



**Consorci  
Administració Oberta  
de Catalunya**

# **Descripción de los perfiles de Certificados Consorci AOC**



LOCALRET

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

### Historial de versiones

<b>Versión</b>	<b>Resumen de los cambios</b>	<b>Fecha</b>
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	<ul style="list-style-type: none"><li>• Revisión anual de la documentación, puesto auditoría eIDAS.</li><li>• “4.4. Perfil de los Certificados de Servidor Seguro (Dispositiu SSL)”: eliminada opción de multidominio o wildcard.</li></ul>	24/07/2019

## Índice

<b>1. Introducción</b>	<b>5</b>
<b>2. Descripción de Perfiles de Certificados Personales del Sector Público</b>	<b>5</b>
2.1. Perfil de los Certificados de autenticación de trabajador público de nivel alto (T-CAT autenticació)	5
2.1.1. Certificado	5
2.1.2. Extensiones	7
2.2. Perfil de los Certificados cualificado de autenticación y firma de trabajador público de nivel medio (T-CATP)	8
2.2.1. Certificado	8
2.2.2. Extensiones	8
2.3. Perfil de los Certificados de autenticación y firma de persona vinculada de nivel medio (T-CATP persona vinculada)	11
2.3.1. Certificado	11
2.3.2. Extensiones	12
2.4. Perfil de los Certificados de autenticación y firma de persona vinculada de nivel alto (T-CAT persona vinculada)	13
2.4.1. Certificado	13
2.4.2. Extensiones	14
2.5. Perfil de los Certificados de autenticación de trabajador público con pseudónimo de nivel alto (T-CAT pseudònim autenticació)	15
2.5.1. Certificado	15
2.5.2. Extensiones	16
2.6. Perfil de los Certificados de firma de trabajador público con pseudónimo de nivel alto (T-CAT pseudònim signatura)	17
2.6.1. Certificado	17
2.6.2. Extensiones	18
2.7. Perfil de los Certificado de autenticación y firma de representante ante las Administraciones Públicas (T-CAT representant)	19
2.7.1. Certificado	19
2.7.2. Common name	20
2.7.3. Extensiones	20
2.8. Perfil de los Certificados de firma de trabajador público de nivel alto (T-CAT signatura)	22
2.8.1. Certificado	22
2.8.2. Extensiones	23
<b>3. Descripción de Perfiles de Certificados de Ciudadanos</b>	<b>24</b>
3.1. Perfil de los Certificados de Ciudadano (idCAT certificat)	24
3.1.1. Certificado	24
3.1.2. Extensiones de los certificados	24
<b>4. Descripción de los Perfiles de Certificados de Dispositivos e Infraestructura</b>	<b>26</b>
4.1. Perfil de los Certificados de Sello Electrónico Avanzado (Segell nivell mig)	26
4.1.1. Certificado	26
4.1.2. Extensiones de los certificados	27

4.1.3. Extensiones de nivel medio	28
4.2. Perfil de los Certificados de Aplicación (Dispositiu aplicació)	29
4.2.1. Certificado	29
4.2.2. Extensiones de los certificados	29
4.3. Perfil de los Certificados de Sede Electrónica (Seu-e nivell mig)	30
4.3.1. Certificado	30
4.3.2. Extensiones de los certificados	31
4.4. Perfil de los Certificados de Servidor Seguro (Dispositiu SSL)	32
4.4.1. Certificado	32
4.4.2. Extensiones de los certificados	33
4.5. Perfil de los Certificados de Servidor Seguro Extended Validation (Dispositiu SSL EV)	34
4.5.1. Certificado	34
4.5.2. Extensiones de los certificados	35
4.6. Perfil de los Certificados de Sello Cualificado de Tiempo	36
4.6.1. Certificado	36
4.6.2. Extensiones de los certificados	36

## 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 de Hacienda y Función Pública; 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 trabajador 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://www.aoc.cat/catcert/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 trabajador 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	“Treballador públic de nivell alt d'autenticació”
Title (opcional)	Cargo	Ha de incloure el cargo de la persona física, que la vincula con la administració, organisme o entitat de dret públic suscriptora del certificat.

