Izenpe
Perfiles de Certificados de Entidad Final

Estado del documento

Fecha	Versión	Autor	Estado
12/5/2009	0.1	César Armenta	Borrador inicial incompleto. Incluye sólo el nuevo perfil Corporativo Privado Reconocido
13/5/2009	0.2	César Armenta	*Incluidos nuevos perfiles fase 11, con algunos campos pendientes de definición. *Resto de perfiles pendientes
13/5/2009	0.3	César Armenta	*Cerrado perfil Corporativo Privado Reconocido
24/6/2009	0.4	César Armenta	*Revisados los perfiles para Sede y Sello
26/6/2009	0.5	César Armenta	*Revisados OIDS de Sede y Sello
7/7/2009	0.6	César Armenta	*Revisados OIDs dentro del SubjectAltName de Sello Nivel Alto
30/7/2009	0.7	César Armenta	*Revisados Sede y Sello *Añadidos todos los perfiles de fases anteriores excepto los obsoletos
25/8/2009	0.8	César Armenta	*Correcciones menores en Sello
27/10/2009	0.9	César Armenta	*Validez de Sede con EV reducida a 2 años
23/11/2009	0.10	César Armenta	*Añadidos perfiles SSL EV - SHA1 y SSL EV - SHA256
4/2/2010	0.11	César Armenta	*Actualizados perfiles de sede y sello según versión V1.7.3 del documento del MPR *Añadidos perfiles de la CA AAPPR2
8/3/2010	0.12	Rocío Martinez	*Revisados perfiles SSL EV -SHA1 y SSL EV - SHA256
26/4/2010	0.13	César Armenta	*Cambios en el campo businessCategory en los perfiles de SSL EV
4/5/2010	0.14	César Armenta	*Cambio de URL OCSP en perfiles de SSL EV
17/9/2010	0.15	César Armenta	*Validez de SSLEV aumentada a 2 años *Añadidos atributos businessCategory y jurisdictionOfIncorporationCountryName en Sede con EV *Modificada extensión authorityKeyIdentifier en los perfiles antiguos *Modificada extensión AIA OCSP en los perfiles de SSLEV
19/10/2010	0.16	César Armenta	*Añadido CIF en CoR y PeP
30/5/2011	0.17	César Armenta	*Corregida extensión netscapeCertType en el perfil Aplicación *Añadido nuevo perfil CoRHw
16/6/2011	0.18	César Armenta	*Corrección de erratas
7/5/2013	0.19	Leire Bengoetxea	*Modificación de perfiles reconocidos en tarjeta y cambios en el perfil de SSL.
25/11/2013	0.20	Leire Bengoetxea	*Cambio de algoritmos de firma y tamaños de clave en todos los perfiles. Cambios en el campo SN de perfiles corporativos y ciudadano.
27/2/2015	0.21	Leire Bengoetxea	*Se añaden nuevos perfiles HW y el nuevo perfil de cifrado para EJGV
25/3/2015	0.22	Leire Bengoetxea	*Se añade nuevo perfil de SSL DV
7/1/2016	0.23	Leire Bengoetxea	*Se adaptan los perfiles a las normas ETSI
12/5/2016	0.24	Leire Bengoetxea	*Nuevos perfiles EIDAS
10/10/2016	0.25	Leire Bengoetxea	*Revisión/modificación perfiles
1/12/2016	1.0	Leire Bengoetxea	*Adaptación de todos los perfiles a EIDAS: personas físicas, personas jurídicas y ssl
27/4/2017	1.1	Leire Bengoetxea	*Correción de algunos perfiles y añadir los nuevos certificados en HSM
13/3/2018	1.2	Leire Bengoetxea	*Correcciones menores
21/3/2018	1.3	Leire Bengoetxea	*Se añade uso clave smartCardLogon a pep_qc_scard
25/4/2018	2	Leire Bengoetxea	*Revisión total. Quitamos los perfiles EPSOS, Sede Medio.
28/3/2019	2.1	Leire Bengoetxea	*Se añade certificado Dispositivo
17/5/2019	2.2	Leire Bengoetxea	*Se elimina campo C y OU del campo Subject del perfil DV
18/6/2019	2.3	Leire Bengoetxea	*Se corrige perfil SSL Cualificado
19/6/2019	2.4	Leire Bengoetxea	*Se actualiza el perfil de Sede EV

Estructura del documento

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 KeyOne® CA

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.

Ciudadano

CA emisora `CCEER`

Nombre en KeyOne® CA `ciudadano_qc_scard`

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		
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)
subjectPublicKeyInfo		RSA 2048 bits mínimo
extensions		
issuerAltName		Igual a la extensión subjectAltName del certificado de la CA emisora
subjectAltName		
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
1.3.6.1.4.1.14777.0.7	Opcional	Email del suscriptor
extendedKeyUsage		clientAuth, documentSigning
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.2.18.1
cpsURI		http://www.izenpe.eus/cps
userNotice		Kontsulta www.izenpe.eus-en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en www.izenpe.eus los términos y condiciones antes de utilizar o confiar en el certificado
policyIdentifier		0.4.0.194112.1.2 (QCP-n-qscd)
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crl2
authorityInfoAccess		
ocsp		http://ocsp.izenpe.com
CA emisora		http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crt
subjectDirectoryAttributes		
dateOfBirth		Fecha de nacimiento
qcStatements		
QcCompliance		Presente
QcType		id-etsi-qct-esign
QcSSCD		Presente
QcRetentiodPeriod		15 años
QcPDS		https://www.izenpe.eus/pds/en/ EN https://www.izenpe.eus/pds/eu/ EU https://www.izenpe.eus/pds/es/ ES
keyUsage	Crítica	digitalSignature, nonRepudiation, keyEncipherment

Ciudadano

CA emisora `CCEER`

Nombre en KeyOne® CA `ciudadano_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		4 años
subject		
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)
subjectPublicKeyInfo		RSA 2048 bits mínimo
extensions		
issuerAltName		Igual a la extensión subjectAltName del certificado de la CA emisora
subjectAltName		
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
1.3.6.1.4.1.14777.0.7	Opcional	Email del suscriptor
extendedKeyUsage		clientAuth, documentSigning
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.2.18.3
cpsURI		http://www.izenpe.eus/cps
userNotice		Kontsulta www.izenpe.eus-en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en www.izenpe.eus los términos y condiciones antes de utilizar o confiar en el certificado
policyIdentifier		0.4.0.194112.1.0 (QCP-n)
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crl2
authorityInfoAccess		
ocsp		http://ocsp.izenpe.com
CA emisora		http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crt
subjectDirectoryAttributes		
dateOfBirth		Fecha de nacimiento
qcStatements		
QcCompliance		Presente
QcType		id-etsi-qct-esign
QcRetentiodPeriod		15 años
QcPDS		https://www.izenpe.eus/pds/en/ EN https://www.izenpe.eus/pds/eu/ EU https://www.izenpe.eus/pds/es/ ES
keyUsage	Crítica	digitalSignature, nonRepudiation, keyEncipherment

Ciudadano No Reconocido

CA emisora `CCEENR`

Nombre en KeyOne® CA `ciudadano_nqc`

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		
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
subjectPublicKeyInfo		RSA 2048 bits mínimo
extensions		
issuerAltName		Igual a la extensión subjectAltName del certificado de la CA emisora
extendedKeyUsage		clientAuth
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.5.2.5 (1.3.6.1.4.1.14777.105.2.5 en Desarrollo)
cpsURI		http://www.izenpe.com/cps
userNotice		Kontsulta www.izenpe.com-en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en www.izenpe.com los términos y condiciones antes de utilizar o confiar en el certificado
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crlscinr2
authorityInfoAccess		ocsp http://ocsp.izenpe.com
subjectDirectoryAttributes		
dateOfBirth		Fecha de nacimiento
keyUsage	Crítica	digitalSignature, nonRepudiation, keyEncipherment

