TERMS AND CONDITIONS FOR THE USE OF ELECTRONIC MEANS OF IDENTIFICATION AND SIGNATURE

ZIURTAPEN ETA ZERBITZU ENPRESA-EMPRESA DE CERTIFICACION Y SERVIC

Firmado digitalmente por ZIURTAPEN ETA ZERBITZU ENPRESA-EMPRESA DE CERTIFICACION Y SERVIC
Fecha: 2022.10.17 11:36:01 +02'00'

TRACK CHANGES

1.0	➢ Alignment with *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.* ➢ Conditions of use are deleted. Subscriber Agreement
1.1	➢ Updating the name of the document. ➢ Paragraph 2, a specific section on definitions is included. ➢ Paragraph 3, a distinction is made between the use of means of identification as an attention and as a signature. ➢ Paragraph 4, a new classification of the obligations of the parties is included. ➢ Paragraph 5, the responsibilities of the certification authority are updated. ➢ Paragraph 2 is deleted Paragraph 2 concerning the types of certificates and the media on which they are issued is deleted.
1.2	➢ Added clarification of policy compliance in section 4.3 Certificate Subscriber Obligations
2.0	➢ In order to provide the user with information regarding the terms and conditions of use of identification means, the PKI Disclosure Statement (PDS) version 1.0 and the Terms and Conditions of Use of Electronic Means for authentication and signature version 1.2 are merged into a single document.
2.1	➢ The eIDAS level of the corporate profile in a container is corrected. ➢ Device profile has been added
2.2	➢ Updating of section 4 Types of certificate, validation procedure and use: inclusion of specificities relating to the certificate*Non-recognised citizen*. ➢ *Deletion* Section 3. Definitions: Bak and BakQ definitions, the possibility that both means of identification can be complemented by other biometric authentication factors such as fingerprint or facial recognition is eliminated.
2.3	Updated contact phone and email Added eIDAS signature type column in each profile

	Added IoT device, mobile and NQC pseudonym profiles Added description of signature usage in application and IoT device certificates Removed reference to publishing service Added obligation to comply with the Supplier Security Policy Removed the amount of Civil Liability Insurance
2.4	This version does not exist, it was a error in the nomenclature
2.5	➢ The definition of BakQ is updated. ➢ Policies for new root CAs are added.

VERSION	DATE	CHANGE
2.6	13/01/2022	Section 12.2: updating of applicable legislation
2.7	23/09/2022	Correction of errors: Section 1: removes reference annex B standard ETSI EN 319 411 Section 4.1: signature level update Update SSL OIDs. Code signature removal Section 5: content update

TABLE OF CONTENTS

1 INTRODUCTION

The purpose of this document is to describe the terms and conditions under which Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, S.A." (hereinafter, Izenpe) issues means of identification and electronic signature.

Izenpe is considered a qualified trust service provider within the scope of 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 (hereinafter, eIDAS).

As such, it issues means for,

- Identification,

  In addition to the identification means based on electronic certificates, it issues other means of identification such as BaK, BaKQ, cloud professional and Izenpe Mobile, which allow the identification of a natural person by means of a reference number coinciding with the user's DNI/NIE and a password.

  BaKQ also incorporates: a 16-position set of coordinates or a single-use code that will be sent by SMS to the user's mobile phone.

- Signature:

  For signature purposes, Izenpe issues electronic-based certificate means of different types and on different media, according to the specifications determined in the corresponding specific Policy and in the *Certification Practice Statement*.

This document has been created in accordance with the technical requirements of ETSI EN 319 401: Electronic signatures and infrastructures (ESI); General policy requirements for Trust Service Providers".

It does not in any way replace the Certification Practice Statement and the certificate policies, available at www.izenpe.eus.

2 CONTACT DETAILS

Provider name	Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, S.A.
Address	c/ Beato Tomás de Zumárraga, nº 71, 1ª planta. 01008 Vitoria-Gasteiz
Email	izenpe@izenpe.eus
Telephone number	900 840 123 / 945 01 62 90

