de un DCCF)
QcStatements	-	Id-etsi-qcs-QcSSCD: 0.4.0.1862.1.4 (indica que la clave privada se custodia en un DCCF)

2.3. Perfil de certificados corporativos de representante sin personalidad jurídica

2.3.1. Nombre distinguido (DN)

Campo del DN	Nombre	Descripción
CN, Common Name	Nombre	Ver tabla específica (12345678Z Pedro Antonio López (R:B0085974Z))
OI, OrganizationIdentifier (2.5.4.97)	Datos Registrales	NIF, tal como figura en los registros oficiales. Codificado según la Norma Europea ETSI EN 319 412-1 (VATES-B0085974Z)
O, Organization	Organización	Razón Social, tal como figura en los registros oficiales.

Description (2.5.4.13)	Codificación del documento público que acredita las facultades del firmante o los datos registrales (*)	Reg:XXX/Hoja:XXX/Tomo:XXX/Sección:XXX/Libro:XXX/Folio:XXX /Fecha: dd-mm-aaaa /Inscripción:XXX Notario: Nombre Apellido1 Apellido2 /Núm Protocolo: XXX /Fecha Otorgamiento: dd-mm-aaaa Boletines Oficiales: Boletín: XXX /Fecha: dd-mm-aaaa /Numero resolución: XXX Otra documentación acreditativa de representación de entidad
C, Country	País	Código de país de dos dígitos según ISO 3166-1. Por defecto "ES".
serialNumber	Número de Serie	NIF, NIE o número de pasaporte del firmante según la Norma Europea ETSI EN 319 412-1 (IDCES-1234567890Z)
SN, surName	Apellidos	Apellidos del firmante tal y como aparecen en el documento de identidad utilizado
GN, givenName	Nombre de Pila	Nombre de pila del firmante tal y como aparece en el documento de identidad utilizado

(*)Los datos se incluirán exactamente igual que en el documento oficial, incluso, si es el caso, caracteres "/".

2.3.1.1. Common Name

Campo	Contenido	Ejemplo	Tamaño*
NIF	Número DNI/NIE	12345678Z	10
Nombre	Tal y como figura en el DNI/NIE	Pedro Antonio	
Apellido 1	Tal y como figura en el DNI/NIE	López	
Literal	(R:		4
NIF de la empresa	NIF de la empresa, tal como figura en los registros oficiales.	B0085974Z	9
Literal	)		2

*(contando espacio en blanco posterior)

2.3.2. Extensiones comunes de los certificados

Extensión	Crítica	Valores
X509v3 Subject Alternative Name	-	RFC822:<email del firmante> (Opcional) directoryName: • 1.3.6.1.4.1.13177.0.1: Nombre de pila de la persona física tal y como aparece en su documento de identidad. • 1.3.6.1.4.1.13177.0.2: Primer apellido de la persona física tal y como aparece en su documento de identidad • 1.3.6.1.4.1.13177.0.3: Segundo apellido de la persona física tal y como aparece en su documento de identidad (este campo puede estar vacío)
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Key Usage	Sí	Digital Signature Content Commitment Key Encipherment,
X509v3 Extended Key Usage	-	TLS Web Client Authentication E-mail Protection
X509v3 Subject Key Identifier	-	<id de la clave pública del certificado, obtenido a partir del hash de la misma>
X509v3 Authority Key Identifier	-	<id de la clave pública del certificado de la CA, obtenido a partir del hash de la misma>
X509v3 CRL Distribution Points	-	<URI de la CRL>
QcStatements	-	Id-etsi-qcs-QcCompliance: 0.4.0.1862.1.1 (indicando que el certificado cualificado) Id-etsi-qcs-QcRetentionPeriod: 0.4.0.1862.1.3 (con un valor de 15 años) Id-etsi-qcs-QcType: 0.4.0.1862.1.6.1 (qct-esign, indica que es un certificado para crear firmas electrónicas).
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI de acceso al servicio OCSP> Access Method: Id-ad-calssuers Access Location: <URI de acceso al certificado de la CA emisora>

2.3.3. Extensiones de los certificados sin DCCF

Extensión	Crítica	Valores
X509v3 Certificate Policies	-	<OID de la política de certificación correspondiente al certificado> 1.3.6.1.4.1.13177.10.1.13.2 <URI de la CPS> User Notice: "Éste es un Certificado Corporativo de Representante de Entidad sin Personalidad Jurídica cualificado. Dirección del prestador de servicios de confianza: Paseo de la Bonanova, 47. 08017 Barcelona" <OID de la política de certificación europea: 0.4.0.194112.1.0> (Corresponde a la política para certificados EU cualificados emitidos a personas físicas "QCP-n", sin uso de un DCCF) <OID de persona física representante de entidad sin personalidad jurídica según Secretaría SGIADSC: 2.16.724.1.3.5.9 >

2.3.4. Extensiones de los certificados con DCCF

Extensión	Crítica	Valores
X509v3 Certificate Policies	-	<OID de la política de certificación correspondiente al certificado> 1.3.6.1.4.1.13177.10.1.13.1: DCCF portable 1.3.6.1.4.1.13177.10.1.13.3: DCCF centralizado <URI de la CPS> User Notice: "Éste es un Certificado Corporativo de Representante de Entidad sin Personalidad Jurídica cualificado en DCCF. Dirección del prestador de servicios de confianza: Paseo de la Bonanova 47 08017 Barcelona" <OID de la política de certificación europea: 0.4.0.194112.1.2> (Corresponde a la política para certificados EU cualificados emitidos a personas físicas "QCP-n-qscd", con uso de un DCCF) <OID de persona física representante de entidad sin personalidad jurídica según Secretaría SGIADSC: 2.16.724.1.3.5.9 >
QcStatements	-	Id-etsi-qcs-QcSSCD: 0.4.0.1862.1.4 (indica que la clave privada se custodia en un DCCF)

2.4. Perfil de certificados corporativos de representante legal

2.4.1. Nombre distinguido (DN)

Campo del DN	Nombre	Descripción
CN, Common Name	Nombre	Ver tabla específica (12345678Z Pedro Antonio López (R:B0085974Z))
OI, OrganizationIdentifier	Datos Registrales	NIF, tal como figura en los registros oficiales. Codificado según la Norma Europea ETSI EN 319 412-1 (VATES-B0085974Z)
O, Organization	Organización	Razón Social, tal como figura en los registros oficiales.
Description (2.5.4.13)	Codificación del documento público que acredita las facultades del firmante o los datos registrales (*)	Reg:XXX/Hoja:XXX/Tomo:XXX/Sección:XXX/Libro:XXX/Folio:XXX /Fecha: dd-mm-aaaa /Inscripción:XXX Notario: Nombre Apellido1 Apellido2 /Núm Protocolo: XXX /Fecha Otorgamiento: dd-mm-aaaa En Boletines Oficiales: Boletín: XXX /Fecha: dd-mm-aaaa /Numero resolución: XXX
C, Country	País	Código de país de dos dígitos según ISO 3166-1. Por defecto "ES".
serialNumber	Número de Serie	NIF, NIE o número de pasaporte del firmante (**)
SN, surName	Apellidos	Apellidos del firmante tal y como aparecen en el documento de identidad utilizado
GN, givenName	Nombre de Pila	Nombre de pila del firmante tal y como aparece en el documento de identidad utilizado

(*)Los datos se incluirán exactamente igual que en el documento oficial, incluso, si es el caso, caracteres "/"
(**)En caso de que el firmante no disponga de NIF o NIE, se indicará el Número de Pasaporte en el formato indicado en el apartado correspondiente de la CPS.

