



DOCUMENTACIÓN ESPECÍFICA PARA EL CERTIFICADO DE ENTIDAD

Referencia: IZENPE-Doc. Entidad
Nº Versión: v 4.0
Fecha: 26 de octubre de 2006

© IZENPE 2007

Este documento es propiedad de IZENPE. Este documento puede ser reproducido, sólo 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 del certificado de Entidad* emitido por Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, S.A. (en adelante, IZENPE).

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

Esta *Documentación* regula de forma específica las remisiones que la *Declaración de Prácticas de Certificación* hace a esta *Documentación específica del certificado de Entidad*.

1.1 Presentación

IZENPE emite el certificado de Entidad en el ámbito del Servicio de Certificación Digital, consistente en la emisión al público de certificados que permitirán a sus poseedores mantener relaciones telemáticas con las Entidades Usuarias e Instituciones Públicas y Privadas en general que hayan admitido su uso bien a través del correspondiente convenio o contrato suscrito con IZENPE, bien a través de cualquier otro medio. Los convenios o contratos suscritos con las instituciones privadas o los instrumentos en las que éstas admitan el uso de los certificados de referencia definirán los ámbitos de uso del certificado, que en todo caso estarán vinculados a servicios públicos.

La identidad y cualquier información que debe contenerse en el certificado serán comprobadas necesariamente por una Entidad de Registro. En cuanto a las actuaciones como Entidad de Registro de los certificados podrán ser desempeñadas por IZENPE o por las Entidades Usuarias con las que IZENPE suscriba el correspondiente convenio.

1.1.1 Descripción del certificado

El certificado Entidad se configura como un certificado de firma electrónica, con la consideración legal de certificado reconocido, de acuerdo con lo establecido en los artículos 7, 8, 11, 12, 13, 18 y 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

Este certificado se emite en tarjeta criptográfica y en soporte software.

El solicitante, responsable de la custodia de los datos de creación de firma, será el poseedor de claves y su identidad se incluirá en el certificado electrónico. Se entenderán hechos por la Entidad los actos en los que se hubiera utilizado la firma electrónica.



1.2 Identificación

Con el objeto de identificar el certificado del tipo Entidad, IZENPE le ha asignado el siguiente identificador del objeto (OID).

CERTIFICADO	OID
Certificado de Entidad (tarjeta criptográfica)	1.3.6.1.4.1.14777.2.7
Certificado de Entidad (soporte software)	1.3.6.1.4.1.14777.2.8

Al tratarse de un certificado con la consideración de reconocido incorpora, 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 aplicabilidad

1.3.1 Usuarios de los certificados

Las Entidades finales usuarias de los certificados de Entidad son las personas y organizaciones destinatarias de los servicios de emisión, gestión y uso de certificados digitales.

Serán Entidades finales del sistema de certificación de las Entidades Usuarias las siguientes entidades:

1. Solicitantes de certificados
2. Firmante del certificado
3. Suscriptores de certificados
4. Poseedores de claves
5. Terceros que confían en los certificados

1.3.1.1 Solicitantes de certificados

El certificado de Entidad debe ser solicitado por una persona, en su propio nombre o en nombre de una organización.



Pueden ser solicitantes:

1. La persona que va a ser el futuro suscriptor del certificado
2. Una persona autorizada por el futuro suscriptor
3. Una persona autorizada por la Entidad de Registro
4. Una persona autorizada por el Prestador de Servicios de Certificación

1.3.1.2 Firmante

El firmante es la entidad identificada en el certificado.

1.3.1.3 Suscriptores de certificados

El suscriptor será la persona jurídica identificada en el certificado.

1.3.1.4 Poseedores de claves

Los poseedores de claves son las personas físicas que poseen o responden de la custodia de las claves de firma digital.

1.3.2 Aplicabilidad

1.3.2.1 Ámbito de uso de los certificados

Los certificados del tipo Entidad, serán utilizados por los suscriptores en las relaciones que mantengan con las Entidades Usuarias e Instituciones Públicas y Privadas en general que hayan admitido su uso.

