Perfiles de certificados

PKI

INFORMACIÓN GENERAL

Tipo	Documentación General Procedimiento Registro **Instrucción Técnica** Plantilla
Clasificación	**Público** Confidencial Uso Interno
Versión	251219
Estado	Borrador en curso **Aprobado** Retirado

HISTÓRICO DE VERSIONES

Versión	Sección y cambios	Autor
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	FP
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	FP
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:	FP

	• Eliminada la extensión que indica la ruta de la PDS, por haber pasado a ser opcional en la normativa.	
190612	• "2.1. Perfil de los certificados corporativos de colegiado" y "2.2. Perfil de los certificados corporativos de persona física", campo "organización" del DN: • Realizadas aclaraciones en sobre el formato del código y número de la RA que gestionó la emisión del certificado. • Añadido punto 3.3 "Perfil de los certificados de sello electrónico para PSD2" • Modificación del punto 4.2 para añadir atributos de certificados de autenticación web para PSD2	FP
200205	• Aclaración de que los certificados están basados en el estándar ITU Telecommunication Standardization Sector (ITU-T) X.509 version 3. • Actualizado *userNotice* de Certificados Corporativos de Sello Empresarial PSD2. • Actualizado perfil de Certificados SSL EV para adaptarlo a los requerimientos de CA/Browser Forum, EV Guidelines, v. 1.7.1. • Reubicación de extensión keyUsage y extendedKeyUsage por coherencia documental.	FP
200930	• Añadido soporte DCCF portable y DCCF centralizado para los certificados Personales. • Añadidos OIDs del CA/B Forum a los certificados de autenticación de sitio web. • Se añade un campo OU adicional al perfil de los certificados corporativos de colegiado, la interpretación del cuál es definida por cada colegio profesional.	FP
210217	• Introducción como opcional de los campos ISO ISO 17442 parte 2 para identificadores LEI: • 1.3.6.1.4.1.52266.1: para Sello Empresarial y Representante Legal • 1.3.6.1.4.1.52266.2: para Representante Legal	FP
210322	• Corrección OIDs CA Browser Forum SSLs	FP
211001	• Correción perfil Empleado Público nivel alto firma: se elimina el EKU • Correcciones menores perfil Colegiado	FP
220216	• Adaptación QEVCP-w de la ETSI 319 411-2 (2021-11)	FP
220330	• Adaptación a los cambios de S/Mime de la política de Apple	FP
220517	• Eliminación campo OU certificados de Sede electrónica	FP
220530	• Eliminación campo StateorProvince de certificados SSL	FP
221109	• Certificado de Empleado Público HW actualización Key Usage y EKU	FP
230419	• Corrección de error apartado 2.7	FP
230510	• Nuevo perfil de Sello Empresarial en DCCF Centralizado • Actualización de apartado 5 • Actualización de referencias a URLs genéricas	FP

	• Clarificar campos opcionales • revisión general	
230828	• Aclaraciones sobre el uso del # de pasaporte en los certificados de firma y eliminación de esta opción en los certificados corporativos de representante voluntario frente a las administraciones publicas. • Se deja de emitir el certificado de persona física con firma de correo. Pasa a estado de obsoleto a partir del 1 de septiembre de 2023. • Se elimina el EKU “email protection del certificado personal.	FP
231104	• Adaptación de los perfiles SSL con las modificaciones introducidas por CABForum	FP
240219	• Eliminación del key usage “Data Encipherment”	FP
240520	• Eliminación del campo RFC822 • Actualización ubicación nuevas oficinas en página inicial • Se añade información sobre eliminación de ciertos EKUs • Actualizado apartado 4.1.2	FP
241216	• Actualización DN del perfil de certificado corporativo de persona física. • Actualización key usage del certificado de sello empresarial. • Actualización del DN del perfil de certificado de TSU.	FP
250502	• Actualización 2.7.1	ACC
250723	• Actualización de los campos opcionales del SAN en los apartados 2.8.3 y 2.8.4 • Actualización de la descripción del campo serialnumber en los apartados 2.1, 2.2, 2.5 y 2.6. • Actualización de los ejemplos de DNI y nombres en los apartados 2.4.1, 2.5.1 y 2.6.1 • Se remarcan las opciones obsoletas en los apartados 2.1.1, 2.1.2, 2.2.1, 2.2.2, 2.4.2, 2.5.2, 2.6.2, 2.7.2, 2.8.2, 3.1.2, 3.1.3, 3.1.4, 3.2.2, 3.2.3 y 5.1.1.2 • Actualización campo “user notice” en todos los perfiles • Actualización campo “description” en los apartados 2.5.1 y 2.6.1	ACC
251219	• Actualización uso campo RFC822Name	ACC