3 DEFINITIONS

- Electronic identification, the process of using a person's identification data in electronic form that uniquely represents a natural or legal person or a natural person representing a legal person.
- Electronic identification means, a tangible and/or intangible unit that contains a person's identification data and is used for authentication in online services.
- Authentication, an electronic process that enables the electronic identification of a natural or legal person, or of the origin and integrity of data in electronic form.
- Electronic signature, the data in electronic format annexed to other electronic data or logically associated with them, used by the signatory to sign.
- Advanced electronic signature, the electronic signature that meets requirements stipulated by article 26 of eIDAS.
- Qualified electronic signature, an advanced electronic signature created with a qualified electronic signature creation device based on a qualified electronic signature certificate.
- Electronic signature certificate, an electronic statement that links the validation data of a signature to a natural person and confirms at least the name or pseudonym of that person.
- Qualified electronic signature certificate, an electronic stamp certificate issued by a qualified trust service provider that meets the requirements established in Annex III of eIDAS..
- Trust service provider, a natural or legal person who provides one or more trust services, either as a qualified provider or as an unqualified provider of trust services.
- Qualified trust service provider, a trust service provider that provides one of several qualified trust services and to whom the supervision authority has granted qualification;
- Registration Entities, entities that perform the tasks of identifying applicants, subscribers and owners of certificate keys, verifying the documentation accrediting the circumstances on the certificates, as well as validating and approving requests to issue, revoke and renew certificates.
- Users of the certificates.
  - Certificate applicant,, a certificate must be applied for by an individual, on their own behalf or on behalf of an organisation.
  - Signatory, the person who holds a signature creation device and who acts on his or her own behalf or on behalf of an individual or legal entity.
  - Certificate subscriber, natural or legal person identified in the certificate.
  - Password holder, natural person who holds or is responsible for the custody of the digital signature passwords.
- Bak is a means that allows the identification and signature of natural persons, consisting of:
  - A reference number coinciding with the user's DNI/NIE/passport and a password.
  - A non-qualified certificate issued in a centralised repository that will be used for signing acts.
- BakQ, is a means that allows the identification and signature of natural persons, consisting of:

- A reference number coinciding with the user's DNI/NIE.
- A password.
- A 16-position set of coordinates or a single-use code that will be sent by SMS to the user's mobile phone.
- A qualified electronic signature certificate issued in an Izenpe secure centralised repository that will be used for signing acts.

4 CERTIFICATE TYPES, VALIDATION PROCEDURE AND USAGE

The specificities for each kind of certificate issued by Izenpe are regulated in the *Specific policy for each certificate*, attached to the *Certification Practice Statement*.

The specificities for each kind of certificate issued by Izenpe are regulated in the *Specific policy for each certificate*, attached to the *Certification Practice Statement*.

4.1 Hierarchy CA root 2007 (CN=Izenpe.com)

GENERAL PUBLIC						
BRIEF description	**Media**	**Policy identifier**	**Policy OID**	**eIDAS identification level**		**Signature type eIDAS**
B@K	HSM	NCP	1.3.6.1.4.1.14777.5.2.5	Low		Basic
B@KQ	HSM	QCP-n	1.3.6.1.4.1.14777.2.18.3	High (with virtual card)	Substantial (with Giltza)	Advanced
Certificate General Public	Cryptographic chip	QCP-n-qscd	eIDAS Profile 1.3.6.1.4.1.14777.2.18.1	High		Advanced
			Profile prior to eIDAS 1.3.6.1.4.1.14777.2.6	High		Qualified
Izenpe Mobile	APP container	NCP	1.3.6.1.4.1.14777.5.2.5.4	Substantial		n/a (the BAKQ is used to sign)
NQC pseudonym	Software	NCP	1.3.6.1.4.1.14777.5.2.7.2	Substantial		Advanced

ENTITY REPRESENTATIVE						
Brief description	**Media**	**Policy identifier**	**Policy OID**	**eIDAS identification level**		**Signature type eIDAS**
Entity representative	HSM	QCP-n	1.3.6.1.4.1.14777.2.14	High (with virtual card)	Substantial (with Giltza)	Advanced
	Cryptographic chip	QCP-n-qscd	1.3.6.1.4.1.14777.2.12	High		Advanced

	Izenpe software container	QCP-n	1.3.6.1.4.1.14777.2.16	Substantial	Advanced

SPJ ENTITY REPRESENTATIVE						
Brief description	**Media**	**Policy identifier**	**Policy OID**	**eIDAS identification level**		**Signature type eIDAS**
SPJ Entity Representative	HSM	QCP-n	1.3.6.1.4.1.14777.2.15	High (with virtual card)	Substantial (with Giltza)	Advanced
	Cryptographic chip	QCP-n-qscd	1.3.6.1.4.1.14777.2.13	High		Advanced
	Izenpe software container	QCP-n	1.3.6.1.4.1.14777.2.17	Substantial		Advanced

PROFESSIONAL						
Brief description	**Media**	**Policy identifier**	**Policy OID**	**eIDAS identification level**		**Signature type eIDAS**
Public Entity Staff	Cryptographic chip	QCP-n-qscd	1.3.6.1.4.1.14777.4.14.1	High		Advanced
	Izenpe software container	QCP-n	1.3.6.1.4.1.14777.4.14.2	Substantial		Advanced
	HSM	QCP-n	1.3.6.1.4.1.14777.4.14.3	High (with virtual card)	Substantial (with Giltza)	Advanced
Public Entity Staff with a pseudonym	Cryptographic chip	QCP-n-qscd	**Signature** 1.3.6.1.4.1.14777.4.13.1.1	High		Advanced
		NCP+	**Authentication** 1.3.6.1.4.1.14777.4.13.1.2	High		n/a
		n/a	**Encryption** 1.3.6.1.4.1.14777.4.13.1.3	High		n/a
	Cryptographic chip	QCP-n-qscd	1.3.6.1.4.1.14777.2.19.1	High		Advanced

