CERTIFICATION PRACTICE STATEMENT

Reference:	IZENPE-CPS
Version no.:	v 5.03
Date:	10th March 2015

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

www.izenpe.com
info@izenpe.com
Tel.: 945 017 490

Table of Contents

Contents

1 Introduction

The Basque public authorities, as promoters of the Information Society, and in the endeavour to guarantee full incorporation of information and communication technologies to the economic and social activities of its citizens, has set up instruments permitting citizens to relate to the different administrations, bodies and companies with a view to guaranteeing data privacy and personal intimacy and protecting their rights, always with the best possible security guarantees.

Based on the above, the Basque Government and the Provincial Councils, through their respective IT companies, decided to collaborate on the development of a common system of certification and electronic signature that would ensure interoperability. This way any certificates issued would be valid in applications and procedures corresponding to the different administrations.

The first expression of this desire to collaborate came in June 2002 with the founding of "Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, IZENPE, S.A." (Certification and Services Company, hereinafter IZENPE), fully owned by the said IT companies.

IZENPE was constituted as the instrument or organization to provide Basque public administration IT companies with management in their joint interest of electronic certification, proving itself to be an ideal means of simplifying citizen/administration relations.

Article 4 of Electronic Signature Act 59/2003, dated 19th December, envisages the possibility that certification services be provided by administrations or by the bodies or companies dependent upon them.

IZENPE is therefore a certification authority dependent on the Basque administrations which has the following corporate purpose:

- To foment the use and development of electronic government based on telecommunications networks and backed by guaranteed security, confidentiality, authenticity and irrevocability of transactions
- To provide technical, administrative and security services with respect to ITC communications.

Similarly, with the objective of effectively developing and introducing electronic certification, it has introduced an information security management system for the processes of Operating and Maintaining Infrastructure and the Issuance, Validation and Revocation of Digital Certificates compliant to ISO standard 2700.1

In addition, IZENPE follows the ETSI standards (European Telecommunications Standards Institute) and has obtained certification under the technical specifications (TS) of the 101 456 standard for issuing qualified certificates generated in a secure signature creation device (QCP Public + SSCD) and the 102 042 standard for issuing qualified and non-qualified certificates. For the secure server certificates that follow the Extended Validation Certificate Policy (EVCP) and for the secure server certificates that follow the Organizational Validation Certificates Policy (OVCP), the guides approved by the CA/Browser Forum will also be followed.

The technical specifications (TS) defined in standards TS 101 456 and TS 102 042 establish the basic requirements for the operation and management practices for certification authorities that issue qualified and non-qualified certificates in accordance with European Parliament Directive 1999/93/EC incorporated into the Spanish legal system in Electronic Signature Act 59/2003, and later with EU Regulation 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS).

1.1 Overview

IZENPE operates a Public Key Infrastructure with a view to providing the following services:

- IZENPE *Digital Certification Service* issues qualified certificates and ordinary certificates without the legal effect of qualified certificates, pursuant to *Electronic Signature Act 59/2003, dated 19th December* (henceforth, LFE).
- The *Time Stamp Service* provides User Entities with proof of the existence of a certain piece of information at a particular time.
- The *Advanced Verification Program* enables user entities to benefit from the certificates issued by IZENPE by verifying the status of certificates based on the OCSP (Online Certificate Status Protocol).
- The Verification Service enables the User Entity to benefit from the use of certificates issued by IZENPE by verifying the status of certificates based on the CRL (Certificate Revocation List).
- ZAIN is a trusted signature services platform which provides a series of online global, standardized security services (authentication, authorization, electronic signature and data protection).
- IZENPE offers id@zki free of charge id@zki is a Java applet application integrated in a browser to provide electronic signature encryption.
- The Izenpe digital signature service is a digital version of the traditional signature folder. It consists of a tray in which the person receives the to-be-signed documents.
- The certified communication service ZIURRA acts as a Trusted Third Party ("digital notary"), giving proof that an email or SMS has been sent and that it has been received by the recipient.
- The Publication Proof and Accreditation Service makes it possible to reliably verify the time the information included in a public contract is first made public.
- EGOITZA is the certificate cloud hosting service which enables secure hosting of end user certificates. "

In the scope of the present Certification Practice Statement and the *Specific documentation for each certificate*, IZENPE issues the following types of certificates:

SCOPE	CERTIFICATE
Natural person	
Citizen	- Citizen

Corporate scope	- Public Entity Personnel Certificate - Basque Government Personnel - Qualified corporate certificate - Non-qualified corporate certificate - Qualified Private Corporate Certificate - Non-qualified Private Corporate Certificate
Others	- Health System Identifier - Basque Centers-Euskal Etxeak
	-
Legal person	
Entity and Entity without legal personality	- Entity - Entity without legal personality
Administrative Body and Electronic Stamp	- Administrative Body - Electronic stamp
Device	
SSL and Electronic office	- SSL - EV SSL - Electronic office - EV Electronic office
Computer device and code signature	- Application - code signature

The specificities for each kind of certificate issued by IZENPE are regulated in the *Specific documentation for each certificate*, attached to this document entitled *Certification Practice Statement.*

1.2 Identification

In order to be able to individually identify each type of certificate issued by IZENPE according to this Certification Practice Statement, an object identifier (OID) is assigned to each one and is indicated in the corresponding section of the certificate.

