Administració Oberta de Catalunya

Descripción de los perfiles de Certificados Consorci AOC

Referencia: D1111_E0650_Perfils_de_Certificats
Versión: 7.2
Fecha: 09/03/2025

La versión original en vigor de este documento se encuentra en formato electrónico publicada en el sitio web del Consorci AOC y puede ser accesible a través de la siguiente URL: https://epscd.aoc.cat/regulacio/

Historial de versiones

Versión	Resumen de los cambios	Fecha
5.0	Adaptación a EIDAS	9/05/2018
6.0	Unificación en un único documento del documento de perfiles emitidos para EC-SECTORPUBLIC y EC-CIUTADANIA	26/07/2018
6.1	● Revisión anual de la documentación, postauditoría eIDAS. ● "4.4. Perfil de los Certificados de Servidor Seguro (Dispositiu SSL)": eliminada opción de multidominio o wildcard.	24/07/2019
6.2	● "2.6: Perfil de los certificados de firma de empleado público con seudónimo nivel alto". Inclusión de EKU ● "2.8. Perfil de los Certificados de firma de empleado público de nivel alto": inclusión de EKU	31/3/2020
6.3	● Inclusión de certificados de autenticación y firma de trabajador público de nivel medio y de nivel alto	03/08/2020
6.4	● Revisión del Documento.	27/01/2021
6.5	● Revisión del Documento.	20/07/2021
6.6	● "3.1.1 Certificado": Alteración en la descripción C = "País de expedición del documento identificativo del suscriptor"	31/03/2022
6.7	● Revisión sin cambios.	29/03/2023
6.8	● Eliminadas referencias a QWAC y QTSA. ● Cambio URLs de regulación y CRL. ● Marcada extensión QCStatements como no crítica.	10/05/2023
6.9	● Apartado 2.7: Inclusión de T-CATP pseudònim. ● Eliminación de la dirección y el NIF de las extensiones de los perfiles de certificado. ● Eliminación del email protection del Extended Key Usage (EKU) y rfc822. Inclusión de la extensión Adobe Authentic Documents Trust.	15/11/2023
6.10	● Apartado 2.7: Ajustes perfil T-CATP pseudònim.	22/05/2024
7.0	● Inclusión de la nueva jerarquía AOC G3. Se numera como versión 7.0 a efectos de gestión documental	31/10/2024
7.1	● Apartado 4.3: Inclusión del Certificado de Servicio de Sello Cualificado de Tiempo.	18/12/2024

7.2	● Eliminación de la inclusión del DNI en el Surname ● Eliminación del KU Key Encipherment de los certificados de persona física ● Eliminación del EKU de Adobe de los certificados de autenticación web ● Introducción de un DN en el SAN para la separación de los apellidos en los certificados de persona vinculada, de representante y de empleado público	09/03/2025

Índice

1. Introducción

El presente documento de Descripción de los perfiles de los certificados tiene como objeto detallar el contenido de los certificados emitidos por el Consorci AOC, en virtud de los requisitos establecidos a estos efectos por el Ministerio competente en servicios electrónicos de confianza; es decir, especifica cuál es la configuración (principalmente, Campo del DN, Nombre y Descripción) y la extensión (Extensión, Crítica -sí/no-, y Valores) de los certificados personales de empleado público, certificados de ciudadanos y certificados de Dispositivos e Infraestructura, cada uno de ellos con una Política de certificación propia (accesibles desde la URL https://epscd.aoc.cat/regulacio). También hace referencia a la composición del campo Common Name (CN) en el caso de aquellos certificados que lo dispongan.

Su emisión se ha efectuado teniendo en cuenta las disposiciones del 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). También se ha seguido como referencia el documento “Perfiles de certificados electrónicos”, 1a edición electrónica de abril de 2016 y disponible en el Portal de Administración Electrónica (PAe): http://administracionelectronica.gob.es/.

2. Descripción de Perfiles de Certificados Personales del Sector Público

2.1. Perfil de los Certificados de autenticación de empleado público de nivel alto (T-CAT autenticació)

2.1.1. 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 vinculado el empleado.
OU, Organization Unit	Unidad en la organización	"Empleat públic de nivell alt d'autenticació"
Title (opcional)	Cargo	Ha de incluir el cargo de la persona física, que la vincula con la administración, organismo o entidad de derecho público suscriptora del certificado.
Serial Number	NIF	Número del documento de identidad del firmante con la semántica propuesta por la norma ETSI EN 319 412-1[1]
SN, Surname	Apellidos (persona física)	Primer y segundo apellidos (de acuerdo con el documento de identidad – DNI / Passaport, …)
Given name	Nombre	Nombre, de acuerdo con el documento de identidad (DNI, pasaporte,...)
CN, Common Name	Nombre, apellidos y NIF	Nombre y dos apellidos de acuerdo con el documento de identidad (DNI / pasaporte) + NIF del empleado público + " (AUT)"
C, Country	País	C = "ES"
Organization Identifier		Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)

