



DOCUMENTACIÓN ESPECÍFICA PARA CERTIFICADOS DE ÁMBITO CORPORATIVO

© IZENPE 2011

Este documento es propiedad de IZENPE, únicamente puede ser reproducido en su totalidad.

■ Beato Tomás de Zumárraga
71 - 1ª Planta
01008
Vitoria - Gasteiz

www.izenpe.com
info@izenpe.com
Tel.: 945 017 490



1. Introducción

El presente documento recoge la *Documentación específica* correspondiente a los certificados emitidos por Ziurtapen eta Zerbitzu Enpresa-Enpresa de Certificación y Servicios, Izenpe, S.A. (en adelante, IZENPE) en el ámbito corporativo.

Su finalidad es detallar y completar para este tipo de certificados lo definido de forma genérica en la *Declaración de Prácticas de Certificación de IZENPE*.

Concretamente esta documentación regula los certificados emitidos en el ámbito,

- De las **Administraciones Públicas y entidades pertenecientes al sector público**,
 - *Personal de las Entidades públicas*
 - *Corporativo reconocido*
 - *Corporativo no reconocido*

NOTA.

A estos efectos IZENPE emite certificados del tipo *Corporativo reconocido a las entidades comprendidas en el artículo 3 de la Ley 30/2007, de 30 de octubre, de Contratos del Sector Público*. Entendiendo por tales:

- Entidades de derecho público creadas por Ley o vinculadas a una o varias Administraciones Públicas o dependientes de las mismas.
- Organismos autónomos.
- Universidades públicas.
- Sociedades mercantiles con participación pública mayoritaria (directa o indirecta).
- Consorcios, fundaciones y asociaciones con participación pública mayoritaria.
- Entes públicos de derecho privado.



- En el ámbito **privado**,
 - *Corporativo privado reconocido.*
 - *Corporativo privado no reconocido.*

1.1 Descripción de certificados

IZENPE, en el ámbito del Servicio de Certificación Digital en virtud del cual las Entidades usuarias del servicio obtienen certificados digitales, emite

- I. En el ámbito de las **Administraciones Públicas y entidades pertenecientes al sector público**, certificados del tipo,

- *Personal de las Entidades públicas.*

Se trata de un certificado emitido en dispositivo criptográfico, en el ámbito de la *CA de Personal de AAPP reconocido*.

Este certificado identifica: a la Administración Pública actuante así como a la persona que desempeña un cargo o puesto en la misma.

La Administración Pública actuará como suscriptora del certificado y además realizará las funciones de identificación de los poseedores de claves pertenecientes a la misma.

El personal al servicio de Administración puede recibir dos certificados:

- El certificado de firma electrónica, con la consideración legal de certificado reconocido, de acuerdo con lo establecido en los artículos 8, 11, 12, 13, 18 y 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.
- El certificado de cifrado, sin la consideración legal de certificado reconocido, para usos de cifrado.

- *Corporativo reconocido*

El certificado *Corporativo reconocido* es un certificado emitido en dispositivo criptográfico en el ámbito de la *CA de personal de AAPP reconocido*.



Este certificado identifica a la entidad actuante, como suscriptora del certificado, y a la persona que desempeña un cargo o puesto en la misma, como poseedor de claves.

El personal al servicio de la entidad solicitante puede recibir:

- El certificado de firma electrónica, con la consideración legal de certificado reconocido, de acuerdo con lo establecido en los artículos 8, 11, 12, 13, 18 y 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.
- El certificado de cifrado, sin la consideración legal de certificado reconocido, para usos de cifrado.

- *Corporativo no reconocido*

El certificado *Corporativo no reconocido* es un certificado con la configuración legal de no reconocido, emitido en dispositivo criptográfico en el ámbito de la *CA de personal de AAPP no reconocido*.

Este certificado identifica a la entidad actuante, como suscriptor del certificado, así como a la persona que desempeña un cargo o puesto en la misma, como poseedor de claves.

II. Entidades pertenecientes al ámbito privado

- *Corporativo privado reconocido*

El certificado *Corporativo privado reconocido* es un certificado con la consideración legal de reconocido, emitido en dispositivo criptográfico en el ámbito de la CA de Ciudadanos y Entidades reconocidos.

Se trata de un certificado que identifica como suscriptor a la entidad identificada en el certificado y como poseedor de claves a la persona física que desempeña un cargo o puesto en la entidad y que posee o responde de la custodia de las claves de firma.



- Corporativo privado no reconocido

El certificado *Corporativo privado no reconocido* es un certificado con la configuración legal de no reconocido emitido en dispositivo criptográfico en el ámbito de la CA de Ciudadanos y Entidades no reconocidos.

Se trata de un certificado que identifica como suscriptor a la entidad identificada en el certificado y como poseedor de claves a la persona física que desempeña un cargo o puesto en la entidad y que posee o responde de la custodia de las claves de firma.

Este certificado tiene limitado su uso únicamente al ámbito del puesto de trabajo desempeñado

La identidad y cualquier información que deba contenerse en los certificados serán comprobadas necesariamente por una Entidad de Registro.

Estas comprobaciones podrán ser desempeñadas por IZENPE o por las Entidades Usuarias con las que IZENPE suscriba el instrumento legal pertinente.

1.2 Identificación

Con el objeto de identificar los certificados, IZENPE les ha asignado los siguientes identificadores de objeto (OID).