SN, Serial Number	NIF	Número del documento de identidad del firmante con la semántica propuesta por la norma ETSI EN 319 412-1 <sup>1</sup>
Surname	Apellidos (persona física)	Primer y segundo apellidos (de acuerdo con el documento de identidad – DNI / Passaport, ...) + " - DNI" + NIF del empleado público
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) + " – DNI" + 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)

<sup>1</sup> SerialNumber = p. ej: IDCES-00000000G. 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-calssuers Access Location: <URI del certificado de la EC emisora>
X509v3 CRL Distribution Points	-	http://epsd.catcert.net/crl/ec-sectorpublic.crl
X509v3 Key Usage	Sí	Digital Signature Key encipherment
X509v3 Extended Key Usage		Email protection 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 de treballador públic de nivell alt d'autenticació . Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A"  <OID de la política de certificació 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 para SMIME) rfc822Name: mail de contacto  (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 de treballador 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 cualificado de autenticación y firma de trabajador 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 suscriptor del certificado, a la que se encuentra vinculado el empleado.
OU, Organization Unit	Unidad en la organización	"Treballador públic de nivell mig"
Title (opcional)	Cargo	Ha de incloure el càrrec de la persona física, que la vincula amb la administració, organisme o entitat de dret públic suscriptor del certificat.
SN, Serial Number	NIF	Número del documento de identidad del firmante, con la semántica propuesta por la norma ETSI EN 319 412-1 <sup>2</sup>
Surname	Apellidos (persona física)	Primer y segundo apellido (de acuerdo con el documento de identidad – DNI / Pasaporte, ...) + " - DNI " + NIF del empleado público
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) + " – DNI " + 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)

<sup>2</sup> SerialNumber = p. ej: IDCES-00000000G. 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-calssuers Access Location: <URI del certificado de la EC emisora>
X509v3 CRL Distribution Points	-	http://epsd.catcert.net/crl/ec-sectorpublic.crl
X509v3 Key Usage	Sí	Digital Signature Content Commitment Key Encipherment
X509v3 Extended Key Usage		Email protection Client Authentication
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 de treballador públic de nivell mig. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A”  <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: https://www.aoc.cat/catcert/pds_en Id-etsi- qcs-QcType-esign 0.4.0.1862.1.6.1

<p>X509v3 Subject Alternative Name</p>	<p>-</p>	<p>rfc822Name: mail de contacto (Opcional)</p> <p>directoryName:          OID: 2.16.724.1.3.5.7.2.1 = Certificado electrónico de trabajador público de nivel medio          OID: 2.16.724.1.3.5.7.2.2 = &lt;O del DN&gt;          OID: 2.16.724.1.3.5.7.2.3 = &lt;CIF de la entidad suscriptora&gt;          OID: 2.16.724.1.3.5.7.2.4 = &lt;serialNumber del DN&gt;          OID: 2.16.724.1.3.5.7.2.6 = &lt;Given name&gt;          OID: 2.16.724.1.3.5.7.2.7 = &lt;Primer apellido del empleado público&gt;          OID: 2.16.724.1.3.5.7.2.8 = &lt;Segundo apellido del empleado público&gt;          OID: 2.16.724.1.3.5.7.2.9 = &lt;correo electrónico del empleado público&gt;</p>
--	----------	--

## 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 suscriptor 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 incloure el cargo de la persona física, que la vincula con la administración, organismo o entidad de derecho público suscriptor del certificado.
SN, Serial Number	NIF	Número del documento de identidad del firmante, con la semántica propuesta por la norma ETSI EN 319 412-1 <sup>3</sup>
Surname	Apellidos (persona física)	Primer y segundo apellidos (de acuerdo con el documento de identidad – DNI / Pasaporte, ...) + " - DNI " + NIF del empleado público.
Given name	Nombre	Nombre, de acuerdo con el documento de identidad (DNI, pasaport, ...)
CN, Common Name	Nombre, apellidos y NIF	Nombre y dos apellidos, de acuerdo con el documento de identidad (DNI / Pasaporte) + " – DNI " + 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)