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/
- El estándar X.509 versión 3 de la ITU Telecommunication Standardization Sector (ITU-T).

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

NOTA: los certificados en los que conste como parte de la identidad del titular el número de pasaporte u otro identidicador diferente del Documento Nacional de Identidad, Número de Identificación de Extranjero o Número de Identificación Fiscal español, NO PODRÁN UTILIZARSE para la tramitación con la Administración Pública Española.

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 = NOMUNO ESPECIMENUNO ESPECIMENUNO / num:4444*
E, E-mail	E-mail	(opcional y no recomendado, por estar obsoleto según RFC 5280) 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. (Ejemplo: Nombre del Colegio Oficial o entidad que actúa como RA) Adicionalmente se incluye 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".
OU, Organization Unit (opcional)	Unidad en la organización	Contendrá información adicional de relevancia para el colegiado o los sistemas de información con los que éste trabaje. La interpretación de este campo es definida por cada colegio profesional.
T, Title	Título	Título o especialidad del firmante
ST, State	Ubicación Geográfica	Ámbito geográfico del firmante (Ej. Provincia).
C, Country	País	Código de país de dos dígitos según ISO 3166-1.
serialNumber	Número de identificación	Número administrativo que la legislación nacional tenga asignado de acuerdo con el valor del campo Country. (*) Ej: "IDCES-99949991H"

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

(*) Se seguirá la codificación acorde a ETSI EN 319 412-1. **El uso de un documento diferente al DNI, NIE o NIF implica la imposibilidad de tramitación con las Administraciones Públicas españolas.**

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 comunes de los certificados

Extensión	Crítica	Valores
Subject Alternative Name	-	RFC822Name:<email del contacto> (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)
Basic Constraints	Sí	CA:FALSE
Key Usage	Sí	Digital Signature Content Commitment Key Encipherment
Extended Key Usage	-	Emailprotection (**Prohibido** a partir de septiembre de 2023)
		TLS Web Client Authentication Adobe Authentic Documents Trust (1.2.840.113583.1.1.5) (Se incluye a partir de septiembre 2023)
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>
CRL Distribution Points	-	<URI de la CRL>
Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI de acceso al servicio OCSP> Access Method: Id-ad-caIssuers Access Location: <URI de acceso al certificado de la CA emisora>

2.1.3 Extensiones de los certificados sin DCCF

Extensión	Crítica	Valores
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." <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
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." <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	*E-mail*	(opcional y no recomendado, por estar obsoleto según RFC 5280) 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. Adicionalmente se puede incluir el código de la RA que gestionó la emisión del certificado, separados por el carácter "/".
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 (Ej. Provincia).
C, Country	País	Código de país de dos dígitos según ISO 3166-1.
serialNumber	Número de Serie	Número administrativo que la legislación nacional tenga asignado de acuerdo con el valor del campo Country. Ej: "IDCzz-nnnnnnnny" (**)
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
1.3.6.1.4.1.4710.1.3.2	NIF de la organización subscriptora	Número de NIF, sin la codificación ETSI (Opcional)

(**)Se seguirá la codificación acorde a ETSI EN 319 412-1. **El uso de un documento diferente al DNI, NIE o NIF implica la imposibilidad de tramitación con las Administraciones Públicas españolas.**

2.2.2 Extensiones comunes de los certificados

Extensión	Crítica	Valores
Subject Alternative Name	-	RFC822Name:<email del contacto> (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)
Basic Constraints	Sí	CA:FALSE
Key Usage	Sí	Digital Signature Content Commitment Key Encipherment