Ciudadano

CA emisora `CCEER`

Nombre en KeyOne® CA `ciudadano_dpc_20`

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		
serialNumber		DNI / NIE
SN		Primer Apellido
G		Nombre
CN		Nombre y Apellidos
dnQualifier		Depende del tipo de documento. En la ONA: DNI: "`-dni [DNI] -TIS [TIS]`" NIE: "`-nie [NIE] -TIS [TIS]`" En la tarjeta verde: "`-dni [DNI]`"
OU		Condiciones de uso en www.izenpe.com nola erabili jakiteko
OU		Herritar ziurtagiria - Certificado de ciudadano
OU		Ziurtagiri onartua - Certificado reconocido
C		ES
subjectPublicKeyInfo		RSA 2048 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		1.3.6.1.4.1.14777.2.6 (1.3.6.1.4.1.14777.102.6 en Desarrollo)
cpsURI		http://www.izenpe.com/rpaciudadano
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
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crl2
authorityInfoAccess		ocsp http://ocsp.izenpe.com
subjectDirectoryAttributes		
dateOfBirth		Fecha de nacimiento
qcStatements		
QcCompliance		Presente
QcSSCD		Presente
QcRetentiodPeriod		15 años
QcPDS		https://www.izenpe.com/pds/en/ EN https://www.izenpe.com/pds/eu/ EU https://www.izenpe.com/pds/es/ ES
keyUsage	Crítica	digitalSignature, nonRepudiation, keyEncipherment

Profesional

CA emisora CCEER

Nombre en KeyOne® CA profesional_qc_scard

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		
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		RSA 2048 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, smartCardLogon
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.2.19.1
cpsURI		http://www.izenpe.eus/cps
userNotice		Kontsulta www.izenpe.eus-en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en www.izenpe.eus los términos y condiciones antes de utilizar o confiar en el certificado
policyIdentifier		0.4.0.194112.1.2 (QCP-n-qscd)
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crl2
authorityInfoAccess		
ocsp		http://ocsp.izenpe.com
CA emisora		http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crt
qcStatements		
QcCompliance		Presente
QcType		id-etsi-qct-esign
QcSSCD		Presente
QcRetentiodPeriod		15 años
QcPDS		https://www.izenpe.eus/pds/en/ EN https://www.izenpe.eus/pds/eu/ EU https://www.izenpe.eus/pds/es/ ES
qcStatement-2		0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)
keyUsage	Crítica	digitalSignature, nonRepudiation, keyEncipherment

Profesional

CA emisora `CCEER`

Nombre en KeyOne® CA `profesional_qc_sw`

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		
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		RSA 2048 bits mínimo
extensions		
issuerAltName		Igual a la extensión subjectAltName del certificado de la CA emisora
subjectAltName		
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
extendedKeyUsage		clientAuth, emailProtection
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.2.19.2
cpsURI		http://www.izenpe.eus/cps
userNotice		Kontsulta www.izenpe.eus-en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en www.izenpe.eus los términos y condiciones antes de utilizar o confiar en el certificado
policyIdentifier		0.4.0.194112.1.0 (QCP-n)
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crl2
authorityInfoAccess		
ocsp		http://ocsp.izenpe.com
CA emisora		http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crt
qcStatements		
QcCompliance		Presente
QcType		id-etsi-qct-esign
QcRetentiodPeriod		15 años
QcPDS		https://www.izenpe.eus/pds/en/ EN https://www.izenpe.eus/pds/eu/ EU https://www.izenpe.eus/pds/es/ ES
qcStatement-2		0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)
keyUsage	Crítica	digitalSignature, nonRepudiation, keyEncipherment

Profesional

CA emisora `CCEER`

Nombre en KeyOne® CA `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		4 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		RSA 2048 bits mínimo
extensions		
issuerAltName		Igual a la extensión subjectAltName del certificado de la CA emisora
subjectAltName		
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
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		http://www.izenpe.eus/cps
userNotice		Kontsulta www.izenpe.eus-en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en www.izenpe.eus los términos y condiciones antes de utilizar o confiar en el certificado
policyIdentifier		0.4.0.194112.1.0 (QCP-n)
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crl2
authorityInfoAccess		
ocsp		http://ocsp.izenpe.com
CA emisora		http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crt
qcStatements		
QcCompliance		Presente
QcType		id-etsi-qct-esign
QcRetentiodPeriod		15 años
QcPDS		https://www.izenpe.eus/pds/en/ EN https://www.izenpe.eus/pds/eu/ EU https://www.izenpe.eus/pds/es/ ES
qcStatement-2		0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)
keyUsage	Crítica	digitalSignature, nonRepudiation, keyEncipherment

Corporativo Privado Reconocido

CA emisora `CCEER`

Nombre en KeyOne® CA `corporativo_privado_reconocido`

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		
serialNumber		DNI / NIE
SN		Primer Apellido
G		Nombre
CN		Nombre y Apellidos
dnQualifier		Depende de tipo de documento. DNI: "`-dni [DNI] -cif [CIF]`" NIE: "`-nie [NIE] -cif [CIF]`"
OU		Condiciones de uso en www.izenpe.com nola erabili jakiteko
OU		Ziurtagiri korporatibo pribatua - Certificado corporativo privado
OU		Ziurtagiri onartua - Certificado reconocido
OU	Opcional	Cargo o Departamento
OU	Opcional	Grupo VPN
O		Organización
C		ES
subjectPublicKeyInfo		RSA 2048 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
extendedKeyUsage		clientAuth, emailProtection, smartCardLogon
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.2.2 (1.3.6.1.4.1.14777.102.2 en Desarrollo)
cpsURI		http://www.izenpe.com/cps
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
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crl2
authorityInfoAccess		ocsp http://ocsp.izenpe.com
qcStatements		
QcCompliance		Presente
QcSSCD		Presente
QcRetentiodPeriod		15 años
QcPDS		https://www.izenpe.com/pds/en/ EN https://www.izenpe.com/pds/eu/ EU https://www.izenpe.com/pds/es/ ES
keyUsage	Crítica	digitalSignature, nonRepudiation, keyEncipherment

Corporativo Privado

CA emisora `CCEENR`

Nombre en KeyOne® CA `corporativo_privado`

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		
serialNumber		DNI / NIE
SN		Primer Apellido
G		Nombre
CN		Nombre y Apellidos
dnQualifier		Depende de tipo de documento. DNI: "`-dni [DNI]`" NIE: "`-nie [NIE]`"
OU		Condiciones de uso en www.izenpe.com nola erabili jakiteko
OU		Ziurtagiri korporatibo pribatua - Certificado corporativo privado
OU	Opcional	Cargo o Departamento
OU	Opcional	Grupo VPN
O		Organización
subjectPublicKeyInfo		RSA 2048 bits mínimo
extensions		
issuerAltName		Igual a la extensión subjectAltName del certificado de la CA emisora
subjectAltName		
rfc822Name		Email del usuario
OtherName: UserPrincipalName	Opcional	Nombre principal de usuario
extendedKeyUsage		clientAuth, emailProtection, smartCardLogon
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.5.2.2 (1.3.6.1.4.1.14777.105.2.2 en Desarrollo)
cpsURI		http://www.izenpe.com/cps
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
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crlscinr2
authorityInfoAccess		ocsp http://ocsp.izenpe.com
keyUsage	Crítica	digitalSignature, nonRepudiation, keyEncipherment

Corporativo Reconocido

CA emisora `AAPPR`

Nombre en KeyOne® CA `corporativo_reconocido`

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		
serialNumber		DNI / NIE
SN		Primer Apellido
G		Nombre
CN		Nombre y Apellidos
dnQualifier		Depende de tipo de documento. DNI: "`-dni [DNI] -TIS [TIS] -cif [CIF]`" 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
subjectPublicKeyInfo		RSA 2048 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
extendedKeyUsage		clientAuth, emailProtection, smartCardLogon
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.4.2 (1.3.6.1.4.1.14777.104.2 en Desarrollo)
cpsURI		http://www.izenpe.com/rpascacorrec
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
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crlscar2
authorityInfoAccess		ocsp http://ocsp.izenpe.com
qcStatements		
QcCompliance		Presente
QcSSCD		Presente
QcRetentiodPeriod		15 años
QcPDS		https://www.izenpe.com/pds/en/ EN https://www.izenpe.com/pds/eu/ EU https://www.izenpe.com/pds/es/ ES
keyUsage	Crítica	digitalSignature, nonRepudiation, keyEncipherment