<sup>3</sup> SerialNumber = p. ej: IDCES-00000000G. 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-calssuers Access Location: <URI del certificado de la EC emisora>
X509v3 CRL Distribution Points	-	http://epsd.catcert.net/crl/ec-sectorpublic.crl
X509v3 Key Usage	Sí	Digital Signature Content Commitment Key encipherment
X509v3 Extended Key Usage		Email protection Client Authentication
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. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A" <OID de la política de certificació 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: https://www.aoc.cat/catcert/pds_en Id-etsi- qcs-QcType-esign 0.4.0.1862.1.6.1
X509v3 Subject Alternative Name	-	rfc822Name: mail de contacto (Opcional)

## 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 suscriptor del certificado, a la que se encuentra vinculada la persona.
OU, Organization Unit	Unitat a l'organització	"Persona vinculada de nivell alt"
Title (opcional)	Càrrec	Ha de incloure el càrrec de la persona física, que la vincula amb l'administració, organisme o entitat de dret públic suscriptor del certificat.
SN, Serial Number	NIF	NIF o NIE del treballador públic. Preferiblement s'aplicarà la semàntica proposada per la norma ETSI EN 319 412-1 <sup>4</sup>
Surname	Apellidos (persona física)	Primer y segundo apellidos (de acuerdo con el documento de identidad – DNI, Pasaporte, ...) + " - DNI " + NIF de la persona vinculada
Given name	Nom	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) + " – DNI " + 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)

<sup>4</sup> SerialNumber = p. ej: IDCES-00000000G. 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-calssuers Access Location: <URI del certificado de la EC emisora>
X509v3 CRL Distribution Points	-	http://epsd.catcert.net/crl/ec-sectorpublic.crl
Qualified Certificate Statements	Sí	Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 anys Id-etsi- qcs-QcSSCD 0.4.0.1862.1.4 Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: https://www.aoc.cat/catcert/pds_en Id-etsi- qcs-QcType 0.4.0.1862.1.6.1
X509v3 Key Usage	Sí	Digital Signature Content Commitment Key encipherment
X509v3 Extended Key Usage		Email protection Client Authentication SmartCardLogon
X509v3 Certificate Policies	-	<OID associat 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. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A"  <OID de la política de certificació ETSI: QCP-n-qscd> 0.4.0.194112.1.2
X509v3 Subject Alternative Name	-	(opcional per SMIME) rfc822Name: mail de contacte  (opcional) otherName-userPrincipalName (UPN): Usuario en el dominio Windows del poseedor de claus

## 2.5. Perfil de los Certificados de autenticación de trabajador 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 suscriptor del certificado, a la que se encuentra vinculado el empleado.
OU, Organization Unit	Unidad en la organización	"Treballador públic amb pseudònim de nivell alt d'autenticació"
Pseudonym	Pseudónimo Obligatorio según ETSI EN 319 412-2	Ej: NIP 111111111
Title (opcional)	Cargo	Ha de incloure el càrrec de la persona física, que la vincula con la Administración, organismo o entidad de derecho público suscriptor del certificado.
CN, Common Name	Informar con el pseudónimo del organismo	Pseudonym + " - " + Title + (AUT) Ex: NIP 111111111 - SUBINSPECTOR (AUT)
C, Country	País	C = "ES"