2.4.1.1. Common Name

Campo	Contenido	Ejemplo	Tamaño*
NIF	Número DNI/NIE	12345678Z	10
Nombre	Tal y como figura en el DNI/NIE	Pedro Antonio	
Apellido 1	Tal y como figura en el DNI/NIE	López	
Literal	(R:		4
NIF de la empresa	NIF de la empresa, tal como figura en los registros oficiales.	B0085974Z	9
Literal	)		2

*(contando espacio en blanco posterior)

2.4.2. Extensiones comunes de los certificados

Extensión	Crítica	Valores
X509v3 Subject Alternative Name	-	(opcional) RFC822:<email del firmante> directoryName: • 1.3.6.1.4.1.13177.0.1: Nombre de pila de la persona física tal y como aparece en su documento de identidad. • 1.3.6.1.4.1.13177.0.2: Primer apellido de la persona física tal y como aparece en su documento de identidad • 1.3.6.1.4.1.13177.0.3: Segundo apellido de la persona física tal y como aparece en su documento de identidad (este campo puede estar vacío)
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Key Usage	Sí	Digital Signature Content Commitment Key Encipherment,
X509v3 Extended Key Usage	-	TLS Web Client Authentication E-mail Protection

X509v3 Subject Key Identifier	-	<id de la clave pública del certificado, obtenido a partir del hash de la misma>
X509v3 Authority Key Identifier	-	<id de la clave pública del certificado de la CA, obtenido a partir del hash de la misma>
X509v3 CRL Distribution Points	-	<URI de la CRL>
X509v3 Authority Informacion Access	-	Access Method: Id-ad-ocsp Access Location: <URI de acceso al servicio OCSP> Access Method: Id-ad-calssuers Access Location: <URI de acceso al certificado de la CA emisora>

2.4.3. Extensiones de los certificados sin DCCF

Extensión	Crítica	Valores
X509v3 Certificate Policies	-	<OID de la política de certificación correspondiente al certificado> 1.3.6.1.4.1.13177.10.1.11.2 <URI de la CPS> User Notice: "Éste es un Certificado Corporativo de Representante Legal cualificado. Dirección del prestador de servicios de confianza: Paseo de la Bonanova, 47. 08017 Barcelona" <OID de la política de certificación europea: 0.4.0.194112.1.0> (Corresponde a la política para certificados EU cualificados emitidos a personas físicas "QCP-n", sin uso de un DCCF) <OID de persona física representante de persona jurídica según Secretaría SGIADSC: 2.16.724.1.3.5.8 >
QcStatements	-	Id-etsi-qcs-QcCompliance: 0.4.0.1862.1.1 (indicando que el certificado cualificado) Id-etsi-qcs-QcRetentionPeriod: 0.4.0.1862.1.3 (con un valor de 15 años) Id-etsi-qcs-QcType: 0.4.0.1862.1.6.1 (qct-esign, indica que es un certificado para crear firmas electrónicas).

2.4.4. Extensiones de los certificados con DCCF

Extensión	Crítica	Valores
X509v3 Certificate Policies	-	<OID de la política de certificación correspondiente al certificado> 1.3.6.1.4.1.13177.10.1.11.1: DCCF portable 1.3.6.1.4.1.13177.10.1.11.3: DCCF centralizado <URI de la CPS> User Notice: "Éste es un Certificado Corporativo de Representante Legal cualificado, en DCCF. Dirección del prestador de servicios de confianza: Paseo de la Bonanova, 47. 08017 Barcelona" <OID de la política de certificación europea: 0.4.0.194112.1.2> (Corresponde a la política para certificados EU cualificados emitidos a personas físicas "QCP-n-qscd", con uso de un DCCF) <OID de persona física representante de persona jurídica según Secretaría SGIADSC: 2.16.724.1.3.5.8 >
QcStatements	-	Id-etsi-qcs-QcCompliance: 0.4.0.1862.1.1 (indicando que el certificado cualificado) Id-etsi-qcs-QcRetentionPeriod: 0.4.0.1862.1.3 (con un valor de 15 años) Id-etsi-qcs-QcType: 0.4.0.1862.1.6.1 (qct-esign, indica que es un certificado para crear firmas electrónicas). Id-etsi-qcs-QcSSCD: 0.4.0.1862.1.4 (indica que la clave privada se custodia en un DCCF)

2.5. Perfil de los certificados de representante voluntario frente a las Administraciones Públicas.

2.5.1. Nombre distinguido (DN)

Campo del DN	Nombre	Descripción
CN, Common Name	Nombre	Ver tabla específica (12345678Z Pedro Antonio López (R:B0085974Z))
OI, OrganizationIdentifier	Datos Registrales	NIF, tal como figura en los registros oficiales. Codificado según la Norma Europea ETSI EN 319 412-1 (VATES-B0085974Z)

O, Organization	Organización	Razón Social, tal como figura en los registros oficiales.
Description (2.5.4.13)	Codificación del documento público que acredita las facultades del firmante o los datos registrales(*)	Reg: XXX /Hoja: XXX /Tomo:XXX /Sección:XXX /Libro:XXX /Folio:XXX /Fecha: dd-mm-aaaa /Inscripción:XXX Notario: Nombre Apellido1 Apellido2 /Núm Protocolo: XXX /Fecha Otorgamiento: dd-mm-aaaa En Boletines Oficiales: Boletín: XXX /Fecha: dd-mm-aaaa /Numero resolución: XXX
C, Country	País	Código de país de dos dígitos según ISO 3166-1. Por defecto "ES".
serialNumber	Número de Serie	NIF, NIE o número de pasaporte del firmante (**)
SN, surName	Apellidos	Apellidos del firmante tal y como aparecen en el documento de identidad utilizado
GN, givenName	Nombre de Pila	Nombre de pila del firmante tal y como aparece en el documento de identidad utilizado

(*)Los datos se incluirán exactamente igual que en el documento oficial, incluso, si es el caso, caracteres "/".
(**)En caso de que el firmante no disponga de NIF o NIE, se indicará el Número de Pasaporte en el formato indicado en el apartado correspondiente de la CPS.

