

**CERTIFICATE POLICY**  
**REPRESENTATIVE**

Reference: Representative certificate policy  
Version no.: v 1.3  
Date: 1 June 2017

---

© IZENPE 2017

This document is the property of IZENPE. This document may only be wholly reproduced.

 IZENPE  
Beato Tomás de Zumarraga 71 - 1ª Planta  
01008 Vitoria - Gasteiz  
Tel.: 945 067 723  
[www.izenpe.com](http://www.izenpe.com)





## TABLE OF CONTENTS

|       |   |                                      |
|-------|---|--------------------------------------|
| 1     | DESCRIPCIÓN DEL CERTIFICADO .....                                   | 3                                    |
| 1.1   | DEFINICIÓN.....   | 3                                    |
| 1.2   | SOPORTE Y NIVEL DE SEGURIDAD .....                                  | 3                                    |
| 1.3   | ÁMBITO DE USO.....  | 4                                    |
| 1.4   | DISPOSICIONES GENERALES .....                                       | 4                                    |
| 1.4.1 | OBLIGACIONES DE IDENTIFICACIÓN .....                                | 4                                    |
| 1.4.2 | OBLIGACIONES DEL SUSCRIPTOR DEL CERTIFICADO .....                   | 4                                    |
| 2     | CICLO DE VIDA DEL CERTIFICADO .....                                 | 5                                    |
| 2.1   | SOLICITUD .....   | 5                                    |
| 2.2   | VERIFICACIÓN DE LA IDENTIDAD DE LA PERSONA FÍSICA SOLICITANTE ..... | 5                                    |
| 2.3   | ACREDITACIÓN DE LA ORGANIZACIÓN Y FACULTADES DEL SOLICITANTE .....  | 5                                    |
| 2.4   | PROCEDIMIENTO DE EMISIÓN Y ENTREGA .....                            | 5                                    |
| 2.5   | VERIFICACIÓN DEL CERTIFICADO .....                                  | 6                                    |
| 2.6   | REVOCACIÓN DEL CERTIFICADO .....                                    | 6                                    |
| 2.7   | RENOVACIÓN DE CERTIFICADOS.....                                     | 7                                    |
| 3     | IMPORTE.....  | 7                                    |
| 4     | PERFILES DE CERTIFICADOS .....                                      | 7                                    |
| 5     | CAMBIOS .....   | 7                                    |
| 5.1   | GESTIÓN DEL CAMBIO .....  | 7                                    |
| 5.2   | CONTROL DE CAMBIOS .....  | 7                                    |
|       | VERSIÓN 1. 0 A VERSIÓN 1.1 .....                                    | <b>¡ERROR! MARCADOR NO DEFINIDO.</b> |
|       | VERSIÓN 1. 1 A VERSIÓN 1.2 .....                                    | 8                                    |
|       | VERSIÓN 1.2 A VERSIÓN 1.3 .....                                     | 9                                    |



This document includes the *Certificate policy for Entity Representative and Entity Representative without legal personality certificates* issued by *Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, S.A.* (hereinafter, Izenpe).

## 1 CERTIFICATE DESCRIPTION

### 1.1 Definition

Both certificates are issued deemed as qualified as natural persons as established in *European Parliament and Council Regulation (EU) Num. 910/2014 dated 23 July 2014, on electronic identification and trust services for electronic transactions on the domestic market, repealing Directive 1999/93/EC.*

They are bound to the entity and accredit the representative's legal status as an identified natural person.

The following are:

- **Subscriber:** the entity
- **Key owner:** this is the natural applicant person identified in the certificate with power to act on the entity's behalf.

All certificates included in this Policy have a 4-year duration.