CERTIFICADO	OID
<i>Personal de las Entidades públicas</i>	1.3.6.1.4.1.14777.4.1
<i>Personal del Gobierno Vasco</i>	1.3.6.1.4.1.14777.7.1
<i>Corporativo reconocido</i>	1.3.6.1.4.1.14777.4.2
<i>Corporativo no reconocido</i>	1.3.6.1.4.1.14777.1.1.1



<i>Corporativo privado reconocido</i>	1.3.6.1.4.1.14777.2.2
<i>Corporativo privado no reconocido</i>	1.3.6.1.4.1.14777.5.2.

Los certificados del tipo *Personal del Gobierno Vasco, Personal de las Entidades Públicas, Corporativo reconocido y Corporativo privado reconocido*, al tratarse de certificados con la consideración de reconocidos incorporan adicionalmente el siguiente identificador de objeto (OID) definido por el TS 101 862, del Instituto Europeo de Normas de Telecomunicaciones, sobre perfiles de certificados reconocidos: 0.4.0.1862.1.1.

1.3 Comunidad y ámbito de uso

Tendrán la consideración de usuarios,

Solicitante del certificado

El certificado debe ser solicitado por una persona en nombre de una organización.

Firmante

El firmante es la persona física identificada en el certificado.

Suscriptor de certificado

El suscriptor es la Administración Pública u Organización identificada en el certificado.

Poseedor de claves

El poseedor de claves es la persona física que posee o responde de la custodia de las claves de firma digital.

El poseedor de claves será el firmante.



Ámbito de uso

Los certificados serán utilizados en el ámbito de las competencias propias de la Administración u Organización usuaria y del puesto o cargo desempeñado.

Respecto a los certificados del tipo *Corporativo no reconocido*, únicamente serán utilizados en el puesto o cargo desempeñado.

No obstante, los poseedores de claves podrán utilizar estos certificados para otros usos siempre que se respeten los límites de uso señalados con terceros en los instrumentos legales pertinentes.

1.4 Disposiciones generales

Obligaciones de identificación

IZENPE comprueba, por si misma o por medio de las Entidades Usuarias con las que suscriba el correspondiente instrumento legal, la identidad y cualesquiera otras circunstancias personales de los solicitantes, suscriptores y poseedores de claves de los certificados.

Asimismo comprueba que el poseedor de claves se encuentra debidamente autorizado por el suscriptor.

Obligaciones del suscriptor del certificado

Son obligaciones del suscriptor,

1. Las recogidas en el apartado 2.1.5 de la Declaración de Prácticas de Certificación
2. Tanto el suscriptor como el poseedor de claves tienen la carga de solicitar la revocación del certificado, en los términos previstos en la Declaración de Prácticas de Certificación.



2 Registro Inicial

Tipos de nombres

Subject (Requisito del Artículo 11.2 letra e) de la Ley 59/2003, de 19 de diciembre de 2003)

Los atributos que componen el nombre diferenciado del campo subject de los certificados son los recogidos en el apartado correspondiente al perfil del certificado.

Significado de los nombres

No se pueden emplear seudónimos.

El nombre del poseedor de claves en los certificados está compuesto por su nombre y apellidos, junto con su número de D.N.I./Pasaporte o N.I.E..

Resolución de conflictos relativos a nombres

Los conflictos de nombres de poseedores de claves que aparezcan identificados en los certificados con su nombre real se solucionan mediante la inclusión, en el nombre diferenciado del certificado, del NIF u otro identificador asignado por el suscriptor, de acuerdo con lo establecido en el apartado precedente.



3 Requisitos operativos

3.1 Solicitud de certificado

El solicitante deberá rellenar el formulario de solicitud del certificado y tramitarlo ante IZENPE a través de dos vías:

- a) Vía telemática: en la dirección web <http://www.izenpe.com> los interesados disponen del formulario de solicitud, que deberá ser completado, firmado electrónicamente mediante un certificado reconocido de acuerdo con lo establecido en la *Ley 59/2003, de 19 de diciembre, de firma electrónica* y enviado telemáticamente a IZENPE.
- b) O presencialmente: El solicitante podrá personarse en cualquiera de las Entidades de Registro señaladas en el listado publicado en <http://www.izenpe.com> y realizar la solicitud de certificado.

3.2 Acreditación

3.2.1 De la identidad del solicitante

El solicitante del certificado deberá acreditar su identidad y presentar, en vigor, original o copia auténtica de la siguiente documentación:

- a) DNI, pasaporte o permiso de conducción, en el caso de ciudadano nacional.
- b) En caso de ciudadano extranjero:
 - I. Miembro de la Unión Europea o de Estados parte del Espacio Económico Europeo, será exigible ,
 - Documento nacional de identidad o equivalente en su país o pasaporte
 - Y certificado emitido por el Registro de Ciudadanos Miembros de la Unión.
 - II. En relación a ciudadanos extracomunitarios, será exigible la tarjeta de residencia.
- c) Podrá prescindirse de la personación ante la Entidad de Registro:



- Si la firma del solicitante en la solicitud de emisión del certificado ha sido legitimada en presencia notarial.
- En el caso de certificados del tipo *Personal de las Entidades Públicas* y en el ámbito municipal, siempre que la identificación la realice el Secretario en el marco de sus funciones de fedatario público.
- O en los supuestos contemplados en el artículo 13.4 de la LFE, salvo que en el procedimiento de emisión fuera exigible la personación del solicitante a efectos distintos a la identificación, por ejemplo garantizar una entrega segura del certificado.