[1] SerialNumber = p. ej: IDCES-99949992L. 3 caracteres para indicar el tipo de documento (IDC= documento nacional de identidad, PAS=pasaport, ...) + 2 caracteres para identificar el país (ES) + Número de identidad (Printable String)) Size [RFC 5280] 64

2.1.2. Extensiones

Extensión	Crítica	Valores
X509v3 Basic Constraints	Sí	CA:FALSE
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-caIssuers Access Location: <URI del certificado de la EC emisora>
X509v3 CRL Distribution Points	-	<URI de la CRL>
X509v3 Key Usage	Sí	Digital Signature
X509v3 Extended Key Usage		Client Authentication SmartCardLogon
X509v3 Certificate Policies	-	<OID asociado a la DPC> 1: 1.3.6.1.4.1.15096.1.3.2.7.1.2 <URI de la DPC> <User Notice> " Certificat electrònic d'empleat públic de nivell alt d'autenticació ." <OID de la política de certificación de empleado público de nivel alto> 2.16.724.1.3.5.7.1 <OID de la política de certificación ETSI: NCP+> 0.4.0.2042.1.2
X509v3 Subject Alternative Name	-	(opcional) otherName-userPrincipalName (UPN): Usuario en el dominio Windows del poseedor de claves directoryName: OID: 2.16.724.1.3.5.7.1.1 = "Certificat electrònic d'empleat públic de nivell alt d'autenticació" 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: 2.16.724.1.3.5.7.1.6 = <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>

2.2. Perfil de los Certificados cualificados de autenticación y firma de empleado público de nivel medio (T-CATP)

2.2.1. 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 vinculado el empleado. .
OU, Organization Unit	Unidad en la organización	"Empleat públic de nivell mig"
Title (opcional)	Cargo	Ha de incluir el cargo de la persona física, que la vincula con la administración, organismo o entidad de derecho público suscriptora del certificado.
Serial Number	NIF	Número del documento de identidad del firmante, con la semántica propuesta por la norma ETSI EN 319 412-1[2]
SN, Surname	Apellidos (persona física)	Primer y segundo apellido (de acuerdo con el documento de identidad – DNI / Pasaporte, …)
Given name	Nombre	Nombre, de acuerdo con el documento de identidad (DNI, pasaporte, ...)
CN, Common Name	Nombre, apellidos y NIF	Nombre y dos apellidos de acuerdo con el documento de identidad (DNI / Pasaporte) + "NIF del empleado público + " (TCAT")"
C, Country	País	C = "ES"
Organization Identifier		Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)

[2] SerialNumber = p. ej: IDCES-99949992L. 3 caracteres para indicar el tipo de documento (IDC= documento nacional de identidad, PAS=pasaporte, ...) + 2 caracteres para identificar el país (ES) + Número de identidad (Printable String)) Size [RFC 5280] 64

2.2.2. Extensiones

Extensión	Crítica	Valores
X509v3 Basic Constraints	Sí	CA:FALSE
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-caIssuers Access Location: <URI del certificado de la EC emisora>
X509v3 CRL Distribution Points	-	<URI de la CRL>
X509v3 Key Usage	Sí	Digital Signature Content Commitment
X509v3 Extended Key Usage		Client Authentication Adobe Authentic Documents Trust
X509v3 Certificate Policies	-	<OID de la DPC> 1.3.6.1.4.1.15096.1.3.2.7.3.1 <URI de la DPC> <User Notice> “Certificat electrònic d'empleat públic de nivell mig. ” <OID que indica certificado de empleado público de nivel medio> 2.16.724.1.3.5.7.2 <OID de la política de certificación ETSI: QCP-n> 0.4.0.194112.1.0
Qualified Certificate Statements		Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 años Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: <URI de la PDS> Id-etsi- qcs-QcType-esign 0.4.0.1862.1.6.1
X509v3 Subject Alternative Name	-	directoryName: OID: 2.16.724.1.3.5.7.2.1 = “Certificat electrònic d’empleat públic de nivell mig” 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 = <serialNumber 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>

2.3. Perfil de los Certificados de autenticación y firma de persona vinculada de nivel medio (T-CATP persona vinculada)

2.3.1. 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 vinculado el empleado.
OU, Organization Unit	Unidad de la organización	"Persona vinculada de nivell mig"
Title (opcional)	Cargo	Ha de incluir el cargo de la persona física, que la vincula con la administración, organismo o entidad de derecho público suscriptora del certificado.
Serial Number	NIF	Número del documento de identidad del firmante, con la semántica propuesta por la norma ETSI EN 319 412-1[3]
SN, Surname	Apellidos (persona física)	Primer y segundo apellidos (de acuerdo con el documento de identidad – DNI / Pasaporte, …)
Given name	Nombre	Nombre, de acuerdo con el documento de identidad (DNI, pasaporte, ...)
CN, Common Name	Nombre, apellidos y NIF	Nombre y dos apellidos, de acuerdo con el documento de identidad (DNI / Pasaporte) + NIF del empleado público + " (TCAT")"
C, Country	País	C = "ES"
Organization Identifier		Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)