Corporativo

CA emisora `AAPPNR`

Nombre en KeyOne® CA `corporativo`

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		
serialNumber		DNI / NIE
SN		Primer Apellido
G		Nombre
CN		Nombre y Apellidos
dnQualifier		Depende de tipo de documento. DNI: "`-dni [DNI]`" NIE: "`-nie [NIE]`"
OU		Condiciones de uso en www.izenpe.com nola erabili jakiteko
OU		Ziurtagiri korporatiboa Certificado corporativo
OU	Opcional	Cargo o Departamento
OU	Opcional	Grupo VPN
O		Organización
subjectPublicKeyInfo		RSA 2048 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
extendedKeyUsage		clientAuth, emailProtection, smartCardLogon
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.1.1.1 (1.3.6.1.4.1.14777.101.1.1 en Desarrollo)
cpsURI		http://www.izenpe.com/cps
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
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crlinterna2
authorityInfoAccess		ocsp http://ocsp.izenpe.com
keyUsage	Crítica	digitalSignature, nonRepudiation, keyEncipherment

Corporativo Reconocido en Hardware

CA emisora `AAPPR`

Nombre en KeyOne® CA `corporativo_reconocido_hardware`

Campo / extensión	Opcional / Crítica	Contenido
version		Versión 3
serialNumber		Número secuencial único
signature		sha256WithRsaSignature
issuer		Igual al campo subject del certificado de la CA emisora
validity		4 años
subject		
serialNumber		DNI / NIE
SN		Apellidos
G		Nombre
CN		Nombre y Apellidos
dnQualifier		Depende de tipo de documento. DNI: "`-dni [DNI] -cif [CIF]`" NIE: "`-nie [NIE] -cif [CIF]`"
OU		Condiciones de uso en www.izenpe.com 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
subjectPublicKeyInfo		RSA 2048 bits mínimo
extensions		
issuerAltName		Igual a la extensión subjectAltName del certificado de la CA emisora
subjectAltName		
rfc822Name		Email del suscriptor
extendedKeyUsage		clientAuth, emailProtection
netscapeCertType		SSL_Client, SMIME_Client
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.4.6 (1.3.6.1.4.1.14777.104.6 en Desarrollo)
cpsURI		http://www.izenpe.com/cps
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
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crlscar2
authorityInfoAccess		ocsp http://ocsp.izenpe.com
qcStatements		
QcCompliance		Presente
QcSSCD		Presente
keyUsage	Crítica	digitalSignature, keyEncipherment, dataEncipherment

Personal de Entidades Públicas

CA emisora `AAPPR`

Nombre en KeyOne® CA `pep_qc_scard`

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		
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**
subjectPublicKeyInfo		RSA 2048 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		
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
2.16.724.1.3.5.7.2.9	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
extendedKeyUsage		clientAuth, emailProtection, smartCardLogon
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.4.14.1
cpsURI		http://www.izenpe.eus/cps
userNotice		Kontsulta www.izenpe.eus-en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en www.izenpe.eus 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)
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crlscar2
authorityInfoAccess		
ocsp		http://ocsp.izenpe.com
CA emisora		http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR_cert_sha256.crt
qcStatements		
QcCompliance		Presente
QcType		id-etsi-qct-esign
QcRetentiodPeriod		15 años
QcPDS		https://www.izenpe.eus/pds/en/ EN https://www.izenpe.eus/pds/eu/ EU https://www.izenpe.eus/pds/es/ ES
qcStatement-2		0.4.0.194121.1.1 (id-etsi-qcs-SemanticsId-Natural)
keyUsage	Crítica	digitalSignature, nonRepudiation, keyEncipherment

Personal de Entidades Públicas

CA emisora `AAPPR`

Nombre en KeyOne® CA `pep_qc_sw`

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		
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**
subjectPublicKeyInfo		RSA 2048 bits mínimo
extensions		
issuerAltName		Igual a la extensión subjectAltName del certificado de la CA emisora
subjectAltName		
rfc822Name		Email del suscriptor
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
2.16.724.1.3.5.7.2.9	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
extendedKeyUsage		clientAuth, emailProtection
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.4.14.2
cpsURI		http://www.izenpe.eus/cps
userNotice		Kontsulta www.izenpe.eus-en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en www.izenpe.eus 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)
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crlscar2
authorityInfoAccess		
ocsp		http://ocsp.izenpe.com
CA emisora		http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR_cert_sha256.crt
qcStatements		
QcCompliance		Presente
QcType		id-etsi-qct-esign
QcRetentiodPeriod		15 años
QcPDS		https://www.izenpe.eus/pds/en/ EN https://www.izenpe.eus/pds/eu/ EU https://www.izenpe.eus/pds/es/ ES
qcStatement-2		0.4.0.194121.1.1 (id-etsi-qcs-SemanticsId-Natural)
keyUsage	Crítica	digitalSignature, nonRepudiation, keyEncipherment

Personal de Entidades Públicas

CA emisora `AAPPR`

Nombre en KeyOne® CA `pep_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		4 años
subject		
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**
subjectPublicKeyInfo		RSA 2048 bits mínimo
extensions		
issuerAltName		Igual a la extensión subjectAltName del certificado de la CA emisora
subjectAltName		
rfc822Name		Email del suscriptor
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
2.16.724.1.3.5.7.2.9	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
extendedKeyUsage		clientAuth, emailProtection
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.4.14.3
cpsURI		http://www.izenpe.eus/cps
userNotice		Kontsulta www.izenpe.eus-en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en www.izenpe.eus 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)
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crlscar2
authorityInfoAccess		
ocsp		http://ocsp.izenpe.com
CA emisora		http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR_cert_sha256.crt
qcStatements		
QcCompliance		Presente
QcType		id-etsi-qct-esign
QcRetentiodPeriod		15 años
QcPDS		https://www.izenpe.eus/pds/en/ EN https://www.izenpe.eus/pds/eu/ EU https://www.izenpe.eus/pds/es/ ES
qcStatement-2		0.4.0.194121.1.1 (id-etsi-qcs-SemanticsId-Natural)
keyUsage	Crítica	digitalSignature, nonRepudiation, keyEncipherment

Personal de Entidades Públicas

CA emisora `AAPPR`

Nombre en KeyOne® CA `pers_entidades_publicas`

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		
serialNumber		DNI / NIE
SN		Primer Apellido
G		Nombre
CN		Nombre y Apellidos
dnQualifier		Depende de tipo de documento. DNI: "`-dni [DNI] -TIS [TIS] -cif [CIF]`" 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
subjectPublicKeyInfo		RSA 2048 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
extendedKeyUsage		clientAuth, emailProtection, smartCardLogon
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.4.1 (1.3.6.1.4.1.14777.104.1 en Desarrollo)
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
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crlscar2
authorityInfoAccess		ocsp http://ocsp.izenpe.com
qcStatements		
QcCompliance		Presente
QcSSCD		Presente
QcRetentiodPeriod		15 años
QcPDS		https://www.izenpe.com/pds/en/ EN https://www.izenpe.com/pds/eu/ EU https://www.izenpe.com/pds/es/ ES
keyUsage	Crítica	digitalSignature, nonRepudiation, keyEncipherment

Personal de Entidades Públicas con Seudónimo (FIRMA)