### 1.2 Format and security level

| REPRESENTATIVE CERTIFICATE       | FORMAT                                 | OID                    | EIDAS ASSURANCE LEVEL* |
|----------------------------------|--|------------------------|------------------------|
| Entity.                          | HSM                                    | 1.3.6.1.4.1.14777.2.14 | Substantial            |
|                                  | Card /USB token: cryptographic chip    | 1.3.6.1.4.1.14777.2.12 | High                   |
|                                  | Software: Izenpe certificate container | 1.3.6.1.4.1.14777.2.16 | Substantial            |
| Entity without legal personality | HSM                                    | 1.3.6.1.4.1.14777.2.15 | Substantial            |
|                                  | Card /USB token: cryptographic chip    | 1.3.6.1.4.1.14777.2.13 | High                   |
|                                  | Software: Izenpe certificate container | 1.3.6.1.4.1.14777.2.17 | Substantial            |

*\*Commission Regulation on Execution (EU) 2015/1502 dated 8 September, 2015, on setting specifications and minimum technical procedures for security levels for electronic identification methods as stipulated in article 8, section 3, of the European Parliament and Council Regulation (EU) number 910/2014, on electronic identification and trust services for electronic transactions on the domestic market.*



### 1.3 Scope of use

---

The certificate shall be used by the user for services offered by third parties that admit their use, with the conditions and limitations defined in Izenpe's [Terms and Conditions](#) document and the [Certification Practises Statement](#) (CPS) .

### 1.4 General stipulations

---

#### 1.4.1 Obligations concerning identification

Izenpe verifies the identity and any other personal circumstances of the certificate subscriber on the certificate that are relevant for their purposes on its own or through the User Entities with which the subscriber subscribes the corresponding legal instrument.

#### 1.4.2 Obligations of certificate subscribers

The subscriber's obligations are stipulated in section 9.6.9 *Certificate subscriber obligations in the [Certification Practises Statement](#)*.



## 2 CERTIFICATE LIFE CYCLE

---

### 2.1 Application

---

By accessing [Izenpe's website](#), the applicant will fill out the certificate application form.

By signing the application, the applicant agrees to the [Terms and Conditions](#) of the certificate.

### 2.2 Verification of the applying natural person's identity

---

Izenpe shall verify the identity of the applicant.

- ✓ **In person** at the Registration Entity, with the following valid documents,
  - Spanish citizen: National ID document, passport or driver's licence.
  - If a citizen of the EU/EEA: Valid Alien ID card and passport/equivalent national identity document in their country.
  - If a non-European citizen: Foreign ID Number and passport.

If the applicant's identification cannot be verified by the aforementioned methods, Izenpe shall determine the documentation required for identification in each case.

The applicant must either provide a photocopy of the identification documents required or authorise Izenpe to verify the data with the Competent Administration through the application form.

- ✓ By **legitimising** the signature of the issue application **in the presence of a notary**.
- ✓ When the issue application is **signed** with eDNI, the **qualified natural person certificate** or certificate for an entity/entity with no legal personality, both issued by Izenpe.

### 2.3 Organisation accreditation and applicant faculties

---

Izenpe shall verify the establishment and validity of the entity and the representation powers of the signatory with documents that accredit this condition or with pertinent registration verifications.

Izenpe publishes the documentation that each entity must provide according to its legal status on [its website](#).

### 2.4 Issue and delivery procedure

---

Izenpe shall then issue and deliver the certificate according to the media selected,

#### IZENPE SOFTWARE\_CONTAINER

1. Izenpe sends an empty container to the applicant by email to the indicated address.
2. The applicant starts the container and generates a key pair and the technical request (csr)
3. The applicant sends the technical request file (csr) to Izenpe.
4. Izenpe issues the certificate using the technical request provided by the applicant.
5. Izenpe sends the certificate to the email address indicated on the application form.



## CARD / USB TOKEN

### ➤ In-person delivery.

Izenpe shall deliver the certificate, PIN and unblocking code (PUK) to the applicant or authorised third party (who must provide signed, notarised authorisation documentation).

### ➤ Remote delivery.

Izenpe shall send the certificate to the postal address indicated in the *Issue application* along with the keys in two different shipments, and the applicant entity is responsible for shipping fees.

Izenpe verifies that the order is only delivered to the key owner.

## HSM

Izenpe,

- Shall generate the certificate in its HSM and a user and password (guaranteeing that they are only delivered to the key owner).
- Shall send an email to the address indicated in the *Issue Application* along with instructions for use.

