Consorci
Administració Oberta
de Catalunya

# Descripción del perfil de certificados de EC-SectorPublic

Generalitat
de Catalunya

LOCALRET

# Control documental

| | | |
|---|---|---|
| **Estado formal** | **Elaborado por:**<br><br>**Servicio de Certificación Digital** | **Aprobado por:**<br><br>**Dirección del Consorci AOC** |
| **Fecha de creación** | 09/05/2018 | |
| **Control de versiones** | **Versión:** | 1.0 |
| | **Fecha:** | 09/05/2018 |
| | **Descripción:** | Adaptación a eIDAS.<br>Adaptación a CertiCA (DTIC de MINHAP). |
| **Nivel acceso información** | Pública | |
| **Título** | Descripción de perfiles de certificados de EC-SectorPublic | |
| **Control de copias** | Únicamente las copias disponibles en la web del Consorci AOC en https://www.aoc.cat/CATCert/Regulacio garantizan la actualización de los documentos. Toda copia impresa o depositada en ubicaciones diferentes, se considerarán copias no controladas. | |
| **Derechos de autor** | Esta obra está sujeta a una licencia Reconocimiento - No comercial-Sin obras derivadas 3.0 España de Creative Commons. Para ver una copia visitar https://creativecommons.org/licenses/by-nc-nd/3.0/es/deed.ca o enviar una carta a Creative Commons, 171 Second Street, Suite 300, San Francisco, California 94105, USA. | |

## Índice

# PERFIL DE LOS CERTIFICADOS CDA-1_SGNM

## 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 i 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. |

## Extensiones de los certificados

| Extensión | Crítica | Valores |
|---|---|---|
| X509v3 Basic Constraints | Sí | CA:FALSE |
| X509v3 Key Usage | Sí | Digital Signature<br>Content Commitment<br>Key Encipherment |
| X509v3 Extended Key Usage | - | Email protection<br>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<br>Access Location: <URI de acceso al servicio OCSP><br>Access Method: Id-ad-calssuers<br>Access Location: <URI del certificado de la EC emisora> |
| X509v3 CRL Distribution Points | - | http://epscd.catcert.net/crl/ec-sectorpublic.crl |
| Qualified Certificate Statements | Sí | Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1<br>Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 años<br>Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: https://www.aoc.cat/catcert/pds_en<br>Id-etsi- qcs-QcType-eseal 0.4.0.1862.1.6.2 |

## Extensiones de nivel medio

| Extensión | Crítica | Valores |
|---|---|---|
| X509v3 Certificate Policies | - | <OID de la política de certificación correspondiente al certificado><br>1.3.6.1.4.1.15096.1.3.2.6.2<br><br><URI de la DPC><br>User Notice: "Certificat de segell electrònic nivell mig. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A"<br><br><OID asociado a los certificados de sello de nivel medio / sustancial><br>2.16.724.1.3.5.6.2<br><br><OID "for EU qualified certificates issued to legal persons" según ETSI EN 319 411-2: QCP-l> 0.4.0.194112.1.1 |
| X509v3 Subject Alternative Name | - | rfc822Name: mail de contacte<br>directoryName:<br>OID: 2.16.724.1.3.5.6.2.1 = "Certificat de segell electrònic nivell mig"<br>OID: 2.16.724.1.3.5.6.2.2 = <O del DN><br>OID: 2.16.724.1.3.5.6.2.3 = <serialNumber del DN><br>OID: 2.16.724.1.3.5.6.2.4 = <NIF/NIE del custodio><br>OID: 2.16.724.1.3.5.6.2.5 = <CN del DN><br>OID: 2.16.724.1.3.5.6.2.6 = <Given name><br>OID: 2.16.724.1.3.5.6.2.7 = <Primer apellido del custodio> (1)<br>OID: 2.16.724.1.3.5.6.2.8 = <Segundo apellido del custodio> (2)<br>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)

# PERFIL DE LOS CERTIFICADOS CDA-1

## Certificado

| Campo del DN | Nom | Descripció |
|---|---|---|
| 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. |

