

# Izenpe

## Perfiles de Certificados de Entidad Final

| Fecha      | Versión | Autor | Estado   |
|------------|---------|-------|--|
| 01/12/2016 | 1.0     |       | *Adaptación de todos los perfiles a EIDAS: personas físicas, personas jurídicas y ssl                      |
| 27/04/2017 | 1.1     |       | *Corrección de algunos perfiles y añadir los nuevos certificados en HSM                                    |
| 13/03/2018 | 1.2     |       | *Correcciones menores  |
| 21/03/2018 | 1.3     |       | *Se añade uso clave smartCardLogon a pep_qc_scared   |
| 25/04/2018 | 2       |       | *Revisión total. Quitamos los perfiles EPSOS, Sede Medio.  |
| 28/03/2019 | 2.1     |       | *Se añade certificado Dispositivo  |
| 17/05/2019 | 2.2     |       | *Se elimina campo C y OU del campo Subject del perfil DV   |
| 18/06/2019 | 2.3     |       | *Se corrige perfil SSL Cualificado   |
| 19/06/2019 | 2.4     |       | *Se actualiza el perfil de Sede EV   |
| 04/11/2019 | 2.5     |       | *Se añade perfil Ciudadano Seudónimo   |
| 04/06/2020 | 3.0     |       | *Se crea indice, se corrigen errores menores, y se quita nombre aplicación                                 |
| 18/03/2022 | 4.2     |       | * Se quita el QcSSCD de los perfiles ciudadano tarjeta, representante/spj tarjeta                          |
| 01/04/2022 | 4.4     |       | * Se cambia la duración de los certificados SMIME de 4 a 3 años  |
| 05/04/2022 | 4,5     |       | * Se modifica el perfil de Seudónimo para quitar el mail y EKU emailprotection                             |
| 01/09/2022 | 4.6     |       | * Se quita el QcSSCD del perfil de firma de seudónimo  |
| 27/04/2023 | 4.7     |       | * Se modifican los perfiles SSL para eliminar de su EKU el emailProtection                                 |
| 26/01/2024 | 4.8     |       | * Se elimina el UserNotice de los perfiles SSL   |
| 02/10/2024 | 5.0     |       | * Se añaden nuevos perfiles de SSL 2024 y Seudónimo Software   |
| 12/11/2024 | 6.0     |       | * Se eliminan todos los perfiles de la jerarquía QC de 2020  |
| 23/05/2025 | 7.0     |       | * Se modifica el endpoint del CPS en los perfiles SSL  |
| 03/10/2025 | 8.0     |       | * Se modifica el tamaño de clave de los certificados y se incluyen los perfiles de la nueva jerarquía 2025 |
| 20/11/2025 | 8.1     |       | * Se modifica el tamaño de clave de los certificados SSL para indicar tamaño mínimo 2048bits               |

## Estructura del documento

### Versión 8.1

Este documento describe los perfiles de certificados de entidad final de Izenpe. Cada perfil está descrito en una hoja independiente que especifica:

**CA emisora** del perfil

**Nombre del perfil** en la aplicación

**Campos y extensiones** incluidos en el perfil, así como su contenido

Este documento está en formato EXCEL. Para facilitar la gestión de las diferentes versiones de este documento, se convertirá a PDF cada vez que se emita una nueva versión.

# Izenpe

## Perfiles de Certificados de Entidad Final

### Indice

[Ciudadano Cualificado Tarjeta](#)  
[B@KQ](#)  
[B@K](#)  
[Izenpe Mobile](#)  
[Autónomo No Cualificado](#)  
[Profesional Cualificado Tarjeta](#)  
[Profesional Cualificado Software](#)  
[Profesional Cualificado HSM](#)  
[Corporativo Privado Reconocido](#)  
[Corporativo Privado](#)  
[Corporativo Reconocido](#)  
[Corporativo](#)  
[Corporativo Reconocido en HW](#)  
[Funcionario Cualificado Tarjeta](#)  
[Funcionario Cualificado Software](#)  
[Funcionario Cualificado HSM](#)  
[Personal Entidades Públicas](#)  
[PeP Seudónimo Tarjeta Firma](#)  
[PeP Seudónimo Tarjeta Autenticación](#)  
[PeP Seudónimo Tarjeta Cifrado](#)  
[Pep Seudónimo Software](#)  
[Representante Entidad Tarjeta](#)  
[Representante Entidad Tarjeta SSCD](#)  
[Representante Entidad HSM](#)  
[Representante Entidad Software](#)  
[Representante Entidad SPJ Tarjeta](#)  
[Representante Entidad SPJ Tarjeta SSCD](#)  
[Representante Entidad SPJ HSM](#)  
[Representante Entidad SPJ Software](#)  
[Sello Entidad](#)  
[Sello Entidad HSM](#)  
[Aplicación](#)  
[Firma de código](#)  
[Dispositivo](#)  
[SSL DV](#)  
[SSL DV 2024](#)  
[SSL OV](#)  
[SSL OV 2024](#)  
[SSL Cualificado](#)  
[SSL Cualificado 2024](#)  
[Sede Cualificado nivel medio](#)  
[Sello nivel medio](#)  
[Sello nivel medio HSM](#)  
[Sello nivel alto](#)  
[Ciudadano Cualificado Tarjeta 2025](#)  
[B@KQ 2025](#)  
[Profesional Cualificado Tarjeta 2025](#)  
[Profesional Cualificado Software 2025](#)  
[Profesional Cualificado HSM 2025](#)  
[Funcionario Cualificado Tarjeta 2025](#)  
[Funcionario Cualificado Software 2025](#)  
[Funcionario Cualificado HSM 2025](#)  
[PeP Seudónimo Tarjeta Firma 2025](#)  
[PeP Seudónimo Tarjeta Autenticación 2025](#)  
[PeP Seudónimo Tarjeta Cifrado 2025](#)  
[Pep Seudónimo Software 2025](#)  
[Representante Entidad Tarjeta 2025](#)  
[Representante Entidad Tarjeta SSCD 2025](#)  
[Representante Entidad HSM 2025](#)  
[Representante Entidad Software 2025](#)  
[Representante Entidad SPJ Tarjeta 2025](#)  
[Representante Entidad SPJ Tarjeta SSCD 2025](#)  
[Representante Entidad SPJ HSM 2025](#)  
[Representante Entidad SPJ Software 2025](#)  
[Sello Entidad 2025](#)  
[Sello Entidad HSM 2025](#)  
[Sello nivel medio 2025](#)  
[Sello nivel medio HSM 2025](#)  
[Sello nivel alto 2025](#)

## Ciudadano

**CA emisora**

CCEER

**Nombre**

ciudadano\_qc\_scard

| Campo / extensión                 | Opcional / Crítica | Contenido  |
|-----------------------------------|--------------------|--|
| <b>version</b>                    |                    | Versión 3  |
| <b>serialNumber</b>               |                    | Número secuencial único  |
| <b>signature</b>                  |                    | sha256WithRSAEncryption  |
| <b>issuer</b>                     |                    | Igual al campo subject del certificado de la CA emisora  |
| <b>validity</b>                   |                    | 4 años   |
| <b>subject</b>                    |                    |  |
| serialNumber                      |                    | DNI / NIE / NIF / PASS   |
| SN                                |                    | Apellidos  |
| G                                 |                    | Nombre   |
| CN                                |                    | Nombre y Apellidos   |
| OU                                |                    | Herritar ziurtagiria - Certificado de ciudadano  |
| C                                 |                    | País (codificado según ISO 3166-1 alpha 2 code)  |
| <b>subjectPublicKeyInfo</b>       |                    | RSA 3072 bits mínimo   |
| <b>extensions</b>                 |                    |  |
| <b>issuerAltName</b>              |                    | Igual a la extensión subjectAltName del certificado de la CA emisora   |
| <b>subjectAltName</b>             |                    |  |
| directoryName                     |                    |  |
| 1.3.6.1.4.1.14777.0.1             |                    | Nombre   |
| 1.3.6.1.4.1.14777.0.2             |                    | Primer Apellido  |
| 1.3.6.1.4.1.14777.0.3             | Opcional           | Segundo Apellido   |
| 1.3.6.1.4.1.14777.0.4             |                    | DNI / NIE / NIF / PASS   |
| <b>extendedKeyUsage</b>           |                    | clientAuth, documentSigning  |
| <b>subjectKeyIdentifier</b>       |                    | Identificador de la clave pública  |
| <b>authorityKeyIdentifier</b>     |                    | Incluir sólo campo keyIdentifier   |
| <b>certificatePolicies</b>        |                    |  |
| policyIdentifier                  |                    | 1.3.6.1.4.1.14777.2.18.1   |
| cpsURI                            |                    | <a href="http://www.izenpe.eus/cps">http://www.izenpe.eus/cps</a>  |
| userNotice                        |                    | Konsulta <a href="http://www.izenpe.eus">www.izenpe.eus</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.eus">www.izenpe.eus</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier                  |                    | 0.4.0.194112.1.0 (QCP-n)   |
| <b>cRLDistributionPoints</b>      |                    | <a href="http://crl.izenpe.com/cgi-bin/crl2">http://crl.izenpe.com/cgi-bin/crl2</a>  |
| <b>authorityInfoAccess</b>        |                    |  |
| ocsp                              |                    | <a href="http://ocsp.izenpe.com">http://ocsp.izenpe.com</a>  |
| CA emisora                        |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crt</a>  |
| <b>subjectDirectoryAttributes</b> |                    |  |
| dateOfBirth                       |                    | Fecha de nacimiento  |
| <b>qcStatements</b>               |                    |  |
| QcCompliance                      |                    | Presente   |
| QcType                            |                    | id-etsi-qct-esign  |
| QcRetentiodPeriod                 |                    | 15 años  |
| QcPDS                             |                    | <a href="https://www.izenpe.eus/pds/en/">https://www.izenpe.eus/pds/en/</a> en<br><a href="https://www.izenpe.eus/pds/eu/">https://www.izenpe.eus/pds/eu/</a> eu<br><a href="https://www.izenpe.eus/pds/es/">https://www.izenpe.eus/pds/es/</a> es                           |
| <b>keyUsage</b>                   | Crítica            | digitalSignature, nonRepudiation, keyEncipherment  |

# Ciudadano

CA emisora

CCEER

Nombre

ciudadano\_qc\_hsm

| Campo / extensión                 | Opcional / Crítica | Contenido   |
|-----------------------------------|--------------------|---|
| <b>version</b>                    |                    | Versión 3   |
| <b>serialNumber</b>               |                    | Número secuencial único   |
| <b>signature</b>                  |                    | sha256WithRSAEncryption   |
| <b>issuer</b>                     |                    | Igual al campo subject del certificado de la CA emisora   |
| <b>validity</b>                   |                    | 4 años  |
| <b>subject</b>                    |                    |   |
| serialNumber                      |                    | DNI / NIE / NIF / PASS  |
| SN                                |                    | Apellidos   |
| G                                 |                    | Nombre  |
| CN                                |                    | Nombre y Apellidos  |
| OU                                |                    | Herritar ziurtagiria - Certificado de ciudadano   |
| C                                 |                    | País (codificado según ISO 3166-1 alpha 2 code)   |
| <b>subjectPublicKeyInfo</b>       |                    | RSA 3072 bits mínimo  |
| <b>extensions</b>                 |                    |   |
| <b>issuerAltName</b>              |                    | Igual a la extensión subjectAltName del certificado de la CA emisora  |
| <b>subjectAltName</b>             |                    |   |
| directoryName                     |                    |   |
| 1.3.6.1.4.1.14777.0.1             |                    | Nombre  |
| 1.3.6.1.4.1.14777.0.2             |                    | Primer Apellido   |
| 1.3.6.1.4.1.14777.0.3             | Opcional           | Segundo Apellido  |
| 1.3.6.1.4.1.14777.0.4             |                    | DNI / NIE / NIF / PASS  |
| 1.3.6.1.4.1.14777.0.7             | Opcional           | Email del suscriptor  |
| <b>extendedKeyUsage</b>           |                    | clientAuth, documentSigning   |
| <b>subjectKeyIdentifier</b>       |                    | Identificador de la clave pública   |
| <b>authorityKeyIdentifier</b>     |                    | Incluir sólo campo keyIdentifier  |
| <b>certificatePolicies</b>        |                    |   |
| policyIdentifier                  |                    | 1.3.6.1.4.1.14777.2.18.3  |
| cpsURI                            |                    | <a href="http://www.izenpe.eus/cps">http://www.izenpe.eus/cps</a>   |
| userNotice                        |                    | Kontsulta <a href="http://www.izenpe.eus">www.izenpe.eus</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.eus">www.izenpe.eus</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier                  |                    | 0.4.0.194112.1.0 (QCP-n)  |
| <b>cRLDistributionPoints</b>      |                    | <a href="http://crl.izenpe.com/cgi-bin/crl2">http://crl.izenpe.com/cgi-bin/crl2</a>   |
| <b>authorityInfoAccess</b>        |                    |   |
| ocsp                              |                    | <a href="http://ocsp.izenpe.com">http://ocsp.izenpe.com</a>   |
| CA emisora                        |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crt</a>   |
| <b>subjectDirectoryAttributes</b> |                    |   |
| dateOfBirth                       |                    | Fecha de nacimiento   |
| <b>qcStatements</b>               |                    |   |
| QcCompliance                      |                    | Presente  |
| QcType                            |                    | id-etsi-qct-esign   |
| QcRetentiodPeriod                 |                    | 15 años   |
| QcPDS                             |                    | <a href="https://www.izenpe.eus/pds/en/en">https://www.izenpe.eus/pds/en/en</a><br><a href="https://www.izenpe.eus/pds/eu/eu">https://www.izenpe.eus/pds/eu/eu</a><br><a href="https://www.izenpe.eus/pds/es/es">https://www.izenpe.eus/pds/es/es</a>                         |
| <b>keyUsage</b>                   | Crítica            | digitalSignature, nonRepudiation, keyEncipherment   |

## Ciudadano No Reconocido

CA emisora

CCEENR

Nombre

ciudadano\_nqc

| Campo / extensión                 | Opcional / Crítica | Contenido   |
|-----------------------------------|--------------------|---|
| <b>version</b>                    |                    | Versión 3   |
| <b>serialNumber</b>               |                    | Número secuencial único   |
| <b>signature</b>                  |                    | sha256WithRSAEncryption   |
| <b>issuer</b>                     |                    | Igual al campo subject del certificado de la CA emisora   |
| <b>validity</b>                   |                    | 4 años  |
| <b>subject</b>                    |                    |   |
| serialNumber                      |                    | DNI / NIE   |
| SN                                |                    | Primer Apellido   |
| G                                 |                    | Nombre  |
| CN                                |                    | Nombre y Apellidos  |
| OU                                |                    | Herritar ziurtagiria - Certificado de ciudadano   |
| OU                                |                    | Ziurtagiri ez onartua - Certificado no cualificado  |
| C                                 |                    | ES  |
| <b>subjectPublicKeyInfo</b>       |                    | RSA 3072 bits mínimo  |
| <b>extensions</b>                 |                    |   |
| <b>issuerAltName</b>              |                    | Igual a la extensión subjectAltName del certificado de la CA emisora  |
| <b>extendedKeyUsage</b>           |                    | clientAuth, documentSigning   |
| <b>subjectKeyIdentifier</b>       |                    | Identificador de la clave pública   |
| <b>authorityKeyIdentifier</b>     |                    | Incluir sólo campo keyIdentifier  |
| <b>certificatePolicies</b>        |                    |   |
| policyIdentifier                  |                    | 1.3.6.1.4.1.14777.5.2.5   |
| cpsURI                            |                    | <a href="http://www.izenpe.com/cps">http://www.izenpe.com/cps</a>   |
| userNotice                        |                    | Kontsulta <a href="http://www.izenpe.com">www.izenpe.com</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.com">www.izenpe.com</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| <b>cRLDistributionPoints</b>      |                    | <a href="http://crl.izenpe.com/cgi-bin/crlscinr2">http://crl.izenpe.com/cgi-bin/crlscinr2</a>   |
| <b>authorityInfoAccess</b>        |                    | ocsp <a href="http://ocsp.izenpe.com">http://ocsp.izenpe.com</a>  |
| <b>subjectDirectoryAttributes</b> |                    |   |
| dateOfBirth                       |                    | Fecha de nacimiento   |
| <b>keyUsage</b>                   | Crítica            | digitalSignature, nonRepudiation, keyEncipherment   |

## Ciudadano No Reconocido

CA emisora

CCEENR

Nombre

ciudadano\_mobile

| Campo / extensión                 | Opcional / Crítica | Contenido   |
|-----------------------------------|--------------------|---|
| <b>version</b>                    |                    | Versión 3   |
| <b>serialNumber</b>               |                    | Número secuencial único   |
| <b>signature</b>                  |                    | sha256WithRSAEncryption   |
| <b>issuer</b>                     |                    | Igual al campo subject del certificado de la CA emisora   |
| <b>validity</b>                   |                    | 4 años  |
| <b>subject</b>                    |                    |   |
| serialNumber                      |                    | DNI / NIE   |
| SN                                |                    | Primer Apellido   |
| G                                 |                    | Nombre  |
| CN                                |                    | Nombre y Apellidos  |
| OU                                |                    | Herritar ziurtagiria - Certificado de ciudadano   |
| C                                 |                    | ES  |
| <b>subjectPublicKeyInfo</b>       |                    | CE 256 bits   |
| <b>extensions</b>                 |                    |   |
| <b>issuerAltName</b>              |                    | Igual a la extensión subjectAltName del certificado de la CA emisora  |
| <b>extendedKeyUsage</b>           |                    | clientAuth, documentSigning   |
| <b>subjectKeyIdentifier</b>       |                    | Identificador de la clave pública   |
| <b>authorityKeyIdentifier</b>     |                    | Incluir sólo campo keyIdentifier  |
| <b>certificatePolicies</b>        |                    |   |
| policyIdentifier                  |                    | 1.3.6.1.4.1.14777.5.2.5.4   |
| cpsURI                            |                    | <a href="http://www.izenpe.com/cps">http://www.izenpe.com/cps</a>   |
| userNotice                        |                    | Kontsulta <a href="http://www.izenpe.com">www.izenpe.com</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.com">www.izenpe.com</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| <b>cRLDistributionPoints</b>      |                    | <a href="http://crl.izenpe.com/cgi-bin/crlscinr2">http://crl.izenpe.com/cgi-bin/crlscinr2</a>   |
| <b>authorityInfoAccess</b>        |                    | ocsp <a href="http://ocsp.izenpe.com">http://ocsp.izenpe.com</a>  |
| <b>subjectDirectoryAttributes</b> |                    |   |
| dateOfBirth                       |                    | Fecha de nacimiento   |
| <b>keyUsage</b>                   | Crítica            | digitalSignature, nonRepudiation, keyEncipherment   |

## Ciudadano No Reconocido

**CA emisora**

CCEENR

**Nombre**

ciudadano\_autonomo\_nqc\_sw

| Campo / extensión             | Opcional / Crítica | Contenido   |
|-------------------------------|--------------------|---|
| <b>version</b>                |                    | Versión 3   |
| <b>serialNumber</b>           |                    | Número secuencial único   |
| <b>signature</b>              |                    | sha256WithRSAEncryption   |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora   |
| <b>validity</b>               |                    | 4 años  |
| <b>subject</b>                |                    |   |
| serialNumber                  |                    | DNI / NIE   |
| SN                            |                    | Primer Apellido   |
| G                             |                    | Nombre  |
| CN                            |                    | Nombre y Apellidos  |
| OU                            |                    | Autonomo ziurtagiria - Certificado de autónomo  |
| C                             |                    | ES  |
| <b>subjectPublicKeyInfo</b>   |                    | RSA 3072 bits mínimo  |
| <b>extensions</b>             |                    |   |
| <b>issuerAltName</b>          |                    | Igual a la extensión subjectAltName del certificado de la CA emisora  |
| <b>extendedKeyUsage</b>       |                    | clientAuth, documentSigning   |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública   |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier  |
| <b>certificatePolicies</b>    |                    |   |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.5.2.7.2   |
| cpsURI                        |                    | <a href="http://www.izenpe.com/cps">http://www.izenpe.com/cps</a>   |
| userNotice                    |                    | Kontsulta <a href="http://www.izenpe.com">www.izenpe.com</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.com">www.izenpe.com</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.com/cgi-bin/crlscinr2">http://crl.izenpe.com/cgi-bin/crlscinr2</a>   |
| <b>authorityInfoAccess</b>    |                    |   |
| ocsp                          |                    | <a href="http://ocsp.izenpe.com">http://ocsp.izenpe.com</a>   |
| CA emisora                    |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEENR_cert_sha256.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEENR_cert_sha256.crt</a>   |
| <b>keyUsage</b>               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment   |

# Profesional

CA emisora

CCEER

Nombre

profesional\_qc\_scard

| Campo / extensión             | Opcional / Crítica | Contenido   |
|-------------------------------|--------------------|---|
| <b>version</b>                |                    | Versión 3   |
| <b>serialNumber</b>           |                    | Número secuencial único   |
| <b>signature</b>              |                    | sha256WithRSAEncryption   |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora   |
| <b>validity</b>               |                    | 3 años  |
| <b>subject</b>                |                    |   |
| serialNumber                  |                    | DNI / NIE / NIF / PASS  |
| SN                            |                    | Apellidos   |
| G                             |                    | Nombre  |
| CN                            |                    | Nombre Apellido1 Apellido 2 - DNI   |
| organizationIdentifier        |                    | 3 caracteres tipo-identidad + Country + - + identificador. Por ejemplo, si usaramos el CIF sería algo como: VATES-A01337260   |
| title                         | Opcional           | Cargo   |
| OU                            |                    | Ziurtagiri Profesionala - Certificado Profesional   |
| OU                            | Opcional           | Departamento  |
| OU                            | Opcional           | Grupo VPN   |
| O                             |                    | Organización  |
| C                             |                    | Pais (codificado según ISO 3166-1 alpha 2 code)   |
| <b>subjectPublicKeyInfo</b>   |                    | RSA 3072 bits mínimo  |
| <b>extensions</b>             |                    |   |
| <b>issuerAltName</b>          |                    | Igual a la extensión subjectAltName del certificado de la CA emisora  |
| <b>subjectAltName</b>         |                    |   |
| rfc822Name                    |                    | Email del suscriptor  |
| OtherName: UserPrincipalName  | Opcional           | Nombre principal de usuario   |
| directoryName                 |                    |   |
| 1.3.6.1.4.1.14777.0.1         |                    | Nombre  |
| 1.3.6.1.4.1.14777.0.2         |                    | Primer Apellido   |
| 1.3.6.1.4.1.14777.0.3         |                    | Segundo Apellido  |
| 1.3.6.1.4.1.14777.0.4         |                    | DNI / NIE / NIF / PASS  |
| 1.3.6.1.4.1.14777.0.5         |                    | Organización  |
| 1.3.6.1.4.1.14777.0.6         |                    | CIF   |
| 1.3.6.1.4.1.14777.0.7         |                    | Email del suscriptor  |
| 1.3.6.1.4.1.14777.0.8         | Opcional           | Cargo   |
| 1.3.6.1.4.1.14777.0.9         | Opcional           | Departamento  |
| <b>extendedKeyUsage</b>       |                    | clientAuth, emailProtection, smartCardLogon   |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública   |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier  |
| <b>certificatePolicies</b>    |                    |   |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.2.19.1  |
| cpsURI                        |                    | <a href="http://www.izenpe.eus/cps">http://www.izenpe.eus/cps</a>   |
| userNotice                    |                    | Kontsulta <a href="http://www.izenpe.eus">www.izenpe.eus</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.eus">www.izenpe.eus</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier              |                    | 0.4.0.194112.1.0 (QCP-n)  |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.com/cgi-bin/crl2">http://crl.izenpe.com/cgi-bin/crl2</a>   |
| <b>authorityInfoAccess</b>    |                    |   |
| ocsp                          |                    | <a href="http://ocsp.izenpe.com">http://ocsp.izenpe.com</a>   |
| CA emisora                    |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crl">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crl</a>   |
| <b>qcStatements</b>           |                    |   |
| QcCompliance                  |                    | Presente  |
| QcType                        |                    | id-etsi-qct-esign   |
| QcRetentiodPeriod             |                    | 15 años   |
| QcPDS                         |                    | <a href="https://www.izenpe.eus/pds/en/">https://www.izenpe.eus/pds/en/</a> en<br><a href="https://www.izenpe.eus/pds/eu/">https://www.izenpe.eus/pds/eu/</a> eu<br><a href="https://www.izenpe.eus/pds/es/">https://www.izenpe.eus/pds/es/</a> es                            |
| qcStatement-2                 |                    | 0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)  |
| <b>keyUsage</b>               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment   |

## Profesional

CA emisora

CCEER

Nombre

profesional\_qc\_sw

| Campo / extensión             | Opcional / Crítica | Contenido  |
|-------------------------------|--------------------|--|
| <b>version</b>                |                    | Versión 3  |
| <b>serialNumber</b>           |                    | Número secuencial único  |
| <b>signature</b>              |                    | sha256WithRSAEncryption  |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora  |
| <b>validity</b>               |                    | 3 años   |
| <b>subject</b>                |                    |  |
| serialNumber                  |                    | DNI / NIE / NIF / PASS   |
| SN                            |                    | Apellidos  |
| G                             |                    | Nombre   |
| CN                            |                    | Nombre Apellido1 Apellido 2 - DNI  |
| organizationIdentifier        |                    | 3 caracteres tipo-identidad + Country + - + identificador. Por ejemplo, si usamos el CIF sería algo como: VATES-A01337260  |
| title                         | Opcional           | Cargo  |
| OU                            |                    | Ziurtagiri Profesionala - Certificado Profesional  |
| OU                            | Opcional           | Departamento   |
| OU                            | Opcional           | Grupo VPN  |
| O                             |                    | Organización   |
| C                             |                    | País (codificado según ISO 3166-1 alpha 2 code)  |
| <b>subjectPublicKeyInfo</b>   |                    | RSA 3072 bits mínimo   |
| <b>extensions</b>             |                    |  |
| <b>issuerAltName</b>          |                    | Igual a la extensión subjectAltName del certificado de la CA emisora   |
| <b>subjectAltName</b>         |                    |  |
| rfc822Name                    |                    | Email del suscriptor   |
| directoryName                 |                    |  |
| 1.3.6.1.4.1.14777.0.1         |                    | Nombre   |
| 1.3.6.1.4.1.14777.0.2         |                    | Primer Apellido  |
| 1.3.6.1.4.1.14777.0.3         |                    | Segundo Apellido   |
| 1.3.6.1.4.1.14777.0.4         |                    | DNI / NIE / NIF / PASS   |
| 1.3.6.1.4.1.14777.0.5         |                    | Organización   |
| 1.3.6.1.4.1.14777.0.6         |                    | CIF  |
| 1.3.6.1.4.1.14777.0.7         |                    | Email del suscriptor   |
| 1.3.6.1.4.1.14777.0.8         | Opcional           | Cargo  |
| 1.3.6.1.4.1.14777.0.9         | Opcional           | Departamento   |
| <b>extendedKeyUsage</b>       |                    | clientAuth, emailProtection  |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública  |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier   |
| <b>certificatePolicies</b>    |                    |  |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.2.19.2   |
| cpsURL                        |                    | <a href="http://www.izenpe.eus/cps">http://www.izenpe.eus/cps</a>  |
| userNotice                    |                    | Konsulta <a href="http://www.izenpe.eus">www.izenpe.eus</a> -en baldintzak eta kondizioak ziurtagiriaren fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.eus">www.izenpe.eus</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier              |                    | 0.4.0.194112.1.0 (QCP-n)   |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.com/cgi-bin/crl2">http://crl.izenpe.com/cgi-bin/crl2</a>  |
| <b>authorityInfoAccess</b>    |                    |  |
| ocsp                          |                    | <a href="http://ocsp.izenpe.com">http://ocsp.izenpe.com</a>  |
| CA emisora                    |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crt</a>  |
| <b>qcStatements</b>           |                    |  |
| QcCompliance                  |                    | Presente   |
| QcType                        |                    | id-etsi-qct-esign  |
| QcRetentiodPeriod             |                    | 15 años  |
| QcPDS                         |                    | <a href="https://www.izenpe.eus/pds/en/">https://www.izenpe.eus/pds/en/</a> en<br><a href="https://www.izenpe.eus/pds/eu/">https://www.izenpe.eus/pds/eu/</a> eu<br><a href="https://www.izenpe.eus/pds/es/">https://www.izenpe.eus/pds/es/</a> es                             |
| qcStatement-2                 |                    | 0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)   |
| <b>keyUsage</b>               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment  |