Extended Key Usage	-	Emailprotection (**Prohibido** a partir de septiembre de 2023)
		TLS Web Client Authentication Adobe Authentic Documents Trust (1.2.840.113583.1.1.5) (Se incluye a partir de septiembre 2023)
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>
CRL Distribution Points	-	<URI de la CRL>
Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI de acceso al servicio OCSP> Access Method: Id-ad-caIssuers 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
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." <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

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." <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 los certificados corporativos de persona física con firma de correo

*Perfil **obsoleto** a partir de 1 de septiembre de 2023.*

2.4 Perfil de certificados corporativos de representante de entidad sin personalidad jurídica

2.4.1 Nombre distinguido (DN)

Campo del DN	Nombre	Descripción
CN, Common Name	Nombre	Ver tabla específica en la siguiente sección. (ejemplo: 99949991H Nomuno Especimenuno Especimenuno (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 o NIE del firmante según la Norma Europea ETSI EN 319 412-1 (IDCES-99949991H)
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
E, E-mail	E-mail	(opcional y no recomendado, por estar obsoleto según RFC 5280) Correo electrónico del firmante

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

2.4.1.1 Common Name

Campo	Contenido	Ejemplo	Tamaño*
NIF	Número DNI/NIE	99949991H	10
Nombre	Tal y como figura en el DNI/NIE	Nomuno	
Apellido 1	Tal y como figura en el DNI/NIE	Especimenuno	
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
Subject Alternative Name	-	RFC822Name:<email del contacto> (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)
Basic Constraints	Sí	CA:FALSE
Key Usage	Sí	Digital Signature Content Commitment Key Encipherment,
Extended Key Usage	-	TLS Web Client Authentication Adobe Authentic Documents Trust (1.2.840.113583.1.1.5) (Se incluye a partir de septiembre 2023)
		Emailprotection (Prohibido a partir de septiembre de 2023)
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>
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).
Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI de acceso al servicio OCSP> Access Method: Id-ad-caIssuers Access Location: <URI de acceso al certificado de la CA emisora>

2.4.3 Extensiones de los certificados sin DCCF

Extensión	Crítica	Valores
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." <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 >

2.4.4 Extensiones de los certificados con DCCF

Extensión	Crítica	Valores
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." <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)

2.5 Perfil de certificados corporativos de representante legal de persona jurídica

2.5.1 Nombre distinguido (DN)

Campo del DN	Nombre	Descripción

CN, Common Name	Nombre	Ver tabla específica en siguiente sección (ejemplo: 99949991H NOMUNO ESPECIMENUNO (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 / IRUS[1]:XXXXXXXX / Hoja:XXX / Tomo[2]:XXX / Sección:XXX / Libro:XXX / Folio[3]: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	Número administrativo que la legislación nacional tenga asignado de acuerdo con el valor del campo Country. Ej: “IDCzz-nnnnnnnny” (**)
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
E, E-mail	E-mail	(opcional y no recomendado, por estar obsoleto según RFC 5280) Correo electrónico del firmante
ISO 17442-2 LEI number (1.3.6.1.4.1.52266.1) (opcional)		LEI es un código alfanumérico de 20 caracteres basado en ISO / IEC 17442 que se conecta a información de referencia clave que permite la identificación única de las entidades legales que participan en transacciones financieras.
ISO 17442-2 LEI role (1.3.6.1.4.1.52266.2) (opcional)		Rol de un individuo en la organización descrita por el certificado.

(**) Se seguirá la codificación acorde a ETSI EN 319 412-1. **El uso de un documento diferente al DNI, NIE o NIF implica la imposibilidad de tramitación con las Administraciones Públicas españolas.**

[1] IRUS: Campo obligatorio a partir del 9/5/2024 por la entrada en vigor del folio electrónico registral. Para las anteriores a esa fecha es opcional.

[2] TOMO: A partir del 9/5/2024 no existe este campo en el registro.

[3] FOLIO: A partir del 9/5/2024 no existe este campo en el registro.