## Extensiones de los certificados

| Extensión | Crítica | Valores |
|---|---|---|
| X509v3 Basic Constraints | Sí | CA:FALSE |
| X509v3 Key Usage | Sí | Digital Signature<br>Content Commitment<br>Key Encipherment |
| X509v3 Extended Key Usage | - | Email protection<br>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<br>Access Location: <URI de acceso al servicio OCSP><br>Access Method: Id-ad-calssuers<br>Access Location: <URI del certificado de la EC emisora> |

| | | |
|---|---|---|
| X509v3 CRL Distribution Points | - | http://epscd.catcert.net/crl/ec-sectorpublic.crl |
| Qualified Certificate Statements | Sí | Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1<br>Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 anys<br>Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: https://www.aoc.cat/catcert/pds_en<br>Id-etsi- qcs-QcType-eseal 0.4.0.1862.1.6.2 |
| X509v3 Certificate Policies | - | <OID de la política de certificación correspondiente al certificado><br>1.3.6.1.4.1.15096.1.3.2.91.1<br><br><URI de la DPC><br>User Notice: "Certificat d'aplicació. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A"<br><br>< OID "for EU qualified certificates issued to legal persons" según ETSI EN 319 411-2: QCP-l> 0.4.0.194112.1.1 |
| X509v3 Subject Alternative Name | - | rfc822Name: mail de contacto (opcional) |

# PERFIL DE LOS CERTIFICADOS CDS-1_SENM

## Certificado

| Campo del DN | Valor | Descripción |
|---|---|---|
| CN, Common Name | Nombre | Denominación de nombre de dominio donde residirá el certificado<br>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 | *"Certificat de seu electrònica nivell mig"* |
| OU, Organizational Unit | Unidad en la organización | *El nombre descriptivo de la sede* |
| SN, SerialNumber | CIF | *Contendrá el NIF de la entidad responsable de la sede electrónica* |
| OrganizationIdentifier | | Identificador de la organización<br>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<br>1.3.6.1.4.1.311.60.2.1.3 | País | Subject Jurisdiction of Incorporation or Registration<br>*C=ES* |
| L, Locality | Municipio | Ciudad |
| S, State or Province | Provincia | Provincia |

## 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<br>Key Encipherment |
| X509v3 Extended Key Usage | - | Autenticación TLS web Server |
| X509v3 Basic Constraints | Sí | CA:FALSE |
| X509v3 CRL Distribution Points | - | http://epscd.catcert.net/crl/ec-sectorpublic.crl |
| X509v3 Authority Information Access | - | Access Method: Id-ad-ocsp<br>Access Location: <URI de acceso al servicio OCSP><br>Access Method: Id-ad-caIssuers<br>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<br><br><URI de la DPC><br>User Notice: "Certificat de seu electrònica de nivell mig. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A"<br><br><OID asociado a los certificados de sede de nivel medio / sustancial><br>2.16.724.1.3.5.5.2<br><br><OID ETSI QCP-w> 0.4.0.194112.1.4 |
| Qualified Certificate Statements | | Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1<br>Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 años<br>Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: https://www.aoc.cat/catcert/pds_en<br>Id-etsi- qcs-QcType-web 0.4.0.1862.1.6.3 |
| X509v3 Subject Alternative Name | - | dNSName: nombre de dominio donde residirá el certificado |

# PERFIL DE LOS CERTIFICADOS CDS-1

## Certificado

| Camp del DN | Valor | Descripció |
|---|---|---|
| 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 |
| OrganizationIdentifier | | Identificador de la organización<br><br>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.<br>Por defecto “ES”.<br>(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.