## Profesional

CA emisora

CCEER

Nombre

profesional\_qc\_hsm

| Campo / extensión            | Opcional / Crítica | Contenido   |
|------------------------------|--------------------|---|
| version                      |                    | Versión 3   |
| serialNumber                 |                    | Número secuencial único   |
| signature                    |                    | sha256WithRSAEncryption   |
| issuer                       |                    | Igual al campo subject del certificado de la CA emisora   |
| validity                     |                    | 3 años  |
| subject                      |                    |   |
| serialNumber                 |                    | DNI / NIE / NIF / PASS  |
| SN                           |                    | Apellidos   |
| G                            |                    | Nombre  |
| CN                           |                    | Nombre Apellido1 Apellido 2 - DNI   |
| organizationIdentifier       |                    | 3 caracteres tipo-identidad + Country + - + identificador. Por ejemplo, si usamos el CIF sería algo como: VATES-A01337260   |
| title                        | Opcional           | Cargo   |
| OU                           |                    | Ziurtagiri Profesionala - Certificado Profesional   |
| OU                           | Opcional           | Departamento  |
| OU                           | Opcional           | Grupo VPN   |
| O                            |                    | Organización  |
| C                            |                    | País (codificado según ISO 3166-1 alpha 2 code)   |
| subjectPublicKeyInfo         |                    | RSA 3072 bits mínimo  |
| extensions                   |                    |   |
| issuerAltName                |                    | Igual a la extensión subjectAltName del certificado de la CA emisora  |
| subjectAltName               |                    |   |
| rfc822Name                   |                    | Email del suscriptor  |
| OtherName: UserPrincipalName | Opcional           | Nombre principal de usuario   |
| directoryName                |                    |   |
| 1.3.6.1.4.1.14777.0.1        |                    | Nombre  |
| 1.3.6.1.4.1.14777.0.2        |                    | Primer Apellido   |
| 1.3.6.1.4.1.14777.0.3        |                    | Segundo Apellido  |
| 1.3.6.1.4.1.14777.0.4        |                    | DNI / NIE / NIF / PASS  |
| 1.3.6.1.4.1.14777.0.5        |                    | Organización  |
| 1.3.6.1.4.1.14777.0.6        |                    | CIF   |
| 1.3.6.1.4.1.14777.0.7        |                    | Email del suscriptor  |
| 1.3.6.1.4.1.14777.0.8        | Opcional           | Cargo   |
| 1.3.6.1.4.1.14777.0.9        | Opcional           | Departamento  |
| extendedKeyUsage             |                    | clientAuth, emailProtection   |
| subjectKeyIdentifier         |                    | Identificador de la clave pública   |
| authorityKeyIdentifier       |                    | Incluir sólo campo keyIdentifier  |
| certificatePolicies          |                    |   |
| policyIdentifier             |                    | 1.3.6.1.4.1.14777.2.19.3  |
| cpsURI                       |                    | <a href="http://www.izenpe.eus/cps">http://www.izenpe.eus/cps</a>   |
| userNotice                   |                    | Kontsulta <a href="http://www.izenpe.eus">www.izenpe.eus</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.eus">www.izenpe.eus</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier             |                    | 0.4.0.194112.1.0 (QCP-n)  |
| cRLDistributionPoints        |                    | <a href="http://crl.izenpe.com/cgi-bin/crl2">http://crl.izenpe.com/cgi-bin/crl2</a>   |
| authorityInfoAccess          |                    |   |
| ocsp                         |                    | <a href="http://ocsp.izenpe.com">http://ocsp.izenpe.com</a>   |
| CA emisora                   |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crt</a>   |
| qcStatements                 |                    |   |
| QcCompliance                 |                    | Presente  |
| QcType                       |                    | id-etsi-qct-esign   |
| QcRetentiodPeriod            |                    | 15 años   |
| QcPDS                        |                    | <a href="https://www.izenpe.eus/pds/en/">https://www.izenpe.eus/pds/en/</a> en<br><a href="https://www.izenpe.eus/pds/eu/">https://www.izenpe.eus/pds/eu/</a> eu<br><a href="https://www.izenpe.eus/pds/es/">https://www.izenpe.eus/pds/es/</a> es                            |
| qcStatement-2                |                    | 0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)  |
| keyUsage                     | Crítica            | digitalSignature, nonRepudiation, keyEncipherment   |

## Corporativo Privado

CA emisora

CCEENR

Nombre

corporativo\_privado

| Campo / extensión             | Opcional / Crítica | Contenido  |
|-------------------------------|--------------------|--|
| <b>version</b>                |                    | Versión 3  |
| <b>serialNumber</b>           |                    | Número secuencial único  |
| <b>signature</b>              |                    | sha256WithRSAEncryption  |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora  |
| <b>validity</b>               |                    | 3 años   |
| <b>subject</b>                |                    |  |
| serialNumber                  |                    | DNI / NIE  |
| SN                            |                    | Primer Apellido  |
| G                             |                    | Nombre   |
| CN                            |                    | Nombre y Apellidos   |
| dnQualifier                   |                    | Depende de tipo de documento.<br>DNI: "-dni [DNI]"<br>NIE: "-nie [NIE]"  |
| OU                            |                    | Condiciones de uso en <a href="http://www.izenpe.com">www.izenpe.com</a> nola erabili jakiteko   |
| OU                            |                    | Ziurtagiri korporatibo pribatua - Certificado corporativo privado  |
| OU                            | Opcional           | Cargo o Departamento   |
| OU                            | Opcional           | Grupo VPN  |
| O                             |                    | Organización   |
| <b>subjectPublicKeyInfo</b>   |                    | RSA 3072 bits mínimo   |
| <b>extensions</b>             |                    |  |
| <b>issuerAltName</b>          |                    | Igual a la extensión subjectAltName del certificado de la CA emisora   |
| <b>subjectAltName</b>         |                    |  |
| rfc822Name                    |                    | Email del usuario  |
| OtherName: UserPrincipalName  | Opcional           | Nombre principal de usuario  |
| <b>extendedKeyUsage</b>       |                    | clientAuth, emailProtection, smartCardLogon  |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública  |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier   |
| <b>certificatePolicies</b>    |                    |  |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.5.2.2  |
| cpsURI                        |                    | <a href="http://www.izenpe.com/cps">http://www.izenpe.com/cps</a>  |
| userNotice                    |                    | Bereen mugak ezagutzeko <a href="http://www.izenpe.com">www.izenpe.com</a> Ziurtagirian konfiantza izan aurretik kontratua irakurri. Limitaciones de garantías en <a href="http://www.izenpe.com">www.izenpe.com</a> Consulte el contrato antes de confiar en el certificado |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.com/cgi-bin/crlscinr2">http://crl.izenpe.com/cgi-bin/crlscinr2</a>  |
| <b>authorityInfoAccess</b>    |                    | ocsp <a href="http://ocsp.izenpe.com">http://ocsp.izenpe.com</a>   |
| <b>keyUsage</b>               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment  |

## Corporativo Reconocido

CA emisora

AAPPR

Nombre

corporativo\_reconocido

| Campo / extensión             | Opcional / Crítica | Contenido  |
|-------------------------------|--------------------|--|
| <b>version</b>                |                    | Versión 3  |
| <b>serialNumber</b>           |                    | Número secuencial único  |
| <b>signature</b>              |                    | sha256WithRSAEncryption  |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora  |
| <b>validity</b>               |                    | 3 años   |
| <b>subject</b>                |                    |  |
| serialNumber                  |                    | DNI / NIE  |
| SN                            |                    | Primer Apellido  |
| G                             |                    | Nombre   |
| CN                            |                    | Nombre y Apellidos   |
| dnQualifier                   |                    | Depende de tipo de documento.<br>DNI: "-dni [DNI] -TIS [TIS] -cif [CIF]"<br>NIE: "-nie [NIE] -TIS [TIS] -cif [CIF]"  |
| OU                            |                    | Condiciones de uso en www.izenpe.com nola erabili jakiteko   |
| OU                            |                    | Ziurtagiri korporatibo onartua - Cert. corporativo reconocido  |
| OU                            |                    | Ziurtagiri onartua - Certificado reconocido  |
| OU                            | Opcional           | Cargo o Departamento   |
| OU                            | Opcional           | Grupo VPN  |
| O                             |                    | Organización   |
| C                             |                    | ES   |
| <b>subjectPublicKeyInfo</b>   |                    | RSA 3072 bits mínimo   |
| <b>extensions</b>             |                    |  |
| <b>issuerAltName</b>          |                    | Igual a la extensión subjectAltName del certificado de la CA emisora   |
| <b>subjectAltName</b>         |                    |  |
| rfc822Name                    |                    | Email del suscriptor   |
| OtherName: UserPrincipalName  | Opcional           | Nombre principal de usuario  |
| <b>extendedKeyUsage</b>       |                    | clientAuth, emailProtection, smartCardLogon  |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública  |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier   |
| <b>certificatePolicies</b>    |                    |  |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.4.2  |
| cpsURI                        |                    | http://www.izenpe.com/rpascacorrec   |
| userNotice                    |                    | Bereen mugak ezagutzeko www.izenpe.com Ziurtagirian konfiantza izan aurretik kontratua irakurri. Limitaciones de garantías en www.izenpe.com Consulte el contrato antes de confiar en el certificado |
| policyIdentifier              |                    | 0.4.0.1456.1.1   |
| <b>cRLDistributionPoints</b>  |                    | http://crl.izenpe.com/cgi-bin/crlscar2   |
| <b>authorityInfoAccess</b>    |                    | ocsp http://ocsp.izenpe.com  |
| <b>qcStatements</b>           |                    |  |
| QcCompliance                  |                    | Presente   |
| QcSSCD                        |                    | Presente   |
| QcRetentiodPeriod             |                    | 15 años  |
| QcPDS                         |                    | https://www.izenpe.eus/pds/en/ en<br>https://www.izenpe.eus/pds/eu/ eu<br>https://www.izenpe.eus/pds/es/ es  |
| <b>keyUsage</b>               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment  |

## Corporativo

CA emisora

AAPPNR

Nombre

corporativo

| Campo / extensión             | Opcional / Crítica | Contenido  |
|-------------------------------|--------------------|--|
| <b>version</b>                |                    | Versión 3  |
| <b>serialNumber</b>           |                    | Número secuencial único  |
| <b>signature</b>              |                    | sha256WithRSAEncryption  |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora  |
| <b>validity</b>               |                    | 3 años   |
| <b>subject</b>                |                    |  |
| serialNumber                  |                    | DNI / NIE  |
| SN                            |                    | Primer Apellido  |
| G                             |                    | Nombre   |
| CN                            |                    | Nombre y Apellidos   |
| dnQualifier                   |                    | Depende de tipo de documento.<br>DNI: "-dni [DNI]"<br>NIE: "-nie [NIE]"  |
| OU                            |                    | Condiciones de uso en <a href="http://www.izenpe.com">www.izenpe.com</a> nola erabili jakiteko   |
| OU                            |                    | Ziurtagiri korporatiboa Certificado corporativo  |
| OU                            | Opcional           | Cargo o Departamento   |
| OU                            | Opcional           | Grupo VPN  |
| O                             |                    | Organización   |
| <b>subjectPublicKeyInfo</b>   |                    | RSA 3072 bits mínimo   |
| <b>extensions</b>             |                    |  |
| <b>issuerAltName</b>          |                    | Igual a la extensión subjectAltName del certificado de la CA emisora   |
| <b>subjectAltName</b>         |                    |  |
| rfc822Name                    |                    | Email del suscriptor   |
| OtherName: UserPrincipalName  | Opcional           | Nombre principal de usuario  |
| <b>extendedKeyUsage</b>       |                    | clientAuth, emailProtection, smartCardLogon  |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública  |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier   |
| <b>certificatePolicies</b>    |                    |  |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.1.1.1  |
| cpsURI                        |                    | <a href="http://www.izenpe.com/cps">http://www.izenpe.com/cps</a>  |
| userNotice                    |                    | Ziurtagiria Euskal Autonomia Erkidegoko sektore publikoko erakundeen barne-sareetan bakarrik erabil daiteke. Uso restringido al ambito de redes internas de Entidades del Sector Publico Vasco |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.com/cgi-bin/crlinterna2">http://crl.izenpe.com/cgi-bin/crlinterna2</a>  |
| <b>authorityInfoAccess</b>    |                    | ocsp <a href="http://ocsp.izenpe.com">http://ocsp.izenpe.com</a>   |
| <b>keyUsage</b>               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment  |

## Corporativo Reconocido en Hardware

CA emisora

AAPPR

Nombre

corporativo\_reconocido\_hardware

| Campo / extensión             | Opcional / Crítica | Contenido  |
|-------------------------------|--------------------|--|
| <b>version</b>                |                    | Versión 3  |
| <b>serialNumber</b>           |                    | Número secuencial único  |
| <b>signature</b>              |                    | sha256WithRsaSignature   |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora  |
| <b>validity</b>               |                    | 4 años   |
| <b>subject</b>                |                    |  |
| serialNumber                  |                    | DNI / NIE  |
| SN                            |                    | Apellidos  |
| G                             |                    | Nombre   |
| CN                            |                    | Nombre y Apellidos   |
| dnQualifier                   |                    | Depende de tipo de documento.<br>DNI: "-dni [DNI] -cif [CIF]"<br>NIE: "-nie [NIE] -cif [CIF]"  |
| OU                            |                    | Condiciones de uso en <a href="http://www.izenpe.com">www.izenpe.com</a> nola erabili jakiteko   |
| OU                            |                    | HSM Ziurtagiri korporatibo onartua - Cert. corporativo reconocido HSM  |
| OU                            |                    | Ziurtagiri onartua - Certificado reconocido  |
| OU                            | Opcional           | Cargo o Departamento   |
| OU                            | Opcional           | Grupo VPN  |
| O                             |                    | Organización   |
| C                             |                    | ES   |
| <b>subjectPublicKeyInfo</b>   |                    | RSA 3072 bits mínimo   |
| <b>extensions</b>             |                    |  |
| <b>issuerAltName</b>          |                    | Igual a la extensión subjectAltName del certificado de la CA emisora   |
| <b>subjectAltName</b>         |                    |  |
| rfc822Name                    |                    | Email del suscriptor   |
| <b>extendedKeyUsage</b>       |                    | clientAuth, emailProtection  |
| <b>netscapeCertType</b>       |                    | SSL_Client, SMIME_Client   |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública  |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier   |
| <b>certificatePolicies</b>    |                    |  |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.4.6  |
| cpsURI                        |                    | <a href="http://www.izenpe.com/cps">http://www.izenpe.com/cps</a>  |
| userNotice                    |                    | Bermeen mugak ezagutzeko <a href="http://www.izenpe.com">www.izenpe.com</a> Ziurtagirian konfiantza izan aurretik kontratua irakurri. Limitaciones de garantías en <a href="http://www.izenpe.com">www.izenpe.com</a><br>Consulte el contrato antes de confiar en el certificado |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.com/cgi-bin/crlscar2">http://crl.izenpe.com/cgi-bin/crlscar2</a>  |
| <b>authorityInfoAccess</b>    |                    | ocsp <a href="http://ocsp.izenpe.com">http://ocsp.izenpe.com</a>   |
| <b>qcStatements</b>           |                    |  |
| QcCompliance                  |                    | Presente   |
| QcSSCD                        |                    | Presente   |
| <b>keyUsage</b>               | Crítica            | digitalSignature, keyEncipherment, dataEncipherment  |

## Personal de Entidades Públicas

CA emisora

AAPPR

Nombre

pep\_qc\_scad

| Campo / extensión             | Opcional / Crítica | Contenido  |
|-------------------------------|--------------------|--|
| <b>version</b>                |                    | Versión 3  |
| <b>serialNumber</b>           |                    | Número secuencial único  |
| <b>signature</b>              |                    | sha256WithRSAEncryption  |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora  |
| <b>validity</b>               |                    | 3 años   |
| <b>subject</b>                |                    |  |
| serialNumber                  |                    | DNI / NIE siguiendo semántica ETSI EN 319 412-1  |
| SN                            |                    | Apellidos  |
| G                             |                    | Nombre   |
| CN                            |                    | Nombre Apellido1 Apellido 2 - DNI  |
| title                         | Opcional           | Cargo  |
| OU                            |                    | <b>CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO</b>   |
| OU                            | Opcional           | Unidad dentro de la administración   |
| OU                            | Opcional           | Código DIR3 de la unidad   |
| OU                            | Opcional           | Numero de identificación del empleado público  |
| O                             |                    | Nombre oficial de la Organización  |
| C                             |                    | <b>ES</b>  |
| <b>subjectPublicKeyInfo</b>   |                    | RSA 3072 bits mínimo   |
| <b>extensions</b>             |                    |  |
| <b>issuerAltName</b>          |                    | Igual a la extensión subjectAltName del certificado de la CA emisora   |
| <b>subjectAltName</b>         |                    |  |
| rfc822Name                    |                    | Email del suscriptor   |
| OtherName: UserPrincipalName  | Opcional           | Nombre principal de usuario  |
| directoryName                 |                    |  |
| 2.16.724.1.3.5.7.2.1          |                    | <b>CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO</b>   |
| 2.16.724.1.3.5.7.2.2          |                    | Nombre oficial de la Organización  |
| 2.16.724.1.3.5.7.2.3          |                    | CIF  |
| 2.16.724.1.3.5.7.2.4          |                    | DNI / NIE  |
| 2.16.724.1.3.5.7.2.5          | Opcional           | Numero de identificación del empleado público  |
| 2.16.724.1.3.5.7.2.6          |                    | Nombre   |
| 2.16.724.1.3.5.7.2.7          |                    | Primer Apellido  |
| 2.16.724.1.3.5.7.2.8          |                    | Segundo Apellido   |
| 2.16.724.1.3.5.7.2.9          | Opcional           | Email del suscriptor   |
| 2.16.724.1.3.5.7.2.10         | Opcional           | Unidad dentro de la administración   |
| 2.16.724.1.3.5.7.2.11         | Opcional           | Puesto o cargo   |
| <b>extendedKeyUsage</b>       |                    | clientAuth, emailProtection, smartCardLogon  |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública  |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier   |
| <b>certificatePolicies</b>    |                    |  |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.4.14.1   |
| cpsURI                        |                    | <a href="http://www.izenpe.eus/cps">http://www.izenpe.eus/cps</a>  |
| userNotice                    |                    | Konsulta <a href="http://www.izenpe.eus">www.izenpe.eus</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.eus">www.izenpe.eus</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier              |                    | 2.16.724.1.3.5.7.2   |
| policyIdentifier              |                    | 0.4.0.194112.1.0 (QCP-n)   |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.com/cgi-bin/crlscar2">http://crl.izenpe.com/cgi-bin/crlscar2</a>  |
| <b>authorityInfoAccess</b>    |                    |  |
| ocsp                          |                    | <a href="http://ocsp.izenpe.com">http://ocsp.izenpe.com</a>  |
| CA emisora                    |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR_cert_sha256.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR_cert_sha256.crt</a>  |
| <b>qcStatements</b>           |                    |  |
| QcCompliance                  |                    | Presente   |
| QcType                        |                    | id-etsi-qct-esign  |
| QcRetentiodPeriod             |                    | 15 años  |
| QcPDS                         |                    | <a href="https://www.izenpe.eus/pds/en/">https://www.izenpe.eus/pds/en/</a> en<br><a href="https://www.izenpe.eus/pds/eu/">https://www.izenpe.eus/pds/eu/</a> eu<br><a href="https://www.izenpe.eus/pds/es/">https://www.izenpe.eus/pds/es/</a> es                           |
| qcStatement-2                 |                    | 0.4.0.194121.1.1 (id-etsi-qcs-SemanticsId-Natural)   |
| <b>keyUsage</b>               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment  |

## Personal de Entidades Públicas

CA emisora

AAPP

Nombre

pep\_qc\_sw

| Campo / extensión             | Opcional / Crítica | Contenido  |
|-------------------------------|--------------------|--|
| <b>version</b>                |                    | Versión 3  |
| <b>serialNumber</b>           |                    | Número secuencial único  |
| <b>signature</b>              |                    | sha256WithRSAEncryption  |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora  |
| <b>validity</b>               |                    | 3 años   |
| <b>subject</b>                |                    |  |
| serialNumber                  |                    | DNI / NIE siguiendo semántica ETSI EN 319 412-1  |
| SN                            |                    | Apellidos  |
| G                             |                    | Nombre   |
| CN                            |                    | Nombre Apellido1 Apellido 2 - DNI  |
| title                         | Opcional           | Cargo  |
| OU                            |                    | <b>CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO</b>   |
| OU                            | Opcional           | Unidad dentro de la administración   |
| OU                            | Opcional           | Código DIR3 de la unidad   |
| OU                            | Opcional           | Numero de identificación del empleado público  |
| O                             |                    | Nombre oficial de la Organización  |
| C                             |                    | <b>ES</b>  |
| <b>subjectPublicKeyInfo</b>   |                    | RSA 3072 bits mínimo   |
| <b>extensions</b>             |                    |  |
| <b>issuerAltName</b>          |                    | Igual a la extensión subjectAltName del certificado de la CA emisora   |
| <b>subjectAltName</b>         |                    |  |
| rfc822Name                    |                    | Email del suscriptor   |
| directoryName                 |                    |  |
| 2.16.724.1.3.5.7.2.1          |                    | <b>CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO</b>   |
| 2.16.724.1.3.5.7.2.2          |                    | Nombre oficial de la Organización  |
| 2.16.724.1.3.5.7.2.3          |                    | CIF  |
| 2.16.724.1.3.5.7.2.4          |                    | DNI / NIE  |
| 2.16.724.1.3.5.7.2.5          | Opcional           | Numero de identificación del empleado público  |
| 2.16.724.1.3.5.7.2.6          |                    | Nombre   |
| 2.16.724.1.3.5.7.2.7          |                    | Primer Apellido  |
| 2.16.724.1.3.5.7.2.8          |                    | Segundo Apellido   |
| 2.16.724.1.3.5.7.2.9          | Opcional           | Email del suscriptor   |
| 2.16.724.1.3.5.7.2.10         | Opcional           | Unidad dentro de la administración   |
| 2.16.724.1.3.5.7.2.11         | Opcional           | Puesto o cargo   |
| <b>extendedKeyUsage</b>       |                    | clientAuth, emailProtection  |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública  |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier   |
| <b>certificatePolicies</b>    |                    |  |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.4.14.2   |
| cpsURI                        |                    | <a href="http://www.izenpe.eus/cps">http://www.izenpe.eus/cps</a>  |
| userNotice                    |                    | Konsulta <a href="http://www.izenpe.eus">www.izenpe.eus</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.eus">www.izenpe.eus</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier              |                    | 2.16.724.1.3.5.7.2   |
| policyIdentifier              |                    | 0.4.0.194112.1.0 (QCP-n)   |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.com/cgi-bin/crlscar2">http://crl.izenpe.com/cgi-bin/crlscar2</a>  |
| <b>authorityInfoAccess</b>    |                    |  |
| ocsp                          |                    | <a href="http://ocsp.izenpe.com">http://ocsp.izenpe.com</a>  |
| CA emisora                    |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPP cert_sha256.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPP cert_sha256.crt</a>  |
| <b>qcStatements</b>           |                    |  |
| QcCompliance                  |                    | Presente   |
| QcType                        |                    | id-etsi-qct-esign  |
| QcRetentiodPeriod             |                    | 15 años  |
| QcPDS                         |                    | <a href="https://www.izenpe.eus/pds/en/">https://www.izenpe.eus/pds/en/</a> en<br><a href="https://www.izenpe.eus/pds/eu/">https://www.izenpe.eus/pds/eu/</a> eu<br><a href="https://www.izenpe.eus/pds/es/">https://www.izenpe.eus/pds/es/</a> es                           |
| qcStatement-2                 |                    | 0.4.0.194121.1.1 (id-etsi-qcs-SemanticsId-Natural)   |
| <b>keyUsage</b>               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment  |

## Personal de Entidades Públicas

CA emisora

AAPP

Nombre

pep\_qc\_hsm

| Campo / extensión             | Opcional / Crítica | Contenido  |
|-------------------------------|--------------------|--|
| <b>version</b>                |                    | Versión 3  |
| <b>serialNumber</b>           |                    | Número secuencial único  |
| <b>signature</b>              |                    | sha256WithRSAEncryption  |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora  |
| <b>validity</b>               |                    | 3 años   |
| <b>subject</b>                |                    |  |
| serialNumber                  |                    | DNI / NIE siguiendo semántica ETSI EN 319 412-1  |
| SN                            |                    | Apellidos  |
| G                             |                    | Nombre   |
| CN                            |                    | Nombre Apellido1 Apellido 2 - DNI  |
| title                         | Opcional           | Cargo  |
| OU                            |                    | <b>CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO</b>   |
| OU                            | Opcional           | Unidad dentro de la administración   |
| OU                            | Opcional           | Código DIR3 de la unidad   |
| OU                            | Opcional           | Numero de identificación del empleado público  |
| O                             |                    | Nombre oficial de la Organización  |
| C                             |                    | <b>ES</b>  |
| <b>subjectPublicKeyInfo</b>   |                    | RSA 3072 bits mínimo   |
| <b>extensions</b>             |                    |  |
| <b>issuerAltName</b>          |                    | Igual a la extensión subjectAltName del certificado de la CA emisora   |
| <b>subjectAltName</b>         |                    |  |
| rfc822Name                    |                    | Email del suscriptor   |
| OtherName: UserPrincipalName  | Opcional           | Nombre principal de usuario  |
| directoryName                 |                    |  |
| 2.16.724.1.3.5.7.2.1          |                    | <b>CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO</b>   |
| 2.16.724.1.3.5.7.2.2          |                    | Nombre oficial de la Organización  |
| 2.16.724.1.3.5.7.2.3          |                    | CIF  |
| 2.16.724.1.3.5.7.2.4          |                    | DNI / NIE  |
| 2.16.724.1.3.5.7.2.5          | Opcional           | Numero de identificación del empleado público  |
| 2.16.724.1.3.5.7.2.6          |                    | Nombre   |
| 2.16.724.1.3.5.7.2.7          |                    | Primer Apellido  |
| 2.16.724.1.3.5.7.2.8          |                    | Segundo Apellido   |
| 2.16.724.1.3.5.7.2.9          | Opcional           | Email del suscriptor   |
| 2.16.724.1.3.5.7.2.10         | Opcional           | Unidad dentro de la administración   |
| 2.16.724.1.3.5.7.2.11         | Opcional           | Puesto o cargo   |
| <b>extendedKeyUsage</b>       |                    | clientAuth, emailProtection  |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública  |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier   |
| <b>certificatePolicies</b>    |                    |  |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.4.14.3   |
| cpsURI                        |                    | <a href="http://www.izenpe.eus/cps">http://www.izenpe.eus/cps</a>  |
| userNotice                    |                    | Konsulta <a href="http://www.izenpe.eus">www.izenpe.eus</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.eus">www.izenpe.eus</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier              |                    | 2.16.724.1.3.5.7.2   |
| policyIdentifier              |                    | 0.4.0.194112.1.0 (QCP-n)   |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.com/cgi-bin/crlscar2">http://crl.izenpe.com/cgi-bin/crlscar2</a>  |
| <b>authorityInfoAccess</b>    |                    |  |
| ocsp                          |                    | <a href="http://ocsp.izenpe.com">http://ocsp.izenpe.com</a>  |
| CA emisora                    |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPP_cert_sha256.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPP_cert_sha256.crt</a>  |
| <b>qcStatements</b>           |                    |  |
| QcCompliance                  |                    | Presente   |
| QcType                        |                    | id-etsi-qct-esign  |
| QcRetentiodPeriod             |                    | 15 años  |
| QcPDS                         |                    | <a href="https://www.izenpe.eus/pds/en/">https://www.izenpe.eus/pds/en/</a><br><a href="https://www.izenpe.eus/pds/eu/">https://www.izenpe.eus/pds/eu/</a><br><a href="https://www.izenpe.eus/pds/es/">https://www.izenpe.eus/pds/es/</a>                                    |
| qcStatement-2                 |                    | 0.4.0.194121.1.1 (id-etsi-qcs-SemanticsId-Natural)   |
| <b>keyUsage</b>               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment  |