2.5.1.1. Common Name

Campo	Contenido	Ejemplo	Tamaño*
NIF	Número DNI/NIE	12345678Z	10
Nombre	Tal y como figura en el DNI/NIE	Pedro Antonio	
Apellido 1	Tal y como figura en el DNI/NIE	López	
Literal	(R:		4
NIF de la empresa	NIF de la empresa, tal como figura en los registros oficiales.	B0085974Z	9
Literal	)		2

*(contando espacio en blanco posterior)

2.5.2. Extensiones comunes de los certificados

Extensión	Crítica	Valores
X509v3 Subject Alternative Name	-	RFC822:<email del firmante> (Opcional) directoryName: • 1.3.6.1.4.1.13177.0.1: Nombre de pila de la persona física tal y como aparece en su documento de identidad. • 1.3.6.1.4.1.13177.0.2: Primer apellido de la persona física tal y como aparece en su documento de identidad • 1.3.6.1.4.1.13177.0.3: Segundo apellido de la persona física tal y como aparece en su documento de identidad (este campo puede estar vacío)
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Key Usage	Sí	Digital Signature Content Commitment Key Encipherment,
X509v3 Extended Key Usage	-	TLS Web Client Authentication E-mail Protection
X509v3 Subject Key Identifier	-	<id de la clave pública del certificado, obtenido a partir del hash de la misma>
X509v3 Authority Key Identifier	-	<id de la clave pública del certificado de la CA, obtenido a partir del hash de la misma>
X509v3 CRL Distribution Points	-	<URI de la CRL>
QcStatements	-	Id-etsi-qcs-QcCompliance: 0.4.0.1862.1.1 (indicando que el certificado cualificado) Id-etsi-qcs-QcRetentionPeriod: 0.4.0.1862.1.3 (con un valor de 15 años) Id-etsi-qcs-QcType: 0.4.0.1862.1.6.1 (qct-esign, indica que es un certificado para crear firmas electrónicas).
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI de acceso al servicio OCSP> Access Method: Id-ad-calssuers Access Location: <URI de acceso al certificado de la CA emisora>

2.5.3. Extensiones de los certificados sin DCCF

Extensión	Crítica	Valores
X509v3 Certificate Policies	-	<OID de la política de certificación correspondiente al certificado> 1.3.6.1.4.1.13177.10.1.12.2 <URI de la CPS> User Notice: "Este es un Certificado Corporativo de Representante Voluntario cualificado frente a las AAPP. Dirección del prestador de servicios de confianza: Paseo de la Bonanova, 47. 08017 Barcelona" <OID de la política de certificación europea: 0.4.0.194112.1.0> (Corresponde a la política para certificados EU cualificados emitidos a personas físicas "QCP-n", sin uso de un DCCF) <OID de persona física representante de persona jurídica según Secretaría SGIADSC: 2.16.724.1.3.5.8 >

2.5.4. Extensiones de los certificados con DCCF

X509v3 Certificate Policies	-	<OID de la política de certificación correspondiente al certificado> 1.3.6.1.4.1.13177.10.1.12.1: DCCF portable 1.3.6.1.4.1.13177.10.1.12.3: DCCF centralizado <URI de la CPS> User Notice: "Este es un Certificado Corporativo de Representante Voluntario cualificado frente a las AAPP, en DCCF. Dirección del prestador de servicios de confianza: Paseo de la Bonanova, 47. 08017 Barcelona" <OID de la política de certificación europea: 0.4.0.194112.1.2> (Corresponde a la política para certificados EU cualificados emitidos a personas físicas "QCP-n-qscd", con uso de un DCCF) <OID de persona física representante de persona jurídica según Secretaría SGIADSC: 2.16.724.1.3.5.8 >
QcStatements	-	Id-etsi-qcs-QcSSCD: 0.4.0.1862.1.4 (indica que la clave privada se custodia en un DCCF)

2.6. Perfil de los certificados Personales

2.6.1. Nombre distinguido (DN)

Campo del DN	Nombre	Descripción
CN, Common Name	Nombre	Nombre y apellidos del firmante
serialNumber	Número de serie	NIF, NIE o número de pasaporte del firmante.(*) Ej: "IDCES-123456789Z"
SN, surName	Apellidos	Apellidos del firmante tal y como aparecen en el documento de identidad utilizado
GN, givenName	Nombre de pila	Nombre de pila del firmante tal y como aparece en el documento de identidad utilizado
C, Country	País	Código de país de dos dígitos según ISO 3166-1. Por defecto "ES".

(*)En caso de que el firmante no disponga de NIF o NIE, se indicará el Número de Pasaporte en el formato indicado en el apartado correspondiente de la CPS. Se seguirá la codificación acorde a ETSI EN 319 412-1

2.6.2. Extensiones de los certificados

Extensión	Crítica	Valor
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Key Usage	Sí	Digital Signature Content Commitment Key Encipherment
X509v3 Extended Key Usage	-	TLS Web Client Authentication
X509v3 Subject Key Identifier	-	<id de la clave pública del certificado, obtenido a partir del hash de la misma>

X509v3 Authority Key Identifier	-	<id de la clave pública del certificado de la CA, obtenido a partir del hash de la misma>
X509v3 CRL Distribution Points	-	<URI de la CRL>
X509v3 Certificate Policies	-	<OID de la política de certificación correspondiente al certificado> 1.3.6.1.4.1.13177.10.1.40.2 <URI de la CPS> User Notice: "Éste es un Certificado Personal de Persona Física cualificado. Dirección del prestador de servicios de confianza: Paseo de la Bonanova, 47. 08017 Barcelona" <OID de la política de certificación europea: 0.4.0.194112.1.0> (Corresponde a la política para certificados EU cualificados emitidos a personas físicas "QCP-n", sin uso de un DCCF)
qcStatements	-	Id-etsi-qcs-QcCompliance: 0.4.0.1862.1.1 (indicando que el certificado cualificado) Id-etsi-qcs-QcRetentionPeriod: 0.4.0.1862.1.3 (con un valor de 15 años) Id-etsi-qcs-QcType: 0.4.0.1862.1.6.1 (qct-esign, indica que es un certificado para crear firmas electrónicas).
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI de acceso al servicio OCSP> Access Method: Id-ad-calssuers Access Location: <URI de acceso al certificado de la CA emisora>
X509v3 Subject Alternative Name	-	(opcional) RFC822:<email del firmante> directoryName: • 1.3.6.1.4.1.13177.0.1: Nombre de pila de la persona física tal y como aparece en su documento de identidad. • 1.3.6.1.4.1.13177.0.2: Primer apellido de la persona física tal y como aparece en su documento de identidad • 1.3.6.1.4.1.13177.0.3: Segundo apellido de la persona física tal y como aparece en su documento de identidad (este campo puede estar vacío)

2.7. Perfil de los certificados de empleado público

2.7.1. Certificado

Campo del DN	Nombre	Descripción
O, Organization	Organización	Denominación (nombre "oficial") de la Administración, organismo o entidad de derecho público suscriptora del certificado, a la que se encuentra vinculada el empleado.
OU, Organization Unit	Descripción del tipo de certificado	"CERTIFICADO ELECTRÓNICO DE EMPLEADO PÚBLICO"(*)
OU, Organization Unit (Opcional)	Unidad en la organización	Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado
OU, Organization Unit (Opcional)	Número de identificación del suscriptor del certificado (supuestamente unívoco).	Se corresponde con el NRP o NIP
Title (opcional)	Puesto o cargo	Debe incluir el puesto o cargo de la persona física, que le vincula con la Administración, organismo o entidad de derecho público suscriptora del certificado.
serialNumber(**)	NIF	NIF o NIE del empleado público. Se utilizará la semántica propuesta por la norma ETSI EN 319 412-1
SN, Surname	Apellidos (persona física)	Primer y segundo apellidos (de acuerdo con documento de identidad -DNI, pasaporte, ...-) + " - DNI " + NIF del empleado público
GN, Given name	Nombre	Nombre de pila del firmante tal y como aparece en el documento de identidad utilizado
CN, Common Name	Nombre, apellidos y NIF	Nombre y dos apellidos de acuerdo con documento de identidad (DNI/Pasaporte) + " - DNI " + NIF del empleado público

C, Country	País	Código de país de dos dígitos según ISO 3166-1. Por defecto "ES".