[3] SerialNumber = p. ej: IDCES-99949992L. 3 caracteres para indicar el tipo de documento (IDC= documento nacional de identidad, PAS=pasaporte, ...) + 2 caracteres para identificar el país (ES) + Número de identidad (Printable String)) Size [RFC 5280] 64

2.3.2. Extensiones

Extensión	Crítica	Valores
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Subject Key Identifier	-	<id de la clave pública del certificado, obtenida 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-caIssuers Access Location: <URI del certificado de la EC emisora>
X509v3 CRL Distribution Points	-	<URI de la CRL>
X509v3 Key Usage	Sí	Digital Signature Content Commitment
X509v3 Extended Key Usage		Client Authentication Adobe Authentic Documents Trust
X509v3 Certificate Policies	-	<OID de la DPC> 1.3.6.1.4.1.15096.1.3.2.86.1 <URI de la DPC> <User Notice> " Certificat electrònic de persona vinculada de nivell mig. " <OID de la política de certificación ETSI: QCP-n> 0.4.0.194112.1.0
Qualified Certificate Statements		Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 años Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: <URI de la PDS> Id-etsi- qcs-QcType-esign 0.4.0.1862.1.6.1
X509v3 Subject Alternative Name		directoryName: OID: 1.3.6.1.4.1.15096.0.1 = "Nom de la persona vinculada" OID: 1.3.6.1.4.1.15096.0.2 = "Primer cognom persona vinculada" OID: 1.3.6.1.4.1.15096.0.3 = "Segon cognom persona vinculada"

2.4. Perfil de los Certificados de autenticación y firma de persona vinculada de nivel alto (T-CAT persona vinculada)

2.4.1. 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 la persona.
OU, Organization Unit	Unidad en la organización	"Persona vinculada de nivell alt"
Title (opcional)	Cargo	Ha de incluir el cargo de la persona física, que lo vincula con la administración, organismo o entidad de derecho público suscriptora del certificado.
Serial Number	NIF	Número del documento de identidad del firmante, con la semántica propuesta por la norma ETSI EN 319 412-1[4]
SN, Surname	Apellidos (persona física)	Primer y segundo apellidos (de acuerdo con el documento de identidad – DNI, Pasaporte, …)
Given name	Nombre	Nombre de pila, de acuerdo con el documento de identidad (DNI, pasaporte, ...)
CN, Common Name	Nombre, apellidos y NIF	Nombre y dos apellidos, de acuerdo con el documento de identidad (DNI / Pasaporte) + NIF de la persona vinculada + " (TCAT)"
C, Country	País	C = "ES"
Organization Identifier		Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)

[4] SerialNumber = p. ej: IDCES-99949992L. 3 caracteres para indicar el tipo de documento (IDC= documento nacional de identidad) + 2 caracteres para identificar el país (ES) + Número de identidad (Printable String)) Size [RFC 5280] 64

2.4.2. Extensiones

Extensión	Crítica	Valores
X509v3 Basic Constraints	Sí	CA:FALSE
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-caIssuers Access Location: <URI del certificado de la EC emisora>
X509v3 CRL Distribution Points	-	<URI de la CRL>
Qualified Certificate Statements	-	Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 años Id-etsi- qcs-QcSSCD 0.4.0.1862.1.4 Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: <URI de la PDS> Id-etsi- qcs-QcType 0.4.0.1862.1.6.1
X509v3 Key Usage	Sí	Digital Signature Content Commitment
X509v3 Extended Key Usage		Client Authentication SmartCardLogon Adobe Authentic Documents Trust
X509v3 Certificate Policies	-	<OID asociado a la DPC> 1.3.6.1.4.1.15096.1.3.2.82.1 <URI de la DPC> User Notice: “Certificat electrònic de persona vinculada de nivell alt. ” <OID de la política de certificación ETSI: QCP-n-qscd> 0.4.0.194112.1.2
X509v3 Subject Alternative Name	-	(opcional) otherName-userPrincipalName (UPN): Usuario en el dominio Windows del poseedor de claves directoryName: OID: 1.3.6.1.4.1.15096.0.1 = “Nom de la persona vinculada” OID: 1.3.6.1.4.1.15096.0.2 = “Primer cognom persona vinculada” OID: 1.3.6.1.4.1.15096.0.3 = “Segon cognom persona vinculada”

2.5. Perfil de los Certificados de autenticación de empleado público con pseudónimo de nivel alto (T-CAT pseudònim autenticació)

2.5.1. 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 vinculado el empleado.
OU, Organization Unit	Unidad en la organización	“Empleat públic amb pseudònim de nivell alt d'autenticació”
Pseudonym	Seudónimo Obligatorio según ETSI EN 319 412-2	Ej: NIP 111111111
Title (opcional)	Cargo	Ha de incluir el cargo de la persona física, que la vincula con la Administración, organismo o entidad de derecho público suscriptora del certificado.
CN, Common Name	Informar con el pseudónimo del organismo	Title/PSEUDONIM + “ - “ + NIP + “ - “ + Organization (AUT) Ex: SUBINSPECTOR - NIP 11111111 - ORGANITZACIÓ DE PROVES (AUT)
C, Country	País	C = “ES”