CA emisora `AAPPR`

Nombre en KeyOne® CA `pep_seudonimo_scard_sign`

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>* **(FIRMA)** o **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**
subjectPublicKeyInfo		RSA 2048 bits mínimo
extensions		
issuerAltName		Igual a la extensión subjectAltName del certificado de la CA emisora
subjectAltName		
rfc822Name	Opcional	Email del suscriptor
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
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.4.13.1.1
cpsURI		http://www.izenpe.eus/cps
userNotice		Kontsulta www.izenpe.eus-en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en www.izenpe.eus los términos y condiciones antes de utilizar o confiar en el certificado
policyIdentifier		OID MINHAP: **2.16.724.1.3.5.4.1**
policyIdentifier		OID QCP-n-qscd: **0.4.0.194112.1.2**
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crlscar2
authorityInfoAccess		
ocsp		http://ocsp.izenpe.com
CA emisora		http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR_cert_sha256.crt
qcStatements		
QcCompliance		Presente
QcSSCD		Presente
QcType		id-etsi-qct-esign
QcEuRetentiodPeriod		15 años
QcPDS		https://www.izenpe.eus/pds/en/ EN https://www.izenpe.eus/pds/eu/ EU https://www.izenpe.eus/pds/es/ ES
keyUsage	Crítica	contentCommitment (no repudio)

Personal de Entidades Públicas con Seudónimo (AUTENTICACION)

CA emisora `AAPPR`

Nombre en KeyOne® CA `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)** o **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 2048 bits mínimo
extensions		
issuerAltName		Igual a la extensión subjectAltName del certificado de la CA emisora
subjectAltName		
rfc822Name	Opcional	Email del suscriptor
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, emailProtection
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		http://www.izenpe.eus/cps
userNotice		Kontsulta www.izenpe.eus-en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en www.izenpe.eus los términos y condiciones antes de utilizar o confiar en el certificado
policyIdentifier		OID MINHAP: **2.16.724.1.3.5.4.1**
policyIdentifier		OID NCP+: **0.4.0.2042.1.2**
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crlscar2
authorityInfoAccess		
ocsp		http://ocsp.izenpe.com
CA emisora		http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR_cert_sha256.crt
keyUsage	Crítica	digitalSignature

Personal de Entidades Públicas con Seudónimo (CIFRADO)

CA emisora `AAPPR`

Nombre en KeyOne® CA `pep_seudonimo_scard_cipher`

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>* **(FIRMA)** o **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**
subjectPublicKeyInfo		RSA 2048 bits mínimo
extensions		
issuerAltName		Igual a la extensión subjectAltName del certificado de la CA emisora
subjectAltName		
rfc822Name	Opcional	Email del suscriptor
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
extendedKeyUsage		clientAuth, emailProtection
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.4.13.1.3
cpsURI		http://www.izenpe.eus/cps
userNotice		Kontsulta www.izenpe.eus-en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en www.izenpe.eus los términos y condiciones antes de utilizar o confiar en el certificado
policyIdentifier		OID MINHAP: **2.16.724.1.3.5.4.1**
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crlscar2
authorityInfoAccess		
ocsp		http://ocsp.izenpe.com
CA emisora		http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR_cert_sha256.crt
keyUsage	Crítica	keyEncipherment, dataEncipherment

Representante Tarjeta

CA emisora `CCEER`

Nombre en KeyOne® CA `representante`

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		Ordezkari 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
subjectPublicKeyInfo		RSA 2048 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		1.3.6.1.4.1.14777.2.12 (1.3.6.1.4.1.14777.102.12 en Desarrollo)
cpsURI		http://www.izenpe.com/cps
userNotice		Kontsulta www.izenpe.com-en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en www.izenpe.com los términos y condiciones antes de utilizar o confiar en el certificado
policyIdentifier		0.4.0.194112.1.2 (OID ETSI QCP-n-qscd)
policyIdentifier		2.16.724.1.3.5.8 (OID PJ MPR)
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crl2
authorityInfoAccess		
ocsp		http://ocsp.izenpe.com
CA emisora		http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crt
qcStatements		
QcCompliance		Presente
QcType		id-etsi-qct-esign
QcSSCD		Presente
QcRetentiodPeriod		15 años
QcPDS		https://www.izenpe.com/pds/en/ EN https://www.izenpe.com/pds/eu/ EU https://www.izenpe.com/pds/es/ ES
qcStatement-2		0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)
keyUsage	Crítica	digitalSignature, nonRepudiation, keyEncipherment

Representante HSM

CA emisora `CCEER`

Nombre en KeyOne® CA `representante_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		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		Ordezkari 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
subjectPublicKeyInfo		RSA 2048 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		1.3.6.1.4.1.14777.2.14
cpsURI		http://www.izenpe.com/cps
userNotice		Kontsulta www.izenpe.com-en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en www.izenpe.com 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)
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crl2
authorityInfoAccess		
ocsp		http://ocsp.izenpe.com
CA emisora		http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crt
qcStatements		
QcCompliance		Presente
QcType		id-etsi-qct-esign
QcRetentiodPeriod		15 años
QcPDS		https://www.izenpe.com/pds/en/ EN https://www.izenpe.com/pds/eu/ EU https://www.izenpe.com/pds/es/ ES
qcStatement-2		0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)
keyUsage	Crítica	digitalSignature, nonRepudiation, keyEncipherment

Representante Software

CA emisora `CCEER`

Nombre en KeyOne® CA `representante_sw`

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		Ordezkari 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
subjectPublicKeyInfo		RSA 2048 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		1.3.6.1.4.1.14777.2.16 (1.3.6.1.4.1.14777.102.16 en Desarrollo)
cpsURI		http://www.izenpe.com/cps
userNotice		Kontsulta www.izenpe.com-en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en www.izenpe.com 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)
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crl2
authorityInfoAccess		
ocsp		http://ocsp.izenpe.com
CA emisora		http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crt
qcStatements		
QcCompliance		Presente
QcType		id-etsi-qct-esign
QcRetentiodPeriod		15 años
QcPDS		https://www.izenpe.com/pds/en/ EN https://www.izenpe.com/pds/eu/ EU https://www.izenpe.com/pds/es/ ES
qcStatement-2		0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)
keyUsage	Crítica	digitalSignature, nonRepudiation, keyEncipherment

Representante SPJ Tarjeta

CA emisora `CCEER`

Nombre en KeyOne® CA `representante_spj`

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 Ordezkari 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
subjectPublicKeyInfo		RSA 2048 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 (1.3.6.1.4.1.14777.102.13 en Desarrollo)
cpsURI		http://www.izenpe.com/cps
userNotice		Kontsulta www.izenpe.com-en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en www.izenpe.com los términos y condiciones antes de utilizar o confiar en el certificado
policyIdentifier		0.4.0.194112.1.2 (OID ETSI QCP-n-qscd)
policyIdentifier		2.16.724.1.3.5.9 (OID PJ MPR)
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crl2
authorityInfoAccess		
ocsp		http://ocsp.izenpe.com
CA emisora		http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crt
qcStatements		
QcCompliance		Presente
QcType		id-etsi-qct-esign
QcSSCD		Presente
QcRetentiodPeriod		15 años
QcPDS		https://www.izenpe.com/pds/en/ EN https://www.izenpe.com/pds/eu/ EU https://www.izenpe.com/pds/es/ 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 en KeyOne® CA `representante_spj_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		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 Ordezkari 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
subjectPublicKeyInfo		RSA 2048 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		1.3.6.1.4.1.14777.2.15
cpsURI		http://www.izenpe.com/cps
userNotice		Kontsulta www.izenpe.com-en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en www.izenpe.com 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)
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crl2
authorityInfoAccess		
ocsp		http://ocsp.izenpe.com
CA emisora		http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crt
qcStatements		
QcCompliance		Presente
QcType		id-etsi-qct-esign
QcRetentiodPeriod		15 años
QcPDS		https://www.izenpe.com/pds/en/ EN https://www.izenpe.com/pds/eu/ EU https://www.izenpe.com/pds/es/ ES
qcStatement-2		0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)
keyUsage	Crítica	digitalSignature, nonRepudiation, keyEncipherment