## Personal de Entidades Públicas

CA emisora

AAPPR

Nombre

pers\_entidades\_publicas

| Campo / extensión             | Opcional / Crítica | Contenido   |
|-------------------------------|--------------------|---|
| <b>version</b>                |                    | Versión 3   |
| <b>serialNumber</b>           |                    | Número secuencial único   |
| <b>signature</b>              |                    | sha256WithRSAEncryption   |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora   |
| <b>validity</b>               |                    | 4 años  |
| <b>subject</b>                |                    |   |
| serialNumber                  |                    | DNI / NIE   |
| SN                            |                    | Primer Apellido   |
| G                             |                    | Nombre  |
| CN                            |                    | Nombre y Apellidos  |
| dnQualifier                   |                    | Depende de tipo de documento.<br>DNI: "-dni [DNI] -TIS [TIS] -cif [CIF]"<br>NIE: "-nie [NIE] -TIS [TIS] -cif [CIF]"   |
| OU                            |                    | Condiciones de uso en www.izenpe.com nola erabili jakiteko  |
| OU                            |                    | Entitate publikoen ziurtagiri - Certificado de entidad publica  |
| OU                            |                    | Ziurtagiri onartua - Certificado reconocido   |
| OU                            | Opcional           | Cargo o Departamento  |
| OU                            | Opcional           | Grupo VPN   |
| O                             |                    | Organización  |
| C                             |                    | ES  |
| <b>subjectPublicKeyInfo</b>   |                    | RSA 3072 bits mínimo  |
| <b>extensions</b>             |                    |   |
| <b>issuerAltName</b>          |                    | Igual a la extensión subjectAltName del certificado de la CA emisora  |
| <b>subjectAltName</b>         |                    |   |
| rfc822Name                    |                    | Email del suscriptor  |
| OtherName: UserPrincipalName  | Opcional           | Nombre principal de usuario   |
| <b>extendedKeyUsage</b>       |                    | clientAuth, emailProtection, smartCardLogon   |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública   |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier  |
| <b>certificatePolicies</b>    |                    |   |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.4.1   |
| cpsURI                        |                    | http://www.izenpe.com/rpascapersentpub  |
| userNotice                    |                    | Bermeen mugak ezagutzeko www.izenpe.com Ziurtagirian konfiantza izan aurretik kontratua irakurri. Limitaciones de garantias en www.izenpe.com Consulte el contrato antes de confiar en el certificado |
| policyIdentifier              |                    | 0.4.0.1456.1.1  |
| <b>cRLDistributionPoints</b>  |                    | http://crl.izenpe.com/cgi-bin/crlscar2  |
| <b>authorityInfoAccess</b>    |                    | ocsp http://ocsp.izenpe.com   |
| <b>qcStatements</b>           |                    |   |
| QcCompliance                  |                    | Presente  |
| QcSSCD                        |                    | Presente  |
| QcRetentiodPeriod             |                    | 15 años   |
| QcPDS                         |                    | https://www.izenpe.eus/pds/en/ en<br>https://www.izenpe.eus/pds/eu/ eu<br>https://www.izenpe.eus/pds/es/ es   |
| <b>keyUsage</b>               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment   |

## Personal de Entidades Públicas con Seudónimo (FIRMA)

CA emisora

AAPPR

Nombre

pep\_seudonimo\_scared\_sign

| Campo / extensión             | Opcional / Crítica | Contenido  |
|-------------------------------|--------------------|--|
| <b>version</b>                |                    | Versión 3  |
| <b>serialNumber</b>           |                    | Número secuencial único  |
| <b>signature</b>              |                    | sha256WithRSAEncryption  |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora  |
| <b>validity</b>               |                    | 4 años   |
| <b>subject</b>                |                    |  |
| title                         | Opcional           | Puesto o cargo de la persona   |
| pseudonym                     |                    | Seudónimo  |
| CN                            |                    | <Cargo> - <seudonimo> - <Organizacion> (FIRMA)<br>o<br>SEUDONIMO - <seudonimo> - <Organizacion> (FIRMA)  |
| OU                            |                    | CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO  |
| OU                            | Opcional           | Unidad dentro de la administración   |
| OU                            | Opcional           | Código DIR3 de la unidad   |
| O                             |                    | Nombre oficial de la Administración a la que pertenece el poseedor   |
| C                             |                    | ES   |
| <b>subjectPublicKeyInfo</b>   |                    | RSA 3072 bits mínimo   |
| <b>extensions</b>             |                    |  |
| <b>issuerAltName</b>          |                    | Igual a la extensión subjectAltName del certificado de la CA emisora   |
| <b>subjectAltName</b>         |                    |  |
| directoryName                 |                    |  |
| 2.16.724.1.3.5.4.1.1          |                    | CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO  |
| 2.16.724.1.3.5.4.1.2          |                    | Nombre oficial de la Administración a la que pertenece el poseedor   |
| 2.16.724.1.3.5.4.1.3          |                    | NIF  |
| 2.16.724.1.3.5.4.1.9          | Opcional           | Email de contacto  |
| 2.16.724.1.3.5.4.1.10         | Opcional           | Unidad dentro de la administración   |
| 2.16.724.1.3.5.4.1.11         | Opcional           | Puesto o cargo del suscriptor  |
| 2.16.724.1.3.5.4.1.12         |                    | Seudónimo  |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública  |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier   |
| <b>certificatePolicies</b>    |                    |  |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.4.13.1.1   |
| cpsURI                        |                    | <a href="http://www.izenpe.eus/cps">http://www.izenpe.eus/cps</a>  |
| userNotice                    |                    | Konsulta <a href="http://www.izenpe.eus">www.izenpe.eus</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.eus">www.izenpe.eus</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier              |                    | OID MINHAP: <b>2.16.724.1.3.5.4.1</b>  |
| policyIdentifier              |                    | OID QCP-n-qscd: <b>0.4.0.194112.1.2</b>  |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.com/cgi-bin/crlscar2">http://crl.izenpe.com/cgi-bin/crlscar2</a>  |
| <b>authorityInfoAccess</b>    |                    |  |
| ocsp                          |                    | <a href="http://ocsp.izenpe.com">http://ocsp.izenpe.com</a>  |
| CA emisora                    |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR_cert_sha256.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR_cert_sha256.crt</a>  |
| <b>qcStatements</b>           |                    |  |
| QcCompliance                  |                    | Presente   |
| QcType                        |                    | id-etsi-qct-esign  |
| QcSSCD                        |                    | Presente   |
| QcEuRetentiodPeriod           |                    | 15 años  |
| QcPDS                         |                    | <a href="https://www.izenpe.eus/pds/en/">https://www.izenpe.eus/pds/en/</a> en<br><a href="https://www.izenpe.eus/pds/eu/">https://www.izenpe.eus/pds/eu/</a> eu<br><a href="https://www.izenpe.eus/pds/es/">https://www.izenpe.eus/pds/es/</a> es                           |
| <b>keyUsage</b>               | Crítica            | contentCommitment (no repudio)   |

## Personal de Entidades Públicas con Seudónimo (AUTENTICACION)

CA emisora

AAPPR

Nombre

pep\_seudonimo\_scard\_auth

| Campo / extensión      | Opcional / Crítica | Contenido   |
|------------------------|--------------------|---|
| version                |                    | Versión 3   |
| serialNumber           |                    | Número secuencial único   |
| signature              |                    | sha256WithRSAEncryption   |
| issuer                 |                    | Igual al campo subject del certificado de la CA emisora   |
| validity               |                    | 4 años  |
| subject                |                    |   |
| title                  | Opcional           | Puesto o cargo de la persona  |
| pseudonym              |                    | Seudónimo   |
| CN                     |                    | <Cargo> - <seudonimo> - <Organizacion> (AUTENTICACION)<br>o<br>SEUDONIMO - <seudonimo> - <Organizacion> (AUTENTICACION)   |
| OU                     |                    | CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO   |
| OU                     | Opcional           | Unidad dentro de la administración  |
| OU                     | Opcional           | Código DIR3 de la unidad  |
| O                      |                    | Nombre oficial de la Administración a la que pertenece el poseedor  |
| C                      |                    | ES  |
| subjectPublicKeyInfo   |                    | RSA 3072 bits mínimo  |
| extensions             |                    |   |
| issuerAltName          |                    | Igual a la extensión subjectAltName del certificado de la CA emisora  |
| subjectAltName         |                    |   |
| directoryName          |                    |   |
| 2.16.724.1.3.5.4.1.1   |                    | CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO   |
| 2.16.724.1.3.5.4.1.2   |                    | Nombre oficial de la Administración a la que pertenece el poseedor  |
| 2.16.724.1.3.5.4.1.3   |                    | NIF   |
| 2.16.724.1.3.5.4.1.9   | Opcional           | Email de contacto   |
| 2.16.724.1.3.5.4.1.10  | Opcional           | Unidad dentro de la administración  |
| 2.16.724.1.3.5.4.1.11  | Opcional           | Puesto o cargo del suscriptor   |
| 2.16.724.1.3.5.4.1.12  |                    | Seudónimo   |
| UserPrincipalName      | Opcional           | UPN para smart card logon   |
| extendedKeyUsage       |                    | clientAuth  |
| subjectKeyIdentifier   |                    | Identificador de la clave pública   |
| authorityKeyIdentifier |                    | Incluir sólo campo keyIdentifier  |
| certificatePolicies    |                    |   |
| policyIdentifier       |                    | 1.3.6.1.4.1.14777.4.13.1.2  |
| cpsURI                 |                    | <a href="http://www.izenpe.eus/cps">http://www.izenpe.eus/cps</a>   |
| userNotice             |                    | Kontsulta <a href="http://www.izenpe.eus">www.izenpe.eus</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.eus">www.izenpe.eus</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier       |                    | OID MINHAP: <b>2.16.724.1.3.5.4.1</b>   |
| policyIdentifier       |                    | OID NCP+: <b>0.4.0.2042.1.2</b>   |
| cRLDistributionPoints  |                    | <a href="http://crl.izenpe.com/cgi-bin/crlscar2">http://crl.izenpe.com/cgi-bin/crlscar2</a>   |
| authorityInfoAccess    |                    |   |
| ocsp                   |                    | <a href="http://ocsp.izenpe.com">http://ocsp.izenpe.com</a>   |
| CA emisora             |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR_cert_sha256.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR_cert_sha256.crt</a>   |
| keyUsage               | Crítica            | digitalSignature  |

## Personal de Entidades Públicas con Seudónimo (CIFRADO)

CA emisora

AAPPR

Nombre

pep\_seudonimo\_scard\_cipher

| Campo / extensión             | Opcional / Crítica | Contenido   |
|-------------------------------|--------------------|---|
| <b>version</b>                |                    | Versión 3   |
| <b>serialNumber</b>           |                    | Número secuencial único   |
| <b>signature</b>              |                    | sha256WithRSAEncryption   |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora   |
| <b>validity</b>               |                    | 4 años  |
| <b>subject</b>                |                    |   |
| title                         | Opcional           | Puesto o cargo de la persona  |
| pseudonym                     |                    | Seudónimo   |
| CN                            |                    | <Cargo> - <seudonimo> - <Organizacion> (FIRMA)<br>o<br>SEUDONIMO - <seudonimo> - <Organizacion> (FIRMA)   |
| OU                            |                    | CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO   |
| OU                            | Opcional           | Unidad dentro de la administración  |
| OU                            | Opcional           | Código DIR3 de la unidad  |
| O                             |                    | Nombre oficial de la Administración a la que pertenece el poseedor  |
| C                             |                    | ES  |
| <b>subjectPublicKeyInfo</b>   |                    | RSA 3072 bits mínimo  |
| <b>extensions</b>             |                    |   |
| <b>issuerAltName</b>          |                    | Igual a la extensión subjectAltName del certificado de la CA emisora  |
| <b>subjectAltName</b>         |                    |   |
| directoryName                 |                    |   |
| 2.16.724.1.3.5.4.1.1          |                    | CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO   |
| 2.16.724.1.3.5.4.1.2          |                    | Nombre oficial de la Administración a la que pertenece el poseedor  |
| 2.16.724.1.3.5.4.1.3          |                    | NIF   |
| 2.16.724.1.3.5.4.1.9          | Opcional           | Email de contacto   |
| 2.16.724.1.3.5.4.1.10         | Opcional           | Unidad dentro de la administración  |
| 2.16.724.1.3.5.4.1.11         | Opcional           | Puesto o cargo del suscriptor   |
| 2.16.724.1.3.5.4.1.12         |                    | Seudónimo   |
| <b>extendedKeyUsage</b>       |                    | clientAuth  |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública   |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier  |
| <b>certificatePolicies</b>    |                    |   |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.4.13.1.3  |
| cpsURI                        |                    | <a href="http://www.izenpe.eus/cps">http://www.izenpe.eus/cps</a>   |
| userNotice                    |                    | Kontsulta <a href="http://www.izenpe.eus">www.izenpe.eus</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.eus">www.izenpe.eus</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier              |                    | OID MINHAP: <b>2.16.724.1.3.5.4.1</b>   |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.com/cgi-bin/crlscar2">http://crl.izenpe.com/cgi-bin/crlscar2</a>   |
| <b>authorityInfoAccess</b>    |                    |   |
| ocsp                          |                    | <a href="http://ocsp.izenpe.com">http://ocsp.izenpe.com</a>   |
| CA emisora                    |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR_cert_sha256.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR_cert_sha256.crt</a>   |
| <b>keyUsage</b>               | Crítica            | keyEncipherment, dataEncipherment   |

## Personal de Entidades Públicas con Seudónimo (FIRMA)

CA emisora

AAPPR

Nombre

pep\_seudonimo\_sw

| Campo / extensión             | Opcional / Crítica | Contenido   |
|-------------------------------|--------------------|---|
| <b>version</b>                |                    | Versión 3   |
| <b>serialNumber</b>           |                    | Número secuencial único   |
| <b>signature</b>              |                    | sha256WithRSAEncryption   |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora   |
| <b>validity</b>               |                    | 4 años  |
| <b>subject</b>                |                    |   |
| title                         | Opcional           | Puesto o cargo de la persona  |
| pseudonym                     |                    | Seudónimo   |
| CN                            |                    | <Cargo> - <seudonimo> - <Organizacion><br>o<br><b>SEUDONIMO</b> - <seudonimo> - <Organizacion>  |
| OU                            |                    | <b>CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO</b>  |
| OU                            | Opcional           | Unidad dentro de la administración  |
| OU                            | Opcional           | Código DIR3 de la unidad  |
| O                             |                    | Nombre oficial de la Administración a la que pertenece el poseedor  |
| C                             |                    | <b>ES</b>   |
| <b>subjectPublicKeyInfo</b>   |                    | RSA 3072 bits mínimo  |
| <b>extensions</b>             |                    |   |
| <b>issuerAltName</b>          |                    | Igual a la extensión subjectAltName del certificado de la CA emisora  |
| <b>subjectAltName</b>         |                    |   |
| directoryName                 |                    |   |
| 2.16.724.1.3.5.4.2.1          |                    | <b>CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO</b>  |
| 2.16.724.1.3.5.4.2.2          |                    | Nombre oficial de la Administración a la que pertenece el poseedor  |
| 2.16.724.1.3.5.4.2.3          |                    | NIF   |
| 2.16.724.1.3.5.4.2.9          | Opcional           | Email de contacto   |
| 2.16.724.1.3.5.4.2.10         | Opcional           | Unidad dentro de la administración  |
| 2.16.724.1.3.5.4.2.11         | Opcional           | Puesto o cargo del suscriptor   |
| 2.16.724.1.3.5.4.2.12         |                    | Seudónimo   |
| UserPrincipalName             | Opcional           | UPN para smart card logon   |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública   |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier  |
| <b>certificatePolicies</b>    |                    |   |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.4.13.2  |
| cpsURI                        |                    | <a href="http://www.izenpe.eus/cps">http://www.izenpe.eus/cps</a>   |
| userNotice                    |                    | Kontsulta <a href="http://www.izenpe.eus">www.izenpe.eus</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.eus">www.izenpe.eus</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier              |                    | OID MINHAP: <b>2.16.724.1.3.5.4.2</b>   |
| policyIdentifier              |                    | OID QCP-n: <b>0.4.0.194112.1.0</b>  |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.com/cgi-bin/crlscar2">http://crl.izenpe.com/cgi-bin/crlscar2</a>   |
| <b>authorityInfoAccess</b>    |                    |   |
| ocsp                          |                    | <a href="http://ocsp.izenpe.com">http://ocsp.izenpe.com</a>   |
| CA emisora                    |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR_cert_sha256.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR_cert_sha256.crt</a>   |
| <b>qcStatements</b>           |                    |   |
| QcCompliance                  |                    | Presente  |
| QcType                        |                    | id-etsi-qct-esign   |
| QcEuRetentiodPeriod           |                    | 15 años   |
| QcPDS                         |                    | <a href="https://www.izenpe.eus/pds/en/en">https://www.izenpe.eus/pds/en/en</a><br><a href="https://www.izenpe.eus/pds/eu/eu">https://www.izenpe.eus/pds/eu/eu</a><br><a href="https://www.izenpe.eus/pds/es/es">https://www.izenpe.eus/pds/es/es</a>                         |
| <b>extendedKeyUsage</b>       |                    | clientAuth  |
| <b>keyUsage</b>               | Crítica            | contentCommitment (no repudio), digitalSignature, keyEncipherment   |

## Representante Tarjeta

CA emisora

CCEER

Nombre

representante

| Campo / extensión             | Opcional / Crítica | Contenido   |
|-------------------------------|--------------------|---|
| <b>version</b>                |                    | Versión 3   |
| <b>serialNumber</b>           |                    | Número secuencial único   |
| <b>signature</b>              |                    | sha256WithRSAEncryption   |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora   |
| <b>validity</b>               |                    | 4 años  |
| <b>subject</b>                |                    |   |
| C                             |                    | País  |
| CN                            |                    | DNI/NIE Nombre Apellido1 (R: NIF)   |
| G                             |                    | Nombre  |
| SN                            |                    | Apellidos   |
| serialNumber                  |                    | DNI / NIE   |
| O                             |                    | Razón social, tal como figura en los registros oficiales  |
| OU                            |                    | Ordezkarri ziurtagiria - Certificado de representante   |
| organizationIdentifier        |                    | 3 caracteres tipo-identidad + Country + - + identificador. Por ejemplo, si usamos el CIF sería algo como: VATES-A01337260   |
| descripción                   |                    | Codificación del documento público que acredita las facultades del firmante o los datos registrales. Hay tres opciones: registro mercantil, poder notarial, Boletines oficiales   |
| <b>subjectPublicKeyInfo</b>   |                    | RSA 3072 bits mínimo  |
| <b>extensions</b>             |                    |   |
| <b>issuerAltName</b>          |                    | Igual a la extensión subjectAltName del certificado de la CA emisora  |
| <b>extendedKeyUsage</b>       |                    | clientAuth, documentSigning   |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública   |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier  |
| <b>certificatePolicies</b>    |                    |   |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.2.12  |
| cpsURI                        |                    | <a href="http://www.izenpe.com/cps">http://www.izenpe.com/cps</a>   |
| userNotice                    |                    | Kontsulta <a href="http://www.izenpe.com">www.izenpe.com</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.com">www.izenpe.com</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier              |                    | 0.4.0.194112.1.0 (QCP-n)  |
| policyIdentifier              |                    | 2.16.724.1.3.5.8 (OID PJ MPR)   |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.com/cgi-bin/crl2">http://crl.izenpe.com/cgi-bin/crl2</a>   |
| <b>authorityInfoAccess</b>    |                    |   |
| ocsp                          |                    | <a href="http://ocsp.izenpe.com">http://ocsp.izenpe.com</a>   |
| CA emisora                    |                    | <a href="http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crt">http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crt</a>   |
| <b>qcStatements</b>           |                    |   |
| QcCompliance                  |                    | Presente  |
| QcType                        |                    | id-etsi-qct-esign   |
| QcRetentiodPeriod             |                    | 15 años   |
| QcPDS                         |                    | <a href="https://www.izenpe.eus/pds/en/en">https://www.izenpe.eus/pds/en/en</a><br><a href="https://www.izenpe.eus/pds/eu/eu">https://www.izenpe.eus/pds/eu/eu</a><br><a href="https://www.izenpe.eus/pds/es/es">https://www.izenpe.eus/pds/es/es</a>                         |
| qcStatement-2                 |                    | 0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)  |
| <b>keyUsage</b>               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment   |

## Representante Tarjeta

CA emisora

CCEER

Nombre

representante\_sscd

| Campo / extensión             | Opcional / Crítica | Contenido   |
|-------------------------------|--------------------|---|
| <b>version</b>                |                    | Versión 3   |
| <b>serialNumber</b>           |                    | Número secuencial único   |
| <b>signature</b>              |                    | sha256WithRSAEncryption   |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora   |
| <b>validity</b>               |                    | 4 años  |
| <b>subject</b>                |                    |   |
| C                             |                    | País  |
| CN                            |                    | DNI/NIE Nombre Apellido1 (R: NIF)   |
| G                             |                    | Nombre  |
| SN                            |                    | Apellidos   |
| serialNumber                  |                    | DNI / NIE   |
| O                             |                    | Razón social, tal como figura en los registros oficiales  |
| OU                            |                    | Ordezkarri ziurtagiria - Certificado de representante   |
| organizationIdentifier        |                    | 3 caracteres tipo-identidad + Country + - + identificador. Por ejemplo, si usamos el CIF sería algo como: VATES-A01337260   |
| descripción                   |                    | Codificación del documento público que acredita las facultades del firmante o los datos registrales. Hay tres opciones: registro mercantil, poder notarial, Boletines oficiales   |
| <b>subjectPublicKeyInfo</b>   |                    | RSA 3072 bits mínimo  |
| <b>extensions</b>             |                    |   |
| <b>issuerAltName</b>          |                    | Igual a la extensión subjectAltName del certificado de la CA emisora  |
| <b>extendedKeyUsage</b>       |                    | clientAuth, documentSigning   |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública   |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier  |
| <b>certificatePolicies</b>    |                    |   |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.2.12.5  |
| cpsURI                        |                    | <a href="http://www.izenpe.com/cps">http://www.izenpe.com/cps</a>   |
| userNotice                    |                    | Kontsulta <a href="http://www.izenpe.com">www.izenpe.com</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.com">www.izenpe.com</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier              |                    | 0.4.0.194112.1.2 (ETSI QCP-n-qscd)  |
| policyIdentifier              |                    | 2.16.724.1.3.5.8 (OID PJ MPR)   |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.com/cgi-bin/crl2">http://crl.izenpe.com/cgi-bin/crl2</a>   |
| <b>authorityInfoAccess</b>    |                    |   |
| ocsp                          |                    | <a href="http://ocsp.izenpe.com">http://ocsp.izenpe.com</a>   |
| CA emisora                    |                    | <a href="http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crt">http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crt</a>   |
| <b>qcStatements</b>           |                    |   |
| QcCompliance                  |                    | Presente  |
| QcType                        |                    | id-etsi-qct-esign   |
| QcSSCD                        |                    | Presente  |
| QcRetentiodPeriod             |                    | 15 años   |
| QcPDS                         |                    | <a href="https://www.izenpe.eus/pds/en/">https://www.izenpe.eus/pds/en/</a> en<br><a href="https://www.izenpe.eus/pds/eu/">https://www.izenpe.eus/pds/eu/</a> eu<br><a href="https://www.izenpe.eus/pds/es/">https://www.izenpe.eus/pds/es/</a> es                            |
| qcStatement-2                 |                    | 0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)  |
| <b>keyUsage</b>               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment   |

## Representante HSM

CA emisora

CCEER

Nombre

representante\_hsm

| Campo / extensión             | Opcional / Crítica | Contenido   |
|-------------------------------|--------------------|---|
| <b>version</b>                |                    | Versión 3   |
| <b>serialNumber</b>           |                    | Número secuencial único   |
| <b>signature</b>              |                    | sha256WithRSAEncryption   |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora   |
| <b>validity</b>               |                    | 4 años  |
| <b>subject</b>                |                    |   |
| C                             |                    | País  |
| CN                            |                    | DNI/NIE Nombre Apellido1 (R: NIF)   |
| G                             |                    | Nombre  |
| SN                            |                    | Apellidos   |
| serialNumber                  |                    | DNI / NIE   |
| O                             |                    | Razón social, tal como figura en los registros oficiales  |
| OU                            |                    | Ordezkarri ziurtagiria - Certificado de representante   |
| organizationIdentifier        |                    | 3 caracteres tipo-identidad + Country + - + identificador. Por ejemplo, si usamos el CIF sería algo como: VATES-A01337260   |
| descripción                   |                    | Codificación del documento público que acredita las facultades del firmante o los datos registrales. Hay tres opciones: registro mercantil, poder notarial, Boletines oficiales   |
| <b>subjectPublicKeyInfo</b>   |                    | RSA 3072 bits mínimo  |
| <b>extensions</b>             |                    |   |
| <b>issuerAltName</b>          |                    | Igual a la extensión subjectAltName del certificado de la CA emisora  |
| <b>extendedKeyUsage</b>       |                    | clientAuth, documentSigning   |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública   |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier  |
| <b>certificatePolicies</b>    |                    |   |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.2.14  |
| cpsURI                        |                    | <a href="http://www.izenpe.com/cps">http://www.izenpe.com/cps</a>   |
| userNotice                    |                    | Kontsulta <a href="http://www.izenpe.com">www.izenpe.com</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.com">www.izenpe.com</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier              |                    | 0.4.0.194112.1.0 (OID ETSI QCP-n)   |
| policyIdentifier              |                    | 2.16.724.1.3.5.8 (OID PJ MPR)   |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.com/cgi-bin/crl2">http://crl.izenpe.com/cgi-bin/crl2</a>   |
| <b>authorityInfoAccess</b>    |                    |   |
| ocsp                          |                    | <a href="http://ocsp.izenpe.com">http://ocsp.izenpe.com</a>   |
| CA emisora                    |                    | <a href="http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crt">http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crt</a>   |
| <b>qcStatements</b>           |                    |   |
| QcCompliance                  |                    | Presente  |
| QcType                        |                    | id-etsi-qct-esign   |
| QcRetentiodPeriod             |                    | 15 años   |
| QcPDS                         |                    | <a href="https://www.izenpe.eus/pds/en/en">https://www.izenpe.eus/pds/en/en</a><br><a href="https://www.izenpe.eus/pds/eu/eu">https://www.izenpe.eus/pds/eu/eu</a><br><a href="https://www.izenpe.eus/pds/es/es">https://www.izenpe.eus/pds/es/es</a>                         |
| qcStatement-2                 |                    | 0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)  |
| <b>keyUsage</b>               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment   |