2.5.2. Extensiones

Extensión	Crítica	Valors
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Subject Key Identifier	-	<id de la clave pública del certificado, obtenido a partir del hash de la mateixa>
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-caIssuers Access Location: < URL de localización del certificado de la CA.>
X509v3 CRL Distribution Points	-	<URI de la CRL>
X509v3 Key Usage	Sí	Digital Signature
X509v3 Extended Key Usage		Client Authentication SmartCardLogon
X509v3 Certificate Policies	-	<OID asociado a la DPC> 1.3.6.1.4.1.15096.1.3.2.4.1.2 <URI de la DPC> User Notice: "Certificat electrònic d'empleat públic amb pseudònim de nivell alt d'autenticació. " <OID asociado a certificado de empleado público con pseudónimo de nivel alto> 2.16.724.1.3.5.4.1 <OID de la política de certificación ETSI: NCP+> 0.4.0.2042.1.2
X509v3 Subject Alternative Name	-	(opcional) otherName-userPrincipalName (UPN): Usuario en el dominio Windows del poseedor de claves directoryName: OID: 2.16.724.1.3.5.4.1.1 = " Certificat electrònic d'empleat públic amb pseudònim de nivell alt d'autenticació" OID: 2.16.724.1.3.5.4.1.2 = <O del DN> OID: 2.16.724.1.3.5.4.1.3 = <CIF de la entidad suscriptora>

2.6. Perfil de los Certificados de firma de empleado público con pseudónimo de nivel alto (T-CAT pseudònim signatura)

2.6.1. Certificado

Campo del DN	Nombre	Descripción
O, Organization	Organización	Denominación (nombre “oficial”) de la Administración, organismo, o entidad de derecho público, a la que se encuentra vinculado el empleado.
OU, Organization Unit	Unidad en la organización	“Empleat públic amb pseudònim de nivell alt de signatura.”
Pseudonym	Seudónimo Obligatorio según ETSI EN 319 412-2	Ex: NIP 111111111
Title (opcional)	Cargo	Ha de incluir el cargo de la persona física, que la vincula con la administración, organismo o entidad de derecho público suscriptora del certificado.
CN, Common Name	Informar con el pseudónimo del organismo	Title/PSEUDONIM + “ - “ + NIP + “ - “ + Organization (SIG) Ex: SUBINSPECTOR - NIP 11111111 - ORGANITZACIÓ DE PROVES (SIG)
C, Country	País	C = “ES”

2.6.2. Extensiones

Extensión	Crítica	Valores
X509v3 Basic Constraints	Sí	CA:FALSE
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: < URL de localización del certificado de la CA.>
X509v3 CRL Distribution Points	-	<URI de la CRL>
X509v3 Certificate Policies	-	<OID de la DPC correspondiente> 1.3.6.1.4.1.15096.1.3.2.4.1.1 <URI de la DPC> User Notice: "Certificat qualificat de signatura d'empleat públic amb pseudònim de nivell alt" <OID asociado a certificado de empleado público con pseudónimo de nivel alto> 2.16.724.1.3.5.4.1 <OID de la política de certificación ETSI: QCP-n-qscd> 0.4.0.194112.1.2
Qualified Certificate Statements	-	Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 años Id-etsi- qcs-QcSSCD 0.4.0.1862.1.4 Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: <URI de la PDS> Id-etsi- qcs-QcType-esign 0.4.0.1862.1.6.1
X509v3 Key Usage	Sí	Content Commitment
X509v3 Extended Key Usage	-	Adobe Authentic Documents Trust
X509v3 Subject Alternative Name	-	directoryName: OID: 2.16.724.1.3.5.4.1.1 = "Certificat qualificat de signatura d'empleat públic amb pseudònim de nivell alt" OID: 2.16.724.1.3.5.4.1.2 = <O del DN> OID: 2.16.724.1.3.5.4.1.3 = <CIF de la entidad suscriptora>

2.7. Perfil de los Certificados cualificados de autenticación y firma de empleado público con pseudónimo de nivel medio/sustancial (T-CATP pseudònim)

2.7.1. Certificado

Campo del DN	Nombre	Descripción
O, Organization	Organización	Denominación (nombre “oficial”) de la Administración, organismo, o entidad de derecho público, a la que se encuentra vinculado el empleado.
OU, Organization Unit	Unidad en la organización	“Empleat públic amb pseudònim de nivell mig.”
Pseudonym	Seudónimo Obligatorio según ETSI EN 319 412-2	Ex: NIP 111111111
Title (opcional)	Cargo	Ha de incluir el cargo de la persona física, que la vincula con la administración, organismo o entidad de derecho público suscriptora del certificado.
CN, Common Name	Informar con el pseudónimo y el organismo	Title/PSEUDONIM + “ - “ + NIP + “ - “ + Organization (TCAT) Ex: SUBINSPECTOR - NIP 11111111 - ORGANITZACIÓ DE PROVES (TCAT)
C, Country	País	C = “ES”