Qualified corporate	Izenpe software container	QCP-n	1.3.6.1.4.1.14777.2.19.2	Substantial	Advanced
	HSM	QCP-n	1.3.6.1.4.1.14777.2.19.3	High (with virtual card) / Substantial (with Giltza)	Advanced
Non-qualified corporate	Cryptographic chip	NCP+	1.3.6.1.4.1.14777.1.1.1	n/a (not qualified)	Advanced
Public Entity Staff (pre-eIDAS)	Cryptographic chip	QCP public + SSCD	1.3.6.1.4.1.14777.4.1	n/a	Recognised
Basque Government Staff (pre-eIDAS)	Cryptographic chip	QCP public + SSCD	1.3.6.1.4.1.14777.7.1	n/a	Recognised
Recognised public corporate (pre-eIDAS)	Cryptographic chip	QCP public + SSCD	1.3.6.1.4.1.14777.4.2	n/a	Recognised
Not recognised public corporate (pre-eIDAS)	Cryptographic chip	NCP+	1.3.6.1.4.1.14777.1.1.1	n/a	Advanced
Recognised private corporate (pre-eIDAS)	Cryptographic chip	QCP public + SSCD	1.3.6.1.4.1.14777.2.2	n/a	Recognised
Unrecognised private corporate (pre-eIDAS)	Cryptographic chip	NCP+	1.3.6.1.4.1.14777.5.2.2	n/a	Advanced

ENTITY SEAL					
Brief description	**Media**	**Policy identifier**	**Policy OID**	**eIDAS identification level**	**Signature type eIDAS**
Entity seal	Izenpe software container	QCP-l	1.3.6.1.4.1.14777.2.11	Substantial	Advanced

	HSM	QCP-l	1.3.6.1.4.1.14777.2.20	Substantial	Advanced

ADMINISTRATION SEAL					
Brief description	**Media**	**Policy identifier**	**Policy OID**	**eIDAS identification level**	**Signature type eIDAS**
Administration stamp	Izenpe container software	QCP-l	1.3.6.1.4.1.14777.4.11.2	Substantial	Advanced
	HSM	QCP-l	1.3.6.1.4.1.14777.4.11.3	Substantial	Advanced
Medium level administration seal (pre-eIDAS)	HSM	NCP+	1.3.6.1.4.1.14777.4.4	n/a	Recognised

SECURE SERVER (SSL/TLS)			
BRIEF DESCRIPTION	**MEDIA**	**POLICY IDENTIFIER**	**POLICY OID**
DV SSL	Software	DVCP	1.3.6.1.4.1.14777.1.2.4
OV SSL	Software	OVCP	1.3.6.1.4.1.14777.1.2.1
Qualified SSL	Software	EVCP	1.3.6.1.4.1.14777.6.1.3

APPLICATION			
BRIEF DESCRIPTION	**MEDIA**	**POLICY IDENTIFIER**	**POLICY OID**
Application	Izenpe container software	NCP	1.3.6.1.4.1.14777.1.2.2

CODE SIGNATURE			
BRIEF DESCRIPTION	**MEDIA**	**POLICY IDENTIFIER**	**POLICY OID**
Code Signature	Cryptographic chip	NCP+	1.3.6.1.4.1.14777.1.3.1

IOT DEVICE			
BRIEF DESCRIPTION	MEDIA	POLICY IDENTIFIER	POLICY OID
Device	Software	NCP	1.3.6.1.4.1.14777.1.3.2

4.2 Hierarchy CA root 2020 qualified (CN=ROOT CA QC IZENPE)

GENERAL PUBLIC						
BRIEF description	Media	Policy identifier	Policy OID	eIDAS identification level		Signature type eIDAS
B@KQ	HSM	QCP-n	1.3.6.1.4.1.14777.8.1.3	High (with virtual card)	Substantial (with Giltza)	Advanced
Certificate General Public	Cryptographic chip	QCP-n-qscd	1.3.6.1.4.1.14777.8.1.1	High		Qualified

ENTITY REPRESENTATIVE						
Brief description	Media	Policy identifier	Policy OID	eIDAS identification level		Signature type eIDAS
Entity representative	HSM	QCP-n	1.3.6.1.4.1.14777.8.3.3	High (with virtual card)	Substantial (with Giltza)	Advanced
	Cryptographic chip	QCP-n-qscd	1.3.6.1.4.1.14777.8.3.1	High		Qualified
	Izenpe software container	QCP-n	1.3.6.1.4.1.14777.8.3.2	Substantial		Advanced