## Representante Software

CA emisora

CCEER

Nombre

representante\_sw

| Campo / extensión             | Opcional / Crítica | Contenido   |
|-------------------------------|--------------------|---|
| <b>version</b>                |                    | Versión 3   |
| <b>serialNumber</b>           |                    | Número secuencial único   |
| <b>signature</b>              |                    | sha256WithRSAEncryption   |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora   |
| <b>validity</b>               |                    | 4 años  |
| <b>subject</b>                |                    |   |
| C                             |                    | País  |
| CN                            |                    | DNI/NIE Nombre Apellido1 (R: NIF)   |
| G                             |                    | Nombre  |
| SN                            |                    | Apellidos   |
| serialNumber                  |                    | DNI / NIE   |
| O                             |                    | Razón social, tal como figura en los registros oficiales  |
| OU                            |                    | Ordezkarri ziurtagiria - Certificado de representante   |
| organizationIdentifier        |                    | 3 caracteres tipo-identidad + Country + - + identificador. Por ejemplo, si usaramos el CIF sería algo como: VATES-A01337260   |
| descripción                   |                    | Codificación del documento público que acredita las facultades del firmante o los datos registrales. Hay tres opciones: registro mercantil, poder notarial, Boletines oficiales   |
| <b>subjectPublicKeyInfo</b>   |                    | RSA 3072 bits mínimo  |
| <b>extensions</b>             |                    |   |
| <b>issuerAltName</b>          |                    | Igual a la extensión subjectAltName del certificado de la CA emisora  |
| <b>extendedKeyUsage</b>       |                    | clientAuth, documentSigning   |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública   |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier  |
| <b>certificatePolicies</b>    |                    |   |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.2.16  |
| cpsURI                        |                    | <a href="http://www.izenpe.com/cps">http://www.izenpe.com/cps</a>   |
| userNotice                    |                    | Kontsulta <a href="http://www.izenpe.com">www.izenpe.com</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.com">www.izenpe.com</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier              |                    | 0.4.0.194112.1.0 (OID ETSI QCP-n)   |
| policyIdentifier              |                    | 2.16.724.1.3.5.8 (OID PJ MPR)   |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.com/cgi-bin/crl2">http://crl.izenpe.com/cgi-bin/crl2</a>   |
| <b>authorityInfoAccess</b>    |                    |   |
| ocsp                          |                    | <a href="http://ocsp.izenpe.com">http://ocsp.izenpe.com</a>   |
| CA emisora                    |                    | <a href="http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crt">http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crt</a>   |
| <b>qcStatements</b>           |                    |   |
| QcCompliance                  |                    | Presente  |
| QcType                        |                    | id-etsi-qct-esign   |
| QcRetentiodPeriod             |                    | 15 años   |
| QcPDS                         |                    | <a href="https://www.izenpe.eus/pds/en/">https://www.izenpe.eus/pds/en/</a> en<br><a href="https://www.izenpe.eus/pds/eu/">https://www.izenpe.eus/pds/eu/</a> eu<br><a href="https://www.izenpe.eus/pds/es/">https://www.izenpe.eus/pds/es/</a> es                            |
| qcStatement-2                 |                    | 0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)  |
| <b>keyUsage</b>               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment   |

## Representante SPJ Tarjeta

CA emisora

CCEER

Nombre

representante\_spj

| Campo / extensión             | Opcional / Crítica | Contenido   |
|-------------------------------|--------------------|---|
| <b>version</b>                |                    | Versión 3   |
| <b>serialNumber</b>           |                    | Número secuencial único   |
| <b>signature</b>              |                    | sha256WithRSAEncryption   |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora   |
| <b>validity</b>               |                    | 4 años  |
| <b>subject</b>                |                    |   |
| C                             |                    | País  |
| CN                            |                    | DNI/NIE Nombre Apellido1 (R: NIF)   |
| G                             |                    | Nombre  |
| SN                            |                    | Apellidos   |
| serialNumber                  |                    | DNI / NIE   |
| O                             |                    | Razón social, tal como figura en los registros oficiales  |
| OU                            |                    | NJG Ordezkarri ziurtagiria - Certificado de representante SPJ   |
| organizationIdentifier        |                    | 3 caracteres tipo-identidad + Country + - + identificador. Por ejemplo, si usamos el CIF sería algo como: VATES-A01337260   |
| descripción                   |                    | Codificación del documento público que acredita las facultades del firmante o los datos registrales. Hay tres opciones: registro mercantil, poder notarial, Boletines oficiales   |
| <b>subjectPublicKeyInfo</b>   |                    | RSA 3072 bits mínimo  |
| <b>extensions</b>             |                    |   |
| <b>issuerAltName</b>          |                    | Igual a la extensión subjectAltName del certificado de la CA emisora  |
| <b>extendedKeyUsage</b>       |                    | clientAuth, documentSigning   |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública   |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier  |
| <b>certificatePolicies</b>    |                    |   |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.2.13  |
| cpsURI                        |                    | <a href="http://www.izenpe.com/cps">http://www.izenpe.com/cps</a>   |
| userNotice                    |                    | Kontsulta <a href="http://www.izenpe.com">www.izenpe.com</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.com">www.izenpe.com</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier              |                    | 0.4.0.194112.1.0 (QCP-n)  |
| policyIdentifier              |                    | 2.16.724.1.3.5.9 (OID PJ MPR)   |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.com/cgi-bin/crl2">http://crl.izenpe.com/cgi-bin/crl2</a>   |
| <b>authorityInfoAccess</b>    |                    |   |
| ocsp                          |                    | <a href="http://ocsp.izenpe.com">http://ocsp.izenpe.com</a>   |
| CA emisora                    |                    | <a href="http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crl">http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crl</a>   |
| <b>qcStatements</b>           |                    |   |
| QcCompliance                  |                    | Presente  |
| QcType                        |                    | id-etsi-qct-esign   |
| QcRetentiodPeriod             |                    | 15 años   |
| QcPDS                         |                    | <a href="https://www.izenpe.eus/pds/en/">https://www.izenpe.eus/pds/en/</a> en<br><a href="https://www.izenpe.eus/pds/eu/">https://www.izenpe.eus/pds/eu/</a> eu<br><a href="https://www.izenpe.eus/pds/es/">https://www.izenpe.eus/pds/es/</a> es                            |
| qcStatement-2                 |                    | 0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)  |
| <b>keyUsage</b>               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment   |

## Representante SPJ Tarjeta

CA emisora

CCEER

Nombre

representante\_spj\_qc

| Campo / extensión      | Opcional / Crítica | Contenido  |
|------------------------|--------------------|--|
| version                |                    | Versión 3  |
| serialNumber           |                    | Número secuencial único  |
| signature              |                    | sha256WithRSAEncryption  |
| issuer                 |                    | Igual al campo subject del certificado de la CA emisora  |
| validity               |                    | 4 años   |
| subject                |                    |  |
| C                      |                    | País   |
| CN                     |                    | DNI/NIE Nombre Apellido1 (R: NIF)  |
| G                      |                    | Nombre   |
| SN                     |                    | Apellidos  |
| serialNumber           |                    | DNI / NIE  |
| O                      |                    | Razón social, tal como figura en los registros oficiales   |
| OU                     |                    | NJG Ordezkarri zuztagiria - Certificado de representante SPJ   |
| organizationIdentifier |                    | 3 caracteres tipo-identidad + Country + - + identificador. Por ejemplo, si usamos el CIF sería algo como: VATES-A01337260  |
| descripción            |                    | Codificación del documento público que acredita las facultades del firmante o los datos registrales. Hay tres opciones: registro mercantil, poder notarial, Boletines oficiales  |
| subjectPublicKeyInfo   |                    | RSA 3072 bits mínimo   |
| extensions             |                    |  |
| issuerAltName          |                    | Igual a la extensión subjectAltName del certificado de la CA emisora   |
| extendedKeyUsage       |                    | clientAuth, documentSigning  |
| subjectKeyIdentifier   |                    | Identificador de la clave pública  |
| authorityKeyIdentifier |                    | Incluir sólo campo keyIdentifier   |
| certificatePolicies    |                    |  |
| policyIdentifier       |                    | 1.3.6.1.4.1.14777.2.13.5   |
| cpsURI                 |                    | <a href="http://www.izenpe.com/cps">http://www.izenpe.com/cps</a>  |
| userNotice             |                    | Kontsulta <a href="http://www.izenpe.com">www.izenpe.com</a> -en baldintzak eta kondizioak zuztagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.com">www.izenpe.com</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier       |                    | 0.4.0.194112.1.2 (ETSI QCP-n-qscd)   |
| policyIdentifier       |                    | 2.16.724.1.3.5.9 (OID PJ MPR)  |
| cRLDistributionPoints  |                    | <a href="http://crl.izenpe.com/cgi-bin/crl2">http://crl.izenpe.com/cgi-bin/crl2</a>  |
| authorityInfoAccess    |                    |  |
| ocsp                   |                    | <a href="http://ocsp.izenpe.com">http://ocsp.izenpe.com</a>  |
| CA emisora             |                    | <a href="http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crf">http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crf</a>  |
| qcStatements           |                    |  |
| QcCompliance           |                    | Presente   |
| QcType                 |                    | id-etsi-qct-esign  |
| QcSSCD                 |                    | Presente   |
| QcRetentiodPeriod      |                    | 15 años  |
| QcPDS                  |                    | <a href="https://www.izenpe.eus/pds/en/">https://www.izenpe.eus/pds/en/</a> en<br><a href="https://www.izenpe.eus/pds/eu/">https://www.izenpe.eus/pds/eu/</a> eu<br><a href="https://www.izenpe.eus/pds/es/">https://www.izenpe.eus/pds/es/</a> es                           |
| qcStatement-2          |                    | 0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)   |
| keyUsage               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment  |

## Representante SPJ HSM

CA emisora

CCEER

Nombre

representante\_spj\_hsm

| Campo / extensión             | Opcional / Crítica | Contenido   |
|-------------------------------|--------------------|---|
| <b>version</b>                |                    | Versión 3   |
| <b>serialNumber</b>           |                    | Número secuencial único   |
| <b>signature</b>              |                    | sha256WithRSAEncryption   |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora   |
| <b>validity</b>               |                    | 4 años  |
| <b>subject</b>                |                    |   |
| C                             |                    | País  |
| CN                            |                    | DNI/NIE Nombre Apellido1 (R: NIF)   |
| G                             |                    | Nombre  |
| SN                            |                    | Apellidos   |
| serialNumber                  |                    | DNI / NIE   |
| O                             |                    | Razón social, tal como figura en los registros oficiales  |
| OU                            |                    | NJG Ordezkarri ziurtagiria - Certificado de representante SPJ   |
| organizationIdentifier        |                    | 3 caracteres tipo-identidad + Country + - + identificador. Por ejemplo, si usaramos el CIF sería algo como: VATES-A01337260   |
| descripción                   |                    | Codificación del documento público que acredita las facultades del firmante o los datos registrales. Hay tres opciones: registro mercantil, poder notarial, Boletines oficiales   |
| <b>subjectPublicKeyInfo</b>   |                    | RSA 3072 bits mínimo  |
| <b>extensions</b>             |                    |   |
| <b>issuerAltName</b>          |                    | Igual a la extensión subjectAltName del certificado de la CA emisora  |
| <b>extendedKeyUsage</b>       |                    | clientAuth, documentSigning   |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública   |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier  |
| <b>certificatePolicies</b>    |                    |   |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.2.15  |
| cpsURI                        |                    | <a href="http://www.izenpe.com/cps">http://www.izenpe.com/cps</a>   |
| userNotice                    |                    | Kontsulta <a href="http://www.izenpe.com">www.izenpe.com</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.com">www.izenpe.com</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier              |                    | 0.4.0.194112.1.0 (OID ETSI QCP-n)   |
| policyIdentifier              |                    | 2.16.724.1.3.5.9 (OID PJ MPR)   |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.com/cgi-bin/crl2">http://crl.izenpe.com/cgi-bin/crl2</a>   |
| <b>authorityInfoAccess</b>    |                    |   |
| ocsp                          |                    | <a href="http://ocsp.izenpe.com">http://ocsp.izenpe.com</a>   |
| CA emisora                    |                    | <a href="http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crt">http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crt</a>   |
| <b>qcStatements</b>           |                    |   |
| QcCompliance                  |                    | Presente  |
| QcType                        |                    | id-etsi-qct-sign  |
| QcRetentiodPeriod             |                    | 15 años   |
| QcPDS                         |                    | <a href="https://www.izenpe.eus/pds/en/">https://www.izenpe.eus/pds/en/</a> en<br><a href="https://www.izenpe.eus/pds/eu/">https://www.izenpe.eus/pds/eu/</a> eu<br><a href="https://www.izenpe.eus/pds/es/">https://www.izenpe.eus/pds/es/</a> es                            |
| qcStatement-2                 |                    | 0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)  |
| <b>keyUsage</b>               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment   |

## Representante SPJ Software

CA emisora

CCEER

Nombre

representante\_spj\_sw

| Campo / extensión             | Opcional / Crítica | Contenido   |
|-------------------------------|--------------------|---|
| <b>version</b>                |                    | Versión 3   |
| <b>serialNumber</b>           |                    | Número secuencial único   |
| <b>signature</b>              |                    | sha256WithRSAEncryption   |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora   |
| <b>validity</b>               |                    | 4 años  |
| <b>subject</b>                |                    |   |
| C                             |                    | País  |
| CN                            |                    | DNI/NIE Nombre Apellido1 (R: NIF)   |
| G                             |                    | Nombre  |
| SN                            |                    | Apellidos   |
| serialNumber                  |                    | DNI / NIE   |
| O                             |                    | Razón social, tal como figura en los registros oficiales  |
| OU                            |                    | NJG Ordezkarri ziurtagiria - Certificado de representante SPJ   |
| organizationIdentifier        |                    | 3 caracteres tipo-identidad + Country + - + identificador. Por ejemplo, si usamos el CIF sería algo como: VATES-A01337260   |
| descripción                   |                    | Codificación del documento público que acredita las facultades del firmante o los datos registrales. Hay tres opciones: registro mercantil, poder notarial, Boletines oficiales   |
| <b>subjectPublicKeyInfo</b>   |                    | RSA 3072 bits mínimo  |
| <b>extensions</b>             |                    |   |
| <b>issuerAltName</b>          |                    | Igual a la extensión subjectAltName del certificado de la CA emisora  |
| <b>extendedKeyUsage</b>       |                    | clientAuth, documentSigning   |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública   |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier  |
| <b>certificatePolicies</b>    |                    |   |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.2.17  |
| cpsURI                        |                    | <a href="http://www.izenpe.com/cps">http://www.izenpe.com/cps</a>   |
| userNotice                    |                    | Kontsulta <a href="http://www.izenpe.com">www.izenpe.com</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.com">www.izenpe.com</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier              |                    | 0.4.0.194112.1.0 (OID ETSI QCP-n)   |
| policyIdentifier              |                    | 2.16.724.1.3.5.9 (OID PJ MPR)   |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.com/cgi-bin/crl2">http://crl.izenpe.com/cgi-bin/crl2</a>   |
| <b>authorityInfoAccess</b>    |                    |   |
| ocsp                          |                    | <a href="http://ocsp.izenpe.com">http://ocsp.izenpe.com</a>   |
| CA emisora                    |                    | <a href="http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crt">http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crt</a>   |
| <b>qcStatements</b>           |                    |   |
| QcCompliance                  |                    | Presente  |
| QcType                        |                    | id-etsi-qct-esign   |
| QcRetentiodPeriod             |                    | 15 años   |
| QcPDS                         |                    | <a href="https://www.izenpe.eus/pds/en/">https://www.izenpe.eus/pds/en/</a> en<br><a href="https://www.izenpe.eus/pds/eu/">https://www.izenpe.eus/pds/eu/</a> eu<br><a href="https://www.izenpe.eus/pds/es/">https://www.izenpe.eus/pds/es/</a> es                            |
| qcStatement-2                 |                    | 0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)  |
| <b>keyUsage</b>               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment   |

## Sello Entidad

CA emisora

CCEER

Nombre

sello\_juridico

| Campo / extensión             | Opcional / Crítica | Contenido  |
|-------------------------------|--------------------|--|
| <b>version</b>                |                    | Versión 3  |
| <b>serialNumber</b>           |                    | Número secuencial único  |
| <b>signature</b>              |                    | sha256WithRSAEncryption  |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora  |
| <b>validity</b>               |                    | 3 años   |
| <b>subject</b>                |                    |  |
| serialNumber                  | Opcional           | DNI/NIE según semántica ETSI EN 319 412 - 1  |
| SN                            | Opcional           | Apellidos  |
| G                             | Opcional           | Nombre   |
| CN                            |                    | Nombre comúnmente utilizado por el sujeto para representarse a sí mismo  |
| organizationIdentifier        |                    | 3 caracteres tipo-identidad + Country + - + identificador. Por ejemplo, si usaramos el CIF sería algo como: VATES-A01337260  |
| O                             |                    | Nombre completo registrado del sujeto/organización   |
| C                             |                    | País   |
| <b>subjectPublicKeyInfo</b>   |                    | RSA 3072 bits mínimo   |
| <b>extensions</b>             |                    |  |
| <b>issuerAltName</b>          |                    | Igual a la extensión subjectAltName del certificado de la CA emisora   |
| <b>extendedKeyUsage</b>       |                    | clientAuth, emailProtection  |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública  |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier   |
| <b>certificatePolicies</b>    |                    |  |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.2.11   |
| cpsURI                        |                    | <a href="http://www.izenpe.eus/cps">http://www.izenpe.eus/cps</a>  |
| userNotice                    |                    | Konsulta <a href="http://www.izenpe.eus">www.izenpe.eus</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.eus">www.izenpe.eus</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier              |                    | 0.4.0.194112.1.1 (OID ETSI QCP-I)  |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.com/cgi-bin/crl2">http://crl.izenpe.com/cgi-bin/crl2</a>  |
| <b>authorityInfoAccess</b>    |                    |  |
| ocsp                          |                    | <a href="http://ocsp.izenpe.com">http://ocsp.izenpe.com</a>  |
| CA emisora                    |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crt</a>  |
| <b>qcStatements</b>           |                    |  |
| QcCompliance                  |                    | Presente   |
| QcType                        |                    | id-etsi-qct-eseal  |
| QcRetentiodPeriod             |                    | 15 años  |
| QcPDS                         |                    | <a href="https://www.izenpe.eus/pds/en/">https://www.izenpe.eus/pds/en/</a> en<br><a href="https://www.izenpe.eus/pds/eu/">https://www.izenpe.eus/pds/eu/</a> eu<br><a href="https://www.izenpe.eus/pds/es/">https://www.izenpe.eus/pds/es/</a> es                           |
| qcStatement-2                 |                    | 0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)   |
| qcStatement-2                 |                    | 0.4.0.194121.1.1 (id-etsi-qcs-SemanticsId-Natural)   |
| <b>keyUsage</b>               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment  |

## Sello Entidad HSM

CA emisora

CCEER

Nombre

sello\_juridico\_hsm

| Campo / extensión             | Opcional / Crítica | Contenido  |
|-------------------------------|--------------------|--|
| <b>version</b>                |                    | Versión 3  |
| <b>serialNumber</b>           |                    | Número secuencial único  |
| <b>signature</b>              |                    | sha256WithRSAEncryption  |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora  |
| <b>validity</b>               |                    | 3 años   |
| <b>subject</b>                |                    |  |
| serialNumber                  | Opcional           | DNI/NIE según semántica ETSI EN 319 412 - 1  |
| SN                            | Opcional           | Apellidos  |
| G                             | Opcional           | Nombre   |
| CN                            |                    | Nombre comúnmente utilizado por el sujeto para representarse a sí mismo  |
| organizationIdentifier        |                    | 3 caracteres tipo-identidad + Country + - + identificador. Por ejemplo, si usamos el CIF sería algo como: VATES-A01337260  |
| O                             |                    | Nombre completo registrado del sujeto/organización   |
| C                             |                    | País   |
| <b>subjectPublicKeyInfo</b>   |                    | RSA 3072 bits mínimo   |
| <b>extensions</b>             |                    |  |
| <b>issuerAltName</b>          |                    | Igual a la extensión subjectAltName del certificado de la CA emisora   |
| <b>extendedKeyUsage</b>       |                    | clientAuth, emailProtection  |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública  |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier   |
| <b>certificatePolicies</b>    |                    |  |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.2.20   |
| cpsURI                        |                    | <a href="http://www.izenpe.eus/cps">http://www.izenpe.eus/cps</a>  |
| userNotice                    |                    | Konsulta <a href="http://www.izenpe.eus">www.izenpe.eus</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.eus">www.izenpe.eus</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier              |                    | 0.4.0.194112.1.1 (OID ETSI QCP-I)  |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.com/cgi-bin/crl2">http://crl.izenpe.com/cgi-bin/crl2</a>  |
| <b>authorityInfoAccess</b>    |                    |  |
| ocsp                          |                    | <a href="http://ocsp.izenpe.com">http://ocsp.izenpe.com</a>  |
| CA emisora                    |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crt</a>  |
| <b>qcStatements</b>           |                    |  |
| QcCompliance                  |                    | Presente   |
| QcType                        |                    | id-etsi-qct-eseal  |
| QcRetentiodPeriod             |                    | 15 años  |
| QcPDS                         |                    | <a href="https://www.izenpe.eus/pds/en/">https://www.izenpe.eus/pds/en/</a> en<br><a href="https://www.izenpe.eus/pds/eu/">https://www.izenpe.eus/pds/eu/</a> eu<br><a href="https://www.izenpe.eus/pds/es/">https://www.izenpe.eus/pds/es/</a> es                           |
| qcStatement-2                 |                    | 0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)   |
| qcStatement-2                 |                    | 0.4.0.194121.1.1 (id-etsi-qcs-SemanticsId-Natural)   |
| <b>keyUsage</b>               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment  |

## Aplicación

**CA emisora**

**AAPPNR**

**Nombre**

**servidores\_aplicacion**

| Campo / extensión             | Opcional / Crítica | Contenido   |
|-------------------------------|--------------------|---|
| <b>version</b>                |                    | Versión 3   |
| <b>serialNumber</b>           |                    | Número secuencial único   |
| <b>signature</b>              |                    | sha256WithRSAEncryption   |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora   |
| <b>validity</b>               |                    | 3 años  |
| <b>subject</b>                |                    |   |
| ST                            |                    | Provincia   |
| L                             |                    | Localidad   |
| EA                            |                    | Correo electrónico  |
| CN                            |                    | Nombre de la aplicación   |
| OU                            |                    | Departamento  |
| O                             |                    | Nombre de la entidad  |
| C                             |                    | ES  |
| <b>subjectPublicKeyInfo</b>   |                    | RSA 3072 bits mínimo  |
| <b>extensions</b>             |                    |   |
| <b>issuerAltName</b>          |                    | Igual a la extensión subjectAltName del certificado de la CA emisora  |
| <b>subjectAltName</b>         | Opcional           | Igual a la extensión subjectAltName de la petición, si está presente  |
| <b>extendedKeyUsage</b>       |                    | clientAuth, emailProtection   |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública   |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier  |
| <b>certificatePolicies</b>    |                    |   |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.1.2.2   |
| cpsURI                        |                    | <a href="http://www.izenpe.com/cps">http://www.izenpe.com/cps</a>   |
| <b>userNotice</b>             |                    | Bermeen mugak ezagutzeko <a href="http://www.izenpe.com">www.izenpe.com</a> Ziurtagirian konfiantza izan aurretik kontratua irakurri. Limitaciones de garantías en <a href="http://www.izenpe.com">www.izenpe.com</a> Consulte el contrato antes de confiar en el certificado |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.com/cgi-bin/crlInterna2">http://crl.izenpe.com/cgi-bin/crlInterna2</a>   |
| <b>authorityInfoAccess</b>    |                    | ocsp <a href="http://ocsp.izenpe.com">http://ocsp.izenpe.com</a>  |
| <b>keyUsage</b>               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment   |

## Firma de Código

CA emisora

AAPPNR

Nombre

firma\_codigo

| Campo / extensión             | Opcional / Crítica | Contenido  |
|-------------------------------|--------------------|--|
| <b>version</b>                |                    | Versión 3  |
| <b>serialNumber</b>           |                    | Número secuencial único  |
| <b>signature</b>              |                    | sha256WithRSAEncryption  |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora  |
| <b>validity</b>               |                    | 3 años   |
| <b>subject</b>                |                    |  |
| CN                            |                    | Debe contener el nombre legal de la entidad  |
| OU                            | Opcional           | Departamento   |
| O                             |                    | Debe contener el nombre legal de la entidad  |
| streetAddress                 | Opcional           | Dirección  |
| L                             |                    | Localidad  |
| ST                            |                    | Provincia  |
| postalCode                    | Opcional           | Código Postal  |
| C                             |                    | País   |
| <b>subjectPublicKeyInfo</b>   |                    | RSA 3072 bits mínimo   |
| <b>extensions</b>             |                    |  |
| <b>issuerAltName</b>          |                    | Igual a la extensión subjectAltName del certificado de la CA emisora   |
| <b>subjectAltName</b>         |                    | Identificador permanente   |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública  |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier   |
| <b>certificatePolicies</b>    |                    |  |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.1.3.1  |
| cpsURI                        |                    | <a href="http://www.izenpe.com/cps">http://www.izenpe.com/cps</a>  |
| userNotice                    |                    | Bermeen mugak ezagutzeko <a href="http://www.izenpe.com">www.izenpe.com</a> Ziurtagirian konfiantza izan aurretik kontratua irakurri. Limitaciones de garantías en <a href="http://www.izenpe.com">www.izenpe.com</a> Consulte el contrato antes de confiar en el certificado  |
| policyIdentifier              |                    | 2.23.140.1.4.1   |
| <b>extendedKeyUsage</b>       |                    | codeSigning  |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.com/cgi-bin/crlinterna2">http://crl.izenpe.com/cgi-bin/crlinterna2</a>  |
| <b>authorityInfoAccess</b>    |                    | <b>ocsp</b> <a href="http://ocsp.izenpe.com">http://ocsp.izenpe.com</a><br><b>root</b> <a href="http://www.izenpe.com/s15-12020/es/contenidos/informacion/cas_izenpe/es_cas/adjuntos/RAIZ2007_cert_sha256.crt">http://www.izenpe.com/s15-12020/es/contenidos/informacion/cas_izenpe/es_cas/adjuntos/RAIZ2007_cert_sha256.crt</a> |
| <b>keyUsage</b>               | Crítica            | digitalSignature   |

## Aplicación

**CA emisora**

**AAPPNR**

**Nombre**

**device**

| Campo / extensión             | Opcional / Crítica | Contenido   |
|-------------------------------|--------------------|---|
| <b>version</b>                |                    | Versión 3   |
| <b>serialNumber</b>           |                    | Número secuencial único   |
| <b>signature</b>              |                    | sha256WithRSAEncryption   |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora   |
| <b>validity</b>               |                    | 10 años   |
| <b>subject</b>                |                    |   |
| CN                            |                    | Número serie dispositivo  |
| OU                            | Opcional           | Tipo dispositivo  |
| OU                            | Opcional           | Modelo dispositivo  |
| OU                            |                    | Gailu ziurtagiria - Certificado de dispositivo  |
| O                             | Opcional           | Nombre del fabricante   |
| C                             |                    | País  |
| <b>subjectPublicKeyInfo</b>   |                    | RSA 4096 bits mínimo  |
| <b>extensions</b>             |                    |   |
| <b>issuerAltName</b>          |                    | Igual a la extensión subjectAltName del certificado de la CA emisora  |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública   |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier  |
| <b>certificatePolicies</b>    |                    |   |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.1.3.2   |
| cpsURI                        |                    | <a href="http://www.izenpe.com/cps">http://www.izenpe.com/cps</a>   |
| userNotice                    |                    | Bermeen mugak ezagutzeko <a href="http://www.izenpe.com">www.izenpe.com</a> Ziurtagirian konfiantza izan aurretik kontratua irakurri. Limitaciones de garantías en <a href="http://www.izenpe.com">www.izenpe.com</a> Consulte el contrato antes de confiar en el certificado |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.com/cgi-bin/crlinterna2">http://crl.izenpe.com/cgi-bin/crlinterna2</a>   |
| <b>authorityInfoAccess</b>    |                    |   |
| ocsp                          |                    | <a href="http://ocsp.izenpe.com">http://ocsp.izenpe.com</a>   |
| CA emisora                    |                    | <a href="http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPNR_cert_sha256.crt">http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPNR_cert_sha256.crt</a>   |
| <b>extendedKeyUsage</b>       |                    | clientAuth, documentSigning   |
| <b>keyUsage</b>               | Crítica            | digitalSignature, keyEncipherment   |