Representante SPJ Software

CA emisora `CCEER`

Nombre en KeyOne® CA `representante_spj_sw`

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 Ordezkari 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
subjectPublicKeyInfo		RSA 2048 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		1.3.6.1.4.1.14777.2.17 (1.3.6.1.4.1.14777.102.17 en Desarrollo)
cpsURI		http://www.izenpe.com/cps
userNotice		Kontsulta www.izenpe.com-en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en www.izenpe.com 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)
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crl2
authorityInfoAccess		
ocsp		http://ocsp.izenpe.com
CA emisora		http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crt
qcStatements		
QcCompliance		Presente
QcType		id-etsi-qct-esign
QcRetentiodPeriod		15 años
QcPDS		https://www.izenpe.com/pds/en/ EN https://www.izenpe.com/pds/eu/ EU https://www.izenpe.com/pds/es/ ES
qcStatement-2		0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)
keyUsage	Crítica	digitalSignature, nonRepudiation, keyEncipherment

Entidad

CA emisora `CCEER`

Nombre en KeyOne® CA `entidad`

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		
1.3.6.1.4.1.18838.1.1		DNI / NIE
serialNumber		CIF
SN		Apellidos
G		Nombre
CN		Nombre de la Entidad
dnQualifier		"-cif [CIF]"
OU		Condiciones de uso en www.izenpe.com nola erabili jakiteko
OU		Entitatearen ziurtagiria - Certificado de entidad
OU		Ziurtagiri onartua - Certificado reconocido
O		Nombre de la Entidad
C		ES
subjectPublicKeyInfo		RSA 2048 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		1.3.6.1.4.1.14777.2.7 (1.3.6.1.4.1.14777.102.7 en Desarrollo)
cpsURI		http://www.izenpe.com/rpaentidad
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
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crl2
authorityInfoAccess		ocsp http://ocsp.izenpe.com
qcStatements		
QcCompliance		Presente
QcSSCD		Presente
QcRetentiodPeriod		15 años
QcPDS		https://www.izenpe.com/pds/en/ EN https://www.izenpe.com/pds/eu/ EU https://www.izenpe.com/pds/es/ ES
keyUsage	Crítica	digitalSignature, nonRepudiation, keyEncipherment

Entidad Sin Personalidad Juridica

CA emisora `CCEER`

Nombre en KeyOne® CA `entidad_spj`

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		
1.3.6.1.4.1.18838.1.1		DNI / NIE
serialNumber		CIF
SN		Apellidos
G		Nombre
CN		Nombre de la Entidad
dnQualifier		"-cif [CIF]"
OU		Condiciones de uso en www.izenpe.com nola erabili jakiteko
OU		Nortasun jur gabeko entitatearen ziurt-Cert entidad sin pers jur
OU		Ziurtagiri onartua - Certificado reconocido
O		Nombre de la Entidad
C		ES
subjectPublicKeyInfo		RSA 2048 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		1.3.6.1.4.1.14777.2.9 (1.3.6.1.4.1.14777.102.9 en Desarrollo)
cpsURI		http://www.izenpe.com/cps
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
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crl2
authorityInfoAccess		ocsp http://ocsp.izenpe.com
qcStatements		
QcCompliance		Presente
QcSSCD		Presente
QcRetentiodPeriod		15 años
QcPDS		https://www.izenpe.com/pds/en/ EN https://www.izenpe.com/pds/eu/ EU https://www.izenpe.com/pds/es/ ES
keyUsage	Crítica	digitalSignature, nonRepudiation, keyEncipherment

Entidad Servidor

CA emisora `CCEER`

Nombre en KeyOne® CA `entidad_servidor`

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		
1.3.6.1.4.1.18838.1.1		DNI / NIE
serialNumber		CIF
SN		Apellidos
G		Nombre
CN		Nombre de la Entidad
dnQualifier		"-cif [CIF]"
OU		Condiciones de uso en www.izenpe.com nola erabili jakiteko
OU		Entitatearen ziurtagiria - Certificado de entidad
OU		Ziurtagiri onartua - Certificado reconocido
O		Nombre de la Entidad
C		ES
subjectPublicKeyInfo		RSA 2048 bits mínimo
extensions		
issuerAltName		Igual a la extensión subjectAltName del certificado de la CA emisora
extendedKeyUsage		clientAuth, emailProtection
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.2.8 (1.3.6.1.4.1.14777.102.8 en Desarrollo)
cpsURI		http://www.izenpe.com/rpaentidadser
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		0.4.0.1456.1.2
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crl2
authorityInfoAccess		ocsp http://ocsp.izenpe.com
qcStatements		
QcCompliance		Presente
QcRetentiodPeriod		15 años
QcPDS		https://www.izenpe.com/pds/en/ EN https://www.izenpe.com/pds/eu/ EU https://www.izenpe.com/pds/es/ ES
keyUsage	Crítica	digitalSignature, nonRepudiation, keyEncipherment

Sello Entidad

CA emisora `CCEER`

Nombre en KeyOne® CA `sello_juridico`

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	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
OU		zigilu elektronikoa - sello electronico
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
subjectPublicKeyInfo		RSA 2048 bits mínimo
extensions		
issuerAltName		Igual a la extensión subjectAltName del certificado de la CA emisora
extendedKeyUsage		clientAuth, emailProtection
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.2.11 (1.3.6.1.4.1.14777.102.11 en Desarrollo)
cpsURI		http://www.izenpe.eus/cps
userNotice		Kontsulta www.izenpe.eus-en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en www.izenpe.eus los términos y condiciones antes de utilizar o confiar en el certificado
policyIdentifier		0.4.0.194112.1.1 (OID ETSI QCP-l)
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crl2
authorityInfoAccess		
ocsp		http://ocsp.izenpe.com
CA emisora		http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crt
qcStatements		
QcCompliance		Presente
QcType		id-etsi-qct-eseal
QcRetentiodPeriod		15 años
QcPDS		https://www.izenpe.eus/pds/en/ EN https://www.izenpe.eus/pds/eu/ EU https://www.izenpe.eus/pds/es/ 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)
keyUsage	Crítica	digitalSignature, nonRepudiation, keyEncipherment

Sello Entidad HSM

CA emisora `CCEER`

Nombre en KeyOne® CA `sello_juridico_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	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
OU		zigilu elektronikoa - sello electronico
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
subjectPublicKeyInfo		RSA 2048 bits mínimo
extensions		
issuerAltName		Igual a la extensión subjectAltName del certificado de la CA emisora
extendedKeyUsage		clientAuth, emailProtection
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.2.20
cpsURI		http://www.izenpe.eus/cps
userNotice		Kontsulta www.izenpe.eus-en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en www.izenpe.eus los términos y condiciones antes de utilizar o confiar en el certificado
policyIdentifier		0.4.0.194112.1.1 (OID ETSI QCP-l)
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crl2
authorityInfoAccess		
ocsp		http://ocsp.izenpe.com
CA emisora		http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/CCEER_cert_sha256.crt
qcStatements		
QcCompliance		Presente
QcType		id-etsi-qct-eseal
QcRetentiodPeriod		15 años
QcPDS		https://www.izenpe.eus/pds/en/ EN https://www.izenpe.eus/pds/eu/ EU https://www.izenpe.eus/pds/es/ 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)
keyUsage	Crítica	digitalSignature, nonRepudiation, keyEncipherment

Entidad Euskal Etxeak

CA emisora `CCEENR`

Nombre en KeyOne® CA `entidad_euskal_etxeak`

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		
1.3.6.1.4.1.14777.100.2		Número de Documento
1.3.6.1.4.1.14777.100.1		Tipo de Documento
serialNumber		Código de Centro
SN		Apellidos
G		Nombre
CN		Nombre del Centro
dnQualifier		"-cen [Código de Centro]"
OU		Condiciones de uso en www.izenpe.com nola erabili jakiteko
OU		Euskal Etxearen ziurtagiria - Certificado de Euskal Etxea
O		Nombre del Centro
C		ES
subjectPublicKeyInfo		RSA 1024 bits mínimo
extensions		
issuerAltName		Igual a la extensión subjectAltName del certificado de la CA emisora
extendedKeyUsage		clientAuth
netscapeCertType		SSL_Client
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.5.2.1 (1.3.6.1.4.1.14777.105.2.1 en Desarrollo)
cpsURI		http://www.izenpe.com/cps
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
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crlscinr2
authorityInfoAccess		ocsp http://ocsp.izenpe.com:8094
keyUsage	Crítica	digitalSignature, keyEncipherment