Los convenios o contratos suscritos con las instituciones privadas o los instrumentos en las que éstas admitan el uso de los certificados de referencia definirán los ámbitos de uso del certificado, que en todo caso estarán vinculados a servicios públicos.

1.4 Disposiciones generales

1.4.1 Obligaciones de identificación

IZENPE comprueba en los registros correspondientes, por si misma o por medio de las Entidades Usuarias con las que suscriba el correspondiente convenio, la identidad y cualesquiera otras circunstancias personales de los solicitantes, suscriptores y poseedores de claves de los certificados, relevantes para el fin propio de éstos.



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

1.4.2 Obligaciones del suscriptor del certificado

En el supuesto del Certificado de Entidad, son obligaciones del solicitante las recogidas en el apartado 2.1.5 de la Declaración de Prácticas de Certificación, salvo las establecidas en las letras a), b), y j).

1.4.3 Responsabilidad civil del suscriptor de certificado

Respecto a las obligaciones inherentes a la condición de suscriptor, 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 Identificación y autenticación

2.1 Registro inicial

2.1.1 Tipos de nombres

El nombre distinguido del campo Subject Name de los certificados de Entidad consiste en el nombre legal de la organización o unidad de dicha organización.

2.1.1.1 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 del certificado de Entidad son los recogidos en el apartado correspondiente al perfil del certificado.

2.1.1.2 Significado de los nombres

No se pueden emplear seudónimos.

El nombre del poseedor de claves en los certificados de Entidad, cuyo suscriptor es una persona jurídica, está compuesto por el nombre y apellidos del poseedor, junto con su número de D.N.I./Pasaporte o N.I.E.

2.1.1.3 Resolución de conflictos relativos a nombres

En los certificados de Entidad, 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.

2.1.2 Autenticación de la identidad de una organización

Para la emisión de certificados de Entidad, la Entidad de Registro comprobará:

- La documentación acreditativa de la constitución de la Entidad que figura en dicho certificado.
- La identidad de la persona que solicite el certificado de acuerdo con la sección siguiente (apartado 3.1.9 *Autenticidad de la identidad de una persona física*)
- Y cuando ésta sea necesaria, su inscripción en el registro público que corresponda.

En concreto, la Entidad de Registro comprueba la documentación justificativa aportada por el solicitante, acerca de los siguientes extremos:



- a. Nombre legal completo de la organización
- b. Estado legal de la organización
- c. Número de identificación fiscal
- d. Datos de identificación registral, en su caso.

Para realizar la comprobación de los datos relativos a la constitución y personalidad jurídica se harán las consultas pertinentes en los Registros Públicos siempre que sean de inscripción obligatoria.

La Entidad de Registro dejará constancia de las comprobaciones efectuadas.

2.1.3 Autenticación de la identidad de una persona física

2.1.3.1 Sujetos de identificación

IZENPE identificará al solicitante del certificado de Entidad.

2.1.3.2 Elementos de identificación requeridos

Para acreditar la identidad del solicitante, se requerirá la siguiente documentación:

- a. DNI o pasaporte, 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 un NIE acompañado de un documento de identidad en vigor a efectos de comprobación de su identidad.
 - II. En relación a ciudadanos extracomunitarios, será exigible la tarjeta de residencia.
- c. Documento público que acredite la condición de administrador, representante legal o voluntario con poder bastante a efectos de solicitar el certificado, del que habrá de mostrar original o copia auténtica con los sellos de inscripción en el registro público, en caso de inscripción obligatoria.

2.1.3.3 Acreditación de los elementos de identificación

La Entidad de Registro procederá a la comprobación de la documentación señalada en el apartado anterior dejando constancia documental de que se ha efectuado.

En particular para realizar la comprobación de los datos relativos a la extensión y vigencia de los poderes de inscripción obligatoria mencionados en el apartado anterior de harán las consultas pertinentes en los Registros Públicos.



2.1.3.4 Necesidad de presencia personal

La identificación y acreditación del solicitante exige su personación ante la Entidad de Registro, de la cual dejará constancia.