SPJ ENTITY REPRESENTATIVE	

Brief description	Media	Policy identifier	Policy OID	eIDAS identification level		Signature type eIDAS
SPJ Entity Representative	HSM	QCP-n	1.3.6.1.4.1.14777.8.4.3	High (with virtual card)	Substantial (with Giltza)	Advanced
	Cryptographic chip	QCP-n-qscd	1.3.6.1.4.1.14777.8.4.1	High		Qualified
	Izenpe software container	QCP-n	1.3.6.1.4.1.14777.8.4.2	Substantial		Advanced

PROFESSIONAL						
Brief description	Media	Policy identifier	Policy OID	eIDAS identification level		Signature type eIDAS
Public Entity Staff	Cryptographic chip	QCP-n-qscd	1.3.6.1.4.1.14777.9.1.1	High		Qualified
	Izenpe software container	QCP-n	1.3.6.1.4.1.14777.9.1.2	Substantial		Advanced
	HSM	QCP-n	1.3.6.1.4.1.14777.9.1.3	High (with virtual card)	Substantial (with Giltza)	Advanced
Public Entity Staff with a pseudonym	Cryptographic chip	QCP-n-qscd	**Signature** 1.3.6.1.4.1.14777.9.2.1	High		Qualified
		NCP+	**Authentication** 1.3.6.1.4.1.14777.9.2.2	High		n/a
		n/a	**Encryption** 1.3.6.1.4.1.14777.9.2.3	High		n/a
Qualified corporate	Cryptographic chip	QCP-n-qscd	1.3.6.1.4.1.14777.8.2.1	High		Qualified
	Izenpe software container	QCP-n	1.3.6.1.4.1.14777.8.2.2	Substantial		Advanced
	HSM	QCP-n	1.3.6.1.4.1.14777.8.2.3	High (with virtual card)	Substantial (with Giltza)	Advanced

ENTITY SEAL					
Brief description	**Media**	**Policy identifier**	**Policy OID**	**eIDAS identification level**	**Signature type eIDAS**
Entity seal	Izenpe software container	QCP-l	1.3.6.1.4.1.14777.8.5.2	Substantial	Advanced
	HSM	QCP-l	1.3.6.1.4.1.14777.8.5.3	Substantial	Advanced

ADMINISTRATION SEAL					
Brief description	**Media**	**Policy identifier**	**Policy OID**	**eIDAS identification level**	**Signature type eIDAS**
Administration stamp	Izenpe container software	QCP-l	1.3.6.1.4.1.14777.9.3.2	Substantial	Advanced
	HSM	QCP-l	1.3.6.1.4.1.14777.9.3.3	Substantial	Advanced

4.3 Hierarchy CA root 2020 qualified (CN=ROOT CA NQC IZENPE)

GENERAL PUBLIC					
BRIEF description	**Media**	**Policy identifier**	**Policy OID**	**eIDAS identification level**	**Signature type eIDAS**
B@K	HSM	NCP	1.3.6.1.4.1.14777.11.1.2	Low	Basic
Mobile	APP container	NCP	1.3.6.1.4.1.14777.11.3.4	Substantial	n/a (the BAKQ is used to sign)
NQC pseudonym	Software	NCP	1.3.6.1.4.1.14777.11.2.2	Substantial	Advanced

PROFESSIONAL					
Brief description	Media	Policy identifier	Policy OID	eIDAS identification level	Signature type eIDAS
Non-qualified professional	Cryptographic chip	NCP+	1.3.6.1.4.1.14777.11.4.2	n/a (not qualified)	Advanced

APPLICATION			
BRIEF DESCRIPTION	MEDIA	POLICY IDENTIFIER	POLICY OID
Application	Izenpe container software	NCP	1.3.6.1.4.1.14777.12.1.2

IOT DEVICE			
BRIEF DESCRIPTION	MEDIA	POLICY IDENTIFIER	POLICY OID
Device	Software	NCP	1.3.6.1.4.1.14777.12.2.2

INTERNAL SECURE SERVER (SSL/TLS)			
BRIEF DESCRIPTION	MEDIA	POLICY IDENTIFIER	POLICY OID
DV SSL	Software	DVCP	1.3.6.1.4.1.14777.14.1.2

5 USES OF ELECTRONIC MEANS

5.3 APPROPRIATE USES,

- FOR AUTHENTICATION,

  These electronic means allow identification and should be used for the electronic identification of the subscriber, or the password holder if applicable, before the Public Authorities who accept them.

  When the mean is used for identification before an electronic service, Izenpe will offer the responsible entity of the service the authentication result.

- FOR SIGNATURE,

- Qualified certificates of an individual or legal entity.

  Qualified signature and stamp certificates can be used, if so defined in the corresponding type of certificate, to sign authentication messages, particularly SSL or TLS client challenges, S/MIME secure e-mail, encryption without key recovery and others. This digital signature guarantees the identity of the signature certificate subscriber.

