



CERTIFICATE POLICY

ENTITY AND ENTITY WITHOUT LEGAL PERSONALITY

Reference: Política certificación Entidad_Entidad spj
Version no: v 1.0
Date: 11 january 2016

© IZENPE 2016

This document is the property of Izenpe. This document may only be reproduced in its entirety.


Beato Tomás de Zumarraga 71 - 1ª Planta
01008 Vitoria - Gasteiz
Tel.: 945 067 723
www.izenpe.com





TABLE OF CONTENTS

1	DESCRIPCIÓN DEL CERTIFICADO	3
1.1	DEFINICIÓN.....	3
1.2	ÁMBITO DE USO.....	4
1.3	IDENTIFICACIÓN DEL CERTIFICADO.....	4
1.4	DISPOSICIONES GENERALES	4
2	CICLO DE VIDA DEL CERTIFICADO	5
2.1	SOLICITUD DEL CERTIFICADO Y ACREDITACIÓN DE LA DOCUMENTACIÓN	5
2.2	PROCEDIMIENTO DE EMISIÓN Y ENTREGA	6
2.3	VERIFICACIÓN DEL CERTIFICADO	7
2.4	REVOCACIÓN DEL CERTIFICADO	7
2.5	RENOVACIÓN DE CERTIFICADOS.....	8
3	IMPORTE.....	8
4	GESTIÓN DEL CAMBIO	8
5	PERFILES DE CERTIFICADOS	8



1 DESCRIPTION OF THE CERTIFICATE

This document includes the *Specific Documentation* for the *Entity Certificate* and the *Certificate for Entities without Legal Personality* issued by *Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, S.A.* (henceforth, Izenpe).

The purpose of this document is to detail and complete the information provided in a more generic form in the *Izenpe Certification Practice Statement*.

1.1 Definition

Both certificates are electronic signature certificates with the legal effect of a recognized certificate, in accordance with the Electronic Signature Law 59/2003 dated 19 December (henceforth LFE), and a qualified certificate under *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*.

Concerning the certificate type,

Entity,

The applicant responsible for safeguarding the signature creation data is the key owner. His or her identity shall be included in the digital certificate.

All documents or contracts using the electronic signature shall be understood as made by the Entity.

Entity without legal personality,

It is issued in accordance with Order EHA/3256/2004, dated 30th September and whose use is limited exclusively to sending and transmitting fiscal data by electronic, computer and telematic means.

This is a certificate in which the subscriber is the entity without legal personality, which will in any case be one of the entities mentioned in article 35.4 of the General Tax Law. The subscriber will be responsible for the custody of the data used to create the signature and his or her identity will be included in the certificate.

Where,

- Certificate applicant, person applying for the certificate on behalf of an organization.
- Signatory, the natural person identified in the certificate.
- Subscriber, the entity identified in the certificate.
- Key owner, the natural person who owns or is responsible for safeguarding the digital signature keys.

With regard to storage media, these certificates can be issued in the following formats,

- Card / USB token: on a cryptographic chip.
- Software: in the Izenpe certificate container.
- Egoitz@ (HSM + Virtual Card): in a secure central repository (HSM), which the user can access via a small piece of software (Virtual Card) installed in the computer. This software manages users' requests to use certificates, connecting with the central repository and requesting the necessary cryptographic operations.



1.2 Scope of use

Concerning the certificate type,

- *Entity*,
This certificate will be used by the subscribers when they deal with the User Entities and Public and Private Institutions in general that have accepted its use.

- *Entity without legal personality*
Its use is limited exclusively to sending and transmitting fiscal data by electronic, computer and telematic means

1.3 Certificate identification

In order to identify certificates, Izenpe has assigned the following object identifiers (OID).