La identificación y acreditación del solicitante en el caso de certificados del tipo *Personal de las Entidades Públicas, Corporativo reconocido y Corporativo privado reconocido* exige su personación ante la Entidad de Registro

La Entidad de Registro dejará constancia documental, a través de la *Solicitud de Emisión*, de la comprobación de la identidad del solicitante.

3.2.2 De la identidad de la organización

Se presentará la siguiente documentación a efectos de su comprobación por la Entidad de Registro:

Documentación acreditativa de la válida constitución de la organización

- Número de Identificación Fiscal (N.I.F.) de la Administración Pública / Entidad.
Se aportará fotocopia compulsada o referencia a la publicación oficial acreditativa del mismo.
- En el caso de certificados del tipo
 - *Personal de las Entidades Públicas*,
 - ✓ A través de la *Solicitud de Emisión*, el solicitante manifestará la veracidad y actualidad de los datos referentes a la Administración Pública solicitante.



- *Corporativo reconocido y Corporativo privado reconocido*
 - ✓ Las sociedades mercantiles y demás personas jurídicas cuya inscripción sea obligatoria en el Registro Mercantil o en cualquier otro registro público, acreditarán la válida constitución mediante la aportación de original o copia auténtica de un certificado del Registro relativo a los datos de constitución y personalidad jurídica de las mismas.
 - ✓ En otro caso se aportará original o copia auténtica del documento público que acredite su constitución de manera fehaciente
- *Corporativo no reconocido y Corporativo privado no reconocido*
 - ✓ Se aportará, a través de la *Solicitud de Emisión*, manifestación responsable del solicitante confirmando la válida constitución de la misma.

Documentación acreditativa del poder suficiente del solicitante

- En el caso de certificados del tipo
 - *Personal de las Entidades Públicas*
 - ✓ A través de la *Solicitud de Emisión*, el solicitante manifestará su capacidad suficiente para solicitar el certificado.
 - *Corporativo reconocido y Corporativo privado reconocido*
 - ✓ Además de los administradores y representantes legales de entidad sujeta a inscripción registral, que aportarán original o copia auténtica del Certificado del Registro correspondiente relativo a su nombramiento y vigencia del cargo, dicho certificado deberá haber sido expedido durante los quince días hábiles anteriores a la fecha de solicitud del certificado.
 - ✓ Se considera que tienen poder suficiente, los representantes voluntarios cuando acrediten poder para la realización de actos de administración o celebración de contratos en nombre de la entidad.

Aportarán original o copia auténtica de la escritura pública o documento oficial donde derive la representación con expresión de sus facultades y su vigencia.
 - *Corporativo no reconocido y Corporativo privado no reconocido*



- ✓ Además de los administradores y representantes legales,
- ✓ Se considera que tienen poder suficiente los representantes voluntarios cuando acrediten poder suficiente para la realización de actos de administración o celebración de contratos en nombre de la entidad.

No será necesario obtener la justificación documental de la existencia de la entidad ni de las facultades de representación de quien actúa en su nombre, siempre que estos hechos estuvieran regulados por norma.

La Entidad de Registro dejará constancia documental, a través de la *Solicitud de Emisión*, de la comprobación de la documentación realizada.

3.2.3 De los poseedores de claves

Los poseedores de claves acreditarán su identidad ante la Entidad de Registro según las mismas condiciones requeridas al solicitante.

NOTA

Formulada la primera *Solicitud de Emisión*, si en posteriores solicitudes de certificados para poseedores de claves los datos que constaran en la *Solicitud de Emisión* inicial hubieran variado, la Organización solicitante será responsable de comunicar a IZENPE los cambios y de enviar nueva *Solicitud*.

3.3 Emisión de certificado

El solicitante deberá firmar la *Solicitud de Emisión* del certificado, aceptando de esta forma el contrato de suscriptor así como las Condiciones de Uso.

3.4 Entrega de certificado

La Entidad de Registro entregará el certificado en la dirección postal determinada en la *Solicitud de Emisión*.



El poseedor de claves deberá devolver firmada a IZENPE la Hoja de Entrega y Aceptación en el plazo máximo de 3 meses. En caso contrario se revocará el certificado.

3.5 Suspensión de certificados

Procedimiento

El certificado se podrá suspender en cualquier momento y, en todo caso en los supuestos de pérdida o robo del certificado llamando al teléfono 902 542 542 e identificándose dando Contraseña de Identificación Telefónica y según el certificado,

- *Personal de las Entidades Públicas: DNI / NIE*
- *Corporativo reconocido y Corporativo privado reconocido: DNI / NIE y NIF de la organización.*
- *Corporativo no reconocido y Corporativo privado no reconocido: DNI / NIE*

Solicitante de la suspensión

Podrán suspender el certificado:

- El poseedor de claves.
- La Entidad de Registro.

Plazo máximo temporal de suspensión

El plazo máximo de la suspensión es de quince días naturales desde que sea solicitada por el poseedor de claves.

Durante dicho plazo el poseedor de claves deberá confirmar la reactivación del certificado en las condiciones previstas para la misma.

Transcurrido dicho plazo sin que la reactivación sea confirmada por el poseedor de claves, el certificado será revocado.