  Additionally, these certificates can support advanced electronic signatures.

  Electronic seal certificates should only be used for the electronic sealing of documents.

- Non-qualified certificates

  Non-qualified certificates do not reliably guarantee the identity of the subscriber and, if applicable, of the private key holder;

  If used for signing, such a signature cannot be equated with a handwritten signature.

  Non-qualified signature certificates may also be used, if defined as such by the corresponding certificate, to sign authentication messages, particularly for client SSL or TLS challenges, secure S/MIME email, encrypted without password recovery, or others.

- Application certificates

  It is a certificate used by a computer application that will be used exclusively to ensure the authenticity and integrity of the messages or files signed by the application itself.

- IoT device certificates

  The IoT device certificate identifies and ensures the integrity of an online communication carried out by an IoT (Internet of Things) device.

- Code signature certificates

  They are issued to the owner entities to guarantee the authentication and integrity of a component of said software.

5.4 PROHIBITED USES OF THE MEANS OF

- AUTHENTICATION must be used for their own function and established purpose, and may not be used in other functions and for other purposes.
- SIGNATURE, must be used for their proper function and established purpose, and may not be used for other functions and purposes, and only in accordance with applicable law.

  The certificates are not designed, cannot be used and are not authorised for use or resale as equipment for monitoring hazardous situations or for uses requiring fail-safe performance, such as the operation of nuclear facilities, airborne navigation or communications systems, or weapons control systems, where failure could directly lead to death, personal injury or severe environmental damage.

6 LIMITATIONS ON TRUST

Izenpe does not apply specific trust limitations to its certificates.

The limitations on the use of each type of certificate can be consulted in the previous section.

In its activity as a trust service provider, Izenpe keeps internal records or ensures the archiving, in a secure manner, of the following elements:

- Evidence of all events related to the life cycle of qualified certificates for 15 years after the date of issue.
- Evidence of all events related to the life cycle of non-qualified certificates for 7 years after the expiry date.

7 IZENPE OBLIGATIONS

7.3

7.3.1 GENERAL OBLIGATIONS

Security,

- Using reliable systems and products that are protected against all alteration, and that guarantee technical security, and if applicable, cryptographic security of the certification processes that they support, as per its Security Policy.
- Taking measures against the forgery of means and guaranteeing confidentiality during the generation process and ensure secure delivery of the certificate to the signatory.
- Using reliable systems to store qualified certificates that verify their authentication and prevent unauthorised individuals from altering the data, restricting their accessibility in the cases, or to the individuals, that the signatory has indicated, and that detect any modification that would affect these security conditions.
- Periodically performing regular security checks to verify compliance with established standards.
- Proper security management, thanks to implementing an Information Security Management System as per the principles stipulated by ISO/IEC 27001, which includes, but is not limited to, the following measures:
    - Comprehensively managing security events, in order to guarantee detection, resolution and optimisation.
    - Maintaining appropriate contact and relationships with special interest groups in security, such as specialists, security forums and professional associations related to information security.
    - Appropriately planning system maintenance and evolution, in order to guarantee appropriate performance at all times, as well as service that is guaranteed to comply with user and client expectations.
- It will require that hosting suppliers meet the security standards and rules (GDPR, ISO, ETSI, CABForum and Izenpe Provider Security Policy).

Staff,

- Employing staff with the qualification, knowledge and experience necessary to provide the services offered and the security and management procedures as required within the scope of electronic signatures.
- It will meet the security standards and rules (General Register of Data Protection, ISO, ETSI and Izenpe Security Policy).

Procedure,

- Prior to the issue and delivery of the means of identification and/or signature, Izenpe informs you of the terms and conditions relating to its use, of its price– where established–of its limitations of use and of the binding legal instruments referred to, where applicable, in the Certification Practices Statement.
- Izenpe has a termination of service plan which specifies the conditions under which such an event would take place.
- Izenpe will inform the key holder about the expiry of their certificate prior to or at the same time as the electronic certificate expires, specifying the reasons and date and time that the certificate will no longer be effective.

7.3.2 AS AN ENTITY ISSUING ELECTRONIC MEANS OF IDENTIFICATION.

- It shall identify the user in accordance with the assurance levels defined in eIDAS.
- It shall ensure the complementarity of identification data.
- It shall ensure that the user is in possession of the elements enabling their identification.
- It will comply with technical and staff requirements stipulated by governing legislation.
- Prior to the issue and delivery of the means of identification Izenpe informs you of the terms and conditions relating to its use, of its price– where established–of its limitations of use and of the binding legal instruments.
- Izenpe provides public verification mechanisms to check the validity of certificates through systems described in the Certification Practice Statement.
- Izenpe will provide authentication mechanisms to check the validity of identification mechanisms.