## Servidor Web

CA emisora

AAPPNR

Nombre

ssl\_dv

| Campo / extensión      | Opcional / Crítica | Contenido   |
|------------------------|--------------------|---|
| version                |                    | Versión 3   |
| serialNumber           |                    | Número aleatorio único  |
| signature              |                    | sha256WithRSAEncryption   |
| issuer                 |                    | Igual al campo subject del certificado de la CA emisora   |
| validity               |                    | 395 días  |
| subject                |                    |   |
| CN                     | Opcional           | Dominio DNS   |
| subjectPublicKeyInfo   |                    | RSA 2048 bits mínimo  |
| extensions             |                    |   |
| issuerAltName          |                    | Igual a la extensión subjectAltName del certificado de la CA emisora  |
| subjectAltName         |                    |   |
| dNSName                |                    | Dominios DNS adicionales  |
| extendedKeyUsage       |                    | serverAuth, clientAuth  |
| subjectKeyIdentifier   |                    | Identificador de la clave pública   |
| authorityKeyIdentifier |                    | Incluir sólo campo keyIdentifier  |
| certificatePolicies    |                    |   |
| policyIdentifier       |                    | 1.3.6.1.4.1.14777.1.2.4   |
| cpsURI                 |                    | <a href="http://www.izenpe.eus/cps-ssl">http://www.izenpe.eus/cps-ssl</a>   |
| policyIdentifier       |                    | 2.23.140.1.2.1  |
| policyIdentifier       |                    | 0.4.0.2042.1.6  |
| cRLDistributionPoints  |                    | <a href="http://crl.izenpe.com/cgi-bin/crlinterna2">http://crl.izenpe.com/cgi-bin/crlinterna2</a>   |
| authorityInfoAccess    |                    |   |
| ocsp                   |                    | <a href="http://ocsp.izenpe.com">http://ocsp.izenpe.com</a>   |
| CA emisora             |                    | <a href="http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPNR_cert_sha256.crt">http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPNR_cert_sha256.crt</a> |
| keyUsage               | Crítica            | digitalSignature, keyEncipherment   |

## Servidor Web

CA emisora

SUBCA SSL 2024

Nombre

ssl\_dv

| Campo / extensión      | Opcional / Crítica | Contenido   |
|------------------------|--------------------|---|
| version                |                    | Versión 3   |
| serialNumber           |                    | Número aleatorio único  |
| signature              |                    | sha384ECDSA   |
| issuer                 |                    | Igual al campo subject del certificado de la CA emisora   |
| validity               |                    | 395 días  |
| subject                |                    |   |
| CN                     | Opcional           | Dominio DNS   |
| subjectPublicKeyInfo   |                    | ECC 256 bits mínimo   |
| extensions             |                    |   |
| issuerAltName          |                    | Igual a la extensión subjectAltName del certificado de la CA emisora  |
| subjectAltName         |                    |   |
| dNSName                |                    | Dominios DNS adicionales  |
| extendedKeyUsage       |                    | serverAuth, clientAuth  |
| authorityKeyIdentifier |                    | Incluir sólo campo keyIdentifier  |
| certificatePolicies    |                    |   |
| policyIdentifier       |                    | 2.23.140.1.2.1  |
| policyIdentifier       |                    | 1.3.6.1.4.1.14777.50.1.2  |
| policyIdentifier       |                    | 0.4.0.2042.1.6  |
| cRLDistributionPoints  |                    | <a href="http://crl.izenpe.eus/2024/crlessl.crt">http://crl.izenpe.eus/2024/crlessl.crt</a>   |
| authorityInfoAccess    |                    |   |
| ocsp                   |                    | <a href="http://ocsp.izenpe.eus">http://ocsp.izenpe.eus</a>   |
| CA emisora             |                    | <a href="http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/SSL2024.crt">http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/SSL2024.crt</a> |
| keyUsage               | Crítica            | digitalSignature  |

## Servidor Web

CA emisora

AAPPNR

Nombre

servidor\_ssl\_sha256 (OV)

| Campo / extensión      | Opcional / Crítica | Contenido   |
|------------------------|--------------------|---|
| version                |                    | Versión 3   |
| serialNumber           |                    | Número aleatorio único  |
| signature              |                    | sha-256WithRSAEncryption  |
| issuer                 |                    | Igual al campo subject del certificado de la CA emisora   |
| validity               |                    | 395 días  |
| subject                |                    |   |
| CN                     |                    | Dominio DNS   |
| O                      |                    | Nombre de la organización   |
| L                      |                    | Localidad   |
| ST                     |                    | Provincia   |
| C                      |                    | País  |
| subjectPublicKeyInfo   |                    | RSA 2048 bits mínimo  |
| extensions             |                    |   |
| issuerAltName          |                    | Igual a la extensión subjectAltName del certificado de la CA emisora  |
| subjectAltName         |                    |   |
| dNSName                |                    | Dominios DNS adicionales  |
| extendedKeyUsage       |                    | serverAuth, clientAuth  |
| subjectKeyIdentifier   |                    | Identificador de la clave pública   |
| authorityKeyIdentifier |                    | Incluir sólo campo keyIdentifier  |
| certificatePolicies    |                    |   |
| policyIdentifier       |                    | 1.3.6.1.4.1.14777.1.2.1   |
| cpsURI                 |                    | <a href="http://www.izenpe.eus/cps-ssl">http://www.izenpe.eus/cps-ssl</a>   |
| policyIdentifier       |                    | 2.23.140.1.2.2  |
| policyIdentifier       |                    | 0.4.0.2042.1.7  |
| cRLDistributionPoints  |                    | <a href="http://crl.izenpe.com/cgi-bin/crlinterna2">http://crl.izenpe.com/cgi-bin/crlinterna2</a>   |
| authorityInfoAccess    |                    |   |
| ocsp                   |                    | <a href="http://ocsp.izenpe.com">http://ocsp.izenpe.com</a>   |
| CA emisora             |                    | <a href="http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPNR_cert_sha256.crt">http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPNR_cert_sha256.crt</a> |
| keyUsage               | Crítica            | digitalSignature, keyEncipherment   |

## Servidor Web

CA emisora

SUBCA SSL 2024

Nombre

ssl\_ov

| Campo / extensión             | Opcional / Crítica | Contenido   |
|-------------------------------|--------------------|---|
| <b>version</b>                |                    | Versión 3   |
| <b>serialNumber</b>           |                    | Número aleatorio único  |
| <b>signature</b>              |                    | sha384ECDSA   |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora   |
| <b>validity</b>               |                    | 395 días  |
| <b>subject</b>                |                    |   |
| C                             |                    | País  |
| ST                            |                    | Provincia   |
| L                             |                    | Localidad   |
| O                             |                    | Nombre de la organización   |
| CN                            | Opcional           | Dominio   |
| <b>subjectPublicKeyInfo</b>   |                    | ECC 256 bits mínimo   |
| <b>extensions</b>             |                    |   |
| <b>issuerAltName</b>          |                    | Igual a la extensión subjectAltName del certificado de la CA emisora  |
| <b>subjectAltName</b>         |                    |   |
| dNSName                       |                    | Dominios DNS adicionales  |
| <b>extendedKeyUsage</b>       |                    | serverAuth, clientAuth  |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier  |
| <b>certificatePolicies</b>    |                    |   |
| policyIdentifier              |                    | 2.23.140.1.2.2  |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.50.2.2  |
| policyIdentifier              |                    | 0.4.0.2042.1.7  |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.eus/2024/crissl.crl">http://crl.izenpe.eus/2024/crissl.crl</a>   |
| <b>authorityInfoAccess</b>    |                    |   |
| ocsp                          |                    | <a href="http://ocsp.izenpe.eus">http://ocsp.izenpe.eus</a>   |
| CA emisora                    |                    | <a href="http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/SSL2024.crt">http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/SSL2024.crt</a> |
| <b>keyUsage</b>               | Crítica            | digitalSignature  |

## Sello Verde

CA emisora

AAPPNR

Nombre

sello\_verde

| Campo / extensión             | Opcional / Crítica | Contenido   |
|-------------------------------|--------------------|---|
| <b>version</b>                |                    | Versión 3   |
| <b>serialNumber</b>           |                    | Número secuencial único   |
| <b>signature</b>              |                    | sha256WithRSAEncryption   |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora   |
| <b>validity</b>               |                    | 3 años  |
| <b>subject</b>                |                    |   |
| CN                            |                    | Nombre comúnmente utilizado por el sujeto para representarse a sí mismo   |
| organizationIdentifier        |                    | 3 caracteres tipo-identidad + Country + - + identificador. Por ejemplo, si usamos el NIF sería algo como: VATES-A01337260   |
| OU                            |                    | <b>"SELLO ELECTRONICO"</b>  |
| O                             |                    | Nombre oficial de la organización   |
| C                             |                    | <b>ES</b>   |
| <b>subjectPublicKeyInfo</b>   |                    | ECC 256 bits  |
| <b>extensions</b>             |                    |   |
| <b>issuerAltName</b>          |                    | Igual a la extensión subjectAltName del certificado de la CA emisora  |
| <b>subjectAltName</b>         |                    |   |
| directoryName                 |                    |   |
| 1.3.6.1.4.1.14777.0.5         |                    | Nombre oficial de la organización   |
| 1.3.6.1.4.1.14777.0.6         |                    | NIF   |
| <b>extendedKeyUsage</b>       |                    | clientAuth  |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública   |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier  |
| <b>certificatePolicies</b>    |                    |   |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.1.2.5   |
| cpsURI                        |                    | <a href="http://www.izenpe.eus/cps">http://www.izenpe.eus/cps</a>   |
| userNotice                    |                    | Kontsulta <a href="http://www.izenpe.eus">www.izenpe.eus</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.eus">www.izenpe.eus</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.com/cgi-bin/crlinterna2">http://crl.izenpe.com/cgi-bin/crlinterna2</a>   |
| <b>authorityInfoAccess</b>    |                    |   |
| ocsp                          |                    | <a href="http://ocsp.izenpe.eus">http://ocsp.izenpe.eus</a>   |
| CA emisora                    |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPNR_cert_sha256.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPNR_cert_sha256.crt</a>   |
| <b>keyUsage</b>               | Crítica            | digitalSignature, nonRepudiation (<>contentCommitment), keyEncipherment   |

## SSL Cualificada

**CA emisora**

**SSLEV**

**Nombre**

**ssl\_qualified**

| Campo / extensión                              | Opcional / Crítica | Contenido   |
|--|--------------------|---|
| <b>version</b>                                 |                    | Versión 3   |
| <b>serialNumber</b>                            |                    | Número aleatorio único  |
| <b>signature</b>                               |                    | sha256WithRSAEncryption   |
| <b>issuer</b>                                  |                    | Igual al campo subject del certificado de la CA emisora   |
| <b>validity</b>                                |                    | 395 días  |
| <b>subject</b>                                 |                    |   |
| CN   | Opcional           | Dominio DNS   |
| O  |                    | Organización  |
| street   | Opcional           | Calle   |
| L  |                    | Localidad   |
| ST   |                    | Provincia   |
| C  |                    | País  |
| postalCode                                     | Opcional           | Código postal   |
| serialNumber                                   |                    | CIF   |
| businessCategory                               |                    | [OID.2.5.4.15]<br>Valores posibles:<br>- "Private Organization" para Organización privada<br>- "Government Entity" para Entidad pública<br>- "Business Entity" para Empresa<br>- "Non-comercial Entity" para Entidad no comercial                     |
| jurisdictionOfIncorporationLocalityName        | Opcional           | [OID: 1.3.6.1.4.1.311.60.2.1.1]<br>Localidad en la que está registrada la empresa   |
| jurisdictionOfIncorporationStateOrProvinceName | Opcional           | [OID: 1.3.6.1.4.1.311.60.2.1.2]<br>Provincia en la que está registrada la empresa   |
| jurisdictionOfIncorporationCountryName         |                    | [OID: 1.3.6.1.4.1.311.60.2.1.3]<br>País en el que está registrada la empresa  |
| <b>subjectPublicKeyInfo</b>                    |                    | RSA 2048 bits mínimo  |
| <b>extensions</b>                              |                    |   |
| <b>issuerAltName</b>                           |                    | Igual a la extensión subjectAltName del certificado de la CA emisora  |
| <b>subjectAltName</b>                          |                    |   |
| dNSName  |                    | Dominios DNS adicionales  |
| <b>extendedKeyUsage</b>                        |                    | serverAuth, clientAuth  |
| <b>subjectKeyIdentifier</b>                    |                    | Identificador de la clave pública   |
| <b>authorityKeyIdentifier</b>                  |                    | Incluir sólo campo keyIdentifier  |
| <b>certificatePolicies</b>                     |                    |   |
| policyIdentifier                               |                    | 1.3.6.1.4.1.14777.6.1.3   |
| cpsURI   |                    | <a href="http://www.izenpe.eus/cps-ssl">http://www.izenpe.eus/cps-ssl</a>   |
| policyIdentifier                               |                    | 0.4.0.194112.1.4 (ETSI QCP-w OID)   |
| policyIdentifier                               |                    | 2.23.140.1.1  |
| <b>authorityInfoAccess</b>                     |                    |   |
| OCSP   |                    | <a href="http://ocsp.izenpe.com">http://ocsp.izenpe.com</a>   |
| CA emisora                                     |                    | <a href="http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/SSLEV_cert_signing_1_2018.crt">http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/SSLEV_cert_signing_1_2018.crt</a>                             |
| <b>qcStatements</b>                            |                    |   |
| QcCompliance                                   |                    | Presente  |
| QcType   |                    | id-etsi-qct-web   |
| QcRetentiodPeriod                              |                    | 15 años   |
| QcPDS  |                    | <a href="https://www.izenpe.com/pds/en/en">https://www.izenpe.com/pds/en/en</a><br><a href="https://www.izenpe.com/pds/eu/eu">https://www.izenpe.com/pds/eu/eu</a><br><a href="https://www.izenpe.com/pds/es/es">https://www.izenpe.com/pds/es/es</a> |
| <b>cRLDistributionPoints</b>                   |                    | <a href="http://crl.izenpe.com/cgi-bin/crsslsev">http://crl.izenpe.com/cgi-bin/crsslsev</a>   |
| <b>keyUsage</b>                                | Crítica            | digitalSignature, keyEncipherment   |

## SSL Cualificada

**CA emisora**

**SUBCA SSL 2024**

**Nombre**

**ssl\_qualified**

| Campo / extensión                              | Opcional / Crítica | Contenido  |
|--|--------------------|--|
| <b>version</b>                                 |                    | Versión 3  |
| <b>serialNumber</b>                            |                    | Número aleatorio único   |
| <b>signature</b>                               |                    | sha384ECDSA  |
| <b>issuer</b>                                  |                    | Igual al campo subject del certificado de la CA emisora  |
| <b>validity</b>                                |                    | 395 días   |
| <b>subject</b>                                 |                    |  |
| C  |                    | País   |
| ST   |                    | Provincia  |
| L  |                    | Localidad  |
| postalCode                                     | Opcional           | Código postal  |
| street   | Opcional           | Calle  |
| O  |                    | Organización   |
| CN   | Opcional           | Dominio DNS  |
| businessCategory                               |                    | [OID: 2.5.4.15]<br>Valores posibles:<br>- "Private Organization" para Organización privada<br>- "Government Entity" para Entidad pública<br>- "Business Entity" para Empresa<br>- "Non-comercial Entity" para Entidad no comercial                 |
| jurisdictionOfIncorporationCountryName         |                    | [OID: 1.3.6.1.4.1.311.60.2.1.3]<br>País en el que está registrada la empresa   |
| jurisdictionOfIncorporationStateOrProvinceName | Opcional           | [OID: 1.3.6.1.4.1.311.60.2.1.2]<br>Provincia en la que está registrada la empresa  |
| jurisdictionOfIncorporationLocalityName        | Opcional           | [OID: 1.3.6.1.4.1.311.60.2.1.1]<br>Localidad en la que está registrada la empresa  |
| serialNumber                                   |                    | CIF  |
| <b>subjectPublicKeyInfo</b>                    |                    | ECC 256 bits mínimo  |
| <b>extensions</b>                              |                    |  |
| issuerAltName                                  |                    | Igual a la extensión subjectAltName del certificado de la CA emisora   |
| subjectAltName                                 |                    |  |
| dNSName  |                    | Dominios DNS adicionales   |
| extendedKeyUsage                               |                    | serverAuth, clientAuth   |
| authorityKeyIdentifier                         |                    | Incluir sólo campo keyIdentifier   |
| certificatePolicies                            |                    |  |
| policyIdentifier                               |                    | 2.23.140.1.1   |
| policyIdentifier                               |                    | 1.3.6.1.4.1.14777.50.3.2   |
| policyIdentifier                               |                    | 0.4.0.194112.1.4 (ETSI QCP-w OID)  |
| <b>authorityInfoAccess</b>                     |                    |  |
| OCSP   |                    | <a href="http://ocsp.izenpe.es">http://ocsp.izenpe.es</a>  |
| CA emisora                                     |                    | <a href="http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/SSL2024.crt">http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/SSL2024.crt</a>  |
| <b>qcStatements</b>                            |                    |  |
| QcCompliance                                   |                    | Presente   |
| QcType   |                    | id-etsi-qct-web  |
| QcRetentiodPeriod                              |                    | 15 años  |
| QcPDS  |                    | <a href="https://www.izenpe.com/pds/en/">https://www.izenpe.com/pds/en/</a> en<br><a href="https://www.izenpe.com/pds/eu/">https://www.izenpe.com/pds/eu/</a> eu<br><a href="https://www.izenpe.com/pds/es/">https://www.izenpe.com/pds/es/</a> es |
| <b>cRLDistributionPoints</b>                   |                    | <a href="http://crl.izenpe.es/2024/crlssl.cr">http://crl.izenpe.es/2024/crlssl.cr</a>  |
| <b>keyUsage</b>                                | Crítica            | digitalSignature   |

## Sello nivel medio EIDAS

CA emisora

AAPPR

Nombre

sello\_nivel\_medio\_eidas

| Campo / extensión             | Opcional / Crítica | Contenido   |
|-------------------------------|--------------------|---|
| <b>version</b>                |                    | Versión 3   |
| <b>serialNumber</b>           |                    | Número secuencial único   |
| <b>signature</b>              |                    | sha256WithRSAEncryption   |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora   |
| <b>validity</b>               |                    | 2 o 3 años  |
| <b>subject</b>                |                    |   |
| CN                            |                    | Nombre descriptivo del sistema o aplicación de proceso automático   |
| G                             | Opcional           | Nombre del responsable  |
| SN                            | Opcional           | [APELLIDO1] [APELLIDO2] - DNI [DNI/NIE]   |
| serialNumber                  |                    | NIF   |
| organizationIdentifier        |                    | 3 caracteres tipo-identidad + Country + - + identificador. Por ejemplo, si usamos el NIF sería algo como: VATES-A01337260   |
| OU                            |                    | "SELLO ELECTRONICO"   |
| O                             |                    | Nombre oficial de la organización   |
| C                             |                    | ES  |
| <b>subjectPublicKeyInfo</b>   |                    | RSA 3072 bits mínimo  |
| <b>extensions</b>             |                    |   |
| <b>issuerAltName</b>          |                    | Igual a la extensión subjectAltName del certificado de la CA emisora  |
| <b>subjectAltName</b>         |                    |   |
| rfc822Name                    | Opcional           | Email de contacto de la organización  |
| directoryName                 |                    |   |
| 2.16.724.1.3.5.6.2.1          |                    | "SELLO ELECTRONICO"   |
| 2.16.724.1.3.5.6.2.2          |                    | Nombre oficial de la organización   |
| 2.16.724.1.3.5.6.2.3          |                    | NIF   |
| 2.16.724.1.3.5.6.2.4          | Opcional           | DNI/NIE   |
| 2.16.724.1.3.5.6.2.5          |                    | Nombre de órgano administrativo, sistema o aplicación   |
| 2.16.724.1.3.5.6.2.6          | Opcional           | Nombre  |
| 2.16.724.1.3.5.6.2.7          | Opcional           | Primer Apellido   |
| 2.16.724.1.3.5.6.2.8          | Opcional           | Segundo Apellido  |
| 2.16.724.1.3.5.6.2.9          | Opcional           | Email del responsable   |
| <b>extendedKeyUsage</b>       |                    | clientAuth, emailProtection   |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública   |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier  |
| <b>certificatePolicies</b>    |                    |   |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.4.11.2  |
| cpsURI                        |                    | <a href="http://www.izenpe.eus/cps">http://www.izenpe.eus/cps</a>   |
| userNotice                    |                    | Kontsulta <a href="http://www.izenpe.eus">www.izenpe.eus</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.eus">www.izenpe.eus</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier              |                    | 2.16.724.1.3.5.6.2  |
| policyIdentifier              |                    | 0.4.0.194112.1.1 (QCP-I)  |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.com/cgi-bin/crlscar2">http://crl.izenpe.com/cgi-bin/crlscar2</a>   |
| <b>authorityInfoAccess</b>    |                    |   |
| ocsp                          |                    | <a href="http://ocsp.izenpe.com">http://ocsp.izenpe.com</a>   |
| CA emisora                    |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR_cert_sha256.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR_cert_sha256.crt</a>   |
| <b>qcStatements</b>           |                    |   |
| QcCompliance                  |                    | Presente  |
| QcType                        |                    | id-etsi-qct-eseal   |
| QcRetentionPeriod             |                    | 15 años   |
| QcPDS                         |                    | <a href="https://www.izenpe.com/pds/en/">https://www.izenpe.com/pds/en/</a> en<br><a href="https://www.izenpe.com/pds/eu/">https://www.izenpe.com/pds/eu/</a> eu<br><a href="https://www.izenpe.com/pds/es/">https://www.izenpe.com/pds/es/</a> es                            |
| qcStatement-2                 |                    | 0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)  |
| <b>keyUsage</b>               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment   |

## Sello nivel medio EIDAS

CA emisora

AAPPR

Nombre

sello\_nivel\_medio\_hsm

| Campo / extensión             | Opcional / Crítica | Contenido   |
|-------------------------------|--------------------|---|
| <b>version</b>                |                    | Versión 3   |
| <b>serialNumber</b>           |                    | Número secuencial único   |
| <b>signature</b>              |                    | sha256WithRSAEncryption   |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora   |
| <b>validity</b>               |                    | 2 o 3 años  |
| <b>subject</b>                |                    |   |
| CN                            |                    | Nombre descriptivo del sistema o aplicación de proceso automático   |
| G                             | Opcional           | Nombre del responsable  |
| SN                            | Opcional           | [APELLIDO1] [APELLIDO2] - DNI [DNI/NIE]   |
| serialNumber                  |                    | NIF   |
| organizationIdentifier        |                    | 3 caracteres tipo-identidad + Country + - + identificador. Por ejemplo, si usamos el NIF sería algo como: VATES-A01337260   |
| OU                            |                    | "SELLO ELECTRONICO"   |
| O                             |                    | Nombre oficial de la organización   |
| C                             |                    | ES  |
| <b>subjectPublicKeyInfo</b>   |                    | RSA 3072 bits mínimo  |
| <b>extensions</b>             |                    |   |
| <b>issuerAltName</b>          |                    | Igual a la extensión subjectAltName del certificado de la CA emisora  |
| <b>subjectAltName</b>         |                    |   |
| rfc822Name                    | Opcional           | Email de contacto de la organización  |
| directoryName                 |                    |   |
| 2.16.724.1.3.5.6.2.1          |                    | "SELLO ELECTRONICO"   |
| 2.16.724.1.3.5.6.2.2          |                    | Nombre oficial de la organización   |
| 2.16.724.1.3.5.6.2.3          |                    | NIF   |
| 2.16.724.1.3.5.6.2.4          | Opcional           | DNI/NIE   |
| 2.16.724.1.3.5.6.2.5          |                    | Nombre de órgano administrativo, sistema o aplicación   |
| 2.16.724.1.3.5.6.2.6          | Opcional           | Nombre  |
| 2.16.724.1.3.5.6.2.7          | Opcional           | Primer Apellido   |
| 2.16.724.1.3.5.6.2.8          | Opcional           | Segundo Apellido  |
| 2.16.724.1.3.5.6.2.9          | Opcional           | Email del responsable   |
| <b>extendedKeyUsage</b>       |                    | clientAuth, emailProtection   |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública   |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier  |
| <b>certificatePolicies</b>    |                    |   |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.4.11.3  |
| cpsURI                        |                    | <a href="http://www.izenpe.eus/cps">http://www.izenpe.eus/cps</a>   |
| userNotice                    |                    | Kontsulta <a href="http://www.izenpe.eus">www.izenpe.eus</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.eus">www.izenpe.eus</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier              |                    | 2.16.724.1.3.5.6.2  |
| policyIdentifier              |                    | 0.4.0.194112.1.1 (QCP-I)  |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.com/cgi-bin/crlscar2">http://crl.izenpe.com/cgi-bin/crlscar2</a>   |
| <b>authorityInfoAccess</b>    |                    |   |
| ocsp                          |                    | <a href="http://ocsp.izenpe.com">http://ocsp.izenpe.com</a>   |
| CA emisora                    |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR_cert_sha256.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR_cert_sha256.crt</a>   |
| <b>qcStatements</b>           |                    |   |
| QcCompliance                  |                    | Presente  |
| QcType                        |                    | id-etsi-qct-eseal   |
| QcRetentionPeriod             |                    | 15 años   |
| QcPDS                         |                    | <a href="https://www.izenpe.com/pds/en/">https://www.izenpe.com/pds/en/</a> en<br><a href="https://www.izenpe.com/pds/eu/">https://www.izenpe.com/pds/eu/</a> eu<br><a href="https://www.izenpe.com/pds/es/">https://www.izenpe.com/pds/es/</a> es                            |
| qcStatement-2                 |                    | 0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)  |
| <b>keyUsage</b>               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment   |

## Sello nivel alto EIDAS

CA emisora

AAPPR

Nombre

sello\_nivel\_alto\_eidas

| Campo / extensión      | Opcional / Crítica | Contenido   |
|------------------------|--------------------|---|
| version                |                    | Versión 3   |
| serialNumber           |                    | Número secuencial único   |
| signature              |                    | sha256WithRSAEncryption   |
| issuer                 |                    | Igual al campo subject del certificado de la CA emisora   |
| validity               |                    | 2 o 3 años  |
| subject                |                    |   |
| CN                     | Opcional           | Nombre descriptivo del sistema o aplicación de proceso automático   |
| G                      | Opcional           | Nombre del responsable  |
| SN                     | Opcional           | [APELLIDO1] [APELLIDO2] - DNI [DNI/NIE]   |
| serialNumber           | Opcional           | NIF   |
| organizationIdentifier |                    | 3 caracteres tipo-identidad + Country + - + identificador. Por ejemplo, si usamos el CIF sería algo como: VATES-A01337260   |
| OU                     |                    | "SELLO ELECTRONICO"   |
| O                      |                    | Nombre oficial de la organización   |
| C                      |                    | ES  |
| subjectPublicKeyInfo   |                    | RSA 3072 bits mínimo  |
| extensions             |                    |   |
| issuerAltName          |                    | Igual a la extensión subjectAltName del certificado de la CA emisora  |
| subjectAltName         |                    |   |
| rfc822Name             | Opcional           | Email de contacto de la organización  |
| directoryName          |                    |   |
| 2.16.724.1.3.5.6.1.1   |                    | "SELLO ELECTRONICO"   |
| 2.16.724.1.3.5.6.1.2   |                    | Nombre oficial de la organización   |
| 2.16.724.1.3.5.6.1.3   |                    | NIF   |
| 2.16.724.1.3.5.6.1.4   | Opcional           | DNI/NIE   |
| 2.16.724.1.3.5.6.1.5   | Opcional           | Nombre de órgano administrativo, sistema o aplicación   |
| 2.16.724.1.3.5.6.1.6   | Opcional           | Nombre  |
| 2.16.724.1.3.5.6.1.7   | Opcional           | Primer Apellido   |
| 2.16.724.1.3.5.6.1.8   | Opcional           | Segundo Apellido  |
| 2.16.724.1.3.5.6.1.9   | Opcional           | Email del responsable   |
| extendedKeyUsage       |                    | clientAuth, emailProtection   |
| subjectKeyIdentifier   |                    | Identificador de la clave pública   |
| authorityKeyIdentifier |                    | Incluir sólo campo keyIdentifier  |
| certificatePolicies    |                    |   |
| policyIdentifier       |                    | 1.3.6.1.4.1.14777.4.12.2  |
| cpsURI                 |                    | <a href="http://www.izenpe.eus/cps">http://www.izenpe.eus/cps</a>   |
| userNotice             |                    | Kontsulta <a href="http://www.izenpe.eus-en">www.izenpe.eus-en</a> baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.eus">www.izenpe.eus</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier       |                    | 0.4.0.194112.1.3 (QCP-I-qscd)   |
| policyIdentifier       |                    | 2.16.724.1.3.5.6.1  |
| cRLDistributionPoints  |                    | <a href="http://crl.izenpe.com/cgi-bin/crlscar2">http://crl.izenpe.com/cgi-bin/crlscar2</a>   |
| authorityInfoAccess    |                    |   |
| ocsp                   |                    | <a href="http://ocsp.izenpe.com">http://ocsp.izenpe.com</a>   |
| CA emisora             |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR_cert_sha256.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR_cert_sha256.crt</a>   |
| qcStatements           |                    |   |
| QcCompliance           |                    | Presente  |
| QcType                 |                    | id-etsi-qct-eseal   |
| QcRetentionPeriod      |                    | 15 años   |
| QcSSCD                 |                    | Presente  |
| QcPDS                  |                    | <a href="https://www.izenpe.com/pds/en/">https://www.izenpe.com/pds/en/</a> en<br><a href="https://www.izenpe.com/pds/eu/">https://www.izenpe.com/pds/eu/</a> eu<br><a href="https://www.izenpe.com/pds/es/">https://www.izenpe.com/pds/es/</a> es                              |
| qcStatement-2          |                    | 0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)  |
| keyUsage               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment   |