## 2.5.2. Extensiones

Extensió	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 clau pública del certificat de la CA, obtingut 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	-	http://epsdc.catcert.net/crl/ec-sectorpublic.crl
X509v3 Key Usage	Sí	Digital Signature Key encipherment
X509v3 Extended Key Usage		Email Protection Client Authentication SmartCardLogon
X509v3 Certificate Policies	-	<OID associat a la DPC> 1.3.6.1.4.1.15096.1.3.2.4.1.2  <URI de la DPC> User Notice: "Certificat electrònic de treballador públic amb pseudònim de nivell alt d'autenticació. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A"  <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 <sup>5</sup>
X509v3 Subject Alternative Name	-	(opcional) otherName-userPrincipalName (UPN): Usuari en el dominio Windows del poseedor de claves  directoryName: OID: 2.16.724.1.3.5.4.1.1 = " Certificat electrònic de treballador 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 trabajador 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	"Treballador públic amb pseudònim de nivell alt."
Pseudonym	Pseudónimo Obligatorio según ETSI EN 319 412-2	Ex: NIP 111111111
Title (opcional)	Cargo	Ha de incloure el càrrec de la persona física, que la vincula amb la administració, organisme o entitat de dret públic subscriptora del certificat.
CN, Common Name	Informar con el pseudónimo del organismo	Pseudonym + " - " + Title + (SIG) Ex: NIP 111111111 – SUBINSPECTOR (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	-	http://epsd.catcert.net/crl/ec-sectorpublic.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 de treballador públic amb pseudònim de nivell alt. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A"  <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	Sí	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: https://www.aoc.cat/catcert/pds_en Id-etsi- qcs-QcType-esign 0.4.0.1862.1.6.1
X509v3 Key Usage	Sí	Content Commitment
X509v3 Subject Alternative Name	-	directoryName: OID: 2.16.724.1.3.5.4.1.1 = "Certificat qualificat de signatura de treballador 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 Certificado de autenticación y firma de representante ante las Administraciones Públicas (T-CAT representant)

### 2.7.1. Certificado

Campo del DN	Nombre	Descripción
O, Organization	Organización	Denominación (nombre "oficial") de la Administración, organismo o entidad de derecho público suscriptor 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 incloure el cargo de la persona física, que la vincula amb la Administració, organisme o entitat de dret públic suscriptor del certificat.
SN, Serial Number	NIF	Número del documento de identidad del empleado público con la semántica propuesta por la norma ETSI EN 319 412-1 <sup>6</sup>
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: "12345678Z Pedro Antonio López (R: B0085974Z)"
C, Country	País	C = "ES"
Organization Identifier		Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad, p.e. VATES-B0085974Z)
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: Nombre Apellido1 Apellido2 /Núm Protocolo: XXX /Fecha Otorgamiento: dd-mm-aaaa  En Boletines o Diarios Oficiales: Boletín: XXX /Fecha: dd-mm-aaaa /Número resolución: XXX

<sup>6</sup> SerialNumber = p. ej: IDCES-00000000G. 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

## 2.7.2. Common name

Campo	Contenido	Ejemplo	Tamaño(*)
NIF	Número DNI/NIE	12345678Z	10
Nom	De acuerdo con el documento de identidad	Pedro Antonio	
Apellido 1	De acuerdo con el documento de identidad	López	
Literal	(R:		4
NIF de la entidad representada	NIF de la entidad representada, tal y com figura en los registros oficiales	Q0085974Z	9
Literal	)		2

(\*) contando espacio en blanco posterior

## 2.7.3. 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-calssuers Access Location: <URI del certificado de la EC emisora>
X509v3 CRL Distribution Points	-	http://epsdc.catcert.net/crl/ec-sectorpublic.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. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A"  <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	Sí	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: https://www.aoc.cat/catcert/pds_en Id-etsi- qcs-QcType-esign 0.4.0.1862.1.6.1

X509v3 Key Usage	Sí	Digital Signature Content Commitment Key encipherment
X509v3 Extended Key Usage		Email protection Client Authentication SmartCardLogon
X509v3 Subject Alternative Name	-	(opcional per SMIME) rfc822Name: mail de contacto (opcional) otherName-userPrincipalName (UPN): Usuario en el dominio Windows del poseedor de claves