7.3.3 AS AN ENTITY ISSUING ELECTRONIC SIGNATURE MEANS.

- Obligations of providing service.

  Izenpe renders certification services in accordance with the Certification Practice Statement, in which its roles, operations procedures and security measures are defined; in particular, IZENPE undertakes to fulfil all of its obligations as described in this CPS except those performed expressly by the Registration Authority when not acting in the capacity thereof.

  These Certification Entity obligations are the following:

  - Not copying signature creation data of the person to whom its services were provided.
  - Keeping a system to indicate the issued certificates and if they are valid or if their validity has been suspended or expired.
  - Keeping a record by any secure means of all information and documentation regarding the qualified certificates and certification practises statements that are valid at all times,

for at least 15 years as of the date of their issue, so that the signatures made with the certificate and in relation to the rest of certificates can be validated for 7 years.

- Ensuring that the signatory possesses the signature creation data for the verification data on the certificate.
- Guaranteeing that the creation and signature verification data are complementary, as long as they are both generated by the certification service supplier. That the identity contained in the certificate unambiguously matches the public key contained therein.
- Rapidity and security in providing the service. In particular, it provides a fast and secure and free service aimed at checking certificate validity and ensures secure and immediate notification of the termination of effectiveness of the certificates in accordance with the Certification Practice Statement. The service is available 24 hours X 7 days a week.
- Compliance with technical and staff requirements stipulated by governing legislation on electronic signatures:
- Demonstrating the reliability necessary to provide certification services.
- Guaranteeing that the date and time when a certificate was issued or expired can be precisely determined.

– Obligations regarding legal regulation of the certification service.

- Izenpe assumes all of the obligations directly incorporated in the certificate or incorporated by reference. Incorporation by reference is the inclusion of an object identifier in the certificate, or another way to link to a document.
- The legal instrument that binds Izenpe and the applicant, subscriber or key holder and the relying party is in writing and in readily understandable language.
- Requirements to comply with the provisions of the Certification Practice Statement.
- Indication of the applicable Certification Practises Statement, if applicable, that the certificates are issued to the public and the need to use a secure signature creation of message decryption device.
- Clauses on the issue, revocation, renewal, and if applicable, recovery of private keys.
- Statement that the information contained in the certificate is correct, excepting a notification otherwise by the subscriber.
- Consent for storing the information used for the subscriber log file, for supplying a cryptographic device and for the disclosure of such information to third parties should Izenpe terminate its services without revocation of valid certificates.
- Limits on the use of the certificate.
- Information on how to validate a certificate, including the requirement of verifying the certificate's status, and the conditions under which one can reasonably trust the certificate.
- Applicable limitations of liability, including the usages for which Izenpe accepts or excludes liability.

- Archive period for information from certification application.
- Archive period for audit records.
- Applicable procedures to dispute resolution.
- Applicable law and competent jurisdiction.
- Whether Izenpe has been declared in conformity with the certification policies of other public entities and, if so, with which system.
- The way in which Izenpe guarantees liability for damages.

7.4 REGISTRATION AUTHORITY

The Registration Authority assumes the following obligations:

- To verify the identity and other personal circumstances of the applicant, subscriber or key holder, if applicable, on the certificates, or that are relevant, as per these procedures.
- Keep all the information and documentation relating thereto, the issue, renewal, revocation or reactivation of which it manages.
- To notify Izenpe of revocation requests with due diligence and in a swift and reliable manner.
- To allow Izenpe access to its procedures archives and audit logs in order to perform its functions and maintain the necessary information.
- To inform Izenpe of all issuance, renewal, revocation requests and any other aspects related to the means issued by Izenpe.
- Verify, with due diligence, the reasons for revocation that may affect the validity of the means.
- Comply with the procedures established by Izenpe and the legislation in force in this area in the performance of its functions of issuing, renewing and revoking means of identification.
- If necessary, it may assume the function of making the technical procedures for signature creation (private key) and electronic signature verification (public key) available to the key holder.

7.5 OBLIGATIONS OF THE CERTIFICATE SUBSCRIBER

- Provide Izenpe with complete and appropriate information in accordance with the requirements described in the Certification Practice Statement, particularly with regard to the registration procedure.
- Be aware of, and accept conditions for certificate use, as well as modifications made to said conditions.
- State their consent prior to issuing and delivering a certificate.
- Guarantee the proper usage and maintenance of certificate media storage.
- Make proper use of the certificate and in particular, comply with the usage limitations thereto.
- Diligently safeguard credentials to prevent unauthorised use in accordance with the Certification Practice Statement.