# Ciudadano

**CA emisora**

**CCEER2025**

**Nombre**

**ciudadano\_qc\_scard**

| Campo / extensión                 | Opcional / Crítica | Contenido   |
|-----------------------------------|--------------------|---|
| <b>version</b>                    |                    | Versión 3   |
| <b>serialNumber</b>               |                    | Número aleatorio único  |
| <b>signature</b>                  |                    | sha384ECDSA   |
| <b>issuer</b>                     |                    | Igual al campo subject del certificado de la CA emisora   |
| <b>validity</b>                   |                    | 4 años  |
| <b>subject</b>                    |                    |   |
| serialNumber                      |                    | DNI / NIE / NIF / PASS  |
| SN                                |                    | Apellidos   |
| G                                 |                    | Nombre  |
| CN                                |                    | Nombre y Apellidos  |
| OU                                |                    | Herritar ziurtagiria - Certificado de ciudadano   |
| C                                 |                    | País (codificado según ISO 3166-1 alpha 2 code)   |
| <b>subjectPublicKeyInfo</b>       |                    | ECC 256 bits mínimo   |
| <b>extensions</b>                 |                    |   |
| <b>subjectAltName</b>             |                    |   |
| directoryName                     |                    |   |
| 1.3.6.1.4.1.14777.0.1             |                    | Nombre  |
| 1.3.6.1.4.1.14777.0.2             |                    | Primer Apellido   |
| 1.3.6.1.4.1.14777.0.3             | Opcional           | Segundo Apellido  |
| 1.3.6.1.4.1.14777.0.4             |                    | DNI / NIE / NIF / PASS  |
| <b>extendedKeyUsage</b>           |                    | clientAuth, documentSigning   |
| <b>subjectKeyIdentifier</b>       |                    | Identificador de la clave pública   |
| <b>authorityKeyIdentifier</b>     |                    | Incluir sólo campo keyIdentifier  |
| <b>certificatePolicies</b>        |                    |   |
| policyIdentifier                  |                    | 1.3.6.1.4.1.14777.51.1.1  |
| cpsURI                            |                    | <a href="http://www.izenpe.eus/cps">http://www.izenpe.eus/cps</a>   |
| userNotice                        |                    | Kontsulta <a href="http://www.izenpe.eus">www.izenpe.eus</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.eus">www.izenpe.eus</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier                  |                    | 0.4.0.194112.1.0 (QCP-n)  |
| <b>cRLDistributionPoints</b>      |                    | <a href="http://crl.izenpe.eus/crls/crlcceer.crl">http://crl.izenpe.eus/crls/crlcceer.crl</a>   |
| <b>authorityInfoAccess</b>        |                    |   |
| ocsp                              |                    | <a href="http://ocsp.izenpe.eus">http://ocsp.izenpe.eus</a>   |
| CA emisora                        |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER2025.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER2025.crt</a>   |
| <b>subjectDirectoryAttributes</b> |                    |   |
| dateOfBirth                       |                    | Fecha de nacimiento   |
| <b>qcStatements</b>               |                    |   |
| QcCompliance                      |                    | Presente  |
| QcType                            |                    | id-etsi-qct-esign   |
| QcRetentiodPeriod                 |                    | 15 años   |
| QcPDS                             |                    | <a href="https://www.izenpe.eus/pds/en/">https://www.izenpe.eus/pds/en/</a> en<br><a href="https://www.izenpe.eus/pds/eu/">https://www.izenpe.eus/pds/eu/</a> eu<br><a href="https://www.izenpe.eus/pds/es/">https://www.izenpe.eus/pds/es/</a> es                            |
| <b>keyUsage</b>                   | Crítica            | digitalSignature, nonRepudiation, keyEncipherment   |

# Ciudadano

**CA emisora**

**CCEER2025**

**Nombre**

**ciudadano\_qc\_hsm**

| Campo / extensión                 | Opcional / Crítica | Contenido   |
|-----------------------------------|--------------------|---|
| <b>version</b>                    |                    | Versión 3   |
| <b>serialNumber</b>               |                    | Número aleatorio único  |
| <b>signature</b>                  |                    | sha384ECDSA   |
| <b>issuer</b>                     |                    | Igual al campo subject del certificado de la CA emisora   |
| <b>validity</b>                   |                    | 4 años  |
| <b>subject</b>                    |                    |   |
| serialNumber                      |                    | DNI / NIE / NIF / PASS  |
| SN                                |                    | Apellidos   |
| G                                 |                    | Nombre  |
| CN                                |                    | Nombre y Apellidos  |
| OU                                |                    | Herritar ziurtagiria - Certificado de ciudadano   |
| C                                 |                    | País (codificado según ISO 3166-1 alpha 2 code)   |
| <b>subjectPublicKeyInfo</b>       |                    | ECC 256 bits mínimo   |
| <b>extensions</b>                 |                    |   |
| <b>subjectAltName</b>             |                    |   |
| directoryName                     |                    |   |
| 1.3.6.1.4.1.14777.0.1             |                    | Nombre  |
| 1.3.6.1.4.1.14777.0.2             |                    | Primer Apellido   |
| 1.3.6.1.4.1.14777.0.3             | Opcional           | Segundo Apellido  |
| 1.3.6.1.4.1.14777.0.4             |                    | DNI / NIE / NIF / PASS  |
| <b>extendedKeyUsage</b>           |                    | clientAuth, documentSigning   |
| <b>subjectKeyIdentifier</b>       |                    | Identificador de la clave pública   |
| <b>authorityKeyIdentifier</b>     |                    | Incluir sólo campo keyIdentifier  |
| <b>certificatePolicies</b>        |                    |   |
| policyIdentifier                  |                    | 1.3.6.1.4.1.14777.51.1.3  |
| cpsURI                            |                    | <a href="http://www.izenpe.eus/cps">http://www.izenpe.eus/cps</a>   |
| userNotice                        |                    | Kontsulta <a href="http://www.izenpe.eus">www.izenpe.eus</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.eus">www.izenpe.eus</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier                  |                    | 0.4.0.194112.1.0 (QCP-n)  |
| <b>cRLDistributionPoints</b>      |                    | <a href="http://crl.izenpe.eus/crls/crlcceer.crl">http://crl.izenpe.eus/crls/crlcceer.crl</a>   |
| <b>authorityInfoAccess</b>        |                    |   |
| ocsp                              |                    | <a href="http://ocsp.izenpe.eus">http://ocsp.izenpe.eus</a>   |
| CA emisora                        |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER2025.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER2025.crt</a>   |
| <b>subjectDirectoryAttributes</b> |                    |   |
| dateOfBirth                       |                    | Fecha de nacimiento   |
| <b>qcStatements</b>               |                    |   |
| QcCompliance                      |                    | Presente  |
| QcType                            |                    | id-etsi-qct-esign   |
| QcRetentiodPeriod                 |                    | 15 años   |
| QcPDS                             |                    | <a href="https://www.izenpe.eus/pds/en/">https://www.izenpe.eus/pds/en/</a> en<br><a href="https://www.izenpe.eus/pds/eu/">https://www.izenpe.eus/pds/eu/</a> eu<br><a href="https://www.izenpe.eus/pds/es/">https://www.izenpe.eus/pds/es/</a> es                            |
| <b>keyUsage</b>                   | Crítica            | digitalSignature, nonRepudiation, keyEncipherment   |

# Profesional

CA emisora

CCEER2025

Nombre

profesional\_qc\_scard

| Campo / extensión            | Opcional / Crítica | Contenido   |
|------------------------------|--------------------|---|
| version                      |                    | Versión 3   |
| serialNumber                 |                    | Número aleatorio único  |
| signature                    |                    | sha384ECDSA   |
| issuer                       |                    | Igual al campo subject del certificado de la CA emisora   |
| validity                     |                    | 3 años  |
| subject                      |                    |   |
| serialNumber                 |                    | DNI / NIE / NIF / PASS  |
| SN                           |                    | Apellidos   |
| G                            |                    | Nombre  |
| CN                           |                    | Nombre Apellido1 Apellido 2 - DNI   |
| organizationIdentifier       |                    | 3 caracteres tipo-identidad + Country + - + identificador. Por ejemplo, si usaramos el CIF sería algo como: VATES-A01337260   |
| title                        | Opcional           | Cargo   |
| OU                           |                    | Ziurtagiri Profesionala - Certificado Profesional   |
| OU                           | Opcional           | Departamento  |
| OU                           | Opcional           | Grupo VPN   |
| O                            |                    | Organización  |
| C                            |                    | País (codificado según ISO 3166-1 alpha 2 code)   |
| subjectPublicKeyInfo         |                    | ECC 256 bits mínimo   |
| extensions                   |                    |   |
| subjectAltName               |                    |   |
| OtherName: UserPrincipalName | Opcional           | Nombre principal de usuario   |
| directoryName                |                    |   |
| 1.3.6.1.4.1.14777.0.1        |                    | Nombre  |
| 1.3.6.1.4.1.14777.0.2        |                    | Primer Apellido   |
| 1.3.6.1.4.1.14777.0.3        |                    | Segundo Apellido  |
| 1.3.6.1.4.1.14777.0.4        |                    | DNI / NIE / NIF / PASS  |
| 1.3.6.1.4.1.14777.0.5        |                    | Organización  |
| 1.3.6.1.4.1.14777.0.6        |                    | CIF   |
| 1.3.6.1.4.1.14777.0.8        | Opcional           | Cargo   |
| 1.3.6.1.4.1.14777.0.9        | Opcional           | Departamento  |
| extendedKeyUsage             |                    | clientAuth, smartCardLogon  |
| subjectKeyIdentifier         |                    | Identificador de la clave pública   |
| authorityKeyIdentifier       |                    | Incluir sólo campo keyIdentifier  |
| certificatePolicies          |                    |   |
| policyIdentifier             |                    | 1.3.6.1.4.1.14777.51.2.1  |
| cpsURI                       |                    | <a href="http://www.izenpe.eus/cps">http://www.izenpe.eus/cps</a>   |
| userNotice                   |                    | Kontsulta <a href="http://www.izenpe.eus">www.izenpe.eus</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.eus">www.izenpe.eus</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier             |                    | 0.4.0.194112.1.0 (QCP-n)  |
| cRLDistributionPoints        |                    | <a href="http://crl.izenpe.eus/crls/crlcceer.crl">http://crl.izenpe.eus/crls/crlcceer.crl</a>   |
| authorityInfoAccess          |                    |   |
| ocsp                         |                    | <a href="http://ocsp.izenpe.eus">http://ocsp.izenpe.eus</a>   |
| CA emisora                   |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER2025.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER2025.crt</a>   |
| qcStatements                 |                    |   |
| QcCompliance                 |                    | Presente  |
| QcType                       |                    | id-etsi-qc-esign  |
| QcRetentiodPeriod            |                    | 15 años   |
| QcPDS                        |                    | <a href="https://www.izenpe.eus/pds/en/">https://www.izenpe.eus/pds/en/</a> en<br><a href="https://www.izenpe.eus/pds/eu/">https://www.izenpe.eus/pds/eu/</a> eu<br><a href="https://www.izenpe.eus/pds/es/">https://www.izenpe.eus/pds/es/</a> es                            |
| qcStatement-2                |                    | 0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)  |
| keyUsage                     | Crítica            | digitalSignature, nonRepudiation, keyEncipherment   |

# Profesional

CA emisora

CCEER2025

Nombre

profesional\_qc\_sw

| Campo / extensión             | Opcional / Crítica | Contenido   |
|-------------------------------|--------------------|---|
| <b>version</b>                |                    | Versión 3   |
| <b>serialNumber</b>           |                    | Número aleatorio único  |
| <b>signature</b>              |                    | sha384ECDSA   |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora   |
| <b>validity</b>               |                    | 3 años  |
| <b>subject</b>                |                    |   |
| serialNumber                  |                    | DNI / NIE / NIF / PASS  |
| SN                            |                    | Apellidos   |
| G                             |                    | Nombre  |
| CN                            |                    | Nombre Apellido1 Apellido 2 - DNI   |
| organizationIdentifier        |                    | 3 caracteres tipo-identidad + Country + - + identificador. Por ejemplo, si usaramos el CIF sería algo como: VATES-A01337260   |
| title                         | Opcional           | Cargo   |
| OU                            |                    | Ziurtagiri Profesionala - Certificado Profesional   |
| OU                            | Opcional           | Departamento  |
| OU                            | Opcional           | Grupo VPN   |
| O                             |                    | Organización  |
| C                             |                    | País (codificado según ISO 3166-1 alpha 2 code)   |
| <b>subjectPublicKeyInfo</b>   |                    | ECC 256 bits mínimo   |
| <b>extensions</b>             |                    |   |
| <b>subjectAltName</b>         |                    |   |
| directoryName                 |                    |   |
| 1.3.6.1.4.1.14777.0.1         |                    | Nombre  |
| 1.3.6.1.4.1.14777.0.2         |                    | Primer Apellido   |
| 1.3.6.1.4.1.14777.0.3         |                    | Segundo Apellido  |
| 1.3.6.1.4.1.14777.0.4         |                    | DNI / NIE / NIF / PASS  |
| 1.3.6.1.4.1.14777.0.5         |                    | Organización  |
| 1.3.6.1.4.1.14777.0.6         |                    | CIF   |
| 1.3.6.1.4.1.14777.0.8         | Opcional           | Cargo   |
| 1.3.6.1.4.1.14777.0.9         | Opcional           | Departamento  |
| <b>extendedKeyUsage</b>       |                    | clientAuth  |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública   |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier  |
| <b>certificatePolicies</b>    |                    |   |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.51.2.2  |
| cpsURI                        |                    | <a href="http://www.izenpe.eus/cps">http://www.izenpe.eus/cps</a>   |
| userNotice                    |                    | Kontsulta <a href="http://www.izenpe.eus">www.izenpe.eus</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.eus">www.izenpe.eus</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier              |                    | 0.4.0.194112.1.0 (QCP-n)  |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.eus/crls/crlcceer.crl">http://crl.izenpe.eus/crls/crlcceer.crl</a>   |
| <b>authorityInfoAccess</b>    |                    |   |
| ocsp                          |                    | <a href="http://ocsp.izenpe.eus">http://ocsp.izenpe.eus</a>   |
| CA emisora                    |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER2025.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER2025.crt</a>   |
| <b>qcStatements</b>           |                    |   |
| QcCompliance                  |                    | Presente  |
| QcType                        |                    | id-etsi-qct-esign   |
| QcRetentiodPeriod             |                    | 15 años   |
| QcPDS                         |                    | <a href="https://www.izenpe.eus/pds/en/">https://www.izenpe.eus/pds/en/</a> en<br><a href="https://www.izenpe.eus/pds/eu/">https://www.izenpe.eus/pds/eu/</a> eu<br><a href="https://www.izenpe.eus/pds/es/">https://www.izenpe.eus/pds/es/</a> es                            |
| qcStatement-2                 |                    | 0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)  |
| <b>keyUsage</b>               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment   |

## Profesional

CA emisora

CCEER2025

Nombre

profesional\_qc\_hsm

| Campo / extensión             | Opcional / Crítica | Contenido   |
|-------------------------------|--------------------|---|
| <b>version</b>                |                    | Versión 3   |
| <b>serialNumber</b>           |                    | Número aleatorio único  |
| <b>signature</b>              |                    | sha384ECDSA   |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora   |
| <b>validity</b>               |                    | 3 años  |
| <b>subject</b>                |                    |   |
| serialNumber                  |                    | DNI / NIE / NIF / PASS  |
| SN                            |                    | Apellidos   |
| G                             |                    | Nombre  |
| CN                            |                    | Nombre Apellido1 Apellido 2 - DNI   |
| organizationIdentifier        |                    | 3 caracteres tipo-identidad + Country + - + identificador. Por ejemplo, si usaramos el CIF sería algo como: VATES-A01337260   |
| title                         | Opcional           | Cargo   |
| OU                            |                    | Ziurtagiri Profesionala - Certificado Profesional   |
| OU                            | Opcional           | Departamento  |
| OU                            | Opcional           | Grupo VPN   |
| O                             |                    | Organización  |
| C                             |                    | Pais (codificado según ISO 3166-1 alpha 2 code)   |
| <b>subjectPublicKeyInfo</b>   |                    | ECC 256 bits mínimo   |
| <b>extensions</b>             |                    |   |
| <b>subjectAltName</b>         |                    |   |
| OtherName: UserPrincipalName  | Opcional           | Nombre principal de usuario   |
| directoryName                 |                    |   |
| 1.3.6.1.4.1.14777.0.1         |                    | Nombre  |
| 1.3.6.1.4.1.14777.0.2         |                    | Primer Apellido   |
| 1.3.6.1.4.1.14777.0.3         |                    | Segundo Apellido  |
| 1.3.6.1.4.1.14777.0.4         |                    | DNI / NIE / NIF / PASS  |
| 1.3.6.1.4.1.14777.0.5         |                    | Organización  |
| 1.3.6.1.4.1.14777.0.6         |                    | CIF   |
| 1.3.6.1.4.1.14777.0.8         | Opcional           | Cargo   |
| 1.3.6.1.4.1.14777.0.9         | Opcional           | Departamento  |
| <b>extendedKeyUsage</b>       |                    | clientAuth  |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública   |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier  |
| <b>certificatePolicies</b>    |                    |   |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.51.2.3  |
| cpsURI                        |                    | <a href="http://www.izenpe.eus/cps">http://www.izenpe.eus/cps</a>   |
| userNotice                    |                    | Kontsulta <a href="http://www.izenpe.eus">www.izenpe.eus</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.eus">www.izenpe.eus</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier              |                    | 0.4.0.194112.1.0 (QCP-n)  |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.eus/crls/crlcceer.crl">http://crl.izenpe.eus/crls/crlcceer.crl</a>   |
| <b>authorityInfoAccess</b>    |                    |   |
| ocsp                          |                    | <a href="http://ocsp.izenpe.eus">http://ocsp.izenpe.eus</a>   |
| CA emisora                    |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER2025.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER2025.crt</a>   |
| <b>qcStatements</b>           |                    |   |
| QcCompliance                  |                    | Presente  |
| QcType                        |                    | id-etsi-qct-esign   |
| QcRetentiodPeriod             |                    | 15 años   |
| QcPDS                         |                    | <a href="https://www.izenpe.eus/pds/en/en">https://www.izenpe.eus/pds/en/en</a><br><a href="https://www.izenpe.eus/pds/eu/eu">https://www.izenpe.eus/pds/eu/eu</a><br><a href="https://www.izenpe.eus/pds/es/es">https://www.izenpe.eus/pds/es/es</a>                         |
| qcStatement-2                 |                    | 0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)  |
| <b>keyUsage</b>               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment   |

## Personal de Entidades Públicas

CA emisora

AAPPR2025

Nombre

pep\_qc\_scard

| Campo / extensión             | Opcional / Crítica | Contenido   |
|-------------------------------|--------------------|---|
| <b>version</b>                |                    | Versión 3   |
| <b>serialNumber</b>           |                    | Número aleatorio único  |
| <b>signature</b>              |                    | sha384ECDSA   |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora   |
| <b>validity</b>               |                    | 3 años  |
| <b>subject</b>                |                    |   |
| serialNumber                  |                    | DNI / NIE siguiendo semántica ETSI EN 319 412-1   |
| SN                            |                    | Apellidos   |
| G                             |                    | Nombre  |
| CN                            |                    | Nombre Apellido1 Apellido 2 - DNI   |
| title                         | Opcional           | Cargo   |
| OU                            |                    | CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO   |
| OU                            | Opcional           | Unidad dentro de la administración  |
| OU                            | Opcional           | Código DIR3 de la unidad  |
| OU                            | Opcional           | Numero de identificación del empleado público   |
| O                             |                    | Nombre oficial de la Organización   |
| C                             |                    | ES  |
| <b>subjectPublicKeyInfo</b>   |                    | ECC 256 bits mínimo   |
| <b>extensions</b>             |                    |   |
| <b>subjectAltName</b>         |                    |   |
| OtherName: UserPrincipalName  | Opcional           | Nombre principal de usuario   |
| directoryName                 |                    |   |
| 2.16.724.1.3.5.7.2.1          |                    | CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO   |
| 2.16.724.1.3.5.7.2.2          |                    | Nombre oficial de la Organización   |
| 2.16.724.1.3.5.7.2.3          |                    | CIF   |
| 2.16.724.1.3.5.7.2.4          |                    | DNI / NIE   |
| 2.16.724.1.3.5.7.2.5          | Opcional           | Numero de identificación del empleado público   |
| 2.16.724.1.3.5.7.2.6          |                    | Nombre  |
| 2.16.724.1.3.5.7.2.7          |                    | Primer Apellido   |
| 2.16.724.1.3.5.7.2.8          |                    | Segundo Apellido  |
| 2.16.724.1.3.5.7.2.10         | Opcional           | Unidad dentro de la administración  |
| 2.16.724.1.3.5.7.2.11         | Opcional           | Puesto o cargo  |
| <b>extendedKeyUsage</b>       |                    | clientAuth, smartCardLogon  |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública   |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier  |
| <b>certificatePolicies</b>    |                    |   |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.52.1.1  |
| cpsURI                        |                    | <a href="http://www.izenpe.eus/cps">http://www.izenpe.eus/cps</a>   |
| userNotice                    |                    | Kontsulta <a href="http://www.izenpe.eus">www.izenpe.eus</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.eus">www.izenpe.eus</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier              |                    | 2.16.724.1.3.5.7.2  |
| policyIdentifier              |                    | 0.4.0.194112.1.0 (QCP-n)  |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.eus/crls/crlaapp.crl">http://crl.izenpe.eus/crls/crlaapp.crl</a>   |
| <b>authorityInfoAccess</b>    |                    |   |
| ocsp                          |                    | <a href="http://ocsp.izenpe.eus">http://ocsp.izenpe.eus</a>   |
| CA emisora                    |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR2025.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR2025.crt</a>   |
| <b>qcStatements</b>           |                    |   |
| QcCompliance                  |                    | Presente  |
| QcType                        |                    | id-etsi-qct-esign   |
| QcRetentiodPeriod             |                    | 15 años   |
| QcPDS                         |                    | <a href="https://www.izenpe.eus/pds/en/">https://www.izenpe.eus/pds/en/</a> en<br><a href="https://www.izenpe.eus/pds/eu/">https://www.izenpe.eus/pds/eu/</a> eu<br><a href="https://www.izenpe.eus/pds/es/">https://www.izenpe.eus/pds/es/</a> es                            |
| qcStatement-2                 |                    | 0.4.0.194121.1.1 (id-etsi-qcs-SemanticsId-Natural)  |
| <b>keyUsage</b>               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment   |

## Personal de Entidades Públicas

CA emisora

AAPPR2025

Nombre

pep\_qc\_sw

| Campo / extensión             | Opcional / Crítica | Contenido   |
|-------------------------------|--------------------|---|
| <b>version</b>                |                    | Versión 3   |
| <b>serialNumber</b>           |                    | Número aleatorio único  |
| <b>signature</b>              |                    | sha384ECDSA   |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora   |
| <b>validity</b>               |                    | 3 años  |
| <b>subject</b>                |                    |   |
| serialNumber                  |                    | DNI / NIE siguiendo semántica ETSI EN 319 412-1   |
| SN                            |                    | Apellidos   |
| G                             |                    | Nombre  |
| CN                            |                    | Nombre Apellido1 Apellido 2 - DNI   |
| title                         | Opcional           | Cargo   |
| OU                            |                    | <b>CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO</b>  |
| OU                            | Opcional           | Unidad dentro de la administración  |
| OU                            | Opcional           | Código DIR3 de la unidad  |
| OU                            | Opcional           | Numero de identificación del empleado público   |
| O                             |                    | Nombre oficial de la Organización   |
| C                             |                    | <b>ES</b>   |
| <b>subjectPublicKeyInfo</b>   |                    | ECC 256 bits mínimo   |
| <b>extensions</b>             |                    |   |
| <b>subjectAltName</b>         |                    |   |
| directoryName                 |                    |   |
| 2.16.724.1.3.5.7.2.1          |                    | <b>CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO</b>  |
| 2.16.724.1.3.5.7.2.2          |                    | Nombre oficial de la Organización   |
| 2.16.724.1.3.5.7.2.3          |                    | CIF   |
| 2.16.724.1.3.5.7.2.4          |                    | DNI / NIE   |
| 2.16.724.1.3.5.7.2.5          | Opcional           | Numero de identificación del empleado público   |
| 2.16.724.1.3.5.7.2.6          |                    | Nombre  |
| 2.16.724.1.3.5.7.2.7          |                    | Primer Apellido   |
| 2.16.724.1.3.5.7.2.10         | Opcional           | Unidad dentro de la administración  |
| 2.16.724.1.3.5.7.2.11         | Opcional           | Puesto o cargo  |
| <b>extendedKeyUsage</b>       |                    | clientAuth  |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública   |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier  |
| <b>certificatePolicies</b>    |                    |   |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.52.1.2  |
| cpsURI                        |                    | <a href="http://www.izenpe.eus/cps">http://www.izenpe.eus/cps</a>   |
| userNotice                    |                    | Kontsulta <a href="http://www.izenpe.eus">www.izenpe.eus</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.eus">www.izenpe.eus</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier              |                    | 2.16.724.1.3.5.7.2  |
| policyIdentifier              |                    | 0.4.0.194112.1.0 (QCP-n)  |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.eus/crls/crlaapp.crl">http://crl.izenpe.eus/crls/crlaapp.crl</a>   |
| <b>authorityInfoAccess</b>    |                    |   |
| ocsp                          |                    | <a href="http://ocsp.izenpe.eus">http://ocsp.izenpe.eus</a>   |
| CA emisora                    |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR2025.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR2025.crt</a>   |
| <b>qcStatements</b>           |                    |   |
| QcCompliance                  |                    | Presente  |
| QcType                        |                    | id-etsi-qct-esign   |
| QcRetentiodPeriod             |                    | 15 años   |
| QcPDS                         |                    | <a href="https://www.izenpe.eus/pds/en/">https://www.izenpe.eus/pds/en/</a> en<br><a href="https://www.izenpe.eus/pds/eu/">https://www.izenpe.eus/pds/eu/</a> eu<br><a href="https://www.izenpe.eus/pds/es/">https://www.izenpe.eus/pds/es/</a> es                            |
| qcStatement-2                 |                    | 0.4.0.194121.1.1 (id-etsi-qcs-SemanticsId-Natural)  |
| <b>keyUsage</b>               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment   |