2.7.2. Extensiones

Extensión	Crítica	Valores
X509v3 Basic Constraints	Sí	CA:FALSE
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-caIssuers Access Location: < URL de localización del certificado de la CA.>
X509v3 CRL Distribution Points	-	<URI de la CRL>
X509v3 Certificate Policies	-	<OID de la DPC correspondiente> 1.3.6.1.4.1.15096.1.3.2.4.2 <URI de la DPC> User Notice: "Certificat qualificat empleat públic amb pseudònim de nivell mig" <OID asociado a certificado de empleado público con pseudónimo de nivel medio/sustancial> 2.16.724.1.3.5.4.2 <OID de la política de certificación ETSI: QCP-n> 0.4.0.194112.1.0
Qualified Certificate Statements	-	Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 años Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: <URI de la PDS> Id-etsi- qcs-QcType-esign 0.4.0.1862.1.6.1
X509v3 Key Usage	Sí	Digital Signature Content Commitment
X509v3 Extended Key Usage	-	Client Authentication Adobe Authentic Documents Trust
X509v3 Subject Alternative Name	-	directoryName: OID: 2.16.724.1.3.5.4.2.1 = "Certificat electrònic empleat públic amb pseudònim de nivell mig" 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>

2.8. Perfil de los Certificados de autenticación y firma de representante ante las Administraciones Públicas (T-CAT representant)

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 representa el representante.
OU, Organization Unit	Unidad en la organización	"Representant davant les AAPP de nivell alt"
Title (opcional)	Cargo	Ha de incluir el cargo de la persona física, que la vincula con la Administración, organismo o entidad de derecho público suscriptora del certificado.
Serial Number	NIF	Número del documento de identidad del empleado público con la semántica propuesta por la norma ETSI EN 319 412-1[5]
SN, Surname	Apellidos (persona física)	Primer y segundo apellidos (de acuerdo con el documento de identidad – DNI / Pasaporte, …)
Given name	Nombre	Nombre, de acuerdo con el documento de identidad (DNI / Pasaporte, ...)
CN, Common Name	Nombre, apellidos y NIF	Ver tabla específica. Ejemplo: "99949992L Nomdos Especimendos Especimendos (R: Q0000000J)"
C, Country	País	C = "ES"
Organization Identifier		Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad, p.ej. VATES- Q0000000J)
Description (2.5.4.13)	Datos de representación	Reg:XXX /Hoja:XXX /Tomo:XXX /Sección:XXX /Libro:XXX/ Folio:XXX /Fecha: dd-mm-aaaa /Inscripción:XXX Notario: NOMDOS SPECIMENDOS SPECIMENDOS /Núm Protocolo: XXX /Fecha Otorgamiento: dd-mm-aaaa En Boletines o Diarios Oficiales: Boletín: XXX /Fecha: dd-mm-aaaa /Número resolución: XXX

[5] SerialNumber = p. ej: IDCES-99949992L. 3 caracteres para indicar el tipo de documento (IDC= documento nacional de identidad, PAS=pasaporte, ...) + 2 caracteres para identificar el país (ES) + Número de identidad (Printable String)) Size [RFC 5280] 64

2.8.2. Common name

Campo	Contenido	Ejemplo	Tamaño (*)
NIF	Número DNI	99949992L	10
Nom	De acuerdo con el documento de identidad	Nomdos	
Apellido 1	De acuerdo con el documento de identidad	Especimendos	
Literal	(R:		4
NIF de la entidad representada	NIF de la entidad representada, tal y como figura en los registros oficiales	Q0000000J	9
Literal	)		2

(*) contando espacio en blanco posterior

2.8.3. Extensiones

Extensión	Crítica	Valores
X509v3 Basic Constraints	Sí	CA:FALSE
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-caIssuers Access Location: <URI del certificado de la EC emisora>
X509v3 CRL Distribution Points	-	<URI de la CRL>
X509v3 Certificate Policies	-	<OID de la política de certificación correspondiente al certificado> 1.3.6.1.4.1.15096.1.3.2.8.1.1 <URI de la DPC> User Notice: “Certificat electrònic de representant davant les AAPP de nivell alt. ” <OID de certificado de representante de persona jurídica> 2.16.724.1.3.5.8 <OID de la política de certificación ETSI QCP-n-qscd> 0.4.0.194112.1.2
Qualified Certificate Statements	-	Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 años Id-etsi- qcs-QcSSCD 0.4.0.1862.1.4 Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: <URI de la PDS> Id-etsi- qcs-QcType-esign 0.4.0.1862.1.6.1
X509v3 Key Usage	Sí	Digital Signature Content Commitment
X509v3 Extended Key Usage		Client Authentication SmartCardLogon Adobe Authentic Documents Trust
X509v3 Subject Alternative Name	-	(opcional) otherName-userPrincipalName (UPN): Usuario en el dominio Windows del poseedor de claves directoryName: OID: 1.3.6.1.4.1.15096.0.1 = “Nom del representant” OID: 1.3.6.1.4.1.15096.0.2 = “Primer cognom del representant” OID: 1.3.6.1.4.1.15096.0.3 = “Segon cognom del representant”