(*) "Todos los literales se introducen en mayúsculas" excepto el dominio/subdominio y el correo electrónico, según documento "Perfiles de Certificados Electrónicos" de 16 de abril de 2016 del Ministerio de Hacienda y Administraciones Públicas.

(**) SerialNumber = p. ej: IDCES-00000000G. 3 caracteres para indicar el número de documento (IDC= documento nacional de iidentidad) + 2 caracteres para identificar el país (ES) + Número de identidad (Printable String)) Size [RFC 5280] 64

2.7.2. Extensiones comunes de los certificados

Extensión	Crítica	Valores
Subject Alternative Name (opcional)	-	rfc822Name: mail de contacto
Basic Constraints	Sí	CA:FALSE
Subject Key Identifier	-	<id de la clave pública del certificado, obtenido a partir del hash de la misma>
Authority Key Identifier	-	<id de la clave pública del certificado de la CA, obtenido a partir del hash de la misma>
Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI de acceso al servicio OCSP> Access Method: Id-ad-calssuers Access Location: <URI de acceso al certificado de la CA emisora>
CRL Distribution Points	-	<URI de la CRL>
Qualified Certificate Statements	Sí	Id-etsi-qcs-QcCompliance: 0.4.0.1862.1.1 (indicando que el certificado cualificado) Id-etsi-qcs-QcRetentionPeriod: 0.4.0.1862.1.3 (con un valor de 15 años) Id-etsi-qcs-QcType: 0.4.0.1862.1.6.1 (qct-esign, indica que es un certificado para crear firmas electrónicas).

2.7.3. Extensiones de los certificados, nivel alto

Extensión	Crítica	Valores
Key Usage	Sí	Digital Signature
Extended Key Usage	-	Certificado de firma electrónica: Content Commitment Certificado de autenticación: Protección de mail Autenticación de cliente
X509v3 Certificate Policies	-	<OID de la política de certificación correspondiente al certificado> 1.3.6.1.4.1.13177.10.1.22.1: DCCF portable 1.3.6.1.4.1.13177.10.1.22.3: DCCF centralizado <URI de la CPS> User Notice: • "Éste es un Certificado Cualificado de personal, nivel alto. Dirección del prestador de servicios de confianza: Paseo de la Bonanova, 47. 08017 Barcelona" • "Éste es un Certificado Cualificado de personal de autenticación, nivel alto. Dirección del prestador de servicios de confianza: Paseo de la Bonanova, 47. 08017 Barcelona" <OID de la política de certificación europea> • 0.4.0.194112.1.2 (Corresponde a la política para certificados EU cualificados emitidos a personas físicas "QCP-n-qscd", con uso de un DCCF) • 0.4.0.2042.1.2 (Corresponde a la política para certificados EU cualificados emitidos a personas físicas "NCP+", con uso de un DCCF <OID de la política de certificación empleado público: 2.16.724.1.3.5.7.1>
Qualified Certificate Statements	Sí	Id-etsi-qcs-QcSSCD: 0.4.0.1862.1.4 (indica que la clave privada se custodia en un DCCF)

Subject Alternative Name	-	directoryName: • OID: 2.16.724.1.3.5.7.1.1 = "certificado electrónico de empleado público de nivel alto" OID: 2.16.724.1.3.5.7.1.2 = <O del DN> OID: 2.16.724.1.3.5.7.1.3 = <CIF de la entidad suscriptora> OID: 2.16.724.1.3.5.7.1.4 = <serialNumber del DN> OID: 2.16.724.1.3.5.7.1.5 = Número de identificación del suscriptor del certificado (supuestamente unívoco). Se corresponde con el NRP o NIP. (tercera entrada <OU del DN>) OID: 2.16.724.1.3.5.7.1.6 = <Given name> OID: 2.16.724.1.3.5.7.1.7 = <Primer apellido del empleado público> OID: 2.16.724.1.3.5.7.1.8 = <Segundo apellido del empleado público> OID: 2.16.724.1.3.5.7.1.9 = <correo electrónico del empleado público> OID: 2.16.724.1.3.5.7.1.10 = Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado (segunda entrada <OU del DN>) OID: 2.16.724.1.3.5.7.1.11 = <Cargo, T del DN>

2.7.4. Extensiones de los certificados, nivel medio

Extensión	Crítica	Valores
Key Usage	Sí	Digital Signature Content Commitment Key Encipherment
Extended Key Usage	-	Email protection TLS Web Client Authentication
Certificate Policies	-	<OID de la política de certificación correspondiente al certificado> 1.3.6.1.4.1.13177.10.1.22.2 <URI de la CPS> User Notice: "Éste es un Certificado Cualificado de personal, nivel medio. Dirección del prestador de servicios de confianza: Paseo de la Bonanova, 47. 08017 Barcelona" <OID de la política de certificación europea: 0.4.0.194112.1.0> (Corresponde a la política para certificados EU cualificados emitidos a personas físicas "QCP-n", sin uso de un DCCF) <OID de la política de certificación empleado público: 2.16.724.1.3.5.7.2>

Subject Alternative Name	-	(opcional) otherName-userPrincipalName (UPN): Usuario en el dominio Windows del empleado público directoryName: OID: 2.16.724.1.3.5.7.2.1 = "certificado electrónico de empleado público" OID: 2.16.724.1.3.5.7.2.2 = <O del DN> OID: 2.16.724.1.3.5.7.2.3 = <CIF de la entidad suscriptora> OID: 2.16.724.1.3.5.7.2.4 = <NIF o NIE del empleado público> OID: 2.16.724.1.3.5.7.2.5 = Número de identificación del suscriptor del certificado (supuestamente unívoco). Se corresponde con el NRP o NIP. (tercera entrada <OU del DN>) OID: 2.16.724.1.3.5.7.2.6 = <Given name> OID: 2.16.724.1.3.5.7.2.7 = <Primer apellido del empleado público> OID: 2.16.724.1.3.5.7.2.8 = <Segundo apellido del empleado público> OID: 2.16.724.1.3.5.7.2.9 = <correo electrónico del empleado público> OID: 2.16.724.1.3.5.7.2.10 = Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado (segunda entrada <OU del DN>) OID: 2.16.724.1.3.5.7.2.11 = <Cargo, T del DN>