## Personal de Entidades Públicas

CA emisora

AAPPR2025

Nombre

pep\_qc\_hsm

| Campo / extensión             | Opcional / Crítica | Contenido   |
|-------------------------------|--------------------|---|
| <b>version</b>                |                    | Versión 3   |
| <b>serialNumber</b>           |                    | Número aleatorio único  |
| <b>signature</b>              |                    | sha384ECDSA   |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora   |
| <b>validity</b>               |                    | 3 años  |
| <b>subject</b>                |                    |   |
| serialNumber                  |                    | DNI / NIE siguiendo semántica ETSI EN 319 412-1   |
| SN                            |                    | Apellidos   |
| G                             |                    | Nombre  |
| CN                            |                    | Nombre Apellido1 Apellido 2 - DNI   |
| title                         | Opcional           | Cargo   |
| OU                            |                    | CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO   |
| OU                            | Opcional           | Unidad dentro de la administración  |
| OU                            | Opcional           | Código DIR3 de la unidad  |
| OU                            | Opcional           | Numero de identificación del empleado público   |
| O                             |                    | Nombre oficial de la Organización   |
| C                             |                    | ES  |
| <b>subjectPublicKeyInfo</b>   |                    | ECC 256 bits mínimo   |
| <b>extensions</b>             |                    |   |
| <b>subjectAltName</b>         |                    |   |
| OtherName: UserPrincipalName  | Opcional           | Nombre principal de usuario   |
| directoryName                 |                    |   |
| 2.16.724.1.3.5.7.2.1          |                    | CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO   |
| 2.16.724.1.3.5.7.2.2          |                    | Nombre oficial de la Organización   |
| 2.16.724.1.3.5.7.2.3          |                    | CIF   |
| 2.16.724.1.3.5.7.2.4          |                    | DNI / NIE   |
| 2.16.724.1.3.5.7.2.5          | Opcional           | Numero de identificación del empleado público   |
| 2.16.724.1.3.5.7.2.6          |                    | Nombre  |
| 2.16.724.1.3.5.7.2.7          |                    | Primer Apellido   |
| 2.16.724.1.3.5.7.2.8          |                    | Segundo Apellido  |
| 2.16.724.1.3.5.7.2.10         | Opcional           | Unidad dentro de la administración  |
| 2.16.724.1.3.5.7.2.11         | Opcional           | Puesto o cargo  |
| <b>extendedKeyUsage</b>       |                    | clientAuth  |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública   |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier  |
| <b>certificatePolicies</b>    |                    |   |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.52.1.3  |
| cpsURI                        |                    | <a href="http://www.izenpe.eus/cps">http://www.izenpe.eus/cps</a>   |
| userNotice                    |                    | Kontsulta <a href="http://www.izenpe.eus">www.izenpe.eus</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.eus">www.izenpe.eus</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier              |                    | 2.16.724.1.3.5.7.2  |
| policyIdentifier              |                    | 0.4.0.194112.1.0 (QCP-n)  |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.eus/crls/crlaapp.crl">http://crl.izenpe.eus/crls/crlaapp.crl</a>   |
| <b>authorityInfoAccess</b>    |                    |   |
| ocsp                          |                    | <a href="http://ocsp.izenpe.eus">http://ocsp.izenpe.eus</a>   |
| CA emisora                    |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR2025.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR2025.crt</a>   |
| <b>qcStatements</b>           |                    |   |
| QcCompliance                  |                    | Presente  |
| QcType                        |                    | id-etsi-qct-esign   |
| QcRetentiodPeriod             |                    | 15 años   |
| QcPDS                         |                    | <a href="https://www.izenpe.eus/pds/en/">https://www.izenpe.eus/pds/en/</a><br><a href="https://www.izenpe.eus/pds/eu/">https://www.izenpe.eus/pds/eu/</a>  |
| qcStatement-2                 |                    | 0.4.0.194121.1.1 (id-etsi-qcs-SemanticsId-Natural)  |
| <b>keyUsage</b>               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment   |

## Personal de Entidades Públicas con Seudónimo (FIRMA)

CA emisora

AAPPR2025

Nombre

pep\_seudonimo\_scard\_sign

| Campo / extensión             | Opcional / Crítica | Contenido  |
|-------------------------------|--------------------|--|
| <b>version</b>                |                    | Versión 3  |
| <b>serialNumber</b>           |                    | Número aleatorio único   |
| <b>signature</b>              |                    | sha384ECDSA  |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora  |
| <b>validity</b>               |                    | 3 años   |
| <b>subject</b>                |                    |  |
| title                         | Opcional           | Puesto o cargo de la persona   |
| pseudonym                     |                    | Seudónimo  |
| CN                            |                    | <Cargo> - <seudonimo> - <Organizacion> (FIRMA)<br>o<br><b>SEUDONIMO</b> - <seudonimo> - <Organizacion> (FIRMA)   |
| OU                            |                    | <b>CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO</b>   |
| OU                            | Opcional           | Unidad dentro de la administración   |
| OU                            | Opcional           | Código DIR3 de la unidad   |
| O                             |                    | Nombre oficial de la Administración a la que pertenece el poseedor   |
| C                             |                    | <b>ES</b>  |
| <b>subjectPublicKeyInfo</b>   |                    | ECC 256 bits mínimo  |
| <b>extensions</b>             |                    |  |
| <b>subjectAltName</b>         |                    |  |
| directoryName                 |                    |  |
| 2.16.724.1.3.5.4.1.1          |                    | <b>CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO</b>   |
| 2.16.724.1.3.5.4.1.2          |                    | Nombre oficial de la Administración a la que pertenece el poseedor   |
| 2.16.724.1.3.5.4.1.3          |                    | NIF  |
| 2.16.724.1.3.5.4.1.10         | Opcional           | Unidad dentro de la administración   |
| 2.16.724.1.3.5.4.1.11         | Opcional           | Puesto o cargo del suscriptor  |
| 2.16.724.1.3.5.4.1.12         |                    | Seudónimo  |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública  |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier   |
| <b>certificatePolicies</b>    |                    |  |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.52.2.1.1   |
| cpsURI                        |                    | <a href="http://www.izenpe.eus/cps">http://www.izenpe.eus/cps</a>  |
| userNotice                    |                    | Konsulta <a href="http://www.izenpe.eus">www.izenpe.eus</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.eus">www.izenpe.eus</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier              |                    | OID MINHAP: <b>2.16.724.1.3.5.4.1</b>  |
| policyIdentifier              |                    | OID QCP-n-qscd: <b>0.4.0.194112.1.2</b>  |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.eus/crls/crlaapp.crl">http://crl.izenpe.eus/crls/crlaapp.crl</a>  |
| <b>authorityInfoAccess</b>    |                    |  |
| ocsp                          |                    | <a href="http://ocsp.izenpe.eus">http://ocsp.izenpe.eus</a>  |
| CA emisora                    |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR2025.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR2025.crt</a>  |
| <b>qcStatements</b>           |                    |  |
| QcCompliance                  |                    | Presente   |
| QcType                        |                    | id-etsi-qct-esign  |
| QcSSCD                        |                    | Presente   |
| QcEuRetentiodPeriod           |                    | 15 años  |
| QcPDS                         |                    | <a href="https://www.izenpe.eus/pds/en/">https://www.izenpe.eus/pds/en/</a> en<br><a href="https://www.izenpe.eus/pds/eu/">https://www.izenpe.eus/pds/eu/</a> eu<br><a href="https://www.izenpe.eus/pds/es/">https://www.izenpe.eus/pds/es/</a> es                           |
| <b>keyUsage</b>               | Crítica            | contentCommitment (no repudio)   |

## Personal de Entidades Públicas con Seudónimo (AUTENTICACION)

CA emisora

AAPPR2025

Nombre

pep\_seudonimo\_scard\_auth

| Campo / extensión      | Opcional / Crítica | Contenido  |
|------------------------|--------------------|--|
| version                |                    | Versión 3  |
| serialNumber           |                    | Número aleatorio único   |
| signature              |                    | sha384ECDSA  |
| issuer                 |                    | Igual al campo subject del certificado de la CA emisora  |
| validity               |                    | 3 años   |
| subject                |                    |  |
| title                  | Opcional           | Puesto o cargo de la persona   |
| pseudonym              |                    | Seudónimo  |
| CN                     |                    | <Cargo> - <seudonimo> - <Organizacion> (AUTENTICACION)<br>o<br><b>SEUDONIMO</b> - <seudonimo> - <Organizacion> (AUTENTICACION)   |
| OU                     |                    | <b>CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO</b>   |
| OU                     | Opcional           | Unidad dentro de la administración   |
| OU                     | Opcional           | Código DIR3 de la unidad   |
| O                      |                    | Nombre oficial de la Administración a la que pertenece el poseedor   |
| C                      |                    | <b>ES</b>  |
| subjectPublicKeyInfo   |                    | ECC 256 bits mínimo  |
| extensions             |                    |  |
| subjectAltName         |                    |  |
| directoryName          |                    |  |
| 2.16.724.1.3.5.4.1.1   |                    | <b>CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO</b>   |
| 2.16.724.1.3.5.4.1.2   |                    | Nombre oficial de la Administración a la que pertenece el poseedor   |
| 2.16.724.1.3.5.4.1.3   |                    | NIF  |
| 2.16.724.1.3.5.4.1.10  | Opcional           | Unidad dentro de la administración   |
| 2.16.724.1.3.5.4.1.11  | Opcional           | Puesto o cargo del suscriptor  |
| 2.16.724.1.3.5.4.1.12  |                    | Seudónimo  |
| UserPrincipalName      | Opcional           | UPN para smart card logon  |
| extendedKeyUsage       |                    | clientAuth   |
| subjectKeyIdentifier   |                    | Identificador de la clave pública  |
| authorityKeyIdentifier |                    | Incluir sólo campo keyIdentifier   |
| certificatePolicies    |                    |  |
| policyIdentifier       |                    | 1.3.6.1.4.1.14777.52.2.1.2   |
| cpsURI                 |                    | <a href="http://www.izenpe.eus/cps">http://www.izenpe.eus/cps</a>  |
| userNotice             |                    | Konsulta <a href="http://www.izenpe.eus">www.izenpe.eus</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.eus">www.izenpe.eus</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier       |                    | OID MINHAP: <b>2.16.724.1.3.5.4.1</b>  |
| policyIdentifier       |                    | OID NCP+: <b>0.4.0.2042.1.2</b>  |
| cRLDistributionPoints  |                    | <a href="http://crl.izenpe.eus/crls/crlaapp.crl">http://crl.izenpe.eus/crls/crlaapp.crl</a>  |
| authorityInfoAccess    |                    |  |
| ocsp                   |                    | <a href="http://ocsp.izenpe.eus">http://ocsp.izenpe.eus</a>  |
| CA emisora             |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR2025.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR2025.crt</a>  |
| keyUsage               | Crítica            | digitalSignature   |



## Personal de Entidades Públicas con Seudónimo (FIRMA)

CA emisora

AAPPR2025

Nombre

pep\_seudonimo\_sw

| Campo / extensión      | Opcional / Crítica | Contenido  |
|------------------------|--------------------|--|
| version                |                    | Versión 3  |
| serialNumber           |                    | Número aleatorio único   |
| signature              |                    | sha384ECDSA  |
| issuer                 |                    | Igual al campo subject del certificado de la CA emisora  |
| validity               |                    | 3 años   |
| subject                |                    |  |
| title                  | Opcional           | Puesto o cargo de la persona   |
| pseudonym              |                    | Seudónimo  |
| CN                     |                    | <Cargo> - <seudonimo> - <Organizacion><br>o<br><b>SEUDONIMO</b> - <seudonimo> - <Organizacion>   |
| OU                     |                    | <b>CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO</b>   |
| OU                     | Opcional           | Unidad dentro de la administración   |
| OU                     | Opcional           | Código DIR3 de la unidad   |
| O                      |                    | Nombre oficial de la Administración a la que pertenece el poseedor   |
| C                      |                    | <b>ES</b>  |
| subjectPublicKeyInfo   |                    | ECC 256 bits mínimo  |
| extensions             |                    |  |
| subjectAltName         |                    |  |
| directoryName          |                    |  |
| 2.16.724.1.3.5.4.2.1   |                    | <b>CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO CON SEUDONIMO</b>   |
| 2.16.724.1.3.5.4.2.2   |                    | Nombre oficial de la Administración a la que pertenece el poseedor   |
| 2.16.724.1.3.5.4.2.3   |                    | NIF  |
| 2.16.724.1.3.5.4.2.10  | Opcional           | Unidad dentro de la administración   |
| 2.16.724.1.3.5.4.2.11  | Opcional           | Puesto o cargo del suscriptor  |
| 2.16.724.1.3.5.4.2.12  |                    | Seudónimo  |
| UserPrincipalName      | Opcional           | UPN para smart card logon  |
| extendedKeyUsage       |                    | clientAuth   |
| subjectKeyIdentifier   |                    | Identificador de la clave pública  |
| authorityKeyIdentifier |                    | Incluir sólo campo keyIdentifier   |
| certificatePolicies    |                    |  |
| policyIdentifier       |                    | 1.3.6.1.4.1.14777.52.2.2   |
| cpsURI                 |                    | <a href="http://www.izenpe.eus/cps">http://www.izenpe.eus/cps</a>  |
| userNotice             |                    | Konsulta <a href="http://www.izenpe.eus">www.izenpe.eus</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.eus">www.izenpe.eus</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier       |                    | OID MINHAP: <b>2.16.724.1.3.5.4.2</b>  |
| policyIdentifier       |                    | OID QCP-n: <b>0.4.0.194112.1.0</b>   |
| cRLDistributionPoints  |                    | <a href="http://crl.izenpe.eus/crls/crlaapp.crl">http://crl.izenpe.eus/crls/crlaapp.crl</a>  |
| authorityInfoAccess    |                    |  |
| ocsp                   |                    | <a href="http://ocsp.izenpe.eus">http://ocsp.izenpe.eus</a>  |
| CA emisora             |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR2025.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR2025.crt</a>  |
| qcStatements           |                    |  |
| QcCompliance           |                    | Presente   |
| QcType                 |                    | id-etsi-qct-esign  |
| QcEuRetentiodPeriod    |                    | 15 años  |
| QcPDS                  |                    | <a href="https://www.izenpe.eus/pds/en/en">https://www.izenpe.eus/pds/en/en</a><br><a href="https://www.izenpe.eus/pds/eu/eu">https://www.izenpe.eus/pds/eu/eu</a><br><a href="https://www.izenpe.eus/pds/es/es">https://www.izenpe.eus/pds/es/es</a>                        |
| keyUsage               | Crítica            | contentCommitment (no repudio), digitalSignature, keyEncipherment  |

## Representante Tarjeta

CA emisora

CCEER2025

Nombre

representante

| Campo / extensión             | Opcional / Crítica | Contenido   |
|-------------------------------|--------------------|---|
| <b>version</b>                |                    | Versión 3   |
| <b>serialNumber</b>           |                    | Número aleatorio único  |
| <b>signature</b>              |                    | sha384ECDSA   |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora   |
| <b>validity</b>               |                    | 4 años  |
| <b>subject</b>                |                    |   |
| CN                            |                    | DNI/NIE Nombre Apellido1 (R: NIF)   |
| G                             |                    | Nombre  |
| SN                            |                    | Apellidos   |
| serialNumber                  |                    | DNI / NIE   |
| descripción                   |                    | Codificación del documento público que acredita las facultades del firmante o los datos registrales. Hay tres opciones: registro mercantil, poder notarial, Boletines oficiales   |
| OU                            |                    | Ordezkarri ziurtagiria - Certificado de representante   |
| organizationIdentifier        |                    | 3 caracteres tipo-identidad + Country + - + identificador. Por ejemplo, si usamos el CIF sería algo como: VATES-A01337260   |
| O                             |                    | Razón social, tal como figura en los registros oficiales  |
| C                             |                    | País  |
| <b>subjectPublicKeyInfo</b>   |                    | ECC 256 bits mínimo   |
| <b>extensions</b>             |                    |   |
| <b>extendedKeyUsage</b>       |                    | clientAuth, documentSigning   |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública   |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier  |
| <b>certificatePolicies</b>    |                    |   |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.51.3.1  |
| cpsURI                        |                    | <a href="http://www.izenpe.com/cps">http://www.izenpe.com/cps</a>   |
| userNotice                    |                    | Kontsulta <a href="http://www.izenpe.com">www.izenpe.com</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.com">www.izenpe.com</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier              |                    | 0.4.0.194112.1.0 (QCP-n)  |
| policyIdentifier              |                    | 2.16.724.1.3.5.8 (OID PJ MPR)   |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.eus/crls/crlcceer.crl">http://crl.izenpe.eus/crls/crlcceer.crl</a>   |
| <b>authorityInfoAccess</b>    |                    |   |
| ocsp                          |                    | <a href="http://ocsp.izenpe.eus">http://ocsp.izenpe.eus</a>   |
| CA emisora                    |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas_adjuntos/CCEER2025.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas_adjuntos/CCEER2025.crt</a>   |
| <b>qcStatements</b>           |                    |   |
| QcCompliance                  |                    | Presente  |
| QcType                        |                    | id-etsi-qct-esign   |
| QcRetentiodPeriod             |                    | 15 años   |
| QcPDS                         |                    | <a href="https://www.izenpe.eus/pds/en/en">https://www.izenpe.eus/pds/en/en</a><br><a href="https://www.izenpe.eus/pds/eu/eu">https://www.izenpe.eus/pds/eu/eu</a><br><a href="https://www.izenpe.eus/pds/es/es">https://www.izenpe.eus/pds/es/es</a>                         |
| qcStatement-2                 |                    | 0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)  |
| <b>keyUsage</b>               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment   |

## Representante Tarjeta

CA emisora

CCEER2025

Nombre

representante\_sscd

| Campo / extensión             | Opcional / Crítica | Contenido   |
|-------------------------------|--------------------|---|
| <b>version</b>                |                    | Versión 3   |
| <b>serialNumber</b>           |                    | Número aleatorio único  |
| <b>signature</b>              |                    | sha384ECDSA   |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora   |
| <b>validity</b>               |                    | 4 años  |
| <b>subject</b>                |                    |   |
| CN                            |                    | DNI/NIE Nombre Apellido1 (R: NIF)   |
| G                             |                    | Nombre  |
| SN                            |                    | Apellidos   |
| serialNumber                  |                    | DNI / NIE   |
| descripción                   |                    | Codificación del documento público que acredita las facultades del firmante o los datos registrales. Hay tres opciones: registro mercantil, poder notarial, Boletines oficiales   |
| OU                            |                    | Ordezkarri ziurtagiria - Certificado de representante   |
| organizationIdentifier        |                    | 3 caracteres tipo-identidad + Country + - + identificador. Por ejemplo, si usáramos el CIF sería algo como: VATES-A01337260   |
| O                             |                    | Razón social, tal como figura en los registros oficiales  |
| C                             |                    | País  |
| <b>subjectPublicKeyInfo</b>   |                    | ECC 256 bits mínimo   |
| <b>extensions</b>             |                    |   |
| <b>extendedKeyUsage</b>       |                    | clientAuth, documentSigning   |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública   |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier  |
| <b>certificatePolicies</b>    |                    |   |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.51.3.5  |
| cpsURI                        |                    | <a href="http://www.izenpe.com/cps">http://www.izenpe.com/cps</a>   |
| userNotice                    |                    | Kontsulta <a href="http://www.izenpe.com">www.izenpe.com</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.com">www.izenpe.com</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier              |                    | 0.4.0.194112.1.2 (ETSI QCP-n-qscd)  |
| policyIdentifier              |                    | 2.16.724.1.3.5.8 (OID PJ MPR)   |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.eus/crls/crlcceer.crl">http://crl.izenpe.eus/crls/crlcceer.crl</a>   |
| <b>authorityInfoAccess</b>    |                    |   |
| ocsp                          |                    | <a href="http://ocsp.izenpe.eus">http://ocsp.izenpe.eus</a>   |
| CA emisora                    |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER2025.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER2025.crt</a>   |
| <b>qcStatements</b>           |                    |   |
| QcCompliance                  |                    | Presente  |
| QcType                        |                    | id-etsi-qct-esign   |
| QcSSCD                        |                    | Presente  |
| QcRetentiodPeriod             |                    | 15 años   |
| QcPDS                         |                    | <a href="https://www.izenpe.eus/pds/en/">https://www.izenpe.eus/pds/en/</a> en<br><a href="https://www.izenpe.eus/pds/eu/">https://www.izenpe.eus/pds/eu/</a> eu<br><a href="https://www.izenpe.eus/pds/es/">https://www.izenpe.eus/pds/es/</a> es                            |
| qcStatement-2                 |                    | 0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)  |
| <b>keyUsage</b>               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment   |

## Representante HSM

CA emisora

CCEER2025

Nombre

representante\_hsm

| Campo / extensión             | Opcional / Crítica | Contenido   |
|-------------------------------|--------------------|---|
| <b>version</b>                |                    | Versión 3   |
| <b>serialNumber</b>           |                    | Número aleatorio único  |
| <b>signature</b>              |                    | sha384ECDSA   |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora   |
| <b>validity</b>               |                    | 4 años  |
| <b>subject</b>                |                    |   |
| CN                            |                    | DNI/NIE Nombre Apellido1 (R: NIF)   |
| G                             |                    | Nombre  |
| SN                            |                    | Apellidos   |
| serialNumber                  |                    | DNI / NIE   |
| descripción                   |                    | Codificación del documento público que acredita las facultades del firmante o los datos registrales. Hay tres opciones: registro mercantil, poder notarial, Boletines oficiales   |
| OU                            |                    | Ordezkarri ziurtagiria - Certificado de representante   |
| organizationIdentifier        |                    | 3 caracteres tipo-identidad + Country + - + identificador. Por ejemplo, si usáramos el CIF sería algo como: VATES-A01337260   |
| O                             |                    | Razón social, tal como figura en los registros oficiales  |
| C                             |                    | País  |
| <b>subjectPublicKeyInfo</b>   |                    | ECC 256 bits mínimo   |
| <b>extensions</b>             |                    |   |
| <b>extendedKeyUsage</b>       |                    | clientAuth, documentSigning   |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública   |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier  |
| <b>certificatePolicies</b>    |                    |   |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.51.3.3  |
| cpsURI                        |                    | <a href="http://www.izenpe.com/cps">http://www.izenpe.com/cps</a>   |
| userNotice                    |                    | Kontsulta <a href="http://www.izenpe.com">www.izenpe.com</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.com">www.izenpe.com</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier              |                    | 0.4.0.194112.1.0 (OID ETSI QCP-n)   |
| policyIdentifier              |                    | 2.16.724.1.3.5.8 (OID PJ MPR)   |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.eus/crls/crlcceer.crl">http://crl.izenpe.eus/crls/crlcceer.crl</a>   |
| <b>authorityInfoAccess</b>    |                    |   |
| ocsp                          |                    | <a href="http://ocsp.izenpe.eus">http://ocsp.izenpe.eus</a>   |
| CA emisora                    |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER2025.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER2025.crt</a>   |
| <b>qcStatements</b>           |                    |   |
| QcCompliance                  |                    | Presente  |
| QcType                        |                    | id-etsi-qct-esign   |
| QcRetentiodPeriod             |                    | 15 años   |
| QcPDS                         |                    | <a href="https://www.izenpe.eus/pds/en/en">https://www.izenpe.eus/pds/en/en</a><br><a href="https://www.izenpe.eus/pds/eu/eu">https://www.izenpe.eus/pds/eu/eu</a><br><a href="https://www.izenpe.eus/pds/es/es">https://www.izenpe.eus/pds/es/es</a>                         |
| qcStatement-2                 |                    | 0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)  |
| <b>keyUsage</b>               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment   |

# Representante Software

CA emisora

CCEER2025

Nombre

representante\_sw

| Campo / extensión             | Opcional / Crítica | Contenido   |
|-------------------------------|--------------------|---|
| <b>version</b>                |                    | Versión 3   |
| <b>serialNumber</b>           |                    | Número aleatorio único  |
| <b>signature</b>              |                    | sha384ECDSA   |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora   |
| <b>validity</b>               |                    | 4 años  |
| <b>subject</b>                |                    |   |
| CN                            |                    | DNI/NIE Nombre Apellido1 (R: NIF)   |
| G                             |                    | Nombre  |
| SN                            |                    | Apellidos   |
| serialNumber                  |                    | DNI / NIE   |
| descripción                   |                    | Codificación del documento público que acredita las facultades del firmante o los datos registrales. Hay tres opciones: registro mercantil, poder notarial, Boletines oficiales   |
| OU                            |                    | Ordezkarri ziurtagiria - Certificado de representante   |
| organizationIdentifier        |                    | 3 caracteres tipo-identidad + Country + - + identificador. Por ejemplo, si usaramos el CIF sería algo como: VATES-A01337260   |
| O                             |                    | Razón social, tal como figura en los registros oficiales  |
| C                             |                    | País  |
| <b>subjectPublicKeyInfo</b>   |                    | ECC 256 bits mínimo   |
| <b>extensions</b>             |                    |   |
| <b>extendedKeyUsage</b>       |                    | clientAuth, documentSigning   |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública   |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier  |
| <b>certificatePolicies</b>    |                    |   |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.51.3.2  |
| cpsURI                        |                    | <a href="http://www.izenpe.com/cps">http://www.izenpe.com/cps</a>   |
| userNotice                    |                    | Kontsulta <a href="http://www.izenpe.com">www.izenpe.com</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.com">www.izenpe.com</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier              |                    | 0.4.0.194112.1.0 (OID ETSI QCP-n)   |
| policyIdentifier              |                    | 2.16.724.1.3.5.8 (OID PJ MPR)   |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.eu/crls/crlcceer.crl">http://crl.izenpe.eu/crls/crlcceer.crl</a>   |
| <b>authorityInfoAccess</b>    |                    |   |
| ocsp                          |                    | <a href="http://ocsp.izenpe.eu">http://ocsp.izenpe.eu</a>   |
| CA emisora                    |                    | <a href="http://www.izenpe.eu/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER2025.crt">http://www.izenpe.eu/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER2025.crt</a>   |
| <b>qcStatements</b>           |                    |   |
| QcCompliance                  |                    | Presente  |
| QcType                        |                    | id-etsi-qct-esign   |
| QcRetentiodPeriod             |                    | 15 años   |
| QcPDS                         |                    | <a href="https://www.izenpe.eu/pds/en/">https://www.izenpe.eu/pds/en/</a> en<br><a href="https://www.izenpe.eu/pds/eu/">https://www.izenpe.eu/pds/eu/</a> eu<br><a href="https://www.izenpe.eu/pds/es/">https://www.izenpe.eu/pds/es/</a> es                                  |
| qcStatement-2                 |                    | 0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)  |
| <b>keyUsage</b>               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment   |

## Representante SPJ Tarjeta

CA emisora

CCEER2025

Nombre

representante\_spj

| Campo / extensión             | Opcional / Crítica | Contenido   |
|-------------------------------|--------------------|---|
| <b>version</b>                |                    | Versión 3   |
| <b>serialNumber</b>           |                    | Número aleatorio único  |
| <b>signature</b>              |                    | sha384ECDSA   |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora   |
| <b>validity</b>               |                    | 4 años  |
| <b>subject</b>                |                    |   |
| CN                            |                    | DNI/NIE Nombre Apellido1 (R: NIF)   |
| G                             |                    | Nombre  |
| SN                            |                    | Apellidos   |
| serialNumber                  |                    | DNI / NIE   |
| descripción                   |                    | Codificación del documento público que acredita las facultades del firmante o los datos registrales. Hay tres opciones: registro mercantil, poder notarial, Boletines oficiales   |
| OU                            |                    | NJG Ordezkaritza ziurtagiria - Certificado de representante SPJ   |
| organizationIdentifier        |                    | 3 caracteres tipo-identidad + Country + - + identificador. Por ejemplo, si usáramos el CIF sería algo como: VATES-A01337260   |
| O                             |                    | Razón social, tal como figura en los registros oficiales  |
| C                             |                    | País  |
| <b>subjectPublicKeyInfo</b>   |                    | ECC 256 bits mínimo   |
| <b>extensions</b>             |                    |   |
| <b>extendedKeyUsage</b>       |                    | clientAuth, documentSigning   |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública   |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier  |
| <b>certificatePolicies</b>    |                    |   |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.51.4.1  |
| cpsURI                        |                    | <a href="http://www.izenpe.com/cps">http://www.izenpe.com/cps</a>   |
| userNotice                    |                    | Kontsulta <a href="http://www.izenpe.com">www.izenpe.com</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.com">www.izenpe.com</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier              |                    | 0.4.0.194112.1.0 (QCP-n)  |
| policyIdentifier              |                    | 2.16.724.1.3.5.9 (OID PJ MPR)   |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.eus/crls/crlcceer.crl">http://crl.izenpe.eus/crls/crlcceer.crl</a>   |
| <b>authorityInfoAccess</b>    |                    |   |
| ocsp                          |                    | <a href="http://ocsp.izenpe.eus">http://ocsp.izenpe.eus</a>   |
| CA emisora                    |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER2025.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER2025.crt</a>   |
| <b>qcStatements</b>           |                    |   |
| QcCompliance                  |                    | Presente  |
| QcType                        |                    | id-etsi-qct-esign   |
| QcRetentiodPeriod             |                    | 15 años   |
| QcPDS                         |                    | <a href="https://www.izenpe.eus/pds/en/">https://www.izenpe.eus/pds/en/</a> en<br><a href="https://www.izenpe.eus/pds/eu/">https://www.izenpe.eus/pds/eu/</a> eu<br><a href="https://www.izenpe.eus/pds/es/">https://www.izenpe.eus/pds/es/</a> es                            |
| qcStatement-2                 |                    | 0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)  |
| <b>keyUsage</b>               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment   |