2.9. Perfil de los Certificados de firma de empleado público de nivel alto (T-CAT signatura)

2.9.1. 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 vinculado el empleado.
OU, Organization Unit	Unidad en la organización	"Empleat públic de nivell alt de signatura"
Title (opcional)	Cargo	Ha de incluir el cargo de la persona física que la vincula con la administración, organismo o entidad de derecho público suscriptora del certificado.
Serial Number	NIF	Número del documento de identidad del empleado público con la semántica propuesta por la norma ETSI EN 319 412-1[6]
SN, Surname	Apellidos (persona física)	Primer y segundo apellidos (de acuerdo con el documento de identidad – DNI / Pasaporte, …)
Given name	Nombre	Nombre, de acuerdo con documento de identidad (DNI, pasaporte, ...)
CN, Common Name	Nombre, apellidos y NIF	Nombre y dos apellidos de acuerdo con documento de identidad (DNI / Pasaporte) + NIF del empleado público + " (SIG)"
C, Country	País	C = "ES"
Organization Identifier		Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)

[6] SerialNumber = p. ex: IDCES-99949992L. 3 caracteres para indicar el tipo de documento (IDC= documento nacional de identidad, PAS=pasaporte, ...) + 2 caracteres para identificar el país (ES) + Número de identidad (Printable String)) Size [RFC 5280] 64

2.9.2. Extensiones

Extensión	Crítica	Valores
X509v3 Basic Constraints	Sí	CA:FALSE
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-caIssuers Access Location: <URI del certificado de la EC emisora>
X509v3 CRL Distribution Points	-	<URI de la CRL>
Qualified Certificate Statements	-	Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 años Id-etsi- qcs-QcSSCD 0.4.0.1862.1.4 Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: <URI de la PDS> Id-etsi- qcs-QcType-esign 0.4.0.1862.1.6.1
X509v3 Key Usage	Sí	Content Commitment
X509v3 Extended Key Usage	-	Adobe Authentic Documents Trust
X509v3 Certificate Policies	-	<OID associat a la DPC> 1.3.6.1.4.1.15096.1.3.2.7.1.1 <URI de la DPC> User Notice: " Certificat qualificat de signatura d'empleat públic de nivell alt. " <OID asociado a certificado de empleado público de nivel alto> 2.16.724.1.3.5.7.1 <OID de la política de certificación ETSI: QCP-n-qscd> 0.4.0.194112.1.2
X509v3 Subject Alternative Name	-	directoryName: OID: 2.16.724.1.3.5.7.1.1 ="Certificat qualificat de signatura d'empleat públic de nivell alt " 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: 2.16.724.1.3.5.7.1.6 = <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>

2.10. Perfil de los Certificados de autenticación y firma de trabajador público de nivel medio (T-CATP Treballador públic)

2.10.1. 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 vinculado el trabajador.
OU, Organization Unit	Unidad de la organización	"Treballador públic de nivell mig"
Title (opcional)	Cargo	Ha de incluir el cargo de la persona física, que la vincula con la administración, organismo o entidad de derecho público suscriptora del certificado.
Serial Number	NIF	Número del documento de identidad del firmante, con la semántica propuesta por la norma ETSI EN 319 412-1[7]
SN, Surname	Apellidos (persona física)	Primer y segundo apellidos (de acuerdo con el documento de identidad – DNI / Pasaporte, …)
Given name	Nombre	Nombre, de acuerdo con el documento de identidad (DNI, pasaporte, ...)
CN, Common Name	Nombre, apellidos y NIF	Nombre y dos apellidos, de acuerdo con el documento de identidad (DNI / Pasaporte) + NIF del trabajador público + " (TCAT")"
C, Country	País	C = "ES"
Organization Identifier		Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)

[7] SerialNumber = p. ex: IDCES-99949992L. 3 caracteres para indicar el tipo de documento (IDC= documento nacional de identidad, PAS=pasaporte, ...) + 2 caracteres para identificar el país (ES) + Número de identidad (Printable String)) Size [RFC 5280] 64