## 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.<br>Para certificados multidominio, la URL serguirá el formato “*.dominio.com” o la IP (esta indicación está prohibida para certificados EV) |
| X509v3 Basic Constraints | Sí | CA:FALSE |
| X509v3 Key Usage | Sí | Digital Signature<br>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)<br>Access Location 1: <URI de acceso al servicio OCSP><br>Access Method 2: id-ad-caissuers (1.3.6.1.5.5.7.48.2)<br>Access Location 2: <URI del certificado de la EC emisora> |
| X509v3 CRL Distribution Points | - | http://epscd.catcert.net/crl/ec-sectorpublic.crl |
| X509v3 Certificate Policies | - | <OID de la política de certificación corresponent al certificado><br>1.3.6.1.4.1.15096.1.3.2.51.1<br><br><URI de la CPS><br>User Notice: “Certificat de dispositiu SSL. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A” |
| X509v3 Subject Alternative Name | - | dNSName: nombre de dominio donde residirá el certificado |

# PERFIL DE LOS CERTIFICADOS CDSQ-1

## Certificado

| Camp del DN | Valor | Descripción |
|---|---|---|
| CN, Common Name | Nombre | (EVG 9.2.3) Nombre de un único dominio.<br>(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 |
| SN, SerialNumber | CIF | CIF de la Organización suscriptora del certificado<br>(EVG 9.2.6) Registration Number |
| OrganizationIdentifier | | Identificador de la organización<br>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.<br>Por defecto "ES".(EVG 9.2.7) Country (required)<br>(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>(BR. 7.1.4.2.2.e) Indicación requerida al existir el campo Organization (O) |
| jurisdictionCountryName<br>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 Requeriments 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.

# 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<br>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 | - | http://epscd.catcert.net/crl/ec-sectorpublic.crl |
| X509v3 Authority Information Access | - | Access Method: Id-ad-ocsp<br>Access Location: <URI de acceso al servicio OCSP><br>Access Method: Id-ad-calssuers<br>Access Location: <URI del certificado de la EC emisora> |
| X509v3 Certificate Policies | - | <OID asociado a la DPC> 1.3.6.1.4.1.15096.1.3.2.51.2<br><br><URI de la DPC><br>User Notice: “Certificat de dispositiu SSL EV. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A”<br><br><OID ETSI QCP-w> 0.4.0.194112.1.4 |
| Qualified Certificate Statements | | Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1<br>Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 años<br>Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: https://www.aoc.cat/catcert/pds_en<br>Id-etsi- qcs-QcType-web 0.4.0.1862.1.6.3 |
| X509v3 Subject Alternative Name | - | dNSName: nombre de dominio donde residirá el certificado |

# PERFIL DE LOS CERTIFICADOS CPI-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 incluir el cargo de la persona física, que la vincula con la administración, organismo o entidad de derecho público suscriptora 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[1] |
| Surname | Apeliidos (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 acuerda 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 tècnica ETSI EN 319 412-1 (VATES + NIF de la entidad) |

[1] SerialNumber = p. ej: IDCES-00000000G. 3 carácteres 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

## 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<br>Access Location: <URI de acceso al servicio OCSP><br>Access Method: Id-ad-caIssuers<br>Access Location: <URI del certificado de la EC emisora> |
| X509v3 CRL Distribution Points | - | http://epscd.catcert.net/crl/ec-sectorpublic.crl |
| X509v3 Key Usage | Sí | Digital Signature<br>Key encipherment |
| X509v3 Extended Key Usage | | Email protection<br>Client Authentication<br>SmartCardLogon |
| X509v3 Certificate Policies | - | <OID asociado a la DPC> 1: 1.3.6.1.4.1.15096.1.3.2.7.1.2<br><URI de la DPC><br><User Notice><br>" Certificat electrònic de treballador públic de nivell alt d'autenticació . Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A"<br><OID de la política de certificación de empleado público de nivel alto> 2.16.724.1.3.5.7.1<br><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<br>(opcional) otherName-userPrincipalName (UPN): Usuario en el dominio Windows del poseedor de claves<br>directoryName:<br>OID: 2.16.724.1.3.5.7.1.1 =<br>"Certificat electrònic de treballador públic de nivell alt d'autenticació"<br>OID: 2.16.724.1.3.5.7.1.2 = <O del DN><br>OID: 2.16.724.1.3.5.7.1.3 = <CIF de la entidad suscriptora><br>OID: 2.16.724.1.3.5.7.1.4 = <serialNumber del DN><br>OID: 2.16.724.1.3.5.7.1.6 = <Given name><br>OID: 2.16.724.1.3.5.7.1.7 = <Primer apellido del empleado público><br>OID: 2.16.724.1.3.5.7.1.8 = <Segundo apellido del empleado público> |