## 2.8. Perfil de los Certificados de firma de trabajador público de nivel alto (T-CAT signatura)

### 2.8.1. Certificado

Campo del DN	Nombre	Descripción
O, Organization	Organización	Denominación (nombre "oficial") de la Administración, organismo o entidad de derecho público suscriptor del certificado, a la que se encuentra vinculado el empleado.
OU, Organization Unit	Unidad en la organización	"Triballador públic de nivell alt de signatura"
Title (opcional)	Cargo	Ha de incloure el càrrec de la persona física que la vincula amb la administració, organisme o entitat de dret públic suscriptora del certificat.
SN, Serial Number	NIF	Número del documento de identidad del empleado público con la semántica propuesta por la norma ETSI EN 319 412-1 <sup>7</sup>
Surname	Apellidos (persona física)	Primer y segundo apellidos (de acuerdo con el documento de identidad – DNI / Pasaporte, ...) + " - DNI " + NIF del empleado público
Given name	Nombre	Nombre, de acuerdo con documento de identidad (DNI, pasaporte, ...)
CN, Common Name	Nom, apellidos y NIF	Nombre y dos apellidos de acuerdo con documento de identidad (DNI / Pasaporte) + " – DNI " + 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)

<sup>7</sup> SerialNumber = p. ex: IDCES-00000000G. 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. 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: <URI del certificado de la EC emisora>
X509v3 CRL Distribution Points	-	http://epsd.catcert.net/crl/ec-sectorpublic.crl
Qualified Certificate Statements	Sí	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: https://www.aoc.cat/catcert/pds_en Id-etsi- qcs-QcType-esign 0.4.0.1862.1.6.1
X509v3 Key Usage	Sí	Content Commitment
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 de treballador públic de nivell alt . Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A"  <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 de treballador 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>

## 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
serialNumber	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	"ES"

#### 3.1.2. Extensiones de los certificados

Extensión	Crítica	Valor
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Key Usage	Sí	Digital Signature Non Repudiation Key Encipherment
X509v3 Extended Key Usage	-	TLS Web Client Authentication E-mail Protection
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	-	<a href="http://epsd.catcert.net/crl/ec-sectorpublic.crl">http://epsd.catcert.net/crl/ec-sectorpublic.crl</a>
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. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A"  <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: <a href="https://www.aoc.cat/catcert/pds_en">https://www.aoc.cat/catcert/pds_en</a> 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-calssuers 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”
SN, Serial Number	CIF	CIF de la Administración Pública, órgano o entidad de derecho público
Surname (Opcional)	Apellidos (persona física)	Primer y segundo apellidos (de acuerdo con el documento de identidad – DNI o NIE-) + “ - DNI ” + NIF del custodio de la clave privada
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.e. “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	-	Email protection TLS Web Client Authentication
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-calssuers Access Location: <URI del certificado de la EC emisora>
X509v3 CRL Distribution Points	-	<a href="http://epsd.catcert.net/crl/ec-sectorpublic.crl">http://epsd.catcert.net/crl/ec-sectorpublic.crl</a>
Qualified Certificate Statements	Sí	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: <a href="https://www.aoc.cat/catcert/pds_en">https://www.aoc.cat/catcert/pds_en</a> 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	-	<p>&lt;OID de la política de certificación correspondiente al certificado&gt; 1.3.6.1.4.1.15096.1.3.2.6.2</p> <p>&lt;URI de la DPC&gt; User Notice: "Certificat de segell electrònic nivell mig. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A"</p> <p>&lt;OID asociado a los certificados de sello de nivel medio / sustancial&gt; 2.16.724.1.3.5.6.2</p> <p>&lt;OID "for EU qualified certificates issued to legal persons" según ETSI EN 319 411-2: QCP-I&gt; 0.4.0.194112.1.1</p>
X509v3 Subject Alternative Name	-	<p>rfc822Name: mail de contacte</p> <p>directoryName:</p> <p>OID: 2.16.724.1.3.5.6.2.1 = "Certificat de segell electrònic nivell mig"</p> <p>OID: 2.16.724.1.3.5.6.2.2 = &lt;O del DN&gt;</p> <p>OID: 2.16.724.1.3.5.6.2.3 = &lt;serialNumber del DN&gt;</p> <p>OID: 2.16.724.1.3.5.6.2.4 = &lt;NIF/NIE del custodio&gt;</p> <p>OID: 2.16.724.1.3.5.6.2.5 = &lt;CN del DN&gt;</p> <p>OID: 2.16.724.1.3.5.6.2.6 = &lt;Given name&gt;</p> <p>OID: 2.16.724.1.3.5.6.2.7 = &lt;Primer apellido del custodio&gt; (1)</p> <p>OID: 2.16.724.1.3.5.6.2.8 = &lt;Segundo apellido del custodio&gt; (2)</p> <p>OID: 2.16.724.1.3.5.6.2.9 = &lt;correo electrónico del custodio&gt;</p>