2.8. Perfil de los certificados de empleado público con seudónimo

2.8.1. Certificado

Campo del DN	Nombre	Descripción
O, Organization	Organización	Denominación (nombre "oficial") de la Administración, organismo o entidad de derecho público suscriptora del certificado, a la que se encuentra vinculada el empleado.
OU, Organization Unit	Descripción del tipo de certificado	"CERTIFICADO ELECTRÓNICO DE EMPLEADO PÚBLICO CON SEUDÓNIMO"(*)
OU, Organization Unit	Unidad en la organización	Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado

(Opcional)		
OU, Organization Unit (Opcional)	Código DIR3 de la unidad	Ej: E04976701
pseudonym 2.5.4.65	Seudónimo	Ej: NIP 111111111
Title (opcional)	Puesto o cargo	Debe incluir el puesto o cargo de la persona física, que le vincula con la Administración, organismo o entidad de derecho público suscriptora del certificado.
CN, Common Name	Nombre, apellidos y NIF	"SEUDÓNIMO - " + valor del campo pseudonym +" - " + valor del campo O
C, Country	País	Código de país de dos dígitos según ISO 3166-1. Por defecto "ES".

(*) Tal como aparece en el boletín correspondiente

2.8.2. Extensiones comunes de los certificados

Extensión	Crítica	Valores
Basic Constraints	Sí	CA:FALSE
Subject Key Identifier	-	<id de la clave pública del certificado, obtenido a partir del hash de la misma>
Authority Key Identifier	-	<id de la clave pública del certificado de la CA, obtenido a partir del hash de la misma>
Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI de acceso al servicio OCSP> Access Method: Id-ad-calssuers Access Location: <URI de acceso al certificado de la CA emisora>

CRL Distribution Points	-	<URI de la CRL>
Qualified Certificate Statements	Sí	Id-etsi-qcs-QcCompliance: 0.4.0.1862.1.1 (indicando que el certificado cualificado) Id-etsi-qcs-QcRetentionPeriod: 0.4.0.1862.1.3 (con un valor de 15 años)

2.8.3. Extensiones de los certificados, nivel medio

Extensión	Crítica	Valores
Key Usage	Sí	Digital Signature Content Commitment Key Encipherment
Extended Key Usage	-	Email protection TLS Web Client Authentication
Certificate Policies	-	<OID de la política de certificación correspondiente al certificado> 1.3.6.1.4.1.13177.10.1.23.2 <URI de la CPS> User Notice: "Éste es un Certificado Cualificado de personal, nivel medio. Dirección del prestador de servicios de confianza: Paseo de la Bonanova, 47. 08017 Barcelona" <OID de la política de certificación europea, correspondiente a la política para certificados EU cualificados emitidos a personas físicas "QCP-n", sin uso de un DCCF> 0.4.0.194112.1.0 <OID de la política de certificación empleado público con seudónimo, de nivel medio> 2.16.724.1.3.5.4.2

Subject Alternative Name	-	(opcional) otherName-userPrincipalName (UPN): Usuario en el dominio Windows del empleado público directoryName: OID: 2.16.724.1.3.5.4.2.1 = "CERTIFICADO ELECTRÓNICO DE EMPLEADO PÚBLICO CON SEUDÓNIMO" OID: 2.16.724.1.3.5.4.2.2 = <O del DN> OID: 2.16.724.1.3.5.4.2.3 = <CIF de la entidad suscriptora> OID: 2.16.724.1.3.5.4.2.10 = Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado (segunda entrada <OU del DN>) OID: 2.16.724.1.3.5.4.2.11 = <Cargo, T del DN> OID: 2.16.724.1.3.5.4.2.12 = <pseudonym del DN>
Qualified Certificate Statements		d-etsi-qcs-QcType: 0.4.0.1862.1.6.1 (qct-esign, indica que es un certificado para crear firmas electrónicas).

3. Descripción de perfiles de los Certificados de Sello Electrónico

3.1. Perfil de los certificados de Sello de órgano, Administración Pública o Entidad de Derecho Público

3.1.1. Certificado

Campo del DN	Nombre	Descripción
O, Organization	Organización	Contendrá la denominación de la Administración a la que pertenece el órgano (p.e. "Ministerio de Igualdad ")
OI, Organization Identifier	Identificador de la organización	Identificador de la organización distinto del nombre. Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)
OU, Organization Unit	Unidad en la organización	"SELLO ELECTRONICO"
Serial Number	CIF	CIF de la Administración Pública, órgano o entidad de derecho público
SN, Surname (opcional)	Apellidos (persona física)	Primer y segundo apellidos (de acuerdo con documento de identidad -DNI, pasaporte, ...-) + " - DNI " + NIF del custodio de la clave privada
GN, Given name (opcional)	Nombre (persona física)	Nombre de pila, de acuerdo con documento de identidad (DNI, pasaporte, ...) del custodio de la clave privada
CN, Common Name	Denominación del sistema o aplicación	p.e. "PLATAFORMA DE VALIDACIÓN DEL AYUNTAMIENTO DE xxx"
C, Country	País	"ES"

3.1.2. Extensiones comunes de los certificados

Extensión	Crítica	Valores
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Key Usage	Sí	Digital Signature Content Commitment Key Encipherment
X509v3 Extended Key Usage	-	Email protection TLS Web Client Authentication
X509v3 Subject Key Identifier	-	<id de la clave pública del certificado, obtenido a partir del hash de la misma>
X509v3 Authority Key Identifier	-	<id de la clave pública del certificado de la CA, obtenido a partir del hash de la misma>
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI de acceso al servicio OCSP> Access Method: Id-ad-calssuers Access Location: <URI de acceso al certificado de la CA emisora>
X509v3 CRL Distribution Points	-	<URI de la CRL>
Qualified Certificate Statements	Sí	Id-etsi-qcs-QcCompliance: 0.4.0.1862.1.1 (indicando que el certificado cualificado) Id-etsi-qcs-QcRetentionPeriod: 0.4.0.1862.1.3 (con un valor de 15 años) Id-etsi-qcs-QcType: 0.4.0.1862.1.6.2 (qct-eseal, indica que es un certificado para crear sellos electrónicos).

