



DOCUMENTACIÓN ESPECÍFICA PARA EL CERTIFICADO DE CIUDADANO

Referencia: IZENPE-Doc. Ciudadano
Nº Versión: v4.0
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 Ciudadano* 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 Ciudadano.

1.1 Presentación

IZENPE emite el certificado de Ciudadano 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 Usuaris 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 Usuaris con las que IZENPE suscriba el correspondiente convenio.

1.1.1 Descripción del certificado

El certificado de Ciudadano se configura como un 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.

Este certificado se emite en tarjeta criptográfica.



1.2 Identificación

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

CERTIFICADO	OID
Certificado de Ciudadano	1.3.6.1.4.1.14777.2.1
Certificado de Ciudadano DPC 2.0	1.3.6.1.4.1.14777.2.6

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 Ciudadano 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 Ciudadano debe ser solicitado por una persona en su propio nombre.

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

Los suscriptores son las personas físicas identificadas 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

1.3.2.1 Ámbito de uso de los certificados

Los certificados del tipo Ciudadano serán utilizados por los suscriptores en las relaciones que mantengan con las Entidades Usuarías 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.



2 Identificación y autenticación

2.1 Registro inicial

2.1.1 Tipos de nombres

El nombre diferenciado del campo Subject Name incluye un componente Common Name (CN).

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 Ciudadano son los recogidos en el apartado correspondiente al perfil del certificado.

2.1.2 Significado de los nombres

No se pueden emplear seudónimos.

En los certificados de Ciudadano en los que el suscriptor es una persona física, el nombre del suscriptor está compuesto por su nombre y apellidos, junto con su número de D.N.I./Pasaporte o N.I.E.

2.1.3 Resolución de conflictos relativos a nombres

En los certificados de Ciudadano cuyo suscriptor es una persona física, los conflictos de nombres de suscriptores que aparezcan identificados en los certificados con su nombre real se solucionan mediante la inclusión, en el nombre diferenciado del certificado, del DNI o pasaporte del suscriptor, el NIE u otro identificador asignado por el suscriptor, de acuerdo con lo establecido en el apartado precedente.

2.1.4 Autenticación de la identidad de una persona física

2.1.4.1 Sujetos de identificación

IZENPE identificará al solicitante del certificado de Ciudadano.

2.1.4.2 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.

2.1.4.3 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.

2.1.4.4 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 3.1.1)



- 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 suscriptor 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.

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 3.1.1).



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 puede 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 puede personarse en cualquiera de las Entidades de Registro señaladas en el listado publicado en <http://www.izenpe.com> y realizar la solicitud de certificado.

3.1.1 Acreditación de la identidad del solicitante

Documentación necesaria

El solicitante, futuro suscriptor 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.



Será requisito para la solicitud que el futuro suscriptor del certificado sea mayor de 16 años.

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.

3.2 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. 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 del certificado, diferenciándose dos momentos:
 - a) 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.



- b) Envío, a la dirección postal del solicitante que consta 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.

3.4 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 3.1.1 *Acreditación de la identidad del solicitante*).
- Fecha de nacimiento.

3.4.1 Entidad solicitante de la suspensión

Podrán suspender el certificado:

- El suscriptor a nombre del cual se ha emitido el certificado.
- 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 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.

3.5 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 3.1.1) 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.

3.6 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 3.1.1), 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

Desde el comienzo de los servicios de Izenpe y hasta la modificación de la DPC versión 2.0 se emitieron certificados bajo este perfil, cuyo OID es 1.3.6.1.4.1.14777.2.1.

Campo	Contenido
X.509v1 Field	
Version	v3
Serial Number	Asignado automáticamente por la CA emisora
Signature Algorithm	SHA-1 con Firma RSA
Signature Value	Firma codificada como cadena de bits
Issuer Distinguished Name	
Country (C)	España
Locality	Avenida del Mediterráneo, 3 – 01010, Vitoria-Gasteiz
Organization (O)	IZENPE S.A.-CIF A-01337260 – RMerc. Vitoria-Gasteiz T1055 F62 S8
Organizational Unit (OU)	NZZ Ziurtagiri Publikoa - Certificado publico SCI
Common Name (CN)	Herritar eta erakundeen CA - CA de ciudadanos y entidades
EmailAddress	info@izenpe.com



Validity	3 años
Not Before	e.g., "00:00:01 01 September 1999"
Not After	e.g., "23:59:59 31 August 2003"
Subject	
Organizational Unit (OU)	Condiciones de uso en www.izenpe.com nola erabili jakiteko
Organizational Unit (OU)	Certificado reconocido de ciudadano Herritar ziurtagiri onartua
dnQualifier	NIF, NIE (*) del suscriptor (*) formato : -dni nnnnnnnnL o -nie XnnnnnnnnL
Common Name (CN)	Nombre y Apellidos del suscriptor, tal como constan en el DNI
Subject Public Key Info	1024-Bit clave pública codificada conforme con RFC2459 & PKCS#1
X.509v3 Extensions	
Authority Key Identifier	
Key Identifier	Identificador de la clave pública del emisor
AuthorityCertIssuer	Nombre de la CA a la que corresponde la clave identificada en keyIdentifier
AuthorityCertSerialNumber	Número de serie del certificado de CA
Subject Key Identifier	