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	Organització	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"
SN, Serial Number	CIF	CIF de la Administración Pública, órgano o entidad de derecho público
CN, Common Name	Denominación del sistema o aplicación	p.e. "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	-	Email protection TLS Web Client Authentication
X509v3 Subject Key Identifier	-	<id de la clave pública del certificado, obtenido a partir del hash de la misma>
X509v3 Authority Key Identifier	-	<id de la clave pública del certificado de la CA, obtenido a partir del hash de la misma>

X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI de acceso al servicio OCSP> Access Method: Id-ad-caIssuers Access Location: <URI del certificado de la EC emisora>
X509v3 CRL Distribution Points	-	http://epsd.catcert.net/crl/ec-sectorpublic.crl
Qualified Certificate Statements	Sí	Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1 Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 anys Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: https://www.aoc.cat/catcert/pds_en 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. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A"  < OID "for EU qualified certificates issued to legal persons" según ETSI EN 319 411-2: QCP-!> 0.4.0.194112.1.1
X509v3 Subject Alternative Name	-	rfc822Name: mail de contacto (opcional)

### 4.3. Perfil de los Certificados de Sede Electrónica (Seu-e nivell mig)

#### 4.3.1. Certificado

Campo del DN	Valor	Descripción
CN, Common Name	Nombre	Denominación de nombre de dominio donde residirá el certificado Ha de coincidir con el que se encuentra en la extensión Subject Alternative Names
O, Organization	Razón Social	Denominación (nombre "oficial" de la organización) del suscriptor de servicios de certificación
OU, Organizational Unit	Unidad en la organización	<i>"Certificat de seu electrònica nivell mig"</i>
OU, Organizational Unit	Unidad en la organización	<i>El nombre descriptivo de la sede</i>

SN, SerialNumber	CIF	Contendrá el NIF de la entidad responsable de la sede electrónica
OrganizationIdentifier		Identificador de la organización Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)
businessCategory	"Government Entity"	Business Category
C, Country	País	C=ES
jurisdictionCountryName 1.3.6.1.4.1.311.60.2.1.3	País	Subject Jurisdiction of Incorporation or Registration C=ES
L, Locality	Municipio	Ciudad
S, State or Province	Provincia	Provincia

#### 4.3.2. Extensiones de los certificados

Extensión	Crítica	Valores
X509v3 Authority Key Identifier	-	<id de la clave pública de la CA, obtenido a partir del hash de la misma>
X509v3 Subject Key Identifier	-	<id de la clave pública del certificado, obtenido a partir del hash de la misma>
X509v3 Key Usage	Sí	Digital Signature Key Encipherment
X509v3 Extended Key Usage	-	Autenticación TLS web Server
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 CRL Distribution Points	-	<a href="http://epsod.catcert.net/crl/ec-sectorpublic.crl">http://epsod.catcert.net/crl/ec-sectorpublic.crl</a>

X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI de acceso al servicio OCSP> Access Method: Id-ad-calssuers Access Location: <URI del certificado de la EC emisora>
X509v3 Certificate Policies	-	<OID asociado a la DPC> 1.3.6.1.4.1.15096.1.3.2.5.2  <URI de la DPC> User Notice: "Certificat de seu electrònica de nivell mig. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A"  <OID asociado a los certificados de sede de nivel medio / sustancial> 2.16.724.1.3.5.5.2  <OID ETSI QCP-w> 0.4.0.194112.1.4
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: <a href="https://www.aoc.cat/catcert/pds_en">https://www.aoc.cat/catcert/pds_en</a> Id-etsi- qcs-QcType-web 0.4.0.1862.1.6.3
X509v3 Subject Alternative Name	-	dnsName: nombre de dominio donde residirá el certificado