# PERFIL DE LOS CERTIFICADOS CPISA-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.<br>. |
| OU, Organization Unit | Unidad en 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. |
| SN, Serial Number | NIF | Número del documento de identidad del firmante, con la semántica propuesta por la norma ETSI EN 319 412-1[2] |
| Surname | Apellidos (persona física) | Primer i segon 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) |

[2] 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

# 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<br>Access Location: <URI de acceso al servicio OCSP><br>Access Method: Id-ad-calssuers<br>Access Location: <URI del certificado de la EC emisora> |
| X509v3 CRL Distribution Points | - | http://epscd.catcert.net/crl/ec-sectorpublic.crl |
| X509v3 Key Usage | Sí | Digital Signature<br>Content Commitment<br>Key Encipherment |
| X509v3 Extended Key Usage | | Email protection<br>Client Authentication |
| X509v3 Certificate Policies | - | <OID de la DPC> 1.3.6.1.4.1.15096.1.3.2.7.3.1<br><br><URI de la DPC><br><User Notice><br>Certificat electrònic de treballador públic de nivell mig. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A"<br><br><OID que indica certificado de empleado público de nivel medio><br>2.16.724.1.3.5.7.2<br><br><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<br>Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 años<br>Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: https://www.aoc.cat/catcert/pds_en<br>Id-etsi- qcs-QcType-esign 0.4.0.1862.1.6.1 |

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

# PERFIL DE LOS CERTIFICADOS CPISA-2

## 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. |
| SN, Serial Number | NIF | Número del documento de identidad del firmante, con la semántica propuesta por la norma ETSI EN 319 412-1[3] |
| 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) |

[3] 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

# 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<br>Access Location: <URI de acceso al servicio OCSP><br>Access Method: Id-ad-calssuers<br>Access Location: <URI del certificado de la EC emisora> |
| X509v3 CRL Distribution Points | - | http://epscd.catcert.net/crl/ec-sectorpublic.crl |
| X509v3 Key Usage | Sí | Digital Signature<br>Content Commitment<br>Key encipherment |
| X509v3 Extended Key Usage | | Email protection<br>Client Authentication |
| X509v3 Certificate Policies | - | <OID de la DPC> 1.3.6.1.4.1.15096.1.3.2.86.1<br><URI de la DPC><br><User Notice><br>" Certificat electrònic de persona vinculada de nivell mig. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A"<br><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<br>Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 años<br>Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: https://www.aoc.cat/catcert/pds_en<br>Id-etsi- qcs-QcType-esign 0.4.0.1862.1.6.1 |
| X509v3 Subject Alternative Name | - | rfc822Name: mail de contacto (Opcional) |

# PERFIL DE LOS CERTIFICADOS CPISQ-2

## 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 | Unitat a l’organització | “Persona vinculada de nivell alt” |
| Title (opcional) | Càrrec | Ha de incluir el cargo de la persona física, que lo vincula con la administración, organismo o entidad de derecho público suscriptora del certificado. |
| SN, Serial Number | NIF | NIF o NIE del empleado público.<br>Preferiblemente se aplicará la semántica propuesta por la norma ETSI EN 319 412-1[4] |
| 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) |

[4] 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

# 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<br>Access Location: <URI de acceso al servicio OCSP><br>Access Method: Id-ad-calssuers<br>Access Location: <URI del certificado de la EC emisora> |
| X509v3 CRL Distribution Points | - | http://epscd.catcert.net/crl/ec-sectorpublic.crl |
| Qualified Certificate Statements | Sí | Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1<br>Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 anys<br>Id-etsi- qcs-QcSSCD 0.4.0.1862.1.4<br>Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: https://www.aoc.cat/catcert/pds_en<br>Id-etsi- qcs-QcType 0.4.0.1862.1.6.1 |
| X509v3 Key Usage | Sí | Digital Signature<br>Content Commitment<br>Key encipherment |
| X509v3 Extended Key Usage | | Email protection<br>Client Authentication<br>SmartCardLogon |
| X509v3 Certificate Policies | - | <OID associat a la DPC> 1.3.6.1.4.1.15096.1.3.2.82.1<br><br><URI de la DPC><br>User Notice: “Certificat electrònic de persona vinculada de nivell alt.<br>Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A”<br><br><OID de la política de certificación ETSI: QCP-n-qscd> 0.4.0.194112.1.2 |
| X509v3 Subject Alternative Name | - | (opcional per SMIME) rfc822Name: mail de contacte<br><br>(opcional) otherName-userPrincipalName (UPN): Usuario en el dominio Windows del poseedor de claus |

