



DOCUMENTACIÓN ESPECÍFICA PARA EL CERTIFICADO CORPORATIVO RECONOCIDO

Referencia: IZENPE-Doc. Corporativo rec.
Nº Versión: v 11
Fecha: 16 de noviembre de 2009

© IZENPE 2009

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 del certificado Corporativo reconocido* 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 Corporativo reconocido*.

1.1 Presentación

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

En el caso de que la Entidad Pública desempeñe potestades administrativas, además de actuar como suscriptor de los certificados realizará las funciones de identificación de los poseedores de claves pertenecientes a dicha Entidad.

Si la Entidad Pública Usuaria suscriptora de los certificados no desempeña potestades administrativas, las funciones de identificación de los titulares de los certificados serán realizadas por las Entidades de Registro.

1.1.1 Descripción del certificado

El certificado Corporativo reconocido identifica a personas que desempeñan cargos o puestos en Entidades Públicas que no ejercen potestades administrativas. Se trata de un certificado en el que el suscriptor será la entidad usuaria.

En este certificado se identifica la Entidad Pública de pertenencia así como en su caso el cargo o puesto desempeñado.

Este certificado se emite en tarjeta criptográfica.

El personal al servicio de una Entidad Pública 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.

1.2 Identificación

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

CERTIFICADO	OID
Certificado Corporativo reconocido	1.3.6.1.4.1.14777.4.2

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 Tendrán la condición de partes intervinientes,

1. Solicitantes de certificados
2. Firmante del certificado
3. Suscriptores de certificados
4. Poseedores de claves

1.3.1.1 Solicitantes de certificados

El certificado Corporativo reconocido debe ser solicitado por una persona en su propio nombre o en el 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 persona física identificada en el certificado.

1.3.1.3 Suscriptores de certificados

El suscriptor es 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.

El poseedor de claves será el firmante.

1.3.2 Aplicabilidad

Los certificados del tipo Corporativo reconocido serán utilizados en el ámbito de las competencias propias del órgano administrativo y del 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 en los convenios o contratos suscritos con las instituciones privadas o los instrumentos en las que éstas admitan el uso de los certificados de referencia que definirán los ámbitos de uso del certificado, que en todo caso estarán vinculados a servicios públicos.



2 Disposiciones generales

2.1 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.

2.1.1 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.



3 Identificación y autenticación

3.1 Registro inicial

3.1.1 Tipos de nombres

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

3.1.1.1 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 Corporativo reconocido son los recogidos en el apartado correspondiente al perfil del certificado.

3.1.1.2 Significado de los nombres

No se pueden emplear seudónimos.

El nombre del poseedor de claves en los certificados Corporativos reconocidos, 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.

3.1.1.3 Resolución de conflictos relativos a nombres

En los certificados Corporativos reconocidos 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.

3.1.2 Autenticación de la identidad de una organización

Para la emisión de certificados del tipo Corporativo reconocido, 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 *Documentación específica del certificado Corporativo reconocido*)
- 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.

3.1.3 Autenticación de la identidad de una persona física

3.1.3.1 Sujetos de identificación

IZENPE identificará al solicitante del certificado.

3.1.3.2 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.



3.1.3.3 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 se harán las consultas pertinentes en los Registros Públicos.

3.1.3.4 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.

3.2 Autenticación de una petición de revocación, suspensión o reactivación

3.2.1 Petición de revocación

3.2.1.1 Podrán solicitar la revocación de un certificado

- El suscriptor del certificado.
- El solicitante.
- El poseedor de claves.
- IZENPE.
- Tercero autorizado por el solicitante.



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

3.2.2 El solicitante de la revocación deberá 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.

3.2.3 Petición de suspensión

El suscriptor podrá solicitar la suspensión vía telefónica (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.

3.2.4 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).



4 Requisitos operativos

4.1 Solicitud de certificado

La Entidad Pública solicitante deberá rellenar el formulario de [solicitud del certificado](#), para las personas físicas que desempeñan cargos o puestos en su organización que estimen oportuno, y tramitarlo ante IZENPE (o Entidad Pública Usuaria con la que IZENPE suscriba el correspondiente convenio) 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.