## 2.5 Certificate verification

The signatory shall have 15 working days as of certificate issue to verify proper operation, and if necessary, communicate operational defects to Izenpe.

Only if operational defects are due to technical defects (e.g. malfunction of certificate media storage, technical error in certificate, etc.) or errors in the data contained on the certificate applicable to Izenpe, shall Izenpe revoke the certificate and issue a new one, assuming the costs derived.

## 2.6 Revoking the certificate

### ➤ Revocation application

The following I apply for certificate revocation,

- Subscriber, the following are authorised to request certificate revocation: the Legal Representative of the subscriber entity, the Personnel Chief or third party authorised by either of the aforementioned.
- Key owner.
- Izenpe, Izenpe's administrators and the Register Entities are authorised to apply for revocation of end entity subscriber certificates.

### ➤ Procedure

The revocation applicant 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, at Izenpe, requesting a prior appointment at [www.izenpe.com](http://www.izenpe.com).



- By post, sending the certificate revocation application signed and validated in the presence of a notary.
- Over the phone, by calling +34 902 542 542.
- Online, at the website [www.izenpe.com](http://www.izenpe.com).

For revoking by telephone and online the following is required for identification:

- Telephone Identification Password
- National/Foreign ID Number Card
- Entity Tax ID Number.

#### ➤ Reasons for revocation

This may be viewed in the Certification Practises Statement [www.izenpe.com](http://www.izenpe.com)

## 2.7 Renewing certificates

---

Within 60 days before the certificate expires, it may be renewed as follows:

- Online: the certificate to be renewed must be valid and the Applicant must know the keys.

Once the required verification has been carried out, Izenpe shall send the certificate to the applicant at the post address indicated in the *Issue application* along with passwords in two different shipments.

Izenpe verifies that the certificate is only delivered to the key owner.

- In person: Izenpe shall process renewal according to the planned issue and delivery procedure.

## 3 COST

---

The certificate applicant must pay the fee for the certificate, according to the payment option selected.

On an annual basis, Izenpe publishes applicable rates on its website [www.izenpe.com](http://www.izenpe.com).

## 4 CERTIFICATE PROFILES

---

Izenpe publishes certificate profiles at [www.izenpe.com](http://www.izenpe.com)

## 5 CHANGES

---

### 5.1 Managing changes

---

Modifications to this document shall be approved by Izenpe's Security Committee.

Updated versions of specific documentation may be viewed at [www.izenpe.com](http://www.izenpe.com).

### 5.2 Change tracking \_

---

Version 1. 0



|                         |  |
|-------------------------|--|
| Additional requirements | ➤ Heading to <i>European Parliament and Council Regulation (EU) Number 910/2014 dated 23 July 2014 on electronic identification and trust services for electronic transactions on the domestic market, repealing Directive 1999/93/EC.</i> |
| Updated requirements    |  |
| Clarifications          |  |
| Publisher               |  |
| Requirements eliminated |  |

#### Version 1. 0 to version 1.1

---

|                         |  |
|-------------------------|--|
| Additional requirements | ➤ The issue and delivery procedure for the Representative and Representative spj certificate in software format is added.<br>➤ Issue of the HSM-format Representative certificate is eliminated. |
| Updated requirements    | ➤ A specific OID per device is defined.  |
| Clarifications          |  |
| Publisher               |  |
| Requirements eliminated |  |

#### Version 1. 1 to version 1.2

---

|                         |   |
|-------------------------|---|
| Additional requirements | ➤ Issue of the HSM-format Representative certificate is eliminated. |
| Updated requirements    |   |
| Clarifications          |   |
| Publisher               |   |





|                         |  |
|-------------------------|--|
| Requirements eliminated |  |
|-------------------------|--|

Version 1.2 to version 1.3

---

|                                 | SECTION / CLARIFICATION   |
|---------------------------------|---|
| Updates to the previous version | <ul style="list-style-type: none"><li>– Version 1.3 of the Representative Policy regulates issuance of this certificate in HSM format.</li><li>– Section 2, the description of the certificate's life cycle is updated.</li></ul> |
| Clarifications                  |   |
| Format updates.                 |   |
| Eliminations.                   |   |