IZENPE tiene capacidad permanente (24x7) para tramitar la suspensión de certificados. Una vez suspendido un certificado éste queda incluido en la nueva lista de revocación (CRL) que se genera automáticamente y en el servicio de verificación avanzada (OCSP). En cualquier caso la CRL se actualiza cada día y con cada nueva revocación.

3.6 Revocación de certificados

Petición de revocación

Podrán solicitar la revocación de un certificado,

- El suscriptor a nombre del cual fue emitido el certificado.
- El solicitante.
- El poseedor de claves.
- IZENPE.
- Tercero autorizado por el suscriptor.

Deberá presentar documento firmado por el suscriptor autorizando al tercero a actuar en su nombre.

Los administradores de IZENPE y las Entidades de Registro están autorizados para solicitar la revocación de certificados de suscriptor de entidad final.

Tramitación

El solicitante de la revocación deberá rellenar el formulario de *Solicitud de Revocación* y tramitarlo ante IZENPE a través de las mismas vías previstas para la solicitud del certificado (ver apartado 3.1).

La Entidad de Registro dejará constancia, a través de la *Solicitud de Revocación*, de la identificación del solicitante.

Causas de revocación

Pueden consultarse en la Declaración de Prácticas de Certificación www.izenpe.com



3.7 Reactivación

Petición de reactivación

En el caso de una petición de reactivación, el solicitante deberá ser:

- El suscriptor
- O en su caso, el poseedor de claves que haya solicitado previamente la suspensión del certificado.

Éste deberá acreditar su identidad ante una Entidad de Registro

Tramitación

El solicitante de la reactivación del certificado dispondrá de 15 días naturales desde la solicitud de la suspensión del mismo para solicitar su reactivación, transcurrido este tiempo se entenderá revocado.

El solicitante deberá rellenar el formulario de solicitud y tramitarlo ante IZENPE a través de las mismas vías previstas para la solicitud del certificado (ver apartado 3.1).

La Entidad de Registro dejará constancia de la identificación del solicitante.

3.8 Renovación de certificados

Para renovar un certificado, bien porque haya sido revocado o porque haya caducado, el suscriptor deberá solicitar un nuevo certificado, siguiendo el proceso de emisión de certificados establecido.



4 Gestión del cambio

Las modificaciones de este documento serán aprobadas por del Comité de Seguridad de IZENPE.

Estas modificaciones estarán recogidas en un documento de Actualización de Documentación Específica cuyo mantenimiento está garantizado por IZENPE.

Las versiones actualizadas de la documentación específica podrán ser consultadas en la dirección www.izenpe.com.



5 Perfiles de certificados y listas de certificados revocados

Usos previstos: firma, cliente ssl, s/mime, scl, vpn, cifrado (sin recuperación de claves).

5.1 Certificado de Personal de las Entidades Públicas

Campo	Contenido
1. X.509v1 Field	
1.1. Versión	v3
1.2. Serial Number	Asignado automáticamente por la CA emisora
1.3. Signature Algorithm	SHA-1 con Firma RSA
1.4. Signature Value	Firma codificada como cadena de bits
1.5. Issuer Distinguished Name	
1.5.1. Country (C)	España
1.5.2. Locality	Avenida del Mediterráneo, 3 – 01010, Vitoria-Gasteiz
1.5.3. Organization (O)	IZENPE S.A.-CIF A-01337260 – RMerc. Vitoria-Gasteiz T1055 F62 S8
1.5.4. Organizational Unit (OU)	Certificado público SCA
1.5.5. Common Name (CN)	EAEko HAetako langileen CA - CA personal de AAPP vascas
1.5.6. EmailAddress	info@izenpe.com
1.6. Validity	
1.6.1. Not Before	Fecha inicio validez del certificado



Campo	Contenido
1.6.2. Not After	Fecha fin validez del certificado
1.7. Subject	
1.7.1. Country (C)	ES
1.7.2. Organization (O)	Nombre completo organización del suscriptor
1.7.3. Organizational Unit (OU)	Grupo interno (vpn)
1.7.4. Organizational Unit (OU)	Cargo y/o departamento
1.7.5. Organizational Unit (OU)	Ziurtagiri onartua - Certificado reconocido
1.7.6. Organizational Unit (OU)	Entitate publikoen ziurtagiri - Certificado de entidad publica
1.7.7. Organizational Unit (OU)	Condiciones de uso en www.izenpe.com nola erabili jakiteko
1.7.8. dnQualifier	NIF, NIE (*) + TIS (opcional) (*) formato : -dni nnnnnnnnL o -nie XnnnnnnnnL -TIS nnnnnnnn
1.7.9. Common Name (CN)	Nombre y Apellidos del poseedor de claves
1.7.10. GivenName	Nombre del poseedor de claves
1.7.11. SurName	Apellidos poseedor de claves
1.7.12. Serialnumber	NIF, NIE (*) del suscriptor persona física o poseedor de claves
1.8. Subject Public Key Info	1024-Bit clave pública codificado conforme con RFC2459 & PKCS#1