2.10.2. Extensiones

Extensión	Crítica	Valores
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Subject Key Identifier	-	<id de la clave pública del certificado, obtenida 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-caIssuers Access Location: <URI del certificado de la EC emisora>
X509v3 CRL Distribution Points	-	<URI de la CRL>
X509v3 Key Usage	Sí	Digital Signature Content Commitment
X509v3 Extended Key Usage	-	Client Authentication Adobe Authentic Documents Trust
X509v3 Certificate Policies	-	<OID associat a la DPC> 1.3.6.1.4.1.15096.1.3.2.86.3 <URI de la DPC> <User Notice> "Certificat electrònic de treballador públic de nivell mig. ” <OID de la política de certificación ETSI: QCP-n> 0.4.0.194112.1.0
Qualified Certificate Statements	-	Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 años Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: <URI de la PDS> Id-etsi- qcs-QcType-esign 0.4.0.1862.1.6.1
X509v3 Subject Alternative Name	-	directoryName: OID: 1.3.6.1.4.1.15096.0.1 = “Nom del treballador públic” OID: 1.3.6.1.4.1.15096.0.2 = “Primer cognom del treballador públic” OID: 1.3.6.1.4.1.15096.0.3 = “Segon cognom del treballador públic”

2.11. Perfil de los Certificados de autenticación y firma de trabajador público de nivel alto (T-CAT Treballador públic)

2.11.1. 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 la persona.
OU, Organization Unit	Unidad de la organización	"Treballador públic de nivell alt"
Title (opcional)	Cargo	Ha de incluir el cargo de la persona física, que lo vincula con la administración, organismo o entidad de derecho público suscriptora del certificado.
Serial Number	NIF	Número del documento de identidad del firmante, con la semántica propuesta por la norma ETSI EN 319 412-1[8]
SN, Surname	Apellidos (persona física)	Primer y segundo apellidos (de acuerdo con el documento de identidad – DNI, Pasaporte, …)
Given name	Nombre	Nombre de pila, de acuerdo con el documento de identidad (DNI, pasaporte, ...)
CN, Common Name	Nombre, apellidos y NIF	Nombre y dos apellidos, de acuerdo con el documento de identidad (DNI / Pasaporte) + NIF del trabajador público + " (TCAT)"
C, Country	País	C = "ES"
Organization Identifier		Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)

[8] SerialNumber = p. ex: IDCES-99949992L. 3 caracteres para indicar el tipo de documento (IDC= documento nacional de identidad, PAS=pasaporte, ...) + 2 caracteres para identificar el país (ES) + Número de identidad (Printable String)) Size [RFC 5280] 64

2.11.2. Extensiones

Extensión	Crítica	Valores
X509v3 Basic Constraints	Sí	CA:FALSE
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-caIssuers Access Location: <URI del certificado de la EC emisora>
X509v3 CRL Distribution Points	-	<URI de la CRL>
Qualified Certificate Statements	-	Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 años Id-etsi- qcs-QcSSCD 0.4.0.1862.1.4 Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: <URI de la PDS> Id-etsi- qcs-QcType 0.4.0.1862.1.6.1
X509v3 Key Usage	Sí	Digital Signature Content Commitment
X509v3 Extended Key Usage		Client Authentication SmartCardLogon Adobe Authentic Documents Trust
X509v3 Certificate Policies	-	<OID asociado a la DPC> 1.3.6.1.4.1.15096.1.3.2.82.2 <URI de la DPC> User Notice: “Certificat electrònic de treballador públic de nivell alt. ” <OID de la política de certificación ETSI: QCP-n-qscd> 0.4.0.194112.1.2
X509v3 Subject Alternative Name	-	(opcional) otherName-userPrincipalName (UPN): Usuario en el dominio Windows del poseedor de claves directoryName: OID: 1.3.6.1.4.1.15096.0.1 = “Nom del treballador públic” OID: 1.3.6.1.4.1.15096.0.2 = “Primer cognom del treballador públic” OID: 1.3.6.1.4.1.15096.0.3 = “Segon cognom del treballador públic”

3. Descripción de Perfiles de Certificados de Ciudadanos

3.1. Perfil de los Certificados de Ciudadano (idCAT certificat)

3.1.1. Certificado

Campo del DN	Nombre	Descripción
CN, Common Name	Nombre	Apellidos y Nombre del firmante + " - DNI " + número del documento de identificación. Ex: PEREZ MAS JOSE – DNI 123456789Z
Serial Number	Número de serie	Número del documento de identidad del firmante, con la semántica propuesta por la norma ETSI EN 319 412-1
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 aparecen en el documento de identidad utilizada
C, Country	País	País de expedición del documento identificativo del suscriptor.

3.1.2. Extensiones de los certificados

Extensión	Crítica	Valor
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Key Usage	Sí	Digital Signature Content Commitment
X509v3 Extended Key Usage	-	TLS Web Client Authentication Adobe Authentic Documents Trust
X509v3 Subject Key Identifier	-	<id de la clave pública del certificado, obtenida 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> 1.3.6.1.4.1.15096.1.3.2.86.2 <URI de la DPC> User Notice: “idCAT Certificat. ” <OID de la política de certificación ETSI: 0.4.0.194112.1.0> (Correspondiente a la política para certificados EU cualificados emitidos a personas físicas “QCP-n”, sin uso de un DSCF)
qcStatements	-	Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 años Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: <URI de la PDS> Id-etsi- qcs-QcType-esign 0.4.0.1862.1.6.1
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI de acceso al servicio OCSP> Access Method: Id-ad-caIssuers Access Location: <URI del certificat de l’EC emisora>