Aplicación

CA emisora `AAPPNR`

Nombre en KeyOne® CA `servidores_aplicacion`

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		
ST		Provincia
L		Localidad
EA		Correo electrónico
CN		Nombre de la aplicación
OU		Departamento
O		Nombre de la entidad
C		ES
subjectPublicKeyInfo		RSA 2048 bits mínimo
extensions		
issuerAltName		Igual a la extensión subjectAltName del certificado de la CA emisora
subjectAltName	Opcional	Igual a la extensión subjectAltName de la petición, si está presente
extendedKeyUsage		clientAuth, emailProtection
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.1.2.2 (1.3.6.1.4.1.14777.101.2.2 en Desarrollo)
cpsURI		http://www.izenpe.com/cps
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
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crlinterna2
authorityInfoAccess		ocsp http://ocsp.izenpe.com
keyUsage	Crítica	digitalSignature, nonRepudiation, keyEncipherment

Firma de Código

CA emisora `AAPPNR`

Nombre en KeyOne® CA `firma_codigo`

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		
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
subjectPublicKeyInfo		RSA 2048 bits mínimo
extensions		
issuerAltName		Igual a la extensión subjectAltName del certificado de la CA emisora
subjectAltName		Identificador permanente
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.1.3.1 (1.3.6.1.4.1.14777.101.3.1 en Desarrollo)
cpsURI		http://www.izenpe.com/cps
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		2.23.140.1.4.1
extendedKeyUsage		codeSigning
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crlinterna2
authorityInfoAccess		**ocsp** http://ocsp.izenpe.com **root** http://www.izenpe.com/s15-12020/es/contenidos/informacion/cas_izenpe/es_cas/adjuntos/RAIZ2007_cert_sha256.crt
keyUsage	Crítica	digitalSignature

Aplicación

CA emisora AAPPNR

Nombre en KeyOne® CA device

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		10 años (todavía no está claro)
subject		
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
subjectPublicKeyInfo		RSA 4096 bits mínimo
extensions		
issuerAltName		Igual a la extensión subjectAltName del certificado de la CA emisora
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.1.3.2 (1.3.6.1.4.1.14777.101.3.2 en Desarrollo)
cpsURI		http://www.izenpe.com/cps
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
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crlinterna2
authorityInfoAccess		
ocsp		http://ocsp.izenpe.com
CA emisora		http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPNR_cert_sha256.crt
keyUsage	Crítica	digitalSignature, keyEncipherment

Órgano Administrativo

CA emisora `AAPPR`

Nombre en KeyOne® CA `organo_administrativo`

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		
1.3.6.1.4.1.18838.1.1		DNI / NIE
EA		Dirección de correo electrónico
serialNumber		CIF
SN		Apellidos
G		Nombre
CN		Nombre del órgano administrativo
dnQualifier		"-cif [CIF]"
OU		Condiciones de uso en www.izenpe.com nola erabili jakiteko
OU		Administrazio-organo ziurtagiria Certificado de organo administrativo
OU		Ziurtagiri onartua - Certificado reconocido
		Departamento
O		Nombre de la Organización
L		Localidad
ST		Provincia
C		ES
subjectPublicKeyInfo		RSA 2048 bits mínimo
extensions		
issuerAltName		Igual a la extensión subjectAltName del certificado de la CA emisora
subjectAltName	Opcional	Igual a la extensión subjectAltName de la petición, si está presente
extendedKeyUsage		clientAuth, emailProtection
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.4.3 (1.3.6.1.4.1.14777.104.3 en Desarrollo)
cpsURI		http://www.izenpe.com/rpascaorgrec
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		0.4.0.1456.1.2
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crlscar2
authorityInfoAccess		ocsp http://ocsp.izenpe.com
qcStatements		
QcCompliance		Presente
QcRetentiodPeriod		15 años
QcPDS		https://www.izenpe.com/pds/en/ EN https://www.izenpe.com/pds/eu/ EU https://www.izenpe.com/pds/es/ ES
keyUsage	Crítica	digitalSignature, nonRepudiation, keyEncipherment

Servidor Web

CA emisora `AAPPNR`

Nombre en KeyOne® CA `ssl_dv`

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		1 o 2 años
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, emailProtection
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.1.2.4 (1.3.6.1.4.1.14777.101.2.4 en Desarrollo)
cpsURI		http://www.izenpe.com/cps
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		2.23.140.1.2.1
policyIdentifier		0.4.0.2042.1.6
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crlinterna2
authorityInfoAccess		
ocsp		http://ocsp.izenpe.com
CA emisora		http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPNR_cert_sha256.crt
keyUsage	Critica	digitalSignature, keyEncipherment

Servidor Web

CA emisora `AAPPNR`

Nombre en KeyOne® CA `servidor_ssl_sha256 (OV)`

Campo / extensión	Opcional / Crítica	Contenido
version		Versión 3
serialNumber		Número secuencial único
signature		sha-256WithRSAEncryption
issuer		Igual al campo subject del certificado de la CA emisora
validity		1 o 2 años
subject		
CN		Dominio DNS
OU	Opcional	Departamento
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, emailProtection
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.1.2.1 (1.3.6.1.4.1.14777.101.2.1 en Desarrollo)
cpsURI		http://www.izenpe.com/cps
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		2.23.140.1.2.2
policyIdentifier		0.4.0.2042.1.7
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crlinterna2
authorityInfoAccess		
ocsp		http://ocsp.izenpe.com
CA emisora		http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPNR_cert_sha256.crt
keyUsage	Critica	digitalSignature, keyEncipherment

Sede nivel medio con EV

CA emisora `SSLEV`

Nombre en KeyOne® CA `sede_nivel_medio_ev`

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		1 o 2 años
subject		
CN		Dominio DNS o dirección IP
serialNumber		CIF
OU		Nombre de la sede
OU		"sede electrónica"
organizationIdentifier		3 caracteres tipo-identidad + Country + - + identificador. Por ejemplo, si usaramos el CIF sería algo como: VATES-A01337260
O		Entidad suscriptora
L		Localidad
ST		Provincia
C		ES
businessCategory		[OID.2.5.4.15] Valor fijo "Government Entity"
jurisdictionOfIncorporationLocalityName	Opcional	[OID: 1.3.6.1.4.1.311.60.2.1.1] Localidad en la que está registrada la empresa
jurisdictionOfIncorporationStateOrProvinceName	Opcional	[OID: 1.3.6.1.4.1.311.60.2.1.2] Provincia en la que está registrada la empresa
jurisdictionOfIncorporationCountryName		[OID: 1.3.6.1.4.1.311.60.2.1.3] Valor fijo "ES"
subjectPublicKeyInfo		RSA 2048 bits mínimo
extensions		
issuerAltName		Igual a la extensión subjectAltName del certificado de la CA emisora
subjectAltName		
rfc822Name		Email de contacto de la sede
dNSName		Dominio DNS o dirección IP
directoryName		
2.16.724.1.3.5.1.2.1		"sede electrónica"
2.16.724.1.3.5.1.2.2		Entidad suscriptora
2.16.724.1.3.5.1.2.3		CIF
2.16.724.1.3.5.1.2.4		Nombre de la sede
2.16.724.1.3.5.1.2.5		Dominio DNS o dirección IP
extendedKeyUsage		serverAuth
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.6.1.2 (1.3.6.1.4.1.14777.106.1.2 en Desarrollo)
cpsURI		http://www.izenpe.com/cps
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
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crlsslev2
authorityInfoAccess		ocsp http://ocsp.izenpe.com
keyUsage	Crítica	digitalSignature, keyEncipherment