# PERFIL DE LOS CERTIFICADOS CPPI-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 amb pseudònim de nivell alt d'autenticació” |
| Pseudonym | Pseudónimo<br>Obligatorio según ETSI EN 319 412-2 | Ej: NIP 111111111 |
| CN, Common Name | Informar con el pseudónimo del organismo | Pseudonym + “ - “ + Title + (AUT)<br>Ex: NIP 11111111 - SUBINSPECTOR (AUT) |
| C, Country | País | C = “ES” |

# 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 clau pública del certificat de la CA, obtingut a partir del hash de la misma> |
| X509v3 Authority Information Access | - | Access Method: Id-ad-ocsp<br>Access Location: <URI de acceso al servicio OCSP><br>Access Method: Id-ad-caIssuers<br>Access Location: < URL de localización del certificado de la CA.> |
| X509v3 CRL Distribution Points | - | http://epscd.catcert.net/crl/ec-sectorpublic.crl |
| X509v3 Key Usage | Sí | Digital Signature<br>Key encipherment |
| X509v3 Extended Key Usage | | Email Protection<br>Client Authentication<br>SmartCardLogon |
| X509v3 Certificate Policies | - | <OID associat a la DPC> 1.3.6.1.4.1.15096.1.3.2.4.1.2<br><br><URI de la DPC><br>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"<br><br><OID asociado a certificado de empleado público con pseudónimo de nivel alto> 2.16.724.1.3.5.4.1<br><br><OID de la política de certificación ETSI: NCP+> 0.4.0.2042.1.2[5] |
| X509v3 Subject Alternative Name | - | (opcional) otherName-userPrincipalName (UPN): Usuari en el dominio Windows del poseedor de claves<br><br>directoryName:<br>OID: 2.16.724.1.3.5.4.1.1 = " Certificat electrònic de treballador públic amb pseudònim de nivell alt d'autenticació"<br>OID: 2.16.724.1.3.5.4.1.2 = <O del DN><br>OID: 2.16.724.1.3.5.4.1.3 = <CIF de la entidad suscriptora> |

5

# PERFIL DE LOS CERTIFICADOS CPPSQ-1

## Certificado

| Campo del DN | Nom | 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<br>Obligatorio según ETSI EN 319 412-2 | Ex: NIP 111111111 |
| CN, Common Name | Informar con el pseudónimo del organismo | Pseudonym + “ - “ + Title + (SIG)<br>Ex: NIP 11111111 – SUBINSPECTOR (SIG) |
| C, Country | País | C = “ES” |

# 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<br>Access Location: <URI de acceso al servicio OCSP><br>Access Method: Id-ad-calssuers<br>Access Location: < URL de localización del certificado de la CA.> |
| X509v3 CRL Distribution Points | - | http://epscd.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<br><URI de la DPC><br>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"<br><OID asociado a certificado de empleado público con pseudónimo de nivel alto> 2.16.724.1.3.5.4.1<br><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<br>Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 años<br>Id-etsi- qcs-QcSSCD 0.4.0.1862.1.4<br>Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: https://www.aoc.cat/catcert/pds_en<br>Id-etsi- qcs-QcType-esign 0.4.0.1862.1.6.1 |
| X509v3 Key Usage | Sí | Content Commitment |
| X509v3 Subject Alternative Name | - | directoryName:<br>OID: 2.16.724.1.3.5.4.1.1 = "Certificat qualificat de signatura de treballador públic amb pseudònim de nivell alt"<br>OID: 2.16.724.1.3.5.4.1.2 = <O del DN><br>OID: 2.16.724.1.3.5.4.1.3 = <CIF de la entidad suscriptora> |

