CERTIFICATE POLICY

ADMINISTRATION SEAL

Reference: Administration Seal certification policy.
Version no.: v 1.2
Date: 1 June 2017

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

TABLE OF CONTENTS

This document includes the Policy *for the* Administration Seal certificate *issued by Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, S.A.* (hereinafter, Izenpe).

1 CERTIFICATE DESCRIPTION

1.1 Definition

Issued under *Spanish Law 40/2015 dated 1 October, on the Legal System for the Public Sector.*

This certificate is issued deemed as qualified 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*, (hereinafter, eIDAS).

This certificate identifies the Administration, entity, public entity or public law entity, as well as, if applicable, the identity of the individual who owns the administrative entity's electronic seal.

The following are:

- Seal subscriber/creator, Administration, body, public entity or public-law entity.
- Applicant: natural person owner.
- Key owner: will be the applicant.

  This information will be on the certificate if the applicant expressly determines this.

According to the assurance levels defined in the Identification and electronic signature system prepared by the Ministry of Public Administrations, Izenpe issues the electronic seal certificate with a medium level.

The certificate included in this Policy have a 3-year duration.

1.2 Format and security level

This certificate is issued in software format, according to the security levels determined in the *eIDAS Regulation.*

FORMAT	OID	EIDAS ASSURANCE LEVEL*
Software: Izenpe certificate container	1.3.6.1.4.1.14777.4.11.2	Substantial
HSM	1.3.6.1.4.1.14777.4.11.3	Substantial

- pre-eIDAS profiles.

CERTIFICATE	OID

Administration Seal medium level	1.3.6.1.4.1.14777.4.4

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 Verification of identity and applying for the certificate

2.2 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.

2.3 Verification of identity of the applicant.

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.

  The key owner may identify him/herself with the Applicant administration with whom Izenpe signed the pertinent legal instrument.

  Certificates applied for in the municipal scope, the applicant may identify him/herself with the Town Hall Secretary, in fulfilling its role as public attester.

- ✓ By **legitimising** the signature of the issue application with 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.

2.4 Organisation accreditation and applicant faculties

Izenpe shall verify the establishment and validity of the entity and the representation powers of the applicant 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.

2.5 Issue and delivery procedure

Izenpe shall issue and deliver the certificate

SOFTWARE

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.

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.

2.6 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.

2.7 Revoking the certificate

➢ Revocation application

The following my 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.
- Applicant.
- 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.
- 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.

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

- ✓ Telephone Identification Password
- ✓ National/Foreign ID Number Card
- ✓ Subscriber's date of birth
- ✓ Support

➢ Reasons for revocation

This may be viewed in the Certification Practises Statement www.izenpe.com

2.8 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.

– 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.

4 CERTIFICATE PROFILES

Izenpe publishes certificate profiles at www.izenpe.com

5 CHANGES

5.1 Managing changes

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

Amendments will be set out in a document entitled Specific Documentation Update, the maintenance of which is guaranteed by IZENPE.

Updated versions of specific documentation may be viewed at www.izenpe.com.

5.2 Change control _for version 1. 0 to 1.1

Additional requirements	➢ Heeding to *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.
Updated requirements	➢ Identifying documentation required. ➢ Terms and conditions for use.
Clarifications	
Publisher	
Requirements eliminated	➢ Delivery note and acceptance. ➢ Conditions for use. ➢ Subscriber contract.

5.3 Track changes_From version 1.1 to 1.2

	SECTION / CLARIFICATION
Updates to the previous version	➢ 1.1. Definition: update of certificate definition. ➢ 2.1. Identity verification: updating identification documents required from extra-EU citizens: Foreign ID Number and passport.
Clarifications	
Format updates	
Eliminations	➢ 1.4. Certificate identification. Issue of high-level Administration Seal certificates. ➢ 1.5. General Terms: these aspects are deemed as regulated in the CPS.

5.4 Track changes_From version 1.2 to 1.3

	SECTION / CLARIFICATION
Updates to the previous version	– Version 1.3 of the Representative Policy regulates issuance of this certificate in HSM format. – Section 2, the description of the certificate's life cycle is updated.
Clarifications	
Format updates.	
Eliminations.	