Campo	Contenido
2. X.509v3 Extensions	
2.1. Authority Key Identifier	
2.1.1. Key Identifier	Identificador de la clave pública del emisor
2.1.2. AuthorityCertIssuer	Nombre de la CA a la que corresponde la clave identificada en keyIdentifier
2.1.3. AuthorityCertSerialNumber	Número de serie del certificado de CA
2.2. Subject Key Identifier	
2.2.1. Key Identifier	Identificador de la clave pública del poseedor de claves
2.3. Key Usage	
2.3.1. Digital Signature	Seleccionado "1"
2.3.2. Non Repudiation	No seleccionado "0"
2.3.3. Key Encipherment	Seleccionado "1"
2.3.4. Data Encipherment	Seleccionado "1"
2.3.5. Key Agreement	No seleccionado "0"
2.3.6. Key Certificate Signature	No seleccionado "0"
2.3.7. CRL Signature	No seleccionado "0"
2.4. Qualified Certificate Statements	
2.4.1. qCStatement OID	0.4.0.1862.1



Campo	Contenido
2.5. Certificate Policies	
2.5.1. Policy Identifier	1.3.6.1.4.1.14777.4.1
2.5.2. Policy Qualifier ID	
2.5.2.1. CPS Pointer	http://www.izenpe.com/rpascapersentpub
2.5.2.2. User Notice	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
2.6. Subject Alternate Names	
2.6.1. rfc822Name	Dirección de email
2.6.2. UserPrincipalName	Usuario@dominio
2.7. Issuer Alternative Name	
2.7.1. dNSName	http://www.izenpe.com
2.8. Extended Key Usage	
2.8.1. emailProtection	1.3.6.1.5.5.7.3.4
2.8.2. clientAuth	1.3.6.1.5.5.7.3.2
2.8.3. smartcardlogon	1.3.6.1.4.1.311.20.2.2
2.9. cRLDistributionPoint	



Campo	Contenido
2.9.1. distributionPoint	CA emitida en 2003: http://crl.izenpe.com/cgi-bin/crlscar CA emitida en 2009: http://crl.izenpe.com/cgi-bin/crlscar2
2.10. NetscapeCertType	SSL client, SMIME client
2.11. Authority Information Access	
2.11.1. Access Description	
2.11.1.1. Access Method	1.3.6.1.5.5.7.1.48.1
2.11.1.2. accessLocation	http://ocsp.izenpe.com:8094



Certificado de Personal de Gobierno Vasco

Campo / extensión	Opcional / Crítica	Contenido
version		Versión 3
serialNumber		Número secuencial único
signature issuer		sha-1WithRSAEncryption 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		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 extensions		RSA 1024 bits mínimo
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 campos keyIdentifier y IssuerAndSerialNumber
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/cps
userNotice		Bermeen mugak ezagutzeko www.izenpe.com Ziurtagirian konfiantza izan aurretik kontratua irakurri. Limitaciones de garantías en www.izenpe.com Consulte el contrato antes de confiar en el certificado
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crlejgv
authorityInfoAccess		ocsp http://ocsp.izenpe.com:8094
qcStatements		
QcCompliance		Presente
keyUsage	Crítica	digitalSignature, keyEncipherment, dataEncipherment



Campo	Contenido
3. X.509v1 Field	
3.1. Versión	v3
3.2. Serial Number	Asignado automáticamente por la CA emisora
3.3. Signature Algorithm	SHA-1 con Firma RSA
3.4. Signature Value	Firma codificada como cadena de bits
3.5. Issuer Distinguished Name	
3.5.1. Country (C)	España
3.5.2. Locality	Avenida del Mediterráneo, 3 – 01010, Vitoria-Gasteiz
3.5.3. Organization (O)	IZENPE S.A.-CIF A-01337260 – RMerc. Vitoria-Gasteiz T1055 F62 S8
3.5.4. Organizational Unit (OU)	AZZ Ziurtagiri Publikoa - Certificado publico SCA
3.5.5. Common Name (CN)	EAEko Herri Administrazioen CA – CA de AAPP Vascas
3.5.6. EmailAddress	info@izenpe.com
3.6. Validity	
3.6.1. Not Before	Fecha inicio validez del certificado
3.6.2. Not After	Fecha fin validez del certificado
3.7. Subject	
3.7.1. Organization (O)	Nombre completo organización del suscriptor
3.7.2. Organizational Unit (OU)	Grupo interno (vpn)
3.7.3. Organizational Unit (OU)	Cargo y/o departamento
3.7.4. Organizational Unit (OU)	Ziurtagiri korporatiboa Certificado corporativo
3.7.5. Organizational Unit (OU)	Condiciones de uso en www.izenpe.com nola erabili jakiteko
3.7.6. dnQualifier	NIF, NIE (*) del poseedor de claves y CIF de la empresa (*) formato : -dni nnnnnnnnL o -nie XnnnnnnnnL
3.7.7. Common Name (CN)	Nombre y Apellidos del poseedor de claves
3.7.8. GivenName	Nombre del poseedor de claves
3.7.9. SurName	Apellidos poseedor de claves
3.7.10. SerialNumber	NIF, NIE (*) del suscriptor persona física o poseedor de claves
3.8. Subject Public Key Info	1024-Bit clave pública codificado conforme con