2.5.1.1 Common Name

Campo	Contenido	Ejemplo	Tamaño*
NIF	Número DNI/NIE	99949991H	10
Nombre	Tal y como figura en el DNI/NIE	Nomuno	
Apellido 1	Tal y como figura en el DNI/NIE	Especimenuno	
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
Subject Alternative Name	-	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)
		RFC822Name:<email del contacto> (Opcional)
Basic Constraints	Sí	CA:FALSE
Key Usage	Sí	Digital Signature Content Commitment Key Encipherment
Extended Key Usage	-	TLS Web Client Authentication

		Adobe Authentic Documents Trust (1.2.840.113583.1.1.5) (Se incluye a partir de septiembre 2023) Emailprotection (**Prohibido** a partir de septiembre de 2023)
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>
CRL Distribution Points	-	<URI de la CRL>
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
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." <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).

2.5.4 Extensiones de los certificados con DCCF

Extensión	Crítica	Valores

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." <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)

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

2.6.1 Nombre distinguido (DN)

Campo del DN	Nombre	Descripción
CN, Common Name	Nombre	Ver tabla específica en siguiente sección (ejemplo: 99949991H Nomuno Especimenuno (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 / IRUS[4]:XXXXXXXX / Hoja:XXX / Tomo[5]:XXX / Sección:XXX / Libro:XXX / Folio[6]: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 o NIE
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
E, E-mail	E-mail	(opcional y no recomendado, por estar obsoleto según RFC 5280) Correo electrónico del firmante

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

2.6.1.1 Common Name

Campo	Contenido	Ejemplo	Tamaño*
NIF	Número DNI/NIE	99949991H	10
Nombre	Tal y como figura en el DNI/NIE	Nomuno	
Apellido 1	Tal y como figura en el DNI/NIE	Especimenuno	

[4] IRUS: Campo obligatorio a partir del 9/5/2024 por la entrada en vigor del folio electrónico registral. Para las anteriores a esa fecha es opcional.

[5] TOMO: A partir del 9/5/2024 no existe este campo en el registro.

[6] FOLIO: A partir del 9/5/2024 no existe este campo en el registro.

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)

2.6.2 Extensiones comunes de los certificados

Extensión	Crítica	Valores
Subject Alternative Name	-	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)
		RFC822Name:<email del contacto> (Opcional)
Basic Constraints	Sí	CA:FALSE
Key Usage	Sí	Digital Signature Content Commitment Key Encipherment,
Extended Key Usage	-	TLS Web Client Authentication Adobe Authentic Documents Trust (1.2.840.113583.1.1.5) (Se incluye a partir de septiembre 2023)
		Emailprotection (**Prohibido** a partir de septiembre de 2023)
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>
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).
Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI de acceso al servicio OCSP> Access Method: Id-ad-caIssuers Access Location: <URI de acceso al certificado de la CA emisora>

2.6.3 Extensiones de los certificados sin DCCF

Extensión	Crítica	Valores
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." <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 >

2.6.4 Extensiones de los certificados con DCCF

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." <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)

2.7 Perfil de los certificados Personales

2.7.1 Nombre distinguido (DN)

Campo del DN	Nombre	Descripción
CN, Common Name	Nombre	Nombre y apellidos del firmante
serialNumber	Número de serie	Número administrativo que la legislación nacional tenga asignado de acuerdo con el valor del campo Country. (*) Ej: "IDCzz-nnnnnnnny"
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.
E, E-mail	E-mail	(opcional y no recomendado, por estar obsoleto según RFC 5280) Correo electrónico del firmante

(*) Se seguirá la codificación acorde a ETSI EN 319 412-1. El uso de un documento diferente al DNI, NIE o NIF implica la imposibilidad de tramitación con las Administraciones Públicas españolas.