- Notify Izenpe and any other person the subscriber thinks might rely on the certificate without any reasonable delay if any of the following occur:
    - Loss, theft or potential compromise of credentials.
    - Inaccuracies or changes to the certificate of which the subscriber is aware or may be aware, urging that the certificate be revoked when said modification is a reason for it to be revoked.
- Stop using the means of identification after the period of validity has expired.
- Transfer specific obligations to key owners.
- Refrain from monitoring, interfering with, or reverse engineering the technical implementation of certification services without prior written approval from the Certification Authority.
- Refrain from intentionally compromising the security of certification services.
- Refrain from using the private keys corresponding to the public keys included in the certificates for the purpose of signing a certificate as if performing the function of a Certification Authority.

The certificate subscriber accepts the terms and conditions of the CPS published at www.izenpe.eus/dpc, and the corresponding certificate policy, also available at www.izenpe.eus.

7.6 OBLIGATIONS OF THE CERTIFICATE VERIFIER USER

The certificate verification user undertakes to:

- Independently ensure that the certificate is appropriate for its intended use.
- Be aware of the conditions for using the certificates in compliance with what is set forth in the Certificate Practice Statement.
- Verify the validity or revocation of issued certificates, to which end the user shall use information on the status of the certificates.
- Verify all certificates in the certificate hierarchy, before trusting the digital signature or any of the certificates in the hierarchy.
- Bear in mind any limitation in the use of the certificate, regardless of whether this is found in the very certificate itself or in the verifying contract.
- Bear in mind any precaution stipulated in a contract or other instrument, regardless of its legal nature.
- Notify any anomalous circumstance or situation regarding the certificate that may be deemed as a cause to revoke it.
- Refrain from monitoring, interfering with, or reverse engineering the technical implementation of certification services without prior written approval from Izenpe.
- Will refrain from intentionally compromising the security of certification services.

- The qualified user of certificates issued on a secure signature creation device must recognise, in the due legal instrument, that such electronic signatures are electronic signatures equivalent to handwritten signatures, as per eIDAS.

8 RESPONSIBILITIES

8.3 RESPONSIBILITIES OF THE CERTIFICATION AUTHORITY

Izenpe shall be liable,

- for harm and damage caused to any individual or entity due to a lack of or delay in inclusion in the consulting service for the validity of certificates or expiry of certificate validity.
- For any damage caused to any person as a result of failure or delay in inclusion in the service for checking the validity of the identification mechanism.
- Furthermore, it shall be held liable to third parties for actions of individuals to whom it has delegated the roles necessary to provide certification services. In this regard, a civil liability insurance policy has been taken out to cover the risk of liability for harm and damage that may arise in using the certificates.

Izenpe is liable for negligence or a lack of due diligence exercised in providing the certification services provided, and for a failure to meet any of the legal obligations set forth in electronic signature legislation, except in the following cases of damages caused by:

- The information contained in the certificates, provided that the content thereof substantially complies with the Certification Practice Statement.
- Certificate expiration, provided that it substantially complies with the publication obligations set forth in this Certification Practice Statement.
- Improper use or after revocation of the means of identification.
- It shall be held liable for any direct, indirect, special, incidental, or consequential damages, or for any loss of profits, loss of data, or punitive damages arising from, or in connection with, the use, delivery, license, performance or non-performance of certificates, digital signatures or any other transactions or services offered or contemplated by this Certification Practice Statement arising from misuse.
- For damages to subscribers or bona fide third parties due to inaccuracies in the information contained in the certificate when such information has been certified by an official, notarised or otherwise authorized document, except in the case of documents supplied by the Registration Authority.

For damages to subscribers or bona fide third parties for failure to comply with the duties attached to subscribers or relying parties.

8.4 REGISTRATION AUTHORITY RESPONSIBILITIES

Any organisation other than Izenpe that acts in the role of Registration Authority shall be liable to Izenpe for damages incurred in the performance of the duties it assumes, under the terms established in the corresponding legal agreement.

8.5 RESPONSIBILITIES OF THE HOLDER OF MEANS OF IDENTIFICATION

- a falsehood or misrepresentation of fact during the registration process
- the use of identification means in electronic transactions with unauthorised persons.
- Failure to take reasonable precautions to prevent the loss, disclosure, alteration or unauthorised use of the identification means.

8.6 RESPONSIBILITIES OF THESUBSCRIBER

The Subscriber shall be responsible for all electronic communications authenticated using a digital signature generated with his/her private key, when the certificate has been validly confirmed through the verification services provided by Izenpe.

If no notification of loss or theft of the certificate is received, as laid down in the Certificate Practice Statement, any liability resulting from the unauthorised use and/or misuse of the certificates shall, in all cases, be the responsibility of the Subscriber.