Campo	Contenido
	RFC2459 & PKCS#1
4. X.509v3 Extensions	
4.1. Authority Key Identifier	
4.1.1. Key Identifier	Identificador de la clave pública del emisor
4.1.2. AuthorityCertIssuer	Nombre de la CA a la que corresponde la clave identificada en keyIdentifier
4.1.3. AuthorityCertSerialNumber	Número de serie del certificado de CA
4.2. Subject Key Identifier	
4.2.1. Key Identifier	Identificador de la clave pública del poseedor de claves
4.3. Key Usage	
4.3.1. Digital Signature	Seleccionado "1"
4.3.2. Non Repudiation	No seleccionado "0"
4.3.3. Key Encipherment	Seleccionado "1"
4.3.4. Data Encipherment	Seleccionado "1"
4.3.5. Key Agreement	No seleccionado "0"
4.3.6. Key Certificate Signature	No seleccionado "0"
4.3.7. CRL Signature	No seleccionado "0"
4.4. Certificate Policies	
4.4.1. Policy Identifier	1.3.6.1.4.1.14777.1.1.1
4.4.2. Policy Qualifier ID	
4.4.2.1. CPS Pointer	http://www.izenpe.com/rpascacorporativo
4.4.2.2. User Notice	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
4.5. Subject Alternate Names	
4.5.1. rfc822Name	Dirección de email
4.5.2. UserPrincipalName	Usuario@dominio
4.6. Issuer Alternative Name	
4.6.1. dNSName	http://www.izenpe.com
4.7. Extended Key Usage	
4.7.1. emailProtection	1.3.6.1.5.5.7.3.4



Campo	Contenido
4.7.2. clientAuth	1.3.6.1.5.5.7.3.2
4.7.3. smartcardlogon	1.3.6.1.4.1.311.20.2.2
4.8. cRLDistributionPoint	
4.8.1. distributionPoint	http://crl.izenpe.com/cgi-bin/crlinterna CA emitida en 2009: http://crl.izenpe.com/cgi-bin/crlinterna2
4.9. NetscapeCertType	SSL client, SMIME client
4.10. Authority Information Access	
4.10.1. Access Description	
4.10.1.1. Access Method	1.3.6.1.5.5.7.1.48.1
4.10.1.2. accessLocation	http://ocsp.izenpe.com:8094



5.2 Corporativo reconocido

Campo	Contenido
5. X.509v1 Field	
5.1. Versión	v3
5.2. Serial Number	Asignado automáticamente por la CA emisora
5.3. Signature Algorithm	SHA-1 con Firma RSA
5.4. Signature Value	Firma codificada como cadena de bits
5.5. Issuer Distinguished Name	
5.5.1. Country (C)	España
5.5.2. Locality	Avenida del Mediterráneo, 3 – 01010, Vitoria-Gasteiz
5.5.3. Organization (O)	IZENPE S.A.-CIF A-01337260 – RMerc. Vitoria-Gasteiz T1055 F62 S8
5.5.4. Organizational Unit (OU)	Certificado público SCA
5.5.5. Common Name (CN)	EAEko HAetako langileen CA - CA personal de AAPP vascas
5.5.6. EmailAddress	info@izenpe.com
5.6. Validity	
5.6.1. Not Before	Fecha inicio validez del certificado
5.6.2. Not After	Fecha fin validez del certificado
5.7. Subject	
5.7.1. Country (C)	ES
5.7.2. Organization (O)	Nombre completo organización del suscriptor



Campo	Contenido
5.7.3. Organizational Unit (OU)	Grupo interno (vpn)
5.7.4. Organizational Unit (OU)	Cargo y/o departamento
5.7.5. Organizational Unit (OU)	Ziurtagiri onartua - Certificado reconocido
5.7.6. Organizational Unit (OU)	Ziurtagiri korporatibo onartua – Cert. corporativo reconocido
5.7.7. Organizational Unit (OU)	Condiciones de uso en www.izenpe.com nola erabili jakiteko
5.7.8. dnQualifier	NIF, NIE (*) + TIS (opcional) (*) formato : -dni nnnnnnnnL o -nie XnnnnnnnnL –TIS nnnnnnnn
5.7.9. Common Name (CN)	Nombre y Apellidos del poseedor de claves
5.7.10. GivenName	Nombre del poseedor de claves
5.7.11. SurName	Apellidos poseedor de claves
5.7.12. Serialnumber	NIF, NIE (*) del suscriptor persona física o poseedor de claves
5.8. Subject Public Key Info	1024-Bit clave pública codificado conforme con RFC2459 & PKCS#1
6. X.509v3 Extensions	
6.1. Authority Key Identifier	
6.1.1. Key Identifier	Identificador de la clave pública del emisor
6.1.2. AuthorityCertIssuer	Nombre de la CA a la que corresponde la clave identificada en keyIdentifier
6.1.3. AuthorityCertSerialNumber	Número de serie del certificado de CA
6.2. Subject Key Identifier	
6.2.1. Key Identifier	Identificador de la clave pública del poseedor de claves



Campo	Contenido
6.3. Key Usage	
6.3.1. Digital Signature	Seleccionado "1"
6.3.2. Non Repudiation	No seleccionado "0"
6.3.3. Key Encipherment	Seleccionado "1"
6.3.4. Data Encipherment	Seleccionado "1"
6.3.5. Key Agreement	No seleccionado "0"
6.3.6. Key Certificate Signature	No seleccionado "0"
6.3.7. CRL Signature	No seleccionado "0"
6.4. Qualified Certificate Statements	
6.4.1. qCStatement OID	0.4.0.1862.1
6.5. Certificate Policies	
6.5.1. Policy Identifier	1.3.6.1.4.1.14777.4.2
6.5.2. Policy Qualifier ID	
6.5.2.1. CPS Pointer	http://www.izenpe.com/rpascacorrec
6.5.2.2. User Notice	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
6.6. Subject Alternate Names	
6.6.1. rfc822Name	Dirección de email
6.6.2. UserPrincipalName	Usuario@dominio



