



# DOCUMENTACIÓN ESPECÍFICA PARA EL CERTIFICADO DE PERSONAL DE LAS ENTIDADES PÚBLICAS

Referencia: IZENPE-Doc. Certificado PEP.  
Nº Versión: v 4.1  
Fecha: 16 de octubre de 2007

---

© IZENPE 2007

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](http://www.izenpe.com)  
[info@izenpe.com](mailto:info@izenpe.com)  
Tel.: 945 017 490



# 1 Introducción

---

El presente documento recoge la *Documentación específica del certificado Personal de las Entidades Públicas* 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 Personal de las Entidades Públicas*.

## 1.1 Presentación

IZENPE emite el certificado Personal de las Entidades Públicas 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 de Personal de las Entidades Públicas identifica a personas que desempeñan cargos o puestos en Entidades Públicas que ejercen potestades administrativas.

Este certificado se emite en tarjeta criptográfica.

Identifica la entidad pública de pertenencia así como, en su caso, el cargo desempeñado.

El personal al servicio de las entidades públicas 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.

## 1.2 Identificación

Con el objeto de identificar el certificado del tipo Personal de las Entidades Públicas, IZENPE le ha asignado el siguiente identificador de objeto (OID).

CERTIFICADO	OID
Certificado Personal de las Entidades Públicas	1.3.6.1.4.1.14777.4.1

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 Personal de las Entidades Públicas 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 Personal de las Entidades Públicas 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**

### **1.3.2.1 Ámbito de uso de los certificados**

Los certificados del tipo Personal de las Entidades Públicas serán utilizados en el ámbito de las competencias propias de la entidad usuaria o 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.

### **2.2 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 diferenciado del campo Subject Name incluye un componente Common Name (CN).

##### **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 de Personal de las Entidades Públicas 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 de Personal de las Entidades Públicas, 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 de Personal de las Entidades Públicas 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 persona física**

#### **3.1.2.1 Sujetos de identificación**

En el supuesto de los certificados de Personal de las Entidades Públicas, no será necesaria la acreditación de los datos contenidos en aquéllos siempre que sea la Entidad Pública Usuaria suscriptora quien asuma las funciones de poner a disposición del poseedor de claves los procedimientos técnicos de creación de firma (clave privada) y de verificación de firma (clave pública). Cuando la Entidad Pública Usuaria



suscriptora no asuma las mencionadas funciones, deberá acreditar ante la Entidad de Registro, los datos contenidos en los certificados. En todo caso, la identificación presencial de los poseedores de claves identificados en los certificados corresponderá a la Entidad Pública Usuaria en el ejercicio de las funciones identificación y comprobación de la documentación acreditativa de las circunstancias que consten en los certificados.

### **3.1.2.2 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.

### **3.1.2.3 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.

### **3.1.2.4 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**

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.

### **3.2.2 Petición de suspensión**

El suscriptor podrá solicitar la suspensión vía telefónica identificándose y dando su contraseña de identificación telefónica o en su defecto los datos requeridos por IZENPE que permiten la correcta identificación del solicitante.

### **3.2.3 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).



## 4 Requisitos operativos

---

### 4.1 Solicitud de certificado

Las Administraciones Públicas deberán completar el [formulario de solicitud](#) para las personas físicas que desempeñan cargos o puestos en su organización que estimen oportuno.

Estas solicitudes serán entregadas a la Entidad de Registro que haya determinado cada una de las Administraciones:

- I Entrega a la Entidad de Registro ubicada en la propia organización de la Administración solicitante.
- II Entrega a IZENPE) cuando la Administración solicitante no disponga de Entidad de Registro.

El suscriptor del certificado será la Administración solicitante y el poseedor de claves será la persona física que desempeña un cargo o puesto en la Administración solicitante, 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

El poseedor de claves, acreditada su identidad ante la Administración Pública Usuaria que realizará funciones de Entidad de Registro, deberá personarse ante:

- I La Entidad Pública Usuaria, cuando se constituya en Entidad de Registro (entidad que asume funciones de poner a disposición del poseedor de claves los procedimientos técnicos de creación de firma (clave privada) y de verificación de firma (clave pública)).

No será necesario obtener justificación documental de la identidad y del carácter del poseedor de claves, considerando que tanto la Entidad de Registro, el suscriptor y el poseedor de claves pertenecen a la misma organización.

- II En el caso de que la Entidad Pública Usuaria no se constituya en Entidad de Registro, el poseedor de claves acreditará ante IZENPE a través de la solicitud de emisión del certificado:

- Su identidad.



- Adscripción a la Administración solicitante.
- Justificación del cargo o puesto desempeñado.

IZENPE dejará constancia de dicha acreditación.

En todo caso los datos que identifiquen al poseedor de claves en el certificado deberán ser los que consten en:

- a. DNI o pasaporte, en el caso de ciudadano nacional
- b. En caso de ciudadanos extranjeros:
  - Miembros 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.
  - En relación a ciudadanos extracomunitarios, será exigible la tarjeta de residencia.

## 4.2 Emisión de certificado

Acreditada la identidad del solicitante ante la Entidad de Registro, éste deberá firmar la solicitud de emisión del certificado, IZENPE procederá a emitir el certificado.

## 4.3 Entrega de certificado

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

1. Entrega al poseedor de claves, 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. Envío postal,
  - a. Del certificado a la dirección postal determinada por el solicitante en la Solicitud de Emisión del certificado.
  - b. Del PIN y el código de desbloqueo del PIN (PUK), la hoja en la que figura la contraseña de identificación telefónica informándole de las [condiciones de](#)



[uso del certificado](#), a la dirección postal indicada por el poseedor de claves en la Solicitud de Emisión del Certificado.

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

## 4.4 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 identificándose dando:

- La contraseña de la identificación telefónica.
- Dirección de correo electrónico.

### 4.4.1 Entidad solicitante de la suspensión

Podrán suspender el certificado:

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

### 4.4.2 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.

## 4.5 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 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.



## 4.6 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 4.1.1), y entregar la [solicitud de reactivación](#) correctamente cumplimentada.

## 4.7 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.



## 5 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	<a href="mailto:info@izenpe.com">info@izenpe.com</a>
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)	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
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



Campo	Contenido
	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
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	<a href="http://www.izenpe.com/rpascapersentpub">http://www.izenpe.com/rpascapersentpub</a>
2.5.2.2. User Notice	Bermeen mugak ezagutzeko <a href="http://www.izenpe.com">www.izenpe.com</a> Ziurtagirian konfiantza izan aurretik kontratua irakurri Limitaciones de garantias en <a href="http://www.izenpe.com">www.izenpe.com</a> Consulte el contrato antes de



Campo	Contenido
	confiar en el certificado
2.6. Subject Alternate Names	
2.6.1. rfc822Name	<a href="#">Dirección de email</a>
2.6.2. UserPrincipalName	Usuario@dominio
2.7. Issuer Alternative Name	
2.7.1. dNSName	<a href="http://www.izenpe.com">http://www.izenpe.com</a>
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	<a href="http://crl.izenpe.com/cgi-bin/crlscar">http://crl.izenpe.com/cgi-bin/crlscar</a>
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	<a href="http://ocsp.izenpe.com:8094">http://ocsp.izenpe.com:8094</a>