Podrá prescindirse de dicha personación, si la firma de la solicitud de expedición del certificado:

- ha sido legitimada en presencia notarial
- 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.

2.2 Autenticación de una petición de revocación, suspensión o reactivación

2.2.1 Petición de revocación

El solicitante de la revocación de un certificado debe personarse ante una Entidad de Registro e:

- Identificarse, presentando los documentos de identificación requeridos a efectos de autenticación de la identidad de una persona física (ver apartado 3.1.9.2).
- Y justificar la solicitud de revocación, si fuera necesario, aportando la documentación que acredite la existencia del hecho que origina la pérdida de vigencia del certificado.

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

Se autentica la identidad de los administradores a través de control de acceso utilizando SSL y autenticación de cliente, antes de permitir que se realicen funciones de revocación / suspensión.

2.2.2 Petición de suspensión

El poseedor de claves podrá solicitar la suspensión vía telefónica (tfno. 902 542 542) identificándose y dando su contraseña de identificación telefónica o en su defecto los datos requeridos por IZENPE que permiten la correcta identificación del solicitante.

2.2.3 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 personarse ante una Entidad de Registro e identificarse, presentando los documentos requeridos a efectos de autenticación de la identidad de una persona física (ver apartado 3.1.9.2).



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:

- Vía telemática: en la dirección web <http://www.izenpe.com> los interesados disponen del formulario de solicitud, que podrá ser rellenado y enviado telemáticamente a la Entidad de Registro la cual lo almacenará como un prerregistro.

(*) Transcurrido un mes desde la realización del prerregistro, si el solicitante no se personara en cualquiera de las oficinas de la Entidad de Registro para realizar la solicitud efectiva del certificado, se procederá a eliminar sus datos del prerregistro.

- 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.

En caso de que el certificado de Entidad se emita en soporte software adicionalmente, el poseedor de claves deberá generar un par de claves en el propio servidor entregando a IZENPE la clave pública junto con el formulario de solicitud.

3.1.1 Acreditación de la identidad del solicitante

Elementos de identificación

El solicitante del certificado deberá personarse ante la Entidad de Registro y presentar original o copia auténtica de la siguiente documentación:

- a. DNI o pasaporte, 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 un NIE acompañado de un documento de identidad en vigor a efectos de comprobación de su identidad.
 - 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](#).
- 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 Entidad de Registro levantará acta de comprobación de la identidad del solicitante.

3.1.2 Acreditación de la identidad de la organización

Documento que acredite la válida constitución de la persona jurídica y poder bastante del solicitante

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

Documentación acreditativa de la válida constitución de la persona jurídica

- Número de Identificación Fiscal (N.I.F.) de la Entidad.
- Las sociedades mercantiles y demás personas jurídicas cuya inscripción sea obligatoria en el Registro Mercantil, acreditarán la válida constitución mediante la aportación de original o copia auténtica de un certificado del Registro Mercantil relativo a los datos de constitución y personalidad jurídica de las mismas.
- Las Asociaciones, Fundaciones y Cooperativas acreditarán la válida constitución mediante la aportación de original o copia auténtica de un certificado del registro público donde consten inscritas, relativo a su constitución.
- Las sociedades civiles y demás personas jurídicas, aportarán original o copia auténtica del documento público que acredite su constitución de manera fehaciente.

Documentación acreditativa del poder bastante del solicitante

Documento que acredite el poder bastante a los efectos de solicitar el certificado electrónico. A tal fin,

- Además de los administradores y representantes legales,
- Se considera que tienen poder bastante los representantes voluntarios cuando tengan otorgado un poder específico, claramente determinado



y enunciado expresamente para solicitar certificado electrónico, en nombre y representación de la persona jurídica.

El solicitante del certificado deberá aportar la siguiente documentación:

- Si es administrador o representante legal de una persona jurídica sujeta a inscripción registral, deberá aportar 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.
- Si el solicitante es representante voluntario de la misma deberá aportar original o copia auténtica del poder notarial que contenga una cláusula especial para solicitar el Certificado Electrónico.