El suscriptor del certificado será la Entidad pública solicitante que no ejerce potestades administrativas y el poseedor de claves será la persona física que desempeña un cargo o puesto en la Entidad, cuya identidad y cargo o puesto constarán en el certificado en el caso en el que de forma voluntaria desee que este dato conste en el certificado.

4.1.1 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) Asimismo el solicitante a través de la solicitud de emisión del certificado acreditará ante la Entidad de Registro, de cada uno de los futuros poseedores de claves:

- Identidad
- Adscripción a la Entidad pública solicitante.
- Justificación del cargo o puesto desempeñado, en su caso.

La Entidad de Registro levantará acta de comprobación de la identidad del solicitante.

4.1.2 Acreditación de la identidad de la organización

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

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

1) 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 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

2) Documentación acreditativa del poder suficiente del solicitante

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

- 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.

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 de la escritura pública o documento oficial donde derive la representación con expresión de sus facultades y su vigencia.

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 acreditará la comprobación de la documentación presentada por el solicitante apoderado.

4.2 Acreditación de la identidad de los poseedores de claves

El poseedor de claves acreditará su identidad ante la Entidad de Registro y presentará, a estos efectos, la misma documentación requerida al solicitante (ver apartado 4.1.1).

Así mismo presentarán ante la Entidad de Registro la solicitud firmada por el solicitante y por la Entidad de Registro en la que constan sus datos, así como copia firmada de la solicitud inicial de emisión del certificado.

4.3 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](#).

4.4 Entrega de certificado

La Entidad de Registro entregará el certificado al poseedor de claves, que podrá optar por las siguientes vías:

1. Entrega en el momento de la emisión el certificado, el PIN y el código de desbloqueo del PIN (PUK) así como una hoja en la que figura la contraseña de identificación telefónica y se le informará de las [condiciones de uso](#) del certificado. Así mismo, el poseedor de claves 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 del certificado y envío por correo ordinario del el PIN y el código de desbloqueo del PIN (PUK) así como una hoja en la que figura la contraseña de identificación telefónica y se le informará de las condiciones de uso del certificado. Así mismo, el poseedor de claves deberá firmar la Hoja de Entrega y Aceptación.

4.5 Suspensión de certificados

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

- Contraseña de Identificación Telefónica o, en su defecto, los datos requeridos por IZENPE que permitan 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*).

4.5.1 Entidad solicitante de la suspensión

Podrán suspender el certificado:

- El poseedor de claves.
- Entidad de Registro.

4.5.2 Plazo máximo temporal de suspensión

El plazo máximo de la suspensión es de quince días naturales desde que sea solicitada por el suscriptor del certificado.

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

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



4.6 Revocación de certificados

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

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

4.7 Reactivación

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

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

4.8 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.

Las modificaciones de este documento serán aprobadas por el Director General de IZENPE con el visto bueno del Comité de Seguridad de IZENPE. Estas modificaciones estarán recogidas en un documento de Actualización de Documentación Específica por certificado cuyo mantenimiento está garantizado por IZENPE.

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

Las modificaciones de este documento serán aprobadas por el Director General de IZENPE con el visto bueno del Comité de Seguridad de IZENPE. Estas modificaciones



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

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



5 Gestión del cambio

Las modificaciones de este documento serán aprobadas por el Director General de IZENPE con el visto bueno del Comité de Seguridad de IZENPE. Estas modificaciones estarán recogidas en un documento de Actualización de Documentación Específica por certificado cuyo mantenimiento está garantizado por IZENPE.

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



6 Perfiles de certificados y listas de certificados revocados

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

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
1.6.2. Not After	Fecha fin validez del certificado



Campo	Contenido
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)	Ziurtagiri korporatibo onartua – Cert. corporativo reconocido
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
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



Campo	Contenido
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
2.5. Certificate Policies	
2.5.1. Policy Identifier	1.3.6.1.4.1.14777.4.2
2.5.2. Policy Qualifier ID	
2.5.2.1. CPS Pointer	http://www.izenpe.com/rpascacorrec
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



Campo	Contenido
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	
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