Campo	Contenido
6.7. Issuer Alternative Name	
6.7.1. dNSName	http://www.izenpe.com
6.8. Extended Key Usage	
6.8.1. emailProtection	1.3.6.1.5.5.7.3.4
6.8.2. clientAuth	1.3.6.1.5.5.7.3.2
6.8.3. smartcardlogon	1.3.6.1.4.1.311.20.2.2
6.9. cRLDistributionPoint	
6.9.1. distributionPoint	CA emitida en 2003 http://crl.izenpe.com/cgi-bin/crlscar CA emitida en 2009 http://crl.izenpe.com/cgi-bin/crlscar2
6.10. NetscapeCertType	SSL client, SMIME client
6.11. Authority Information Access	
6.11.1. Access Description	
6.11.1.1. Access Method	1.3.6.1.5.5.7.1.48.1
6.11.1.2. accessLocation	http://ocsp.izenpe.com:8094



5.3 Corporativo no reconocido

Campo	Contenido
7. X.509v1 Field	
7.1. Versión	v3
7.2. Serial Number	Asignado automáticamente por la CA emisora
7.3. Signature Algorithm	SHA-1 con Firma RSA
7.4. Signature Value	Firma codificada como cadena de bits
7.5. Issuer Distinguished Name	
7.5.1. Country (C)	España
7.5.2. Locality	Avenida del Mediterráneo, 3 – 01010, Vitoria-Gasteiz
7.5.3. Organization (O)	IZENPE S.A.-CIF A-01337260 – RMerc. Vitoria-Gasteiz T1055 F62 S8
7.5.4. Organizational Unit (OU)	AZZ Ziurtagiri Publikoa - Certificado publico SCA
7.5.5. Common Name (CN)	EAEko Herri Administrazioen CA – CA de AAPP Vascas
7.5.6. EmailAddress	info@izenpe.com
7.6. Validity	
7.6.1. Not Before	Fecha inicio validez del certificado
7.6.2. Not After	Fecha fin validez del certificado
7.7. Subject	
7.7.1. Organization (O)	Nombre completo organización del suscriptor
7.7.2. Organizational Unit (OU)	Grupo interno (vpn)



Campo	Contenido
7.7.3. Organizational Unit (OU)	Cargo y/o departamento
7.7.4. Organizational Unit (OU)	Ziurtagiri korporatiboa Certificado corporativo
7.7.5. Organizational Unit (OU)	Condiciones de uso en www.izenpe.com nola erabili jakiteko
7.7.6. dnQualifier	NIF, NIE (*) del poseedor de claves y CIF de la empresa (*) formato : -dni nnnnnnnnL o -nie XnnnnnnnnL
7.7.7. Common Name (CN)	Nombre y Apellidos del poseedor de claves
7.7.8. GivenName	Nombre del poseedor de claves
7.7.9. SurName	Apellidos poseedor de claves
7.7.10. Serialnumber	NIF, NIE (*) del suscriptor persona física o poseedor de claves
7.8. Subject Public Key Info	1024-Bit clave pública codificado conforme con RFC2459 & PKCS#1
8. X.509v3 Extensions	
8.1. Authority Key Identifier	
8.1.1. Key Identifier	Identificador de la clave pública del emisor
8.1.2. AuthorityCertIssuer	Nombre de la CA a la que corresponde la clave identificada en keyIdentifier
8.1.3. AuthorityCertSerialNumber	Número de serie del certificado de CA
8.2. Subject Key Identifier	
8.2.1. Key Identifier	Identificador de la clave pública del poseedor de claves
8.3. Key Usage	
8.3.1. Digital Signature	Seleccionado "1"



Campo	Contenido
8.3.2. Non Repudiation	No seleccionado "0"
8.3.3. Key Encipherment	Seleccionado "1"
8.3.4. Data Encipherment	Seleccionado "1"
8.3.5. Key Agreement	No seleccionado "0"
8.3.6. Key Certificate Signature	No seleccionado "0"
8.3.7. CRL Signature	No seleccionado "0"
8.4. Certificate Policies	
8.4.1. Policy Identifier	1.3.6.1.4.1.14777.1.1.1
8.4.2. Policy Qualifier ID	
8.4.2.1. CPS Pointer	http://www.izenpe.com/rpascacorporativo
8.4.2.2. User Notice	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
8.5. Subject Alternate Names	
8.5.1. rfc822Name	Dirección de email
8.5.2. UserPrincipalName	Usuario@dominio
8.6. Issuer Alternative Name	
8.6.1. dNSName	http://www.izenpe.com
8.7. Extended Key Usage	
8.7.1. emailProtection	1.3.6.1.5.5.7.3.4
8.7.2. clientAuth	1.3.6.1.5.5.7.3.2



Campo	Contenido
8.7.3. smartcardlogon	1.3.6.1.4.1.311.20.2.2
8.8. cRLDistributionPoint	
8.8.1. distributionPoint	http://crl.izenpe.com/cgi-bin/crlinterna CA emitida en 2009: http://crl.izenpe.com/cgi-bin/crlinterna2
8.9. NetscapeCertType	SSL client, SMIME client
8.10. Authority Information Access	
8.10.1. Access Description	
8.10.1.1. Access Method	1.3.6.1.5.5.7.1.48.1
8.10.1.2. accessLocation	http://ocsp.izenpe.com:8094