2.7.2 Extensiones comunes de los certificados

Extensión	Crítica	Valor
Basic Constraints	Sí	CA:FALSE
Key Usage	Sí	Digital Signature Content Commitment Key Encipherment
Extended Key Usage	-	TLS Web Client Authentication Adobe Authentic Documents Trust (1.2.840.113583.1.1.5) (Se incluye a partir de septiembre 2023)
		Emailprotection (Prohibido a partir de septiembre de 2023)

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>
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).
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>
Subject Alternative Name	-	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)
		RFC822Name:<email del contacto> (Opcional)

2.7.3 Extensiones de los certificados sin DCCF

Extensión	Crítica	Valores

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 para su uso sin DCCF." <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)

2.7.4 Extensiones de los certificados con DCCF

Certificate Policies	-	<OID de la política de certificación correspondiente al certificado> 1.3.6.1.4.1.13177.10.1.40.3: DCCF centralizado <URI de la CPS> User Notice: "Este es un Certificado Personal de Persona Física cualificado, en DCCF." <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)

2.8 Perfil de los certificados de empleado público

2.8.1 Nombre distinguido (DN)

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, NIE, ...-) + " - 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".
E, E-mail	E-mail	(opcional y no recomendado, por estar obsoleto según RFC 5280) Correo electrónico del firmante

(*) "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 identidad o NIE) + 2 caracteres para identificar el país (ES) + Número de identidad (Printable String)) Size [RFC 5280] 64

2.8.2 Extensiones comunes de los certificados

Extensión	Crítica	Valores
Subject Alternative Name (opcional)	-	RFC822Name:<email del contacto> (Opcional)
Basic Constraints	Sí	CA:FALSE

Key Usage	Sí	Content Commitment Digital Signature Key Encipherment
Extended Key Usage	-	Adobe Authentic Documents Trust (1.2.840.113583.1.1.5) (Se incluye a partir de septiembre 2023) TLS Web Client Authentication Emailprotection (**Prohibido** a partir de septiembre de 2023)
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).

2.8.3 Extensiones de los certificados, nivel alto

Extensión	Crítica	Valores
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." <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 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> (opcional) 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> (Opcional) OID: 2.16.724.1.3.5.7.1.8 = <Segundo apellido del empleado público> (Opcional) OID: 2.16.724.1.3.5.7.1.9 = <correo electrónico del empleado público> (Opcional) 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>) (Opcional) OID: 2.16.724.1.3.5.7.1.11 = <Cargo, T del DN>

2.8.4 Extensiones de los certificados, nivel medio

Extensión	Crítica	Valores
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" <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> (Opcional) 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> (Opcional) OID: 2.16.724.1.3.5.7.2.8 = <Segundo apellido del empleado público> (Opcional) OID: 2.16.724.1.3.5.7.2.9 = <correo electrónico del empleado público> (Opcional) 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>) (Opcional) OID: 2.16.724.1.3.5.7.2.11 = <Cargo, T del DN>

2.9 Perfil de los certificados de empleado público con seudónimo o con número de identificación profesional

2.9.1 Nombre distinguido (DN)

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 (opcional)	Unidad en la organización	Unidad, dentro de la Administración, en la que está incluida el suscriptor del certificado
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	seudónimo	"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".

(*) "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.

2.9.2 Extensiones comunes de los certificados

Extensión	Crítica	Valores
Basic Constraints	Sí	CA:FALSE
Extended Key Usage	-	Adobe Authentic Documents Trust (1.2.840.113583.1.1.5) (Se incluye a partir de septiembre 2023)
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-caIssuers 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)

2.9.3 Extensiones de los certificados, nivel medio

Extensión	Crítica	Valores
Key Usage	Sí	Digital Signature Content Commitment Key Encipherment
Extended Key Usage	-	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." <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> (Opcional) OID: 2.16.724.1.3.5.4.2.9 = <correo electrónico> (Opcional) 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>) (Opcional)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 Nombre distinguido (DN)

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 (Ej. VATES + NIF de la entidad; NTRES-08005. 6789…)
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, NIE, ...-) + " - 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, TIE, ...) 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
Basic Constraints	Sí	CA:FALSE
Key Usage	Sí	Digital Signature Content Commitment Key Encipherment
Extended Key Usage	-	Adobe Authentic Documents Trust (1.2.840.113583.1.1.5) (Se incluye a partir de septiembre 2023) TLS Web Client Authentication
		Emailprotection (**Prohibido** a partir de septiembre de 2023)
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-caIssuers 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: 0.4.0.1862.1.6.2 (qct-eseal, indica que es un certificado para crear sellos electrónicos).

