CERTIFICATE POLICY

PROFESSIONAL CERTIFICATE

Reference:	Professional certificate policy.
Version Num.:	v 1.3.
Date:	1 June 2017.

Beato Tomás de Zumárraga
71 - 1ª Planta
01008 Vitoria - Gasteiz

www.izenpe.com
info@izenpe.com
Tel.: 945 06 77 23

TABLE OF CONTENTS

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

1 CERTIFICATE DESCRIPTION

1.1 Definition

According to the scope of issue, Izenpe issues the following certificates,

- *Professional-Personal for Public Entities*,

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

  It is configured as a qualified natural person certificate 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 Public Administration acting as subscriber, as well as the individual holding a position or role at said Administration as key owner.

  The subscribing Administration may carry out tasks to identify key owners that belong to said Administration.

  Within this cope, Izenpe issues certificates with a pseudonym, as determined in the document *Electronic Certificate Profiles* from the Ministry of Hacienda y Administraciones Públicas (Treasury and Public Administrations).

- *Professional-Corporate*,

  Issued within the scope of an organisation that belongs both to the public sector or the private sphere.

  Types,

  - *Qualified professional-corporate*,

    Configured as an electronic signature certificate, deemed qualified per *eIDAS.*

    It identifies as the entity acting as certificate subscriber and the individual who holds a position or role at said entity as key owner who holds custody over the keys.

  - *Non-qualified professional-corporate*,

    This identifies the entity acting as certificate subscriber with a medium degree of assurance, as well as the individual who holds a position or role at said entity, as key owner.

    eIDAS does not deem this qualified.

The following are:

- Subscriber: Public Administration or entity identified on the certificate.

- Key owner: natural person identified on the certificate who owns or holds custody over the digital signature keys.
- Applicant: person who applies for the certificate on behalf of an organisation (Public Administration and/or entity).

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

1.2 Format and security level

The *Professional* certificate is issued in different formats, according to the assurance levels determined in,

PROFESSIONAL CERTIFICATE	FORMAT	OID	eIDAS ASSURANCE LEVEL
Public Entity Staff	Card /USB token: cryptographic chip	1.3.6.1.4.1.14777.4.14.1	High
	Software: Izenpe certificate container.	1.3.6.1.4.1.14777.4.14.2	Substantial
	HSM	1.3.6.1.4.1.14777.4.14.3	Substantial
Public Entity staff with pseudonym	Card /USB token: cryptographic chip	**Signature** 1.3.6.1.4.1.14777.4.13.1.1	High
		Authentication 1.3.6.1.4.1.14777.4.13.1.2	High
		Encryption 1.3.6.1.4.1.14777.4.13.1.3	High
Qualified corporate	Card /USB token: cryptographic chip	1.3.6.1.4.1.14777.2.19.1	High
	Software: Izenpe certificate container	1.3.6.1.4.1.14777.2.19.2	High
	HSM	1.3.6.1.4.1.14777.2.19.3	Substantial
Non-qualified corporate	Card / USB token.	1.3.6.1.4.1.14777.1.1.1	n/a (not qualified)

- pre-eIDAS profiles.

SCOPE	CORPORATE CERTIFICATE	OID
Public Administration	*Public Entity Personnel*	1.3.6.1.4.1.14777.4.1
	Basque Government Staff	1.3.6.1.4.1.14777.7.1
Public Corporate	*Recognised Public Corporate*	1.3.6.1.4.1.14777.4.2
	Non-Recognised Public Corporate	1.3.6.1.4.1.14777.1.1.1
Private corporate	*Recognised private corporate*	1.3.6.1.4.1.14777.2.2
	Non-recognised private corporate	1.3.6.1.4.1.14777.5.2.2

1.3 Scope of use

The certificate shall be used by the key owner 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) .

2 CERTIFICATE LIFE CYCLE

2.1 Application

By accessing Izenpe's website, the applicant and the key owner will fill out the certificate application form.

By signing the application, the key owner agrees to the Terms and Conditions of the certificate.

2.2 Verification of the key owner's identity.

2.2.1 Non-qualified certificate.

For the non-qualified citizen certificate, it shall not be necessary to verify the key owner's identity in person or with an equivalent method, although it shall require a signed application.

2.2.2 Qualified certificate,

Izenpe shall verify the key owner's identity,

- ✓ **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 a **qualified natural person certificate** for which in-person identification was required.

2.3 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.

2.4 Issue and delivery procedure

Izenpe shall issue and deliver the certificate

IZENPE CONTAINER

1. Izenpe sends an empty container to the key owner by email to the indicated address.
2. The key owner starts the container and generates a key pair and the technical request (csr).
3. The key owner sends the technical request file (csr) to Izenpe.
4. Izenpe issues the certificate using the technical request provided by the key owner.
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 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.
- Key owner.
- Izenpe, Izenpe's administrators and the Register Entities are authorised to apply for revocation of end entity subscriber certificates.

➢ Procedure.

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/Alien Identity Card Number.
  ✓ Entity.

➢ Reasons for revocation

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

2.7 Renewing certificates

To renew a certificate, the applicant must follow the established certificate issue process.

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.

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

5.2 Version 1. 0

Updates to the previous version.	➢ Adaptation to *eIDAS regulations.* ➢ Identifying documentation required. ➢ Terms and conditions for use.
Clarifications	
Format updates	
Eliminations	➢ Delivery note and acceptance. ➢ Conditions for use. ➢ Subscriber contract.

5.3 Version 1.0 to version 1.1

	SECTION / CLARIFICATION
Updates to the previous version	➢ 1.1. Definition: issue of *Public Entity Professional-personal* certificates with pseudonym. ➢ 1.2. Format and security level. Professional certificate issue in card/USB token and software format. ➢ 1.3. Scope of use: the scope of use of professional certificates is corrected. ➢ 1.4. Certificate identification: a new OID is assigned for *Professional* certificates issued in card/USB token and software format.

	➢ 2.1. Identity verification: updating identification documents required from extra-EU citizens: Foreign ID Number and passport. ➢ 3. Cost: notification of different payment modalities based on specific projects.
Clarifications	
Format updates.	
Eliminations.	➢ Section 1.1. Version 1.0 defined different types of certificates based on the subscriber entity's status as belonging to the public or the private sector. Version 1.1 eliminates this differentiation. ➢ Section 1.2. Formats: HSM and browser-format certificate issue is eliminated. ➢ Section 1.5. General Terms: these aspects are deemed as regulated in the CPS.

5.4 Version 1.1 to version 1.2

	SECTION / CLARIFICATION
Updates to the previous version	
Clarifications	
Format updates.	
Eliminations.	➢ Section 1.2. HSM-format certificate issue is eliminated.

5.5 Version 1.2 to version 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.	