3.1.3. Extensiones de los certificados, nivel alto

Extensión	Crítica	Valores
X509v3 Certificate Policies	-	<OID de la política de certificación correspondiente al certificado> 1.3.6.1.4.1.13177.10.1.21.1: DCCF portable 1.3.6.1.4.1.13177.10.1.21.3: DCCF centralizado <URI de la CPS> User Notice: "Certificado cualificado de sello de Administración, órgano o entidad de derecho público, nivel alto. Dirección del prestador de servicios de confianza: Paseo de la Bonanova, 47. 08017 Barcelona" <OID de la política de certificación según Secretaría SGIADSC: 2.16.724.1.3.5.6.1> < OID "for EU qualified certificates issued to legal persons" según ETSI EN 319 411-2: QCP-l-qscd: 0.4.0.194112.1.3>
Qualified Certificate Statements	Sí	Id-etsi-qcs-QcSSCD: 0.4.0.1862.1.4 (indica que la clave privada se custodia en un DCCF)
X509v3 Subject Alternative Name	-	rfc822Name: mail de contacto (Opcional) directoryName: OID: 2.16.724.1.3.5.6.1.1 = "SELLO ELECTRONICO DE NIVEL ALTO" OID: 2.16.724.1.3.5.6.1.2 = <O del DN> OID: 2.16.724.1.3.5.6.1 .3 = <serialNumber del DN> OID: 2.16.724.1.3.5.6.1 .4 = <NIF/NIE del custodio> (opcional) OID: 2.16.724.1.3.5.6.1 .5 = <CN del DN> OID: 2.16.724.1.3.5.6.1 .6 = <Given name> (opcional) OID: 2.16.724.1.3.5.6.1 .7 = <Primer apellido del custodio>(*) (opcional) OID: 2.16.724.1.3.5.6.1 .8 = <Segundo apellido del custodio>(*) (opcional) OID: 2.16.724.1.3.5.6.1 .9 = <correo electrónico del custodio> (opcional)

(*) de acuerdo con documento de identidad (DNI, pasaporte, ...)

3.1.4. Extensiones de los certificados, nivel medio

Extensión	Crítica	Valores
X509v3 Certificate Policies	-	<OID de la política de certificación correspondiente al certificado> 1.3.6.1.4.1.13177.10.1.21.2 <URI de la CPS> User Notice: "Certificado cualificado de sello de Administración, órgano o entidad de derecho público, nivel medio. Dirección del prestador de servicios de confianza: Paseo de la Bonanova, 47. 08017 Barcelona" <OID de la política de certificación del MHAP: 2.16.724.1.3.5.6.2> < OID "for EU qualified certificates issued to legal persons" según ETSI EN 319 411-2: QCP-l: 0.4.0.194112.1.1>
X509v3 Subject Alternative Name	-	rfc822Name: mail de contacto (Opcional) directoryName: OID: 2.16.724.1.3.5.6.2.1 = "SELLO ELECTRONICO DE NIVEL MEDIO" OID: 2.16.724.1.3.5.6.2.2 = <O del DN> OID: 2.16.724.1.3.5.6.2.3 = <serialNumber del DN> OID: 2.16.724.1.3.5.6.2.4 = <NIF/NIE del custodio> (opcional) OID: 2.16.724.1.3.5.6.2.5 = <CN del DN> OID: 2.16.724.1.3.5.6.2.6 = <Given name> (opcional) OID: 2.16.724.1.3.5.6.2.7 = <Primer apellido del custodio>(*) (opcional) OID: 2.16.724.1.3.5.6.2.8 = <Segundo apellido del custodio> (*) (opcional) OID: 2.16.724.1.3.5.6.2.9 = <correo electrónico del custodio> (opcional

(*)de acuerdo con documento de identidad (DNI, pasaporte, ...)

3.2. Perfil de los certificados de Sello Empresarial

3.2.1. Nombre distinguido (DN)

Campo del DN	Nombre	Descripción
CN, Common Name	Nombre	Contendrá el nombre comercial de la persona jurídica
serialNumber	CIF	<CIF de la persona jurídica>
O, Organization	Organización	Contendrá la denominación exacta de la persona jurídica según aparezca en el Registro mercantil
OI, organizationIdentifier	Identificador de la organización	VATES-<CIF de la persona jurídica>(*)
OU, Organization Unit (opcional)	Unidad en la organización	Contendrá el Departamento o Unidad
E, Email Address (Opcional)	Correo electrónico	Contendrá una dirección de correo electrónico de contacto con la empresa
ST, State	Ubicación Geográfica	Ámbito geográfico de vinculación del suscriptor.
C, Country	País	Código de país de dos dígitos según ISO 3166-1. Por defecto "ES".

(*) Según lo estipulado en los borradores estables ETSI EN 319 412-1 y ETSI EN 319 412-3

3.2.2. Extensiones de los certificados

Extensión	Crítica	Valores
X509v3 Basic Constraints	Sí	CA:FALSE

X509v3 Key Usage	Sí	Digital Signature Content Commitment Key Encipherment
X509v3 Extended Key Usage	-	TLS Web Client Authentication Email Protection
X509v3 Subject Key Identifier	-	<id de la clave pública del certificado, obtenido a partir del hash de la misma>
X509v3 Authority Key Identifier	-	<id de la clave pública del certificado de la CA, obtenido a partir del hash de la misma>
X509v3 Authority Information Access	-	<URI dónde se encuentra el certificado de la CA> Access Method: Id-ad-ocsp Access Location: <URI de acceso al servicio OCSP>
X509v3 CRL Distribution Points	-	<URI de la CRL>
X509v3 Certificate Policies	-	<OID de la política de certificación correspondiente al certificado> 1.3.6.1.4.1.13177.10.1.10.2 <URI de la CPS> User Notice: "Éste es un Certificado Corporativo de Sello Empresarial cualificado.Dirección del prestador de servicios de confianza: Paseo de la Bonanova, 47. 08017 Barcelona" < OID "for EU qualified certificates issued to legal persons" según ETSI EN 319 411-2: QCP-l: 0.4.0.194112.1.1>
X509v3 Subject Alternative Name (opcional)	-	<Email de contacto>
QcStatements	-	Id-etsi-qcs-QcCompliance: 0.4.0.1862.1.1 (indicando que el certificado cualificado) Id-etsi-qcs-QcRetentionPeriod: 0.4.0.1862.1.3 (con un valor de 15 años) Id-etsi-qcs-QcType: 0.4.0.1862.1.6.2 (qct-eseal, indica que es un certificado para crear firmas electrónicas).

4. Descripción de perfiles de los Certificados de Autenticación de sitios web

4.1. Perfil de los certificados de Sede Electrónica

4.1.1. Certificado

Campo del DN	Nombre	Descripción
CN, Common Name	Nombre	Denominación de nombre de dominio donde residirá el certificado Debe coincidir con el que se encuentra en la extensión Subject Alternative Names
O, Organization	Organización	Denominación (nombre "oficial" de la organización) del suscriptor de servicios de certificación
OU, Organization Unit	Unidad en la organización	"SEDE ELECTRONICA"
OU, Organization Unit	Unidad en la organización	El nombre descriptivo de la sede
serialNumber opcional)(*)	Número de serie	Contendrá el NIF de la entidad responsable de la sede electrónica
organizationIdentifier		Identificador de la organización Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)
C, Country	País	C= ES
L, Localty		Ciudad
businessCategory		Categoría de organización: "Government Entity"
jurisdictionCountryName		Jurisdicción JurisdictionCountryName= "ES"

(*)Se marca el campo SerialNumber como opcional, dado que la misma información la contiene el campo OrganizationIdentifier