By accepting the certificates, the Subscriber undertakes to protect and, where applicable, indemnify Izenpe, the Registration Authorities and the User Entities for any act or omission that may result in damages, loss, debts, legal fees or any other type of expense, including payment for professional services, incurred by Izenpe, the Registration Authorities and the User Entities, caused by the use or publication of certificates, and which result from:

- the failure to comply with the terms and conditions laid down in the legal instrument that binds it to the Certification Authority.
- the use of digital certificates in electronic transactions with unauthorised persons.
- a falsehood or misrepresentation of fact by the Subscriber.
- failure by the Subscriber to disclose a material fact in the certificates, if the misrepresentation or omission was made negligently or with intent to deceive Izenpe, the Public Entity Users or parties relying on the subscriber's certificate.
- the failure to protect the private key or to otherwise take reasonable precautions to prevent the loss, disclosure, modification or unauthorized use of the private keys.

In this sense, Izenpe shall not be held liable for damages to subscribers or bona fide third parties for failure to comply with the following duties attached to the subscriber:

- Provide Izenpe or the Registration Authority with full, complete and precise information on their certificate applications and the any other information needed for the issuance or revocation thereof, when inaccuracies in the information have not been detected by the service provider.
- Promptly notify Izenpe or the Registration Authority of any changes in the information submitted for the certificate.
- Diligently save signature creation data in order to ensure confidentiality and protect the data from any access or revelation.

- Apply for certificate revocation if there is any doubt regarding maintaining the confidentiality of signature creation data.
- Abstain from using the signature creation data from the time the certificate's validity period expires, or the service provider notifies that it is no longer valid.
- Follow the limits on the certificate regarding its possible uses, and using it as per the established conditions communicated to the certification services signatory.

8.7 RESPONSIBILITIES OF THIRD PARTIES RELYING ON CERTIFICATES

A relying party who vests trust in a certificate that has not been verified assumes all of the risks associated therewith and under no circumstances shall hold Izenpe, the Registration Authorities, User Entities or Subscribers liable for any circumstance resulting from their trust in such certificates and signatures.

In this sense, Izenpe shall not be held liable for damages to subscribers or bona fide third parties if the recipient of the electronically signed documents fails to comply with any of the following due diligence obligations:

- Verifying and bearing in mind the restrictions on the certificate regarding its possible uses and the itemised amount of transactions that can be made with it.
- Ensuring the validity of the certificate.

9 AGREEMENTS, CERTIFICATION PRACTICE STATEMENTS AND APPLICABLE CERTIFICATE POLICIES

All applicable agreements, CPS and Policies can be found at www.izenpe.eus

10 REFUND POLICY

Izenpe does not have a refund policy and abides by the legislation in force.

11 PERSONAL DATA PROTECTION

The regime applicable to the processing of personal data carried out by Izenpe shall be that provided for in REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (hereinafter, GDPR) and its implementing regulations and any other applicable legislation in force.

Izenpe has information regarding the processing at the following address www.izenpe.eus/datos

12 APPLICABLE LEGISLATION CONFLICT RESOLUTION MECHANISMS

12.1 Applicable regulations

The implementation, preparation, interpretation and validity of this Certification Practice Statement are governed in accordance with Spanish law on electronic signatures.

The applicable regulations to this document and the operations deriving from them are as follows:

- Law 6/2020, of 11 November, regulating certain aspects of electronic trust services.
- Public Administration Common Administrative Procedural Law 39-2015
- Public Sector Legal Scheme Law 40-2015
- REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 27 April on the protection of natural persons regarding personal data processing and the free circulation of these data, repealing Directive 95/46/).
- European Regulation 910/2014 on electronic identification and trust services for electronic transactions in the domestic market (eIDAS).

12.2 Complaints and dispute resolution.

Izenpe is subject to the commercial arbitration system pursuant to the provisions of applicable law as a means of addressing and resolving disputes or claims lodged by applicants or subscribers of citizen certificates; all decisions are deemed to be final and binding by both parties.

To this effect it is understood that the applicant or subscriber conforms to the system from the time the claim for arbitration is submitted to the corresponding commercial arbitration board.

Any other contentious matters brought forward by applicants or subscribers with regard to citizen certificates not regulated by the commercial arbitration system shall be subject to the competent jurisdiction.

13 AC AND REPOSITORY AUDITS, CERTIFICATIONS AND TRUSTMARKS

In order to develop and effectively implement these services, Izenpe has established an information security system for processes related to trust services, as per standard ISO 27001.

Izenpe also follows the indications of the ETSI (European Telecommunications Standards Institute) standards and has achieved certification under the technical specifications of the EN 319 411-2 standard for the issue of qualified certificates, the EN 319 411-1 standard for the issue of public key certificates, and the EN ETSI EN 319 422 standard for the issue of time-stamp tokens. These standards are those required by Regulation 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS).

For secure server certificates that follow the Extended Validation Certificate Policy (EVCP), for secure server certificates that follow the Organisation Validation Policy (OVCP) and for secure server certificates that follow the Domain Validation Policy (DVCP), the guidelines approved by the CA/Browser Forum, available at www.cabforum.org, are also followed.

All accreditations are available for consultation at www.izenpe.eus