Key Identifier	Identificador de la clave pública del suscriptor
Key Usage	
Digital Signature	Seleccionado "1"
Non Repudiation	No seleccionado "0"
Key Encipherment	Seleccionado "1"
Data Encipherment	No seleccionado "0"
Key Agreement	No seleccionado "0"
Key Certificate Signature	No seleccionado "0"
CRL Signature	No seleccionado "0"
Qualified Certificate Statements	
qCStatement OID	0.4.0.1862.1
Certificate Policies	
Policy Identifier	1.3.6.1.4.1.14777.2.1
Policy Qualifier ID	
CPS Pointer	http://www.izenpe.com/rpaciudadano
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
Subject Alternate Names	
Issuer Alternative Name	
dNSName	www.izenpe.com



Extended Key Usage	
clientAuth	1.3.6.1.5.5.7.3.2
cRLDistributionPoint	
distributionPoint	http://crl.izenpe.com/cgi-bin/crl
NetscapeCertType	SSL client
Subject Directory Attributes	
Date of Birth	12-06-2000
Authority Information Access	
Access Description	
Access Method	1.3.6.1.5.5.7.1.48.1
accessLocation	http://ocsp.izenpe.com:8094



4.1 Perfil de certificado de ciudadano DPC 2.0

Este es el perfil con el que se emiten actualmente los certificados de ciudadano OID 1.3.6.1.4.1.14777.2.6.

Usos: firma, ssl

Campo	Contenido
X.509v1 Field	
Versión	V3
Serial Number	Asignado automáticamente por la CA emisora
Signature Algorithm	SHA-1 con Firma RSA
Signature Value	Firma codificada como cadena de bits
Issuer Distinguished Name	
Country (C)	España
Locality	Avenida del Mediterráneo, 3 – 01010, Vitoria-Gasteiz
Organization (O)	IZENPE S.A.-CIF A-01337260 – RMerc. Vitoria-Gasteiz T1055 F62 S8
Organizational Unit (OU)	NZZ Ziurtagiri Publikoa - Certificado publico SCI
Common Name (CN)	Herritar eta erakundeen CA - CA de ciudadanos y entidades
EmailAddress	info@izenpe.com
Validity	3 años
Not Before	e.g., "00:00:01 01 September 1999"



Campo	Contenido
Not After	e.g., "23:59:59 31 August 2003"
Subject	
CountryName	ES
Organizational Unit (OU)	Ziurtagiri onartua - Certificado reconocido
Organizational Unit (OU)	Herritar ziurtagiria - Certificado de ciudadano
Organizational Unit (OU)	Condiciones de uso en www.izenpe.com nola erabili jakiteko
dnQualifier	NIF, NIE (*) del suscriptor + TIS del usuario (opcional) (*) formato : -dni nnnnnnnnL o -nie XnnnnnnnnL -TIS nnnnnnnn
Common Name (CN)	Nombre y Apellidos del suscriptor, tal como constan en el DNI
givenName	Nombre del suscriptor, tal como consta en el DNI
surname	Apellidos del suscriptor, tal como constan en el DNI
serialNumber	NIF o NIE del suscriptor
Subject Public Key Info	1024-Bit clave pública codificada conforme con RFC2459 & PKCS#1
X.509v3 Extensions	
Authority Key Identifier	
Key Identifier	Identificador de la clave pública del emisor
AuthorityCertIssuer	Nombre de la CA a la que corresponde la clave identificada en keyIdentifier



Campo	Contenido
AuthorityCertSerialNumber	Número de serie del certificado de CA
Subject Key Identifier	
Key Identifier	Identificador de la clave pública del suscriptor
Key Usage	
Digital Signature	Seleccionado "1"
Non Repudiation	No seleccionado "0"
Key Encipherment	Seleccionado "1"
Data Encipherment	No seleccionado "0"
Key Agreement	No seleccionado "0"
Key Certificate Signature	No seleccionado "0"
CRL Signature	No seleccionado "0"
Qualified Certificate Statements	
qCStatement OID	0.4.0.1862.1
Certificate Policies	
Policy Identifier	1.3.6.1.4.1.14777.2.6
Policy Qualifier ID	
CPS Pointer	http://www.izenpe.com/rpaciudadano
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
Subject Alternate Names	



Campo	Contenido
rfc822Name	
Issuer Alternative Name	
dNSName	http://www.izenpe.com
Extended Key Usage	
clientAuth	1.3.6.1.5.5.7.3.2
cRLDistributionPoint	
distributionPoint	http://crl.izenpe.com/cgi-bin/crl
NetscapeCertType	SSL client
Subject Directory Attributes	
Date of Birth	12-06-2000
Authority Information Access	
Access Description	
Access Method	1.3.6.1.5.5.7.1.48.1
accessLocation	http://ocsp.izenpe.com:8094