4. Descripción de los Perfiles de Certificados de Dispositivos e Infraestructura

4.1. Perfil de los Certificados de Sello Electrónico Avanzado (Segell nivell mig)

4.1.1. Certificado

Campo del DN	Nombre	Descripción
O, Organization	Organización	Contendrá la denominación de la Administración a la que pertenece el organismo.
Organization Identifier		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 de la organización	"Certificat de segell electrònic nivell mig"
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 el documento de identidad – DNI o NIE-)
Given name (Opcional)	Nombre (persona física)	Nombre, de acuerdo con el documento de identidad (DNI, NIE) del custodio de la clave privada
CN, Common Name	Denominación del sistema o aplicación	p.ej. "PLATAFORMA DE VALIDACIÓN DE L'AJUNTAMENT DE xxx"
C, Country	País	C= ES.

4.1.2. 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 Adobe Authentic Documents Trust
X509v3 Subject Key Identifier	-	<id de la clave pública del certificado, obtenida 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-caIssuers Access Location: <URI del certificado de la EC emisora>
X509v3 CRL Distribution Points	-	<URI de la CRL>
Qualified Certificate Statements	-	Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 años Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: <URI de la PDS> Id-etsi- qcs-QcType-eseal 0.4.0.1862.1.6.2

4.1.3. Extensiones de nivel medio

Extensión	Crítica	Valores
X509v3 Certificate Policies	-	<OID de la política de certificación correspondiente al certificado> 1.3.6.1.4.1.15096.1.3.2.6.2 <URI de la DPC> User Notice: "Certificat de segell electrònic nivell mig. ” <OID asociado a los certificados de sello de nivel medio / sustancial> 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	-	directoryName: OID: 2.16.724.1.3.5.6.2.1 = “Certificat de segell electrònic nivell mig” 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> 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> OID: 2.16.724.1.3.5.6.2.7 = <Primer apellido del custodio> (1) OID: 2.16.724.1.3.5.6.2.8 = <Segundo apellido del custodio> (2) OID: 2.16.724.1.3.5.6.2.9 = <Correo electrónico del custodio>

1. De acuerdo con documento de identidad (DNI, NIE)
2. De acuerdo con documento de identidad (DNI, NIE)

4.2. Perfil de los Certificados de Aplicación (Dispositiu aplicació)

4.2.1. Certificado

Campo del DN	Nombre	Descripción
O, Organization	Organización	Contendrá la denominación de la Administración a la que pertenece el organismo
Organization Identifier		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	"Certificat d'aplicació"
Serial Number	CIF	CIF de la Administración Pública, órgano o entidad de derecho público
CN, Common Name	Denominación del sistema o aplicación	p.ej. "PLATAFORMA DE VALIDACIÓN DE L'AJUNTAMENT DE xxx"
C, Country	País	C= ES.

4.2.2. 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 Adobe Authentic Documents Trust
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-caIssuers Access Location: <URI del certificado de la EC emisora>
X509v3 CRL Distribution Points	-	<URI de la CRL>
Qualified Certificate Statements	-	Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 años Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: <URI de la PDS> Id-etsi- qcs-QcType-eseal 0.4.0.1862.1.6.2
X509v3 Certificate Policies	-	<OID de la política de certificación correspondiente al certificado> 1.3.6.1.4.1.15096.1.3.2.91.1 <URI de la DPC> User Notice: "Certificat d'aplicació. " < OID "for EU qualified certificates issued to legal persons" según ETSI EN 319 411-2: QCP-l> 0.4.0.194112.1.1

4.3. Perfil de los Certificados de Sello Cualificado de Tiempo

4.3.1. Certificado

Campo del DN	Nombre	Descripción
O, Organization	Organización	Consorci Administració Oberta de Catalunya
Organization Identifier		Identificador de la organización distinto del nombre según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)
CN, Common Name	Nombre	*CONSORCI AOC Q TSU + "año de la emisión"*
C, Country	País	C = "ES"

4.3.2. Extensiones de los certificados cualificados

Extensión	Crítica	Valores
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Key Usage	Sí	Digital Signature Content Commitment
X509v3 Extended Key Usage	Sí	Time Stamping
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 asociado a la DPC> 1.3.6.1.4.1.15096.1.3.2.112 <URI de la DPC> User Notice: “Certificat de Servei de Segell Qualificat de Temps” < OID “for EU qualified certificates issued to legal persons” según ETSI EN 319 411-2: QCP-l> 0.4.0.194112.1.1
Qualified Certificate Statements	-	Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 años Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: <URI de la PDS> Id-etsi- qcs-QcType-eseal 0.4.0.1862.1.6.2
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI de acceso al servicio OCSP> Access Method: Id-ad-caIssuers Access Location: <URL de localización del certificado de la CA.>
Private Key Usage Period		<Fecha inicio de validez y fecha final de validez, máximo 2 años>