3.1.3 Extensiones de los certificados, nivel alto

Extensión	Crítica	Valores
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." <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)
Subject Alternative Name	-	RFC822Name:<email del 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> (opcional) OID: 2.16.724.1.3.5.6.1 .4 = <NIF/NIE del custodio> OID: 2.16.724.1.3.5.6.1 .5 = <CN del DN> (opcional) 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 contacto>

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

3.1.4 Extensiones de los certificados, nivel medio

Extensión	Crítica	Valores
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." <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>
Subject Alternative Name	-	RFC822Name:<email del 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> (opcional) OID: 2.16.724.1.3.5.6.2.4 = <NIF/NIE del custodio> OID: 2.16.724.1.3.5.6.2.5 = <CN del DN> (opcional) 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>

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

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 o en el caso de certificados para PSD2, en el Registro público de la Autoridad Nacional Competente del Estado Miembro de origen o que resulte de las notificaciones a la EBA (Autoridad Bancaria Europea)
OI, organizationIdentifier	Identificador de la organización	Identificador de la organización, según la norma técnica ETSI EN 319 412-1 (Ej. VATES + NIF de la entidad; NTRES-08005.56789,...) (*) Para certificados de autenticación web para PSD2, identificador de la organización, según la especificación técnica ETSI TS 119 495
OU, Organization Unit (opcional)	Unidad en la organización	Contendrá el Departamento o Unidad
E, E-mail	E-mail	(opcional, por estar obsoleto según RFC 5280) Correo electrónico del contacto.
ST, State	Ubicación Geográfica	Ámbito geográfico de vinculación del suscriptor (Ej. Provincia)
C, Country	País	Código de país de dos dígitos según ISO 3166-1. Por defecto "ES".
ISO 17442-2 LEI number (1.3.6.1.4.1.52266.1) (opcional)		LEI es un código alfanumérico de 20 caracteres basado en ISO / IEC 17442 que se conecta a información de referencia clave que permite la identificación única de las entidades legales que participan en transacciones financieras.

(*) Según lo estipulado en ETSI EN 319 412-3

3.2.2 Extensiones de los certificados, con DCCF

Extensión	Crítica	Valores
Basic Constraints	Sí	CA:FALSE
Key Usage	Sí	Digital Signature Content Commitment Key Encipherment (Opcional, y únicamente para RSA)
Extended Key Usage	-	TLS Web Client Authentication

		Adobe Authentic Documents Trust (1.2.840.113583.1.1.5) (Se incluye a partir de septiembre 2023)
		Emailprotection (**Prohibido** a partir de septiembre de 2023)
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-caIssuers Access Location: <URI de acceso al certificado de la CA emisora>
CRL Distribution Points	-	<URI de la CRL>
Certificate Policies	-	<OID de la política de certificación correspondiente al certificado> 1.3.6.1.4.1.13177.10.1.10.3: : DCCF centralizado <URI de la CPS> User Notice: "Éste es un Certificado Corporativo de Sello Empresarial Cualificado emitido en DCCF." < OID "for EU qualified certificates issued to legal persons" según ETSI EN 319 411-2: QCP-l-qscd: 0.4.0.194112.1.3>
Subject Alternative Name (opcional)	-	
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 sellos electrónicos). Id-etsi-qcs-QcSSCD: 0.4.0.1862.1.4 (indica que la clave privada se custodia en un DCCF)

3.2.3 Extensiones de los certificados sin DCCF

Extensión	Crítica	Valores
Basic Constraints	Sí	CA:FALSE
Key Usage	Sí	Digital Signature Content Commitment Key Encipherment (Opcional, y únicamente para RSA) Data Encipherment (Opcional, y únicamente para RSA)
Extended Key Usage	-	TLS Web Client Authentication Adobe Authentic Documents Trust (1.2.840.113583.1.1.5) (Se incluye a partir de septiembre 2023)
		Emailprotection (**Prohibido** a partir de septiembre de 2023)
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>
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." En certificados de sello empresarial para PSD2: User Notice "Éste es un Certificado Corporativo de Sello Empresarial Cualificado PSD2."