4.1.2. Extensiones comunes de los certificados

Extensión	Crítica	Valores
X509v3 Authority Key Identifier	-	<id de la clave pública de la CA, obtenido a partir del hash de la misma>
X509v3 Subject Key Identifier	-	<id de la clave pública del certificado, obtenido a partir del hash de la misma>
X509v3 Key Usage	Sí	Digital Signature Key Encipherment
X509v3 Extended Key Usage	-	Autenticación TSL web Server
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 CRL Distribution Points	-	<URI de la CRL>
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: http://ocsp.firmaprofesional.com Access Method: Id-ad-calssuers Access Location: http://crl.firmaprofesional.com/infraestructura.crt
X509v3 Certificate Policies	-	<URI de la CPS> http://www.firmaprofesional.com/cps <OID "EU qualified website authentication certificates" según ETSI EN 319 411-2: QCP-w: 0.4.0.194112.1.4> <OID de la política de certificación correspondiente al certificado: 0.4.0.2042.1.4>
Qualified Certificate Statements		Id-etsi-qcs-QcCompliance: 0.4.0.1862.1.1 (indicando que el certificado cualificado) Id-etsi-qcs-QcRetentionPeriod: 0.4.0.1862.1.3 (con un valor de 15 años) Id-etsi-qcs-QcType: 0.4.0.1862.1.6.3 (qct-web, indica que es un certificado para crear firmas electrónicas).
X509v3 Subject Alternative Name	-	dNSName: nombre de dominio donde residirá el certificado

4.1.3. Extensiones de los certificados, nivel alto

Extensión	Crítica	Valores
X509v3 Certificate Policies	-	<OID de la política de certificación correspondiente al certificado> 1.3.6.1.4.1.13177.10.1.20.1 User Notice: "Certificado de Sede Electronica Nivel Alto" <OID de la política de certificación del MHAP 2.16.724.1.3.5.5.1>

4.1.4. Extensiones de los certificados, nivel medio

Extensión	Crítica	Valores
X509v3 Certificate Policies	-	<OID de la política de certificación correspondiente al certificado> 1.3.6.1.4.1.13177.10.1.20.2 User Notice: "Certificado de Sede Electronica Nivel Medio" <OID de la política de certificación del MHAP 2.16.724.1.3.5.5.2>

4.2. Perfil de los certificados de Servidor Web SSL

4.2.1. Nombre distinguido (DN)

Campo	Valor	Descripción
CN, Common Name	Nombre	(EVG 9.2.3) Nombre de un único dominio. (BR. 7.1.4.2.2.a) Este dominio debe coincidir con el indicado (o con uno de los indicados) en el Subject Alt Names).
O, Organization	Razón Social	Nombre Oficial de la Organización subscriptora del certificado

OU, Organizational Unit	Departamento	Opcional hasta versión 6.3 (incluida) de la presente política. No presente en adelante. (BR. 7.1.4.2.2.i) Opcional
serialNumber (opcional)(*)	CIF	CIF de la Organización subscriptora del certificado
OrganizationIdentifier		Identificador de la organización, según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)
businessCategory	Private Organization Government Entity Business Entity Non-Commercial Entity	(EVG 9.2.4) Business Category
L, Locality	Ciudad	Address of Place of Business: City
ST, StateOfProvince	Provincia	Provincia de registro de la organización
C, Country	País	Código de país de dos dígitos según ISO 3166-1. Por defecto "ES".
jurisdictionCountryName 1.3.6.1.4.1.311.60.2.1.3	País	(EVG 9.2.5) Subject Jurisdiction of Incorporation or Registration

(*)Se marca el campo SerialNumber como opcional, dado que la misma información la contiene el campo OrganizationIdentifier

Los campos (EVG 9.2.X) son requerimientos específicos para certificados Extended Validation según establece el CA/Browser Forum.

Las indicaciones (BR.X) son requerimientos de la Baseline Requeriments Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates del CA/Browser Forum, vigente en el momento de la publicación del presente documento.

4.2.2. Extensiones de los certificados

Extensión	Crítica	Valores
X509v3 Subject Alternative Name	-	URL, nombre de dominio o identificación del dispositivo o servicio poseedor de las claves o de la aplicación. (EVG 9.2.2) Se puede incluir más de 1 dominio, pero no wilcards. Para certificados multidominio, la URL seguirá el formato "*.dominio.com" (esta indicación está prohibida para certificados EV)
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Key Usage	Sí	Digital Signature Key Encipherment Data Encipherement
X509v3 Extended Key Usage	-	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)
X509v3 Subject Key Identifier	-	<id de la clave pública del certificado, obtenido a partir del hash de la misma>
X509v3 Authority Key Identifier	-	<id de la clave pública del certificado de la CA, obtenido a partir del hash de la misma>
X509v3 Authority Information Access	-	Access Method 1: Id-ad-ocsp (1.3.6.1.5.5.7.48.1) Access Location 1: http://ocsp.firmaprofesional.com Access Method 2: id-ad-caissuers (1.3.6.1.5.5.7.48.2) Access Location 2: http://crl.firmaprofesional.com/infraestructura.crt
X509v3 CRL Distribution Points	-	http://crl.firmaprofesional.com/infraestructura.crl

X509v3 Certificate Policies	-	<OID de la política de certificación correspondiente al certificado> 1.3.6.1.4.1.13177.10.1.3.1 SSL OV 1.3.6.1.4.1.13177.10.1.3.10 SSL EV / Cualificado <URI de la CPS> User Notice: "Este es un Certificado de Servidor Web cualificado con Validación Extendida" (para los certificados EV) User Notice: "Este es un Certificado de Servidor Web" (para los certificados sin EV) <OID "EU qualified website authentication certificates" según ETSI EN 319 411-2: QCP-w: 0.4.0.194112.1.4 > (para los certificados EV) <OID de la política EV de certificación correspondiente al certificado: 0.4.0.2042.1.4> (para los certificados EV)
Qualified Certificate Statements (solo para EV)	-	Id-etsi-qcs-QcCompliance: 0.4.0.1862.1.1 (indicando que el certificado cualificado) Id-etsi-qcs-QcRetentionPeriod: 0.4.0.1862.1.3 (con un valor de 15 años) Id-etsi-qcs-QcType: 0.4.0.1862.1.6.3 (qct-web, indica que es un certificado para crear firmas electrónicas).