Sede nivel medio con EV EIDAS

CA emisora `SSLEV`

Nombre en KeyOne® CA `sede_nivel_medio_ev_eidas`

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		1 o 2 años
subject		
CN	opcional	Dominio DNS
serialNumber		CIF
OU		Nombre descriptivo de la sede
OU		"**SEDE ELECTRONICA**"
organizationIdentifier		3 caracteres tipo-identidad + Country + **-** + identificador. Por ejemplo, si usaramos el CIF sería algo como: VATES-A01337260
O		Entidad suscriptora
L		Localidad
ST		Provincia
C		"**ES**"
businessCategory		[OID.2.5.4.15] "**Government Entity**"
jurisdictionOfIncorporationLocalityName	Opcional	[OID: 1.3.6.1.4.1.311.60.2.1.1] Localidad en la que está registrada la empresa
jurisdictionOfIncorporationStateOrProvinceName	Opcional	[OID: 1.3.6.1.4.1.311.60.2.1.2] Provincia en la que está registrada la empresa
jurisdictionOfIncorporationCountryName		[OID: 1.3.6.1.4.1.311.60.2.1.3] "**ES**"
subjectPublicKeyInfo		RSA 2048 bits mínimo
extensions		
issuerAltName	Opcional	Igual a la extensión subjectAltName del certificado de la CA emisora
subjectAltName		
dNSName		Dominio DNS
extendedKeyUsage		serverAuth
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.6.1.4 (1.3.6.1.4.1.14777.106.1.4 en Desarrollo)
cpsURI		http://www.izenpe.com/cps
userNotice		Kontsulta www.izenpe.com-en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en www.izenpe.com los términos y condiciones antes de utilizar o confiar en el certificado
policyIdentifier		2.16.724.1.3.5.5.2 (OID MINHAP)
policyIdentifier		0.4.0.194112.1.4 (ETSI QCP-w OID)
policyIdentifier		0.4.0.2042.1.4
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crlsslev2
authorityInfoAccess		
ocsp		http://ocsp.izenpe.com
CA emisora		http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/SSLEV_cert_signing_1_2018.crt
qcStatements		
QcCompliance		Presente
QcType		id-etsi-qct-web
QcRetentiodPeriod		15 años
QcPDS		https://www.izenpe.com/pds/en/ EN https://www.izenpe.com/pds/eu/ EU https://www.izenpe.com/pds/es/ ES
qcStatement-2		0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)
keyUsage	Crítica	digitalSignature, keyEncipherment

SSL EV - SHA2

CA emisora `SSLEV`

Nombre en KeyOne® CA `servidor_ssl_sha2`

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		1-2 años
subject		
CN		Dominio DNS
OU	Opcional	Departamento
O		Organización
street	Opcional	Calle
L		Localidad
ST		Provincia
C		País
postalCode	Opcional	Código postal
serialNumber		CIF
businessCategory		[OID.2.5.4.15] Valores posibles: - "Private Organization" para Organización privada - "Government Entity" para Entidad pública - "Business Entity" para Empresa - "Non-comercial Entity" para Entidad no comercial
jurisdictionOfIncorporationLocalityName	Opcional	[OID: 1.3.6.1.4.1.311.60.2.1.1] Localidad en la que está registrada la empresa
jurisdictionOfIncorporationStateOrProvinceName	Opcional	[OID: 1.3.6.1.4.1.311.60.2.1.2] Provincia en la que está registrada la empresa
jurisdictionOfIncorporationCountryName		[OID: 1.3.6.1.4.1.311.60.2.1.3] País en el que está registrada la empresa
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
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.6.1.1 (1.3.6.1.4.1.14777.106.1.1 en Desarrollo)
cpsURI		http://www.izenpe.com/cps
policyIdentifier		0.4.0.2042.1.4
authorityInfoAccess		
ocsp		http://ocsp.izenpe.com
CA emisora		http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/SSLEV_cert_sha256.cr http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/SSLEV_cert_signing_1_2018.crt
cRLDistributionPoints		
keyUsage	Crítica	http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/SSLEV_cert_signing_1_2018.crt

SSL Cualificada

CA emisora `SSLEV`

Nombre en KeyOne® CA `ssl_qualified`

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		1-2 años
subject		
CN	Opcional	Dominio DNS
OU	Opcional	Departamento
O		Organización
street	Opcional	Calle
L		Localidad
ST		Provincia
C		País
postalCode	Opcional	Código postal
serialNumber		CIF
businessCategory		[OID.2.5.4.15] Valores posibles: - "Private Organization" para Organización privada - "Government Entity" para Entidad pública - "Business Entity" para Empresa - "Non-comercial Entity" para Entidad no comercial
jurisdictionOfIncorporationLocalityName	Opcional	[OID: 1.3.6.1.4.1.311.60.2.1.1] Localidad en la que está registrada la empresa
jurisdictionOfIncorporationStateOrProvinceName	Opcional	[OID: 1.3.6.1.4.1.311.60.2.1.2] Provincia en la que está registrada la empresa
jurisdictionOfIncorporationCountryName		[OID: 1.3.6.1.4.1.311.60.2.1.3] País en el que está registrada la empresa
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,emailProtection
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.6.1.3 (1.3.6.1.4.1.14777.106.1.3 en Desarrollo)
cpsURI		http://www.izenpe.com/cps
policyIdentifier		0.4.0.194112.1.4 (ETSI QCP-w OID)
policyIdentifier		0.4.0.2042.1.4
authorityInfoAccess		
OCSP		http://ocsp.izenpe.com
CA emisora		http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/SSLEV_cert_signing_1_2018.crt
qcStatements		
QcCompliance		Presente
QcType		id-etsi-qct-web
QcRetentiodPeriod		15 años
QcPDS		https://www.izenpe.com/pds/en/ EN https://www.izenpe.com/pds/eu/ EU https://www.izenpe.com/pds/es/ ES
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crlsslev2
keyUsage	Crítica	digitalSignature, keyEncipherment

Sello nivel medio

CA emisora `AAPPR`

Nombre en KeyOne® CA `sello_nivel_medio`

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		
CN		Nombre de órgano administrativo, sistema o aplicación
G	Opcional	Nombre
SN	Opcional	[APELLIDO1] [APELLIDO2] - DNI [DNI/NIE]
serialNumber		CIF
OU		"sello electrónico"
OU		ZIURTAGIRI ONARTUA - CERTIFICADO RECONOCIDO
O		Nombre oficial de la organización
C		ES
subjectPublicKeyInfo		RSA 2048 bits mínimo
extensions		
issuerAltName		Igual a la extensión subjectAltName del certificado de la CA emisora
subjectAltName		
rfc822Name		Email de contacto de la organización
directoryName		
2.16.724.1.3.5.2.2.1		"sello electrónico"
2.16.724.1.3.5.2.2.2		Nombre oficial de la organización
2.16.724.1.3.5.2.2.3		CIF
2.16.724.1.3.5.2.2.4	Opcional	DNI/NIE
2.16.724.1.3.5.2.2.5		Nombre de órgano administrativo, sistema o aplicación
2.16.724.1.3.5.2.2.6	Opcional	Nombre
2.16.724.1.3.5.2.2.7	Opcional	Primer Apellido
2.16.724.1.3.5.2.2.8	Opcional	Segundo Apellido
2.16.724.1.3.5.2.2.9	Opcional	Email del responsable
extendedKeyUsage		clientAuth, emailProtection
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.4.4 (1.3.6.1.4.1.14777.104.4 en Desarrollo)
cpsURI		http://www.izenpe.com/cps
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		0.4.0.1456.1.2
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crlscar2
authorityInfoAccess		ocsp http://ocsp.izenpe.com
qcStatements		
QcCompliance		Presente
QcRetentionPeriod		15 años
QcPDS		https://www.izenpe.com/pds/en/ EN https://www.izenpe.com/pds/eu/ EU https://www.izenpe.com/pds/es/ ES
keyUsage	Crítica	digitalSignature, nonRepudiation (<>contentCommitment), keyEncipherment, dataEncipherment