		< OID “for EU qualified certificates issued to legal persons” según ETSI EN 319 411-2: QCP-l: 0.4.0.194112.1.1>
Subject Alternative Name (opcional)	-	
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 sellos electrónicos). En certificados de sello empresarial para PSD2: etsi-psd2-qcStatement de conformidad con ETSI TS 119 495

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". No presente a partir de la versión 220517 del presente documento. *BR (1.7.9) Prohibido a partir del 01/09/2022*
OU, Organization Unit	Unidad en la organización	El nombre descriptivo de la sede. No presente a partir de la versión 220517 del presente documento. *BR (1.7.9) Prohibido a partir del 01/09/2022*
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 (Ej. VATES + NIF de la entidad; NTRES-08005.56789,...)
C, Country	País	C= ES
L, Localty		Ciudad, Provincia o Estado.
businessCategory		Categoría de organización: "Government Entity"

jurisdictionCountryNam e		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
Authority Key Identifier	-	<id de la clave pública de la CA, obtenido a partir del hash de la misma>
Subject Key Identifier	-	<id de la clave pública del certificado, obtenido a partir del hash de la misma>
Key Usage	Sí	Digital Signature Key Encipherment
Extended Key Usage	-	TSL web Server Authentication
Basic Constraints	Sí	CA:FALSE
CRL Distribution Points	-	<URI de la CRL>
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>
Certificate Policies	-	<URI de la CPS> <OID ca-browser-forum.certificate-policies.extended-validation : 2.23.140.1.1> (De acuerdo con BRG 2.0.0 indicar primero el OID de Cabforum) <OID “EU qualified website authentication certificates” según ETSI EN 319 411-2: QEVCP-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 autenticación sitios web).
Subject Alternative Name	-	dNSName: nombre de dominio donde residirá el certificado

cabfOrganizationIdentifier (2.23.140.3.1)	-	Esquema: identificador de esquema de tres dígitos (VAT, PSD, …) País: código de país de dos dígitos ISO 3166-1 Referencia: identificado de la organización de acuerdo al esquema y país

4.1.3 Extensiones de los certificados, nivel alto

Extensión	Crítica	Valores
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 Electrónica Nivel Alto". (**Eliminado por BRG 2.0.0**).* <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
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 Electrónica Nivel Medio". (**Eliminado por BRG 2.0.0**).* <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 suscriptora del certificado

OU, Organizational Unit	Departamento	Opcional hasta versión 6.3 (incluida) de la presente política. No presente en adelante. BR (1.7.9) Prohibido a partir del 01/09/2022
serialNumber (opcional)(*)	CIF	CIF de la Organización suscriptora del certificado
OI, OrganizationIdentifier		Identificador de la organización, según la norma técnica ETSI EN 319 412-1(Ej. VATES + NIF de la entidad; NTRES-08005.56789,...) Para certificados de autenticación web para PSD2, identificador de la organización, según la especificación técnica ETSI TS 119 495
businessCategory	Private Organization Government Entity Business Entity Non-Commercial Entity	(EVG 9.2.4) Business Category
L, Locality	Ciudad	Ciudad, Provincia o Estado.
ST, StateOfProvince	Provincia	Provincia de registro de la organización. No presente a partir de la versión 220530.
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
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)
Basic Constraints	Sí	CA:FALSE
Key Usage	Sí	Digital Signature Key Encipherment (No aparece si las claves del certificado son en curvas elípticas)
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) (opcional)
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-caIssuers Access Location: <URI de acceso al certificado de la CA emisora>
CRL Distribution Points	-	<URI de la CRL>
Certificate Policies	-	<OID ca-browser-forum.certificate-policies.baseline-requirements.organization-validated: 2.23.140.1.2.2> (para los certificados SSL OV) (De acuerdo con BRG 2.0.0 indicar primero el OID de Cabforum) <OID ca-browser-forum.certificate-policies.extended-validation : 2.23.140.1.1> (para los certificados EV y PSD2) (De acuerdo con BRG 2.0.0 indicar primero el OID de Cabforum) <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 Y PSD2 <URI de la CPS> <OID "EU qualified website authentication certificates" según ETSI EN 319 411-2: QEVCP-w: 0.4.0.194112.1.4 > (para los certificados EV y PSD2)