La Entidad de Registro levantará acta de comprobación de la documentación presentada por el solicitante apoderado.

3.2 Emisión de certificado

Acreditada la identidad del solicitante ante la Entidad de Registro, éste deberá firmar la solicitud de emisión del certificado, aceptando de esta forma el [contrato de suscriptor](#).

3.3 Entrega de certificado

La Entidad de Registro entregará al solicitante el certificado, pudiendo optar el solicitante entre las siguientes vías:

1 Certificado emitido en tarjeta criptográfica

Si el certificado se emite en tarjeta criptográfica, el solicitante podrá optar por una de las dos vías siguientes:

1. Entrega en el momento de la emisión del certificado, el PIN y el código de desbloqueo del PIN (PUK), la hoja en la que figura la contraseña de identificación telefónica y se le informará de las [condiciones de uso](#) del certificado. En este momento, el solicitante deberá firmar la [Hoja de Entrega y Aceptación](#).
2. Entrega personal del certificado al solicitante en la dirección postal de entrega determinada en la solicitud de emisión. El solicitante deberá devolver firmada a IZENPE la Hoja de Entrega y Aceptación en el plazo máximo de 1 mes, en caso contrario se revocará el certificado.



Y envío a la dirección postal de la entidad indicada por el solicitante en la Solicitud de Emisión del Certificado, del PIN y el código de desbloqueo del PIN (PUK), de la hoja en la que figura la contraseña de identificación telefónica informándole de las condiciones de uso del certificado.

2 Certificado emitido en soporte software

En el caso de que el certificado se emita en soporte software IZENPE entregará al solicitante el certificado y se le informará de las condiciones de uso del certificado.

El solicitante deberá devolver firmada a IZENPE la [Hoja de Entrega y Aceptación](#) en el plazo máximo de 1 mes, en caso contrario se revocará el certificado.

3.4 Suspensión de certificados

El poseedor de claves podrá solicitar la suspensión del certificado cuando quiera, y en cualquier caso en los supuestos de pérdida o robo llamando al teléfono 902 542 542, identificándose dando:

- La contraseña de la identificación telefónica o en su defecto los datos requeridos por IZENPE que permiten la correcta identificación del solicitante.
- Elementos de identificación requeridos para acreditar la identidad del solicitante (ver apartado 4.1.1 *Acreditación de la identidad del solicitante*).
- CIF de la entidad.

3.4.1 Entidad solicitante de la suspensión

Podrán suspender el certificado:

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

3.4.2 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.

3.5 Revocación de certificados

El solicitante de la revocación deberá personarse en cualquiera de las oficinas de la Entidad Registro, para, una vez identificado mediante la documentación acreditativa de su identidad (ver apartado 4.1.1 *Acreditación de la identidad del solicitante*) rellenar la [solicitud de revocación](#) del certificado y si fuera necesario entregar la documentación que acredita la causa de la revocación.

Las causas de revocación y quienes pueden solicitarla pueden consultarse la Declaración de Prácticas de Certificación.

3.6 Reactivación

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

El poseedor de claves solicitará la reactivación del certificado personándose ante una Entidad de Registro, donde deberá identificarse mediante la documentación acreditativa de su identidad (ver apartado 4.1.1 *Acreditación de la identidad del solicitante*) y entregar la [solicitud de reactivación](#) correctamente cumplimentada.

3.7 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 Perfiles de certificados y listas de certificados revocados

4.1 Perfil de certificado de entidad (en tarjeta)

Usos: firma, ssl

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)	NZZ Ziurtagiri Publikoa - Certificado publico SCI
1.5.5. Common Name (CN)	Herritar eta erakundeen CA - CA de ciudadanos y entidades
1.5.6. EmailAddress	info@izenpe.com
1.6. Validity	3 años
1.6.1. Not Before	e.g., "00:00:01 01 September 1999"
1.6.2. Not After	e.g., "23:59:59 31 August 2003"