CERTIFICATE	OID
Entity Certificate (cryptographic card)	1.3.6.1.4.1.14777.2.7
Entity Certificate (software mechanism)	1.3.6.1.4.1.14777.2.8
Certificate for Entity without legal personality	1.3.6.1.4.1.14777.2.9

As these are recognized certificates, it also includes the following object identifier (OID) defined by TS 101 862, produced by the European Institute of Telecommunication Standards, on recognized certificate profiles: 0.4.0.1862.1.1.

1.4 General provisions

Identification obligations

Izenpe, either directly or through the User Entities with which it has signed the corresponding agreement, checks the corresponding registries to verify the identity and any other personal information concerning applicants, subscribers, and certificate key holders relevant for this purpose.

In addition, it verifies that the key holder is duly authorized by the subscriber.

Certificate subscriber obligations

The subscribers' obligations are compiled in the Certificate Practice Statement, Certificate Subscriber Obligations.



2 CERTIFICATE LIFE CYCLE

2.1 Certificate request and documentation accreditation

The applicant shall complete and sign the *Issue Application* and accept the Subscriber Contract.

The *Application* can be signed using the following options,

➤ Electronically.

The applicant

- shall access www.izenpe.com and use his/her eDNI (electronic DNI) to sign the *Issue Application for Citizen, Entity or Professional* electronic certificates issued by Izenpe and accept the Subscriber Contract.
- Pay the corresponding fee for the certificate.
- The required documentation shall be sent by post to IZENPE, S.A.- C/ BEATO TOMAS DE ZUMARRAGA, 71 -1ª PLANTA – 01008 VITORIA-GASTEIZ.

Izenpe publishes on www.izenpe.com the documentation that each organization must supply according to legal status.

Note.

If Izenpe has not identified the applicant face-to-face in the past 5 days, he/she should schedule and appointment with the Registration Authority.

➤ Or in paper format.

The applicant,

- shall access www.izenpe.com, complete the *Application* and accept the Subscriber Contract.
- Pay the corresponding fee for the certificate.
- Provide the documentation,
 - Izenpe publishes on www.izenpe.com which entities are required to send by post to IZENPE, S.A.- C/ BEATO TOMAS DE ZUMARRAGA, 71 -1ª PLANTA – 01008 VITORIA-GASTEIZ the documentation required before a certificate can be issued.
Once the documentation has been validated, the applicant shall schedule an appointment to appear before the Registration Authority.
 - In other cases, the applicant shall schedule an appointment with the Registration Authority at www.izenpe.com to hand in the documentation.
- Applicants will identify themselves as follows:
 - For Spanish citizens: DNI, passport or a valid driver's license.
 - For citizens of a EU member state: valid national identity document or equivalent, or passport and certificate issued by the EU Member State registry.
 - For non-EU citizens: Residence Card or valid passport

If the applicant cannot be identified by one of the above methods, Izenpe will determine the documentation needed for identification purposes on a case-by-case basis.



Note.

- The applicant shall either provide a photocopy of the identification documents (DNI/NIE/Residence Card) or authorize Izenpe to verify the information with the appropriate administrative body via the application form.
- Face-to-face identification before the Registration Authority is not necessary if Izenpe has identified the applicant in person within the past 5 years. In this case, the signed *Issue application* can be sent to Izenpe.

2.2 Issuance and delivery procedure

Izenpe will issue the certificate based on,

- The selected storage media.
- The method of delivery:
 - Not in person, delivery to the street/email address indicated, in the case of,
 - Electronic Signature for the Application
 - Or *Issue Application* on paper format signed by the applicant and notarized by a notary public.
 - In person, appearance before the Registration Authority by.
 - The applicant
 - Or a third party authorized by the Applicant, who shall submit to Izenpe,
 - The *Issue Application* in paper format, signed by the applicant and notarized by a notary public.
 - And a document authorizing the third party to collect the certificate / Unique Registration Number (URN) signed and duly notarized.

Card / USB token

➤ Delivery not in person.

Izenpe will send the certificate and the keys separately to the street address indicated on the *Issue Application*. Shipment shall be paid by the requesting entity.