5.4 Corporativo privado reconocido

Campo / extensión	Opcional / Crítica	Contenido
version		Versión 3
serialNumber		Número secuencial único
signature		sha-1WithRSAEncryption
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 jakitek nola erabili o
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 1024 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
cpsURI		http://www.izenpe.com/cps
userNotice		Bermeen mugak ezagutzeko www.izenpe.com Ziurtagirian konfiantza izan aurretik kontratua irakurri. Limitaciones de garantías en www.izenpe.com Consulte el contrato antes de confiar en el certificado
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crl2
authorityInfoAccess		ocsp http://ocsp.izenpe.com:8094
qcStatements		
QcCompliance		Presente
keyUsage	Crítica	digitalSignature, keyEncipherment, dataEncipherment



5.5 Corporativo privado no reconocido

Campo	Contenido
9. X.509v1 Field	5.5.1
9.1. Versión	v3
9.2. Serial Number	Asignado automáticamente por la CA emisora
9.3. Signature Algorithm	SHA-1 con Firma RSA
9.4. Signature Value	Firma codificada como cadena de bits
9.5. Issuer Distinguished Name	5.5.2
9.5.1. Country (C)	ES
9.5.2. Locality	Avenida del Mediterráneo, 3 – 01010, Vitoria-Gasteiz
9.5.3. Organization (O)	IZENPE S.A.-CIF A-01337260 – RMerc. Vitoria-Gasteiz T1055 F62 S8
9.5.4. Common Name (CN)	Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (2)
9.5.5. EmailAddress	info@izenpe.com
9.6. Validity	
9.6.1. Not Before	Fecha inicio validez del certificado
9.6.2. Not After	Fecha fin validez del certificado
9.7. Subject	5.5.3
9.7.1. Organization (O)	<i>Nombre completo organización del suscriptor</i>
9.7.2. Organizational Unit (OU)	Grupo interno (vpn)
9.7.3. Organizational Unit (OU)	Cargo y/o departamento



Campo	Contenido
9.7.4. Organizational Unit (OU)	Ziurtagiri korporatibo pribatua - Certificado corporativo privado
9.7.5. Organizational Unit (OU)	Condiciones de uso en www.izenpe.com nola erabili jakiteko
9.7.6. dnQualifier	NIF, NIE (*) (*) formato : -dni nnnnnnnnL o -nie XnnnnnnnnL
9.7.7. Common Name (CN)	Nombre y Apellidos del poseedor de claves
9.7.8. GivenName	Nombre del poseedor de claves
9.7.9. SurName	Apellidos poseedor de claves
9.7.10. Serialnumber	NIF, NIE (*) del suscriptor persona física o poseedor de claves
9.8. Subject Public Key Info	1024-Bit clave pública codificado conforme con RFC2459 & PKCS#1
10. X.509v3 Extensions	5.5.4
10.1. Authority Key Identifier	5.5.5
10.1.1. Key Identifier	Identificador de la clave pública del emisor
10.1.2. AuthorityCertIssuer	Nombre de la CA a la que corresponde la clave identificada en keyIdentifier
10.1.3. AuthorityCertSerialNumber	Número de serie del certificado de CA
10.2. Subject Key Identifier	5.5.6
10.2.1. Key Identifier	Identificador de la clave pública del poseedor de claves
10.3. Key Usage	5.5.7
10.3.1. Digital Signature	Seleccionado "1"
10.3.2. Non Repudiation	No seleccionado "0"



Campo	Contenido
10.3.3. Key Encipherment	Seleccionado "1"
10.3.4. Data Encipherment	Seleccionado "1"
10.3.5. Key Agreement	No seleccionado "0"
10.3.6. Key Certificate Signature	No seleccionado "0"
10.3.7. CRL Signature	No seleccionado "0"
10.4. Certificate Policies	5.5.8
10.4.1. Policy Identifier	1.3.6.1.4.1.14777.5.2.2
10.4.2. Policy Qualifier ID	5.5.9
10.4.2.1. CPS Pointer	http://www.izenpe.com/cpscorppriv
10.4.2.2. User Notice	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
10.5. Subject Alternate Names	5.5.10
10.5.1. rfc822Name	Dirección de correo electrónico
10.5.2. UserPrincipalName	Usuario@dominio
10.6. Issuer Alternative Name	5.5.11
10.6.1. dNSName	http://www.izenpe.com
10.7. Extended Key Usage	5.5.12
10.7.1. emailProtection	1.3.6.1.5.5.7.3.4
10.7.2. clientAuth	1.3.6.1.5.5.7.3.2



Campo	Contenido
10.7.3. smartcardlogon	1.3.6.1.4.1.311.20.2.2
10.8. cRLDistributionPoint	5.5.13
10.8.1. distributionPoint	http://crl.izenpe.com/cgi-bin/crlscinr
10.9. NetscapeCertType	SSL client, SMIME client
10.10. Authority Information Access	5.5.14
10.10.1. Access Description	5.5.15
10.10.1.1. Access Method	1.3.6.1.5.5.7.1.48.1
10.10.1.2. accessLocation	http://ocsp.izenpe.com:8094