		<OID de la política EV de certificación correspondiente al certificado: 0.4.0.2042.1.4> (para los certificados EV y PSD2)
Qualified Certificate Statements (solo para EV y PSD2)	-	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). En certificados para PSD2: etsi-psd2-qcStatement de conformidad con ETSI TS 119 495
cabfOrganizationIdentifier (for EV and PSD2 only)	-	Esquema: identificador de esquema de tres dígitos (VAT, PSD, …) País: código de país de dos dígitos ISO 3166-1 Referencia: identificado de la organización de acuerdo al esquema y país

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
Basic Constraints	Sí	CA:TRUE
Key Usage	Sí	keyCertificateSignature cRLSignature
Extended Key Usage (Opcional)	-	<Variable según el tipo de certificado: serverAuth, clientAuth, timeStamping, OCSPSigning, Smartcard Logon, etc. > Adobe Authentic Documents Trust, (Se puede incluir a partir 15/9/2023)
		Emailprotection (**Prohibido** a partir de septiembre de 2023)
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>
CRL Distribution Points	-	<URI de la CRL>

Certificate Policies	-	policyIdentifier: 1.3.6.1.4.1.13177.10.10.2 o AnyPolicy (2.5.29.32.0) (Opcional) cPSURI: http://www.firmaprofesional.com/cps userNotice: "Certificado de Autoridad de Certificación. Consulte las condiciones de uso en http://www.firmaprofesional.com/cps"
Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI de acceso al servicio OCSP> 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 (Ej. VATES + NIF de la entidad; NTRES-08005.56789,...)
OU, Organization Unit (Opcional)	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
Certificate Policies	-	policyIdentifier: 1.3.6.1.4.1.13177.10.10.1 o AnyPolicy (2.5.29.32.0) (Opcional) cPSURI: http://www.firmaprofesional.com/cps userNotice: " Certificado de Autoridad de Certificación. Consulte las condiciones de uso en http://www.firmaprofesional.com/cps
Authority Information Access	-	accessMethod: Id-ad-ocsp accessLocation: <URI de acceso al servicio OCSP> accessMethod: Id-ad-calssuers accessLocation: <URI de acceso al certificado de la CA emisora>

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	Descripción 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
Basic Constraints	Sí	CA:FALSE
Key Usage	Sí	digitalSignature
Extended Key Usage	-	id-kp-OCSPSigning
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>
1.3.6.1.5.5.7.48.1.5 id-pkix-ocsp-nocheck	-	oCSPNoCheck

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. (siempre en caso de qTSA) (inclusión nombre del subscriptor, opcionalmente para servicio no cualificado)
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
Basic Constraints	Sí	CA:FALSE
Key Usage	Sí	digitalSignature contentCommitment
Extended Key Usage	Sí	id-kp-timeStamping {1.3.6.1.5.5.7.3.8}
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>
CRL Distribution Points	-	<URI de la CRL>
Certificate Policies	-	policyIdentifier: 1.3.6.1.4.1.13177.10.1.4.2 <URI de la CPS> userNotice: “Certificado de Servicio Seguro de TSA”
Authority Information Access	-	accessMethod: Id-ad-caIssuers accessLocation: <URI de acceso al certificado de la CA emisora> accessMethod: Id-ad-ocsp accessLocation: <URI de acceso al servicio OCSP>

5.3.2 Certificados de QTSA (TSA para servicio Cualificado)

Adicionalmente, el perfil de los certificados de TSA para servicios cualificados (QTSA) 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
Certificate Policies	-	policyIdentifier: 1.3.6.1.4.1.13177.10.1.4.1 <URI de la CPS> userNotice: "Certificado de Servicio Seguro de TSA cualificada"
id-ce-privateKeyUsagePeriod 2.5.29.16 (opcional)		Tiene por objetivo limitar la validez de la clave privada: 3 años. Esta extensión se suprime cuando el certificado es emitido en curvas elípticas.
Authority Information Access		accessMethod: Id-ad-caIssuers accessLocation: <URI de acceso al certificado de la CA emisora> 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 .