Campo	Contenido
1.7. Subject	
1.7.1. countryname	ES
1.7.2. Organization (O)	Razón Social registrada de la entidad.
1.7.3. Organizational Unit (OU)	Ziurtagiri onartua - Certificado reconocido
1.7.4. Organizational Unit (OU)	<u>Entitatearen ziurtagiria</u> - Certificado de entidad
1.7.5. Organizational Unit (OU)	Condiciones de uso en www.izenpe.com nola erabili jakiteko
1.1.1. dnQualifier	CIF de la empresa (* formato : -CIF Lnnnnnnn
1.7.6. Common Name (CN)	Razón Social
1.7.7. givenName	Nombre propio del responsable (como consta en el dni)
1.7.8. surName	Apellidos del responsable (como constan en el DNI)
1.7.9. serialNumber	NIF o CIF de la entidad jurídica
1.7.10. 1.3.6.1.4.1.18838.1.1	NIF o NIE del responsable
1.8. Subject Public Key Info	1024-Bit clave pública codificado conforme con RFC2459 & PKCS#1
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	



Campo	Contenido
2.2.1. Key Identifier	Identificador de la clave pública del suscriptor
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	No seleccionado "0"
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
2.5. Certificate Policies	
2.5.1. Policy Identifier	1.3.6.1.4.1.14777.2.7
2.5.2. Policy Qualifier ID	
2.5.2.1. CPS Pointer	http://www.izenpe.com/rpaentidad
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	
2.7. Issuer Alternative Name	



Campo	Contenido
2.7.1. dNSName	http://www.izenpe.com
2.8. Extended Key Usage	
2.8.1. clientAuth	1.3.6.1.5.5.7.3.2
2.9. cRLDistributionPoint	
2.9.1. distributionPoint	http://crl.izenpe.com/cgi-bin/crl
2.10. NetscapeCertType	SSL 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
2.11.1.3.	



4.2 Perfil de certificado de entidad (servidor)

Usos: firma, ssl

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)	NZZ Ziurtagiri Publikoa - Certificado publico SCI
3.5.5. Common Name (CN)	Herritar eta erakundeen CA - CA de ciudadanos y entidades
3.5.6. EmailAddress	info@izenpe.com
3.6. Validity	3 años
3.6.1. Not Before	e.g., "00:00:01 01 September 1999"
3.6.2. Not After	e.g., "23:59:59 31 August 2003"
3.7. Subject	
3.7.1. countryname	ES



Campo	Contenido
3.7.2. Organization (O)	Razón Social registrada de la entidad.
3.7.3. Organizational Unit (OU)	Condiciones de uso en www.izenpe.com nola erabili jakiteko
3.7.4. Organizational Unit (OU)	<u>Entitatearen ziurtagiria</u> - Certificado de entidad
3.7.5. Organizational Unit (OU)	Ziurtagiri onartua - Certificado reconocido
1.1.2. dnQualifier	CIF de la empresa (* formatu : -CIF Lnnnnnnn
3.7.6. Common Name (CN)	Razón Social
3.7.7. givenName	Nombre propio del responsable (como consta en el dni)
3.7.8. surName	Apellidos del responsable (como constan en el DNI)
3.7.9. serialNumber	NIF o CIF de la entidad jurídica
3.7.10. 1.3.6.1.4.1.18838.1.1	NIF o NIE del responsable
3.8. Subject Public Key Info	1024-Bit clave pública codificado conforme con 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 suscriptor
4.3. Key Usage	



Campo	Contenido
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. Qualified Certificate Statements	
4.4.1. qCStatement OID	0.4.0.1862.1
4.5. Certificate Policies	
4.5.1. Policy Identifier	1.3.6.1.4.1.14777.2.8
4.5.2. Policy Qualifier ID	
4.5.2.1. CPS Pointer	http://www.izenpe.com/rpaentidadser
4.5.2.2. User Notice	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
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
4.7.2. clientAuth	1.3.6.1.5.5.7.3.2



Campo	Contenido
4.8. cRLDistributionPoint	
4.8.1. distributionPoint	http://crl.izenpe.com/cgi-bin/crl
4.9. NetscapeCertType	SMIME
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
4.10.1.3.	