The Applicant must sign the Delivery and Acceptance Sheet published at www.izenpe.com and deliver it to Izenpe if signed by hand or to servicios@colaboradores.izenpe.net if signed electronically.

➤ Delivery in person,

Izenpe will issue the certificate, the PIN and the unlock code (PUK) to the Applicant, who will sign a confirmation of delivery form.

SOFTWARE

Izenpe will send to the email indicated on the *Issue Application* a software container and instruction manual to generate the technical request for the certificate.

This request shall be sent to operaciones@izenpe.net to issue the certificate.



Once the Applicant has received the certificate, it can then be installed.

After generating the certificate, the Applicant must return the digitally signed *Delivery and Acceptance Sheet* to servicios@colaboradores.izenpe.net.

EGOITZ@ (HSM + VIRTUAL CARD)

Izenpe shall:

1. Generate the certificate on the Izenpe HSM.
2. Generate a username and password, which will be sent in an SMS to the mobile phone indicated on the application.
3. Once the process has been completed, Izenpe will send the software and instruction manual by certified email to the address indicated on the *Issue Application*.

The Applicant must sign the Delivery and Acceptance Sheet published at www.izenpe.com and deliver it to Izenpe is signed by hand or to servicios@colaboradores.izenpe.net if signed electronically.

2.3 Verification of certificate

The signatory will have 15 working days from the date of issuance to make sure the certificate works properly; if operational defects are detected, Izenpe must be notified.

Only if operating defects are due to technical reasons (such as: the certificate media does not work properly, technical error in the certificate, etc.) or to data errors made by Izenpe, will Izenpe revoke the certificate and issue a new one at its own expense.

2.4 Certificate revocation

Revocation request

The revocation of a certificate can be requested by:

- [Subscriber](#), the following individual are authorized to request the revocation of a certificate: the legal representative of the subscriber entity, the personnel manager or a third party authorized or either of the two.
- [Applicant](#).
- [Key owner](#).
- [Izenpe](#), the Izenpe administrators and Registration Authorities are authorized to request the revocation of end-entity subscriber certificates.

Procedure

The person requesting revocation will process the Revocation Application through Izenpe.

The certificate can be revoked at any time and in all cases involving loss or theft.

The applicant can revoke the certificate through the following channels:

- [In person](#), after scheduling an appointment with Izenpe at www.izenpe.com
- [By post](#), submitting a signed and notarized revocation request
- [By phone](#), at 902 542 542.
- [Online](#), at www.izenpe.com.



The following is required for [phone and online](#) revocation:

- ✓ Telephone identification password.
- ✓ DNI / NIE
- ✓ Subscriber's date of birth.
- ✓ Medium

Causes for revocation

Causes can be found in the Certification Practice Statement available at www.izenpe.com

2.5 Renewal of certificates

Certificates can be renewed within sixty days before the expiration date as follows:

- Online: the certificate must be valid and the Applicant must know the keys.
After performing the required verifications, Izenpe will send the certificate and the keys separately to the street address provided in the *Issue Application*.
The Applicant must sign the Delivery and Acceptance Sheet published at www.izenpe.com and deliver it to Izenpe if signed by hand or to [services@izenpe](mailto:services@izenpe.com) if signed electronically.
- In person: Izenpe will process the certificate renewal according to the determined issuance and delivery procedure.

3 FEE

The applicable fees are posted on the Izenpe website www.izenpe.com.

Payment options,

- For electronically signed issue applications,
 - Online using the payment gateway.
 - Direct debit with proof of payment
- Credit card payment in person at an Izenpe Registration Authority.

4 MANAGEMENT OF CHANGE

The modifications made to this document will be approved by the IZENPE Security Committee.

These modifications will be included in a Specific Documentation Update Document per certificate. Its maintenance is guaranteed by IZENPE.

The updated versions of the specific documentation can be consulted at www.izenpe.com.

5 CERTIFICATE PROFILES

Izenpe publishes the certificate profiles at www.izenpe.com.