Sello nivel alto

CA emisora `AAPPR`

Nombre en KeyOne® CA `sello_nivel_alto`

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		
CN		Nombre de órgano administrativo, sistema o aplicación
G	Opcional	Nombre
SN	Opcional	`[APELLIDO1] [APELLIDO2] - DNI [DNI/NIE]`
serialNumber		CIF
OU		"sello electrónico"
OU		ZIURTAGIRI ONARTUA - CERTIFICADO RECONOCIDO
O		Nombre oficial de la organización
C		ES
subjectPublicKeyInfo		RSA 2048 bits mínimo
extensions		
issuerAltName		Igual a la extensión subjectAltName del certificado de la CA emisora
subjectAltName		
rfc822Name		Email de contacto de la organización
directoryName		
2.16.724.1.3.5.2.1.1		"sello electrónico"
2.16.724.1.3.5.2.1.2		Nombre oficial de la organización
2.16.724.1.3.5.2.1.3		CIF
2.16.724.1.3.5.2.1.4	Opcional	DNI/NIE
2.16.724.1.3.5.2.1.5		Nombre de órgano administrativo, sistema o aplicación
2.16.724.1.3.5.2.1.6	Opcional	Nombre
2.16.724.1.3.5.2.1.7	Opcional	Primer Apellido
2.16.724.1.3.5.2.1.8	Opcional	Segundo Apellido
2.16.724.1.3.5.2.1.9	Opcional	Email del responsable
extendedKeyUsage		clientAuth, emailProtection
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.4.5 (1.3.6.1.4.1.14777.104.5 en Desarrollo)
cpsURI		http://www.izenpe.com/cps
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
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crlscar2
authorityInfoAccess		ocsp http://ocsp.izenpe.com
qcStatements		
QcCompliance		Presente
QcRetentionPeriod		15 años
QcSSCD		Presente
QcPDS		https://www.izenpe.com/pds/en/ EN https://www.izenpe.com/pds/eu/ EU https://www.izenpe.com/pds/es/ ES
keyUsage	Crítica	digitalSignature, nonRepudiation (<>contentCommitment), keyEncipherment, dataEncipherment

Sello nivel medio EIDAS

CA emisora `AAPPR`

Nombre en KeyOne® CA `sello_nivel_medio_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		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 usaramos el NIF sería algo como: VATES-A01337260
OU		**"SELLO ELECTRONICO"**
O		Nombre oficial de la organización
C		**ES**
subjectPublicKeyInfo		RSA 2048 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		
2.16.724.1.3.5.6.2.1		**"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	Opcional	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
extendedKeyUsage		clientAuth, emailProtection
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.4.11.2
cpsURI		http://www.izenpe.eus/cps
userNotice		Kontsulta www.izenpe.eus-en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en www.izenpe.eus 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-l)
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crlscar2
authorityInfoAccess		
ocsp		http://ocsp.izenpe.com
CA emisora		http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR_cert_sha256.crt
qcStatements		
QcCompliance		Presente
QcType		id-etsi-qct-eseal
QcRetentionPeriod		15 años
QcPDS		https://www.izenpe.eus/pds/en/ EN https://www.izenpe.eus/pds/eu/ EU https://www.izenpe.eus/pds/es/ ES
qcStatement-2		0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)
keyUsage	Crítica	digitalSignature, nonRepudiation (<>contentCommitment), keyEncipherment, dataEncipherment

Sello nivel medio EIDAS

CA emisora `AAPPR`

Nombre en KeyOne® CA `sello_nivel_medio_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		
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 usaramos el NIF sería algo como: VATES-A01337260
OU		**"SELLO ELECTRONICO"**
O		Nombre oficial de la organización
C		**ES**
subjectPublicKeyInfo		RSA 2048 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		
2.16.724.1.3.5.6.2.1		**"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	Opcional	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
extendedKeyUsage		clientAuth, emailProtection
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.4.11.3
cpsURI		http://www.izenpe.eus/cps
userNotice		Kontsulta www.izenpe.eus-en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en www.izenpe.eus 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-l)
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crlscar2
authorityInfoAccess		
ocsp		http://ocsp.izenpe.com
CA emisora		http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR_cert_sha256.crt
qcStatements		
QcCompliance		Presente
QcType		id-etsi-qct-eseal
QcRetentionPeriod		15 años
QcPDS		https://www.izenpe.eus/pds/en/ EN https://www.izenpe.eus/pds/eu/ EU https://www.izenpe.eus/pds/es/ ES
qcStatement-2		0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)
keyUsage	Crítica	digitalSignature, nonRepudiation (<>contentCommitment), keyEncipherment, , dataEncipherment

Sello nivel alto EIDAS

CA emisora `AAPPR`

Nombre en KeyOne® CA `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		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 usaramos el CIF sería algo como: VATES-A01337260
OU		**"SELLO ELECTRONICO"**
O		Nombre oficial de la organización
C		**ES**
subjectPublicKeyInfo		RSA 2048 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		http://www.izenpe.eus/cps
userNotice		Kontsulta www.izenpe.eus-en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en www.izenpe.eus los términos y condiciones antes de utilizar o confiar en el certificado
policyIdentifier		0.4.0.194112.1.3 (QCP-l-qscd)
policyIdentifier		2.16.724.1.3.5.6.1
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crlscar2
authorityInfoAccess		
ocsp		http://ocsp.izenpe.com
CA emisora		http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPR_cert_sha256.crt
qcStatements		
QcCompliance		Presente
QcType		id-etsi-qct-eseal
QcRetentionPeriod		15 años
QcSSCD		Presente
QcPDS		https://www.izenpe.eus/pds/en/ EN https://www.izenpe.eus/pds/eu/ EU https://www.izenpe.eus/pds/es/ ES
qcStatement-2		0.4.0.194121.1.2 (id-etsi-qcs-SemanticsId-Legal)
keyUsage	Crítica	digitalSignature, nonRepudiation (<>contentCommitment), keyEncipherment, , dataEncipherment

Personal de Entidades Públicas (EJGV)

CA emisora `AAPPR2`

Nombre en KeyOne® CA `pers_entidades_publicas`

Campo / extensión	Opcional / Crítica	Contenido
version		Versión 3
serialNumber		Número secuencial único
signature		sha1WithRSAEncryption
issuer		Igual al campo subject del certificado de la CA emisora
validity		4 años
subject		
serialNumber		DNI / NIE
SN		Primer Apellido
G		Nombre
CN		Nombre y Apellidos
dnQualifier		Depende de tipo de documento. DNI: "`-dni [DNI] -cif [CIF]`" NIE: "`-nie [NIE] -cif [CIF]`"
OU		Condiciones de uso en www.izenpe.com nola erabili jakiteko
OU		Entitate publikoen ziurtagiri - Certificado de entidad publica
		Ziurtagiri onartua - Certificado reconocido
OU	Opcional	Cargo o Departamento
OU	Opcional	Grupo VPN
O		Organización
C		ES
subjectPublicKeyInfo		RSA 2048 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
extendedKeyUsage		clientAuth, emailProtection, smartCardLogon
netscapeCertType		SSL_Client, SMIME_Client
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.7.1 (1.3.6.1.4.1.14777.107.1 en Desarrollo)
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
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crlejgv
authorityInfoAccess		ocsp http://ocsp.izenpe.com:8094
qcStatements		
QcCompliance		Presente
QcSSCD		Presente
keyUsage	Crítica	digitalSignature

Servidor Web (EJGV)

CA emisora `AAPPR2`

Nombre en KeyOne® CA `servidores`

Campo / extensión	Opcional / Crítica	Contenido
version		Versión 3
serialNumber		Número secuencial único
signature		sha1WithRSAEncryption
issuer		Igual al campo subject del certificado de la CA emisora
validity		3 años
subject		
CN		Dominio DNS o dirección IP
OU		Departamento
O		Nombre de la organización
L		Localidad
ST		Provincia
C		ES
subjectPublicKeyInfo		RSA 2048 bits mínimo
extensions		
issuerAltName		Igual a la extensión subjectAltName del certificado de la CA emisora
subjectAltName	Opcional	Igual a la extensión subjectAltName de la petición, si está presente
extendedKeyUsage		serverAuth
netscapeCertType		SSL_Server
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.7.2.1 (1.3.6.1.4.1.14777.107.2.1 en Desarrollo)
cpsURI		http://www.izenpe.com/rpaservidor
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
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crlejgv
authorityInfoAccess		ocsp http://ocsp.izenpe.com:8094
keyUsage	Crítica	digitalSignature, nonRepudiation, keyEncipherment