## Representante SPJ Tarjeta

CA emisora

CCEER2025

Nombre

representante\_spj\_sscd

| Campo / extensión             | Opcional / Crítica | Contenido   |
|-------------------------------|--------------------|---|
| <b>version</b>                |                    | Versión 3   |
| <b>serialNumber</b>           |                    | Número aleatorio único  |
| <b>signature</b>              |                    | sha384ECDSA   |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora   |
| <b>validity</b>               |                    | 4 años  |
| <b>subject</b>                |                    |   |
| CN                            |                    | DNI/NIE Nombre Apellido1 (R: NIF)   |
| G                             |                    | Nombre  |
| SN                            |                    | Apellidos   |
| serialNumber                  |                    | DNI / NIE   |
| descripción                   |                    | Codificación del documento público que acredita las facultades del firmante o los datos registrales. Hay tres opciones: registro mercantil, poder notarial, Boletines oficiales   |
| OU                            |                    | NJG Ordezkarri ziurtagiria - Certificado de representante SPJ   |
| organizationIdentifier        |                    | 3 caracteres tipo-identidad + Country + - + identificador. Por ejemplo, si usaramos el CIF sería algo como: VATES-A01337260   |
| O                             |                    | Razón social, tal como figura en los registros oficiales  |
| C                             |                    | País  |
| <b>subjectPublicKeyInfo</b>   |                    | ECC 256 bits mínimo   |
| <b>extensions</b>             |                    |   |
| <b>extendedKeyUsage</b>       |                    | clientAuth, documentSigning   |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública   |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier  |
| <b>certificatePolicies</b>    |                    |   |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.51.4.5  |
| cpsURI                        |                    | <a href="http://www.izenpe.com/cps">http://www.izenpe.com/cps</a>   |
| userNotice                    |                    | Kontsulta <a href="http://www.izenpe.com">www.izenpe.com</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.com">www.izenpe.com</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier              |                    | 0.4.0.194112.1.2 (ETSI QCP-n-qscd)  |
| policyIdentifier              |                    | 2.16.724.1.3.5.9 (OID PJ MPR)   |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.eus/crls/crlcceer.crl">http://crl.izenpe.eus/crls/crlcceer.crl</a>   |
| <b>authorityInfoAccess</b>    |                    |   |
| ocsp                          |                    | <a href="http://ocsp.izenpe.eus">http://ocsp.izenpe.eus</a>   |
| CA emisora                    |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER2025.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER2025.crt</a>   |
| <b>qcStatements</b>           |                    |   |
| QcCompliance                  |                    | Presente  |
| QcType                        |                    | id-etsi-qct-esign   |
| QcSSCD                        |                    | Presente  |
| QcRetentiodPeriod             |                    | 15 años   |
| QcPDS                         |                    | <a href="https://www.izenpe.eus/pds/en/">https://www.izenpe.eus/pds/en/</a> en<br><a href="https://www.izenpe.eus/pds/eu/">https://www.izenpe.eus/pds/eu/</a> eu<br><a href="https://www.izenpe.eus/pds/es/">https://www.izenpe.eus/pds/es/</a> es                            |
| qcStatement-2                 |                    | 0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)  |
| <b>keyUsage</b>               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment   |

## Representante SPJ HSM

CA emisora

CCEER2025

Nombre

representante\_spj\_hsm

| Campo / extensión             | Opcional / Crítica | Contenido   |
|-------------------------------|--------------------|---|
| <b>version</b>                |                    | Versión 3   |
| <b>serialNumber</b>           |                    | Número aleatorio único  |
| <b>signature</b>              |                    | sha384ECDSA   |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora   |
| <b>validity</b>               |                    | 4 años  |
| <b>subject</b>                |                    |   |
| CN                            |                    | DNI/NIE Nombre Apellido1 (R: NIF)   |
| G                             |                    | Nombre  |
| SN                            |                    | Apellidos   |
| serialNumber                  |                    | DNI / NIE   |
| descripción                   |                    | Codificación del documento público que acredita las facultades del firmante o los datos registrales. Hay tres opciones: registro mercantil, poder notarial, Boletines oficiales   |
| OU                            |                    | NJG Ordezkarri ziurtagiria - Certificado de representante SPJ   |
| organizationIdentifier        |                    | 3 caracteres tipo-identidad + Country + - + identificador. Por ejemplo, si usaramos el CIF sería algo como: VATES-A01337260   |
| O                             |                    | Razón social, tal como figura en los registros oficiales  |
| C                             |                    | País  |
| <b>subjectPublicKeyInfo</b>   |                    | ECC 256 bits mínimo   |
| <b>extensions</b>             |                    |   |
| <b>extendedKeyUsage</b>       |                    | clientAuth, documentSigning   |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública   |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier  |
| <b>certificatePolicies</b>    |                    |   |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.51.4.3  |
| cpsURI                        |                    | <a href="http://www.izenpe.com/cps">http://www.izenpe.com/cps</a>   |
| userNotice                    |                    | Kontsulta <a href="http://www.izenpe.com">www.izenpe.com</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.com">www.izenpe.com</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier              |                    | 0.4.0.194112.1.0 (OID ETSI QCP-n)   |
| policyIdentifier              |                    | 2.16.724.1.3.5.9 (OID PJ MPR)   |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.eus/crls/crlcceer.crl">http://crl.izenpe.eus/crls/crlcceer.crl</a>   |
| <b>authorityInfoAccess</b>    |                    |   |
| ocsp                          |                    | <a href="http://ocsp.izenpe.eus">http://ocsp.izenpe.eus</a>   |
| CA emisora                    |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER2025.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER2025.crt</a>   |
| <b>qcStatements</b>           |                    |   |
| QcCompliance                  |                    | Presente  |
| QcType                        |                    | id-etsi-qct-esign   |
| QcRetentiodPeriod             |                    | 15 años   |
| QcPDS                         |                    | <a href="https://www.izenpe.eus/pds/en/en">https://www.izenpe.eus/pds/en/en</a><br><a href="https://www.izenpe.eus/pds/eu/eu">https://www.izenpe.eus/pds/eu/eu</a><br><a href="https://www.izenpe.eus/pds/es/es">https://www.izenpe.eus/pds/es/es</a>                         |
| qcStatement-2                 |                    | 0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)  |
| <b>keyUsage</b>               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment   |

## Representante SPJ Software

CA emisora

CCEER2025

Nombre

representante\_spj\_sw

| Campo / extensión             | Opcional / Crítica | Contenido   |
|-------------------------------|--------------------|---|
| <b>version</b>                |                    | Versión 3   |
| <b>serialNumber</b>           |                    | Número aleatorio único  |
| <b>signature</b>              |                    | sha384ECDSA   |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora   |
| <b>validity</b>               |                    | 4 años  |
| <b>subject</b>                |                    |   |
| CN                            |                    | DNI/NIE Nombre Apellido1 (R: NIF)   |
| G                             |                    | Nombre  |
| SN                            |                    | Apellidos   |
| serialNumber                  |                    | DNI / NIE   |
| descripción                   |                    | Codificación del documento público que acredita las facultades del firmante o los datos registrales. Hay tres opciones: registro mercantil, poder notarial, Boletines oficiales   |
| OU                            |                    | NJG Ordezkarri ziurtagiria - Certificado de representante SPJ   |
| organizationIdentifier        |                    | 3 caracteres tipo-identidad + Country + - + identificador. Por ejemplo, si usamos el CIF sería algo como: VATES-A01337260   |
| O                             |                    | Razón social, tal como figura en los registros oficiales  |
| C                             |                    | País  |
| <b>subjectPublicKeyInfo</b>   |                    | ECC 256 bits mínimo   |
| <b>extensions</b>             |                    |   |
| <b>extendedKeyUsage</b>       |                    | clientAuth, documentSigning   |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública   |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier  |
| <b>certificatePolicies</b>    |                    |   |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.51.4.2  |
| cpsURI                        |                    | <a href="http://www.izenpe.com/cps">http://www.izenpe.com/cps</a>   |
| userNotice                    |                    | Kontsulta <a href="http://www.izenpe.com">www.izenpe.com</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.com">www.izenpe.com</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier              |                    | 0.4.0.194112.1.0 (OID ETSI QCP-n)   |
| policyIdentifier              |                    | 2.16.724.1.3.5.9 (OID PJ MPR)   |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.eus/crls/crlcceer.crl">http://crl.izenpe.eus/crls/crlcceer.crl</a>   |
| <b>authorityInfoAccess</b>    |                    |   |
| ocsp                          |                    | <a href="http://ocsp.izenpe.eus">http://ocsp.izenpe.eus</a>   |
| CA emisora                    |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER2025.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER2025.crt</a>   |
| <b>qcStatements</b>           |                    |   |
| QcCompliance                  |                    | Presente  |
| QcType                        |                    | id-etsi-qct-esign   |
| QcRetentiodPeriod             |                    | 15 años   |
| QcPDS                         |                    | <a href="https://www.izenpe.eus/pds/en/en">https://www.izenpe.eus/pds/en/en</a><br><a href="https://www.izenpe.eus/pds/eu/eu">https://www.izenpe.eus/pds/eu/eu</a><br><a href="https://www.izenpe.eus/pds/es/es">https://www.izenpe.eus/pds/es/es</a>                         |
| qcStatement-2                 |                    | 0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)  |
| <b>keyUsage</b>               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment   |

## Sello Entidad

CA emisora

CCEER2025

Nombre

sello\_juridico

| Campo / extensión             | Opcional / Crítica | Contenido   |
|-------------------------------|--------------------|---|
| <b>version</b>                |                    | Versión 3   |
| <b>serialNumber</b>           |                    | Número aleatorio único  |
| <b>signature</b>              |                    | sha384ECDSA   |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora   |
| <b>validity</b>               |                    | 3 años  |
| <b>subject</b>                |                    |   |
| serialNumber                  | Opcional           | DNI/NIE según semántica ETSI EN 319 412 - 1   |
| SN                            | Opcional           | Apellidos   |
| G                             | Opcional           | Nombre  |
| CN                            |                    | Nombre comúnmente utilizado por el sujeto para representarse a sí mismo   |
| organizationIdentifier        |                    | 3 caracteres tipo-identidad + Country + - + identificador. Por ejemplo, si usáramos el CIF sería algo como: VATES-A01337260   |
| O                             |                    | Nombre completo registrado del sujeto/organización  |
| C                             |                    | País  |
| <b>subjectPublicKeyInfo</b>   |                    | ECC 256 bits mínimo   |
| <b>extensions</b>             |                    |   |
| <b>extendedKeyUsage</b>       |                    | clientAuth, emailProtection   |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública   |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier  |
| <b>certificatePolicies</b>    |                    |   |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.51.5.2  |
| cpsURI                        |                    | <a href="http://www.izenpe.eus/cps">http://www.izenpe.eus/cps</a>   |
| userNotice                    |                    | Kontsulta <a href="http://www.izenpe.eus">www.izenpe.eus</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.eus">www.izenpe.eus</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier              |                    | 0.4.0.194112.1.1 (OID ETSI QCP-I)   |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.eus/crls/crlcceer.crl">http://crl.izenpe.eus/crls/crlcceer.crl</a>   |
| <b>authorityInfoAccess</b>    |                    |   |
| ocsp                          |                    | <a href="http://ocsp.izenpe.eus">http://ocsp.izenpe.eus</a>   |
| CA emisora                    |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER2025.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER2025.crt</a>   |
| <b>qcStatements</b>           |                    |   |
| QcCompliance                  |                    | Presente  |
| QcType                        |                    | id-etsi-qct-eseal   |
| QcRetentiodPeriod             |                    | 15 años   |
| QcPDS                         |                    | <a href="https://www.izenpe.eus/pds/en/en">https://www.izenpe.eus/pds/en/en</a><br><a href="https://www.izenpe.eus/pds/eu/eu">https://www.izenpe.eus/pds/eu/eu</a><br><a href="https://www.izenpe.eus/pds/es/es">https://www.izenpe.eus/pds/es/es</a>                         |
| qcStatement-2                 |                    | 0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)  |
| qcStatement-2                 |                    | 0.4.0.194121.1.1 (id-etsi-qcs-SemanticsId-Natural)  |
| <b>keyUsage</b>               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment   |

## Sello Entidad HSM

CA emisora

CCEER2025

Nombre

sello\_juridico\_hsm

| Campo / extensión             | Opcional / Crítica | Contenido  |
|-------------------------------|--------------------|--|
| <b>version</b>                |                    | Versión 3  |
| <b>serialNumber</b>           |                    | Número aleatorio único   |
| <b>signature</b>              |                    | sha384ECDSA  |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora  |
| <b>validity</b>               |                    | 3 años   |
| <b>subject</b>                |                    |  |
| serialNumber                  | Opcional           | DNI/NIE según semántica ETSI EN 319 412 - 1  |
| SN                            | Opcional           | Apellidos  |
| G                             | Opcional           | Nombre   |
| CN                            |                    | Nombre comúnmente utilizado por el sujeto para representarse a sí mismo  |
| organizationIdentifier        |                    | 3 caracteres tipo-identidad + Country + - + identificador. Por ejemplo, si usaramos el CIF sería algo como: VATES-A01337260  |
| O                             |                    | Nombre completo registrado del sujeto/organización   |
| C                             |                    | País   |
| <b>subjectPublicKeyInfo</b>   |                    | ECC 256 bits mínimo  |
| <b>extensions</b>             |                    |  |
| <b>extendedKeyUsage</b>       |                    | clientAuth, emailProtection  |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública  |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier   |
| <b>certificatePolicies</b>    |                    |  |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.51.5.3   |
| cpsURI                        |                    | <a href="http://www.izenpe.eus/cps">http://www.izenpe.eus/cps</a>  |
| userNotice                    |                    | Konsulta <a href="http://www.izenpe.eus">www.izenpe.eus</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.eus">www.izenpe.eus</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier              |                    | 0.4.0.194112.1.1 (OID ETSI QCP-I)  |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.eus/crls/crlcceer.crl">http://crl.izenpe.eus/crls/crlcceer.crl</a>  |
| <b>authorityInfoAccess</b>    |                    |  |
| ocsp                          |                    | <a href="http://ocsp.izenpe.eus">http://ocsp.izenpe.eus</a>  |
| CA emisora                    |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas_adjuntos/CCEER2025.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas_adjuntos/CCEER2025.crt</a>  |
| <b>qcStatements</b>           |                    |  |
| QcCompliance                  |                    | Presente   |
| QcType                        |                    | id-etsi-qct-eseal  |
| QcRetentiodPeriod             |                    | 15 años  |
| QcPDS                         |                    | <a href="https://www.izenpe.eus/pds/en/">https://www.izenpe.eus/pds/en/</a> en<br><a href="https://www.izenpe.eus/pds/eu/">https://www.izenpe.eus/pds/eu/</a> eu<br><a href="https://www.izenpe.eus/pds/es/">https://www.izenpe.eus/pds/es/</a> es                           |
| qcStatement-2                 |                    | 0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)   |
| qcStatement-2                 |                    | 0.4.0.194121.1.1 (id-etsi-qcs-SemanticsId-Natural)   |
| <b>keyUsage</b>               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment  |

## Sello nivel medio EIDAS

CA emisora

AAPPR2025

Nombre

sello\_nivel\_medio\_eidas

| Campo / extensión             | Opcional / Crítica | Contenido   |
|-------------------------------|--------------------|---|
| <b>version</b>                |                    | Versión 3   |
| <b>serialNumber</b>           |                    | Número aleatorio único  |
| <b>signature</b>              |                    | sha384ECDSA   |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora   |
| <b>validity</b>               |                    | 2 o 3 años  |
| <b>subject</b>                |                    |   |
| CN                            |                    | Nombre descriptivo del sistema o aplicación de proceso automático   |
| G                             | Opcional           | Nombre del responsable  |
| SN                            | Opcional           | [APELLIDO1] [APELLIDO2] - DNI [DNI/NIE]   |
| serialNumber                  |                    | NIF   |
| organizationIdentifier        |                    | 3 caracteres tipo-identidad + Country + - + identificador. Por ejemplo, si usaramos el NIF sería algo como: VATES-A01337260   |
| OU                            |                    | "SELLO ELECTRONICO"   |
| O                             |                    | Nombre oficial de la organización   |
| C                             |                    | ES  |
| <b>subjectPublicKeyInfo</b>   |                    | ECC 256 bits mínimo   |
| <b>extensions</b>             |                    |   |
| <b>subjectAltName</b>         |                    |   |
| rfc822Name                    | Opcional           | Email de contacto de la organización  |
| directoryName                 |                    |   |
| 2.16.724.1.3.5.6.2.1          |                    | "SELLO ELECTRONICO"   |
| 2.16.724.1.3.5.6.2.2          |                    | Nombre oficial de la organización   |
| 2.16.724.1.3.5.6.2.3          |                    | NIF   |
| 2.16.724.1.3.5.6.2.4          | Opcional           | DNI/NIE   |
| 2.16.724.1.3.5.6.2.5          |                    | Nombre de órgano administrativo, sistema o aplicación   |
| 2.16.724.1.3.5.6.2.6          | Opcional           | Nombre  |
| 2.16.724.1.3.5.6.2.7          | Opcional           | Primer Apellido   |
| 2.16.724.1.3.5.6.2.8          | Opcional           | Segundo Apellido  |
| 2.16.724.1.3.5.6.2.9          | Opcional           | Email del responsable   |
| <b>extendedKeyUsage</b>       |                    | clientAuth, emailProtection   |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública   |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier  |
| <b>certificatePolicies</b>    |                    |   |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.52.3.2  |
| cpsURI                        |                    | <a href="http://www.izenpe.eus/cps">http://www.izenpe.eus/cps</a>   |
| userNotice                    |                    | Kontsulta <a href="http://www.izenpe.eus">www.izenpe.eus</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.eus">www.izenpe.eus</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier              |                    | 2.16.724.1.3.5.6.2  |
| policyIdentifier              |                    | 0.4.0.194112.1.1 (QCP-I)  |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.eus/crls/crlaapp.crl">http://crl.izenpe.eus/crls/crlaapp.crl</a>   |
| <b>authorityInfoAccess</b>    |                    |   |
| ocsp                          |                    | <a href="http://ocsp.izenpe.eus">http://ocsp.izenpe.eus</a>   |
| CA emisora                    |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR2025.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR2025.crt</a>   |
| <b>qcStatements</b>           |                    |   |
| QcCompliance                  |                    | Presente  |
| QcType                        |                    | id-etsi-qct-eseal   |
| QcRetentionPeriod             |                    | 15 años   |
| QcPDS                         |                    | <a href="https://www.izenpe.com/pds/en/">https://www.izenpe.com/pds/en/</a> en<br><a href="https://www.izenpe.com/pds/eu/">https://www.izenpe.com/pds/eu/</a> eu<br><a href="https://www.izenpe.com/pds/es/">https://www.izenpe.com/pds/es/</a> es                            |
| qcStatement-2                 |                    | 0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)  |
| <b>keyUsage</b>               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment   |

## Sello nivel medio EIDAS

CA emisora

AAPPR2025

Nombre

sello\_nivel\_medio\_hsm

| Campo / extensión             | Opcional / Crítica | Contenido   |
|-------------------------------|--------------------|---|
| <b>version</b>                |                    | Versión 3   |
| <b>serialNumber</b>           |                    | Número aleatorio único  |
| <b>signature</b>              |                    | sha384ECDSA   |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora   |
| <b>validity</b>               |                    | 2 o 3 años  |
| <b>subject</b>                |                    |   |
| CN                            |                    | Nombre descriptivo del sistema o aplicación de proceso automático   |
| G                             | Opcional           | Nombre del responsable  |
| SN                            | Opcional           | [APELLIDO1] [APELLIDO2] - DNI [DNI/NIE]   |
| serialNumber                  |                    | NIF   |
| organizationIdentifier        |                    | 3 caracteres tipo-identidad + Country + - + identificador. Por ejemplo, si usaramos el NIF sería algo como: VATES-A01337260   |
| OU                            |                    | "SELLO ELECTRONICO"   |
| O                             |                    | Nombre oficial de la organización   |
| C                             |                    | ES  |
| <b>subjectPublicKeyInfo</b>   |                    | ECC 256 bits mínimo   |
| <b>extensions</b>             |                    |   |
| <b>subjectAltName</b>         |                    |   |
| rfc822Name                    | Opcional           | Email de contacto de la organización  |
| directoryName                 |                    |   |
| 2.16.724.1.3.5.6.2.1          |                    | "SELLO ELECTRONICO"   |
| 2.16.724.1.3.5.6.2.2          |                    | Nombre oficial de la organización   |
| 2.16.724.1.3.5.6.2.3          |                    | NIF   |
| 2.16.724.1.3.5.6.2.4          | Opcional           | DNI/NIE   |
| 2.16.724.1.3.5.6.2.5          |                    | Nombre de órgano administrativo, sistema o aplicación   |
| 2.16.724.1.3.5.6.2.6          | Opcional           | Nombre  |
| 2.16.724.1.3.5.6.2.7          | Opcional           | Primer Apellido   |
| 2.16.724.1.3.5.6.2.8          | Opcional           | Segundo Apellido  |
| 2.16.724.1.3.5.6.2.9          | Opcional           | Email del responsable   |
| <b>extendedKeyUsage</b>       |                    | clientAuth, emailProtection   |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública   |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier  |
| <b>certificatePolicies</b>    |                    |   |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.52.3.3  |
| cpsURI                        |                    | <a href="http://www.izenpe.eus/cps">http://www.izenpe.eus/cps</a>   |
| userNotice                    |                    | Kontsulta <a href="http://www.izenpe.eus">www.izenpe.eus</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.eus">www.izenpe.eus</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier              |                    | 2.16.724.1.3.5.6.2  |
| policyIdentifier              |                    | 0.4.0.19412.1.1 (QCP-I)   |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.eus/crls/crlaapp.crl">http://crl.izenpe.eus/crls/crlaapp.crl</a>   |
| <b>authorityInfoAccess</b>    |                    |   |
| ocsp                          |                    | <a href="http://ocsp.izenpe.eus">http://ocsp.izenpe.eus</a>   |
| CA emisora                    |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR2025.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR2025.crt</a>   |
| <b>qcStatements</b>           |                    |   |
| QcCompliance                  |                    | Presente  |
| QcType                        |                    | id-etsi-qct-eseal   |
| QcRetentionPeriod             |                    | 15 años   |
| QcPDS                         |                    | <a href="https://www.izenpe.com/pds/en/">https://www.izenpe.com/pds/en/</a> en<br><a href="https://www.izenpe.com/pds/eu/">https://www.izenpe.com/pds/eu/</a> eu<br><a href="https://www.izenpe.com/pds/es/">https://www.izenpe.com/pds/es/</a> es                            |
| qcStatement-2                 |                    | 0.4.0.19412.1.2 (id-etsi-qcs-SemanticsId-Legal)   |
| <b>keyUsage</b>               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment   |

## Sello nivel alto EIDAS

CA emisora

AAPPR2025

Nombre

sello\_nivel\_alto\_eidas

| Campo / extensión             | Opcional / Crítica | Contenido  |
|-------------------------------|--------------------|--|
| <b>version</b>                |                    | Versión 3  |
| <b>serialNumber</b>           |                    | Número aleatorio único   |
| <b>signature</b>              |                    | sha384ECDSA  |
| <b>issuer</b>                 |                    | Igual al campo subject del certificado de la CA emisora  |
| <b>validity</b>               |                    | 2 o 3 años   |
| <b>subject</b>                |                    |  |
| CN                            | Opcional           | Nombre descriptivo del sistema o aplicación de proceso automático  |
| G                             | Opcional           | Nombre del responsable   |
| SN                            | Opcional           | [APELLIDO1] [APELLIDO2] - DNI [DNI/NIE]  |
| serialNumber                  | Opcional           | NIF  |
| organizationIdentifier        |                    | 3 caracteres tipo-identidad + Country + - + identificador. Por ejemplo, si usamos el CIF sería algo como: VATES-A01337260  |
| OU                            |                    | "SELLO ELECTRONICO"  |
| O                             |                    | Nombre oficial de la organización  |
| C                             |                    | ES   |
| <b>subjectPublicKeyInfo</b>   |                    | ECC 256 bits mínimo  |
| <b>extensions</b>             |                    |  |
| <b>subjectAltName</b>         |                    |  |
| rfc822Name                    | Opcional           | Email de contacto de la organización   |
| directoryName                 |                    |  |
| 2.16.724.1.3.5.6.1.1          |                    | "SELLO ELECTRONICO"  |
| 2.16.724.1.3.5.6.1.2          |                    | Nombre oficial de la organización  |
| 2.16.724.1.3.5.6.1.3          |                    | NIF  |
| 2.16.724.1.3.5.6.1.4          | Opcional           | DNI/NIE  |
| 2.16.724.1.3.5.6.1.5          | Opcional           | Nombre de órgano administrativo, sistema o aplicación  |
| 2.16.724.1.3.5.6.1.6          | Opcional           | Nombre   |
| 2.16.724.1.3.5.6.1.7          | Opcional           | Primer Apellido  |
| 2.16.724.1.3.5.6.1.8          | Opcional           | Segundo Apellido   |
| 2.16.724.1.3.5.6.1.9          | Opcional           | Email del responsable  |
| <b>extendedKeyUsage</b>       |                    | clientAuth, emailProtection  |
| <b>subjectKeyIdentifier</b>   |                    | Identificador de la clave pública  |
| <b>authorityKeyIdentifier</b> |                    | Incluir sólo campo keyIdentifier   |
| <b>certificatePolicies</b>    |                    |  |
| policyIdentifier              |                    | 1.3.6.1.4.1.14777.52.4.2   |
| cpsURI                        |                    | <a href="http://www.izenpe.eus/cps">http://www.izenpe.eus/cps</a>  |
| userNotice                    |                    | Konsulta <a href="http://www.izenpe.eus">www.izenpe.eus</a> -en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en <a href="http://www.izenpe.eus">www.izenpe.eus</a> los términos y condiciones antes de utilizar o confiar en el certificado |
| policyIdentifier              |                    | 0.4.0.194112.1.3 (QCP-I-qscd)  |
| policyIdentifier              |                    | 2.16.724.1.3.5.6.1   |
| <b>cRLDistributionPoints</b>  |                    | <a href="http://crl.izenpe.eus/crls/crlaapp.crl">http://crl.izenpe.eus/crls/crlaapp.crl</a>  |
| <b>authorityInfoAccess</b>    |                    |  |
| ocsp                          |                    | <a href="http://ocsp.izenpe.eus">http://ocsp.izenpe.eus</a>  |
| CA emisora                    |                    | <a href="http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR2025.crt">http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR2025.crt</a>  |
| <b>qcStatements</b>           |                    |  |
| QcCompliance                  |                    | Presente   |
| QcType                        |                    | id-etsi-qct-eseal  |
| QcRetentionPeriod             |                    | 15 años  |
| QcSSCD                        |                    | Presente   |
| QcPDS                         |                    | <a href="https://www.izenpe.com/pds/en/">https://www.izenpe.com/pds/en/</a> en<br><a href="https://www.izenpe.com/pds/eu/">https://www.izenpe.com/pds/eu/</a> eu<br><a href="https://www.izenpe.com/pds/es/">https://www.izenpe.com/pds/es/</a> es                           |
| qcStatement-2                 |                    | 0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)   |
| <b>keyUsage</b>               | Crítica            | digitalSignature, nonRepudiation, keyEncipherment  |