# PERFIL DE LOS CERTIFICADOS CPRISQ-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" |
| SN, Serial Number | NIF | Número del documento de identidad del empleado público con la semántica propuesta por la norma ETSI EN 319 412-1[6] |
| 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.<br>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<br><br>Notario: Nombre Apellido1 Apellido2 /Núm Protocolo: XXX /Fecha Otorgamiento: dd-mm-aaaa<br><br>En Boletines o Diarios Oficiales: Boletín: XXX /Fecha: dd-mm-aaaa /Número resolución: XXX |

## Common name

| Campo | Contenido | Ejemplo | Tamaño(*) |
|---|---|---|---|
| NIF | Número DNI/NIE | 12345678Z | 10 |

[6] 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

| | | | |
|---|---|---|---|
| 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

## 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<br>Access Location: <URI de acceso al servicio OCSP><br>Access Method: Id-ad-calssuers<br>Access Location: <URI del certificado de la EC emisora> |
| X509v3 CRL Distribution Points | - | http://epscd.catcert.net/crl/ec-sectorpublic.crl |
| X509v3 Certificate Policies | - | <OID de la política de certificación correspondiente al certificado><br>1.3.6.1.4.1.15096.1.3.2.8.1.1<br><br><URI de la DPC><br>User Notice: “Certificat electrònic de representant davant les AAPP de nivell alt. Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A”<br><br><OID de certificado de representante de persona jurídica><br>2.16.724.1.3.5.8<br><br><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<br>Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 años<br>Id-etsi- qcs-QcSSCD 0.4.0.1862.1.4<br>Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: https://www.aoc.cat/catcert/pds_en<br>Id-etsi- qcs-QcType-esign 0.4.0.1862.1.6.1 |
| X509v3 Key Usage | Sí | Digital Signature<br>Content Commitment<br>Key encipherment |
| X509v3 Extended Key Usage | | Email protection<br>Client Authentication<br>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 |

# PERFIL DE LOS CERTIFICADOS CPSQ-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 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. |
| SN, Serial Number | NIF | Número del documento de identidad del empleado público con la semántica propuesta por la norma ETSI EN 319 412-1[7] |
| 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 | Nom i 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) |

[7] 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

# 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<br>Access Location: <URI de acceso al servicio OCSP><br>Access Method: Id-ad-calssuers<br>Access Location: <URI del certificado de la EC emisora> |
| X509v3 CRL Distribution Points | - | http://epscd.catcert.net/crl/ec-sectorpublic.crl |
| Qualified Certificate Statements | Sí | Id-etsi- qcs-QcCompliance 0.4.0.1862.1.1<br>Id-etsi- qcs-QcRetentionPeriod 0.4.0.1862.1.3: 15 años<br>Id-etsi- qcs-QcSSCD 0.4.0.1862.1.4<br>Id-etsi- qcs-QcPDS 0.4.0.1862.1.5: https://www.aoc.cat/catcert/pds_en<br>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<br><br><URI de la DPC><br>User Notice: " Certificat qualificat de signatura de treballador públic de nivell alt . Adreça i NIF del prestador: Via Laietana 26 08003 Barcelona Q0801175A"<br><br><OID asociado a certificado de empleado público de nivel alto> 2.16.724.1.3.5.7.1<br><br><OID de la política de certificación ETSI: QCP-n-qscd> 0.4.0.194112.1.2 |
| X509v3 Subject Alternative Name | - | directoryName:<br>OID: 2.16.724.1.3.5.7.1.1 ="Certificat qualificat de signatura de treballador públic de nivell alt "<br>OID: 2.16.724.1.3.5.7.1.2 = <O del DN><br>OID: 2.16.724.1.3.5.7.1.3 = <CIF de la entidad suscriptora><br>OID: 2.16.724.1.3.5.7.1.4 = <serialNumber del DN><br>OID: 2.16.724.1.3.5.7.1.6 = <Given name><br>OID: 2.16.724.1.3.5.7.1.7 = <Primer apellido del empleado público><br>OID: 2.16.724.1.3.5.7.1.8 = <Segundo apellido del empleado público> |