## 4.4. Perfil de los Certificados de Servidor Seguro (Dispositiu SSL)

### 4.4.1. Certificado

Campo del DN	Valor	Descripción
CN, Common Name	Nombre	(BR. 7.1.4.2.2.a) Este dominio ha de coincidir con el indicado (o con uno de los indicados) en el Subject Alt Names).
O, Organization	Razón Social	Denominación (nombre "oficial" de la organización) del suscriptor de servicios de certificación
OU, Organizational Unit (Opcional)	Unidad en la organización	<i>El nombre descriptivo del departamento</i>

OrganizationIdentifier		Identificador de la organización  Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)
L, Locality	Ciudad	(BR. 7.1.4.2.2.e) Indicación requerida al existir el campo Organization (O)
C, Country	País	Código de país de dos dígitos según ISO 3166-1. Por defecto "ES". (BR. 7.1.4.2.2.h) Indicación requerida al existir el campo Organization (O)

Las indicaciones (BR.X) son requisitos de la *Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates* del CA/Browser Forum, en la versión vigente en el momento de la publicación de este perfil.

#### 4.4.2. Extensiones de los certificados

Extensión	Crítica	Valores
X509v3 Subject Alternative Name	-	URL, nombre de dominio o identificación del dispositivo o servicio poseedor de las claves o de la aplicación.
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Key Usage	Sí	Digital Signature Key Encipherment
X509v3 Extended Key Usage	-	Server Authentication (1.3.6.1.5.5.7.3.1)
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 1: Id-ad-ocsp (1.3.6.1.5.5.7.48.1) Access Location 1: <URI de acceso al servicio OCSP> Access Method 2: id-ad-caissuers (1.3.6.1.5.5.7.48.2) Access Location 2: <URI del certificado de la EC emisora>
X509v3 CRL Distribution Points	-	<a href="http://epsd.catcert.net/crl/ec-sectorpublic.crl">http://epsd.catcert.net/crl/ec-sectorpublic.crl</a>

X509v3 Certificate Policies	-	<p>&lt;OID de la política de certificación corresponent al certificado&gt; 1.3.6.1.4.1.15096.1.3.2.51.1</p> <p>&lt;URI de la CPS&gt;</p> <p>User Notice: "Certificat de dispositiu SSL. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A"</p>
X509v3 Subject Alternative Name	-	dNSName: nombre de dominio donde residirá el certificado

## 4.5. Perfil de los Certificados de Servidor Seguro Extended Validation (Dispositiu SSL EV)

### 4.5.1. Certificado

Camp del DN	Valor	Descripción
CN, Common Name	Nombre	(EVG 9.2.3) Nombre de un único dominio. (BR. 7.1.4.2.2.a) Este dominio ha de coincidir con lo indicado (o uno de los indicados) en el Subject Alt Names).
O, Organization	Raó Social	Nombre Oficial de la Organización suscriptora del certificado
OU, Organizational Unit (Opcional)	Unidad en la organización	<i>El nombre descriptivo del departamento</i>
SN, SerialNumber	CIF	CIF de la Organización suscriptora del certificado (EVG 9.2.6) Registration Number
OrganizationIdentifier		Identificador de la organización Según la norma técnica ETSI EN 319 412-1 (VATES + NIF de la entidad)
businessCategory	"Government Entity"	(EVG 9.2.4) Business Category
C, Country	País	Código de país de dos dígitos según ISO 3166-1. Por defecto "ES".(EVG 9.2.7) Country (required) (BR. 7.1.4.2.2.h) Indicación requerida al existir el campo Organization (O)

L, Locality		(EVG 9.2.7) Address of Place of Business: City (required) (BR. 7.1.4.2.2.e) Indicación requerida al existir el campo Organization (O)
jurisdictionCountryName 1.3.6.1.4.1.311.60.2.1.3	País	(EVG 9.2.5) Subject Jurisdiction of Incorporation or Registration

Las indicaciones (BR.X) son requisitos de la *Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates* del CA/Browser Forum, en la versión vigente en el momento de la publicación de este perfil.