5. Descripción de perfiles de los Certificados de Servicio Seguro CA, TSA, VA

5.1. Perfiles de los certificados de CA

5.1.1. Certificados de CA

5.1.1.1. Nombre Distinguido (DN)

Campo del DN	Nombre	Descripción
CN, Common Name	Nombre	Nombre común de la organización prestadora de servicios de certificación
O, Organization	Organización	Denominación (nombre "oficial" de la organización) del prestador de servicios de certificación (emisor del certificado)(*)
C, Country	País	C=ES

(*)MINHAP 7. Certificado de SubCA 1.4.2 Organization

5.1.1.2. Extensiones de los certificados

Extensión	Crítica	Valores
X509v3 Basic Constraints	Sí	CA:TRUE
X509v3 Key Usage	Sí	keyCertificateSignature cRLSignature
X509v3 Subject Key Identifier	-	<id de la clave pública del certificado, obtenido a partir del hash de la misma>
X509v3 Authority Key Identifier	-	<id de la clave pública del certificado de la CA, obtenido a partir del hash de la misma>
X509v3 CRL Distribution Points	-	<URI de la CRL>

X509v3 Certificate Policies	-	policyIdentifier: 1.3.6.1.4.1.13177.10.10.2 cPSURI: http://www.firmaprofesional.com/cps userNotice: "Certificado de Autoridad de Certificación"
Authority Information Access		accessMethod: Id-ad-calssuers accessLocation: <URI de acceso al certificado de la CA emisora>

5.1.2. Certificados de QCA (CA Cualificados)

5.1.2.1. Nombre Distinguido (DN)

Adicionalmente, el DN de los certificados de CA cualificados (QCA) deben cumplir los siguientes requisitos:

Campo del DN	Nombre	Descripción
OI, Organization Identifier	Identificador de Organización	Identificador de la organización distinto del nombre Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)
OU, Organization Unit	Unidad Organizativa	Unidad organizativa dentro del prestador de servicios, responsable de la emisión del certificado.

5.1.2.2. Extensiones de los certificados

Extensión	Crítica	Valores
X509v3 Certificate Policies	-	policyIdentifier: 1.3.6.1.4.1.13177.10.10.1 cPSURI: http://www.firmaprofesional.com/cps userNotice: "Certificado de Autoridad de Certificación Cualificada"
Authority Information Access		accessMethod: Id-ad-ocsp accessLocation: <URI de acceso al servicio OCSP>

5.2. Perfiles de los certificados de VA

5.2.1. Certificados de VA

5.2.1.1. Nombre Distinguido (DN)

Campo del DN	Nombre	Descripción
CN, Common Name	Nombre	URL del servicio.
O, Organization	Organización	Nombre de la Organización que ofrece el servicio seguro
C, Country	País	C=ES

5.2.1.2. Extensiones de los certificados

Extensión	Crítica	Valores
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Key Usage	Sí	digitalSignature cRLSignature
X509v3 Extended Key Usage	Sí	id-kp-OCSPSigning
X509v3 Subject Key Identifier	-	<id de la clave pública del certificado, obtenido a partir del hash de la misma>
X509v3 Authority Key Identifier	-	<id de la clave pública del certificado de la CA, obtenido a partir del hash de la misma>
X509v3 CRL Distribution Points	-	<URI de la CRL>
X509v3 Certificate Policies	-	policyIdentifier: 1.3.6.1.4.1.13177.10.1.31.2 cPSURI: http://www.firmaprofesional.com/cps userNotice: "Certificado de firma de respuestas OCSP"
1.3.6.1.5.5.7.48.1.5 id-pkix-ocsp-nocheck (Opcional)	-	oCSPNoCheck

Authority Information Access	-	accessMethod: Id-ad-calssuers accessLocation: <URI de acceso al certificado de la CA emisora>

5.2.2. Certificados de QVA (VA Cualificados)

Adicionalmente, el perfil de los certificados de CA cualificados (QCA) deben cumplir los siguientes requisitos:

5.2.2.1. Nombre Distinguido (DN)

Campo del DN	Nombre	Descripción
OI, Organization Identifier	Identificador de Organización	De acuerdo con lo definido en la Cláusula 5 de ETSI EN 319 312-1

5.2.2.2. Extensiones de los certificados

Extensión	Crítica	Valores
X509v3 Certificate Policies	-	policyIdentifier: 1.3.6.1.4.1.13177.10.1.31.1 cPSURI: http://www.firmaprofesional.com/cps userNotice: "Certificado de firma de respuestas OCSP cualificado"
1.3.6.1.5.5.7.48.1.5 id-pkix-ocsp-nocheck	-	oCSPNoCheck
QCStatements	-	Id-etsi-qcs-QcCompliance: 0.4.0.1862.1.1 (indica que el certificado cualificado) Id-etsi-qcs-QcRetentionPeriod: 0.4.0.1862.1.3 = 15 (con un valor de 15 años) Id-etsi-qcs-QcType: 0.4.0.1862.1.6.2 (indica que es un certificado para crear sellos electrónicos) Id-etsi-qcs-QcSSCD: 0.4.0.1862.1.4 (indica que la clave privada se custodia en un DCCF

5.3. Perfiles de los Certificados de TSA

5.3.1. Certificados de TSA

5.3.1.1. Nombre Distinguido (DN)

Campo del DN	Nombre	Descripción
CN, Common Name	Nombre	Debe contener un Identificador de TSU que debe identificar de manera única la TSU correspondiente, incluyendo referencia al cliente
O, Organization	Organización	Firmaprofesional S.A.
C, Country	País	C=ES Debe especificar el país donde la TSA está establecida (no necesariamente donde está ubicada físicamente la TSU)

5.3.1.2. Extensiones de los certificados

Extensión	Crítica	Valores
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Key Usage	Sí	digitalSignature contentCommitment
X509v3 Extended Key Usage	Sí	id-kp-timeStamping {1.3.6.1.5.5.7.3.8}
X509v3 Subject Key Identifier	-	<id de la clave pública del certificado, obtenido a partir del hash de la misma>
X509v3 Authority Key Identifier	-	<id de la clave pública del certificado de la CA, obtenido a partir del hash de la misma>
X509v3 CRL Distribution Points	-	<URI de la CRL>
X509v3 Certificate Policies	-	policyIdentifier: 1.3.6.1.4.1.13177.10.1.4.2 cPSURI: http://www.firmaprofesional.com/cps userNotice: "Certificado de Servicio Seguro de TSA"

Authority Information Access	-	accessMethod: Id-ad-calssuers accessLocation: <URI de acceso al certificado de la CA emisora>

5.3.2. Certificados de QTSA (TSA Cualificados)

Adicionalmente, el perfil de los certificados de CA cualificados (QCA) deben cumplir los siguientes requisitos:

5.3.2.1. Nombre Distinguido (DN)

Campo del DN	Nombre	Descripción
OI, Organization Identifier	Identificador de Organización	"VATES-A62634068"

5.3.2.2. Extensiones de los certificados

Extensión	Crítica	Valores
X509v3 Certificate Policies	-	policyIdentifier: 1.3.6.1.4.1.13177.10.1.4.1 cPSURI: http://www.firmaprofesional.com/cps userNotice: "Certificado de Servicio Seguro de TSA cualificada"
id-ce-privateKeyUsagePeriod 2.5.29.16		Tiene por objetivo limitar la validez de la clave privada: 3 años
Authority Information Access		accessMethod: Id-ad-ocsp accessLocation: <URI de acceso al servicio OCSP>

Los Tokens de Timestamp cualificados, deberían incluir una instancia de la extensión qcStatements, de acuerdo con la sintaxis definida en IETF RFC 3739 [i.3], cláusula 3.2.6.

La extensión debería incluir una instancia de "esi4-qtstStatement-1" de acuerdo con lo definido en el Anexo B de la norma ETSI TS 319 422 .

Firmaprofesional, S.A.

Mayo de 2019