Las indicaciones (EVG 9.2.X) son requisitos específicos para certificados *Extended Validation* según establece el CA/Browser Forum en las *Guidelines For The Issuance And Management Of Extended Validation Certificates*, en la versión vigente en el momento de publicación de este perfil.

#### 4.5.2. Extensiones de los certificados

Extensión	Crítica	Valores
X509v3 Authority Key Identifier	-	<id de la clave pública del certificado de la CA, obtenido a partir del hash de la misma>
X509v3 Subject Key Identifier	-	<id de la clave pública del certificado, obtenido a partir del hash de la misma>
X509v3 Key Usage	Sí	Digital Signature Key Encipherment
X509v3 Extended Key Usage	-	Server Authentication (1.3.6.1.5.5.7.3.1)
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 CRL Distribution Points	-	<a href="http://epsd.catcert.net/crl/ec-sectorpublic.crl">http://epsd.catcert.net/crl/ec-sectorpublic.crl</a>
X509v3 Authority Information Access	-	Access Method: Id-ad-ocsp Access Location: <URI de acceso al servicio OCSP> Access Method: Id-ad-calssuers Access Location: <URI del certificado de la EC emisora>

X509v3 Certificate Policies	-	<p>&lt;OID asociado a la DPC&gt; 1.3.6.1.4.1.15096.1.3.2.51.2</p> <p>&lt;URI de la DPC&gt; User Notice: "Certificat de dispositiu SSL EV. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A"</p> <p>&lt;OID ETSI QCP-w&gt; 0.4.0.194112.1.4</p>
Qualified Certificate Statements		<p>Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1</p> <p>Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 años</p> <p>Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: <a href="https://www.aoc.cat/catcert/pds_en">https://www.aoc.cat/catcert/pds_en</a></p> <p>Id-etsi- qcs-QcType-web 0.4.0.1862.1.6.3</p>
X509v3 Subject Alternative Name	-	dNSName: nombre de dominio donde residirá el certificado

## 4.6. Perfil de los Certificados de Sello Cualificado de Tiempo

### 4.6.1. Certificado

Camp del DN	Valor	Descripción
CN, Common Name	Nombre	<i>Debe contener un Identificador de TSU que debe identificar de manera única la TSU correspondiente, incluyendo referencia al cliente</i>
O, Organization	Organización	Consorci Administració Oberta de Catalunya
OI, Organization Identifier	Identificador de Organización	"VATES-Q0801175A"
C, Country	País	C=ES

### 4.6.2. Extensiones de los certificados

Extensión	Crítica	Valores
X509v3 Basic Constraints	Sí	CA:FALSE
X509v3 Key Usage	Sí	digitalSignature contentCommitment
X509v3 Extended Key Usage	Sí	id-kp-timeStamping {1.3.6.1.5.5.7.3.8}

X509v3 Subject Key Identifier	-	<id de la clave pública del certificado, obtenido a partir del hash de la misma>
X509v3 Authority Key Identifier	-	<id de la clave pública del certificado de la CA, obtenido a partir del hash de la misma>
X509v3 CRL Distribution Points	-	http://epsd.catcert.net/crl/ec-sectorpublic.crl
X509v3 Certificate Policies	-	<OID asociado a la DPC> 1.3.6.1.4.1.15096.1.3.2.111  <URI de la PC>https://www.aoc.cat/catcert/regulacio  userNotice: "Certificat de Servei Segur de TSA qualificada"
id-ce-privateKeyUsagePeriod 2.5.29.16		<i>Tiene por objetivo limitar la validez de la clave privada: 3 años</i>
Authority Information Access	-	accessMethod: Id-ad-calssuers 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 .