This OID always starts with the following sequence: 1.3.6.1.4.1.14777.

1.3 Participants in the Public Key Infrastructure (PKI)

The parties involved in the management and operations of the Certification Authority are:

- Certification Authorities
- Registration Authorities
- Certificate Users

1.3.1 Certification Authorities

IZENPE has the following certification authorities:

- Root Certification Authority
- Subordinate Certification Authorities

ROOT CERTIFICATION AUTHORITY

This is the certification authority that issues certificates for the subordinate certification authorities.

IZENPE has the following root certification authorities.

Root CA 2003

Subject	E = Info@izenpe.com CN = Izenpe.com L = Avda del Mediterraneo Etorbidea 3 - 01010 Vitoria-Gasteiz O = IZENPE S.A. - CIF A-01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8 C = ES
Validity dates	From 31/1/2003 until 31/1/2018
SHA1 thumbprint	4a 3f 8d 6b dc 0e 1e cf cd 72 e3 77 de f2 d7 ff 92 c1 9b c7

Root CA 2007

SHA-1

Subject	CN = Izenpe.com O = IZENPE S.A. C = ES
Validity dates	From 13/12/2007 until 13/12/2037
Thumbprint	30 77 9e 93 15 02 2e 94 85 6a 3f f8 bc f8 15 b0 82 f9 ae fd
Subject alternative name	Directory name: RFC822=info@izenpe.com Directory address: STREET= Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz

	O = IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8

SHA-256

Subject	CN = Izenpe.com O = IZENPE S.A. C = ES
Validity dates	From 13/12/2007 until 13/12/2037
Thumbprint	2f 78 3d 25 52 18 a7 4a 65 39 71 b5 2c a2 9c 45 15 6f e9 19
Subject alternative name	Directory name: RFC822=info@izenpe.com Directory address: STREET= Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz O = IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8

Subordinate Certification Authorities

The following are certification authorities that issue digital certificates to end entities.

- CA for Citizens/Qualified entities
- CA for Citizens /NON-qualified entities
- CA for NON-qualified public administrations
- CA for Qualified public administrations
- CA for Basque Government Personnel
- CA for EV SSL

Subordinate certification authorities **2009**

CA Citizens/Qualified entities

SHA1

Subject	CN = Herritar eta Erakundeen CA - Citizen and Entity CA (4) OU = NZZ Ziurtagiri publikoa - ICS Public certificate O = IZENPE S.A. C = ES
Subject alternative name	URL=http://www.izenpe.com Directory name: RFC822=info@izenpe.com Directory address: STREET= Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz O = IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
Validity dates	From February 24, 2009 9:05:46 until Sunday, December 13, 2037 0:00:00

SHA1 thumbprint	9f dc e9 42 9b 3d 7e 59 49 9d c3 f8 3c 93 66 65 22 69 a7 59

SHA 256

Subject	CN = Herritar eta Erakundeen CA - Citizen and Entity CA (4) OU = NZZ Ziurtagiri publikoa - ICS Public certificate O = IZENPE S.A. C = ES
SubjectAlternativeName	URL=http://www.izenpe.com Directory name: RFC822=info@izenpe.com Directory address: STREET= Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz O = IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
Validity dates	From Wednesday, October 20 2010 9:16:02 until Sunday, December 13 2037 0:00:00
Thumbprint	08 d8 d6 2a 1a 15 36 c5 3a 0f 9a 18 35 bf 82 c9 f0 96 83 23

CA Citizens /NON-qualified entities

SHA1

Subject	CN = Herritar eta Erakundeen CA - Citizen and Entity CA (3) OU = NZZ Ziurtagiri publikoa - ICS Public certificate O = IZENPE S.A. C = ES
Subject alternative name	URL=http://www.izenpe.com Directory name: RFC822=info@izenpe.com Directory address: STREET= Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz O = IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
Validity dates	From Wednesday, January 30, 2008 10:54:24 until Sunday, December 13, 2037 0:00:00
SHA1 thumbprint	06 fb ac 35 ae 18 fc bf 22 29 78 8d d1 2d ac 89 8e 74 52 ae

SHA 256

Subject	CN = Herritar eta Erakundeen CA - Citizen and Entity CA (3) OU = NZZ Ziurtagiri publikoa - ICS Public certificate O = IZENPE S.A.

	C = ES
SubjectAlternativeName	URL=http://www.izenpe.com Directory name: RFC822=info@izenpe.com Directory address: STREET= Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz O = IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
Validity dates	From Wednesday, October 20 2010 9:18:07 until Sunday, December 13 2037 0:00:00
Thumbprint	87 56 60 a3 5c b1 03 d7 e0 bb 00 44 24 f1 6d bf bf 21 e0 b4

CA Qualified public administrations

SHA1

Subject	CN = EAEko HAetako langileen CA - Basque PA personnel CA (2) OU = AZZ Ziurtagiri publikoa - ACS Public certificate O = IZENPE S.A. C = ES
Subject alternative name	URL=http://www.izenpe.com Directory name: RFC822=info@izenpe.com Directory address: STREET= Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz O = IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
Validity dates	From Tuesday, February 24, 2009 9:03:29 until Sunday, December 13, 2037 0:00:00
SHA1 thumbprint	e5 c8 62 ed dc f1 14 c8 26 61 98 4a d6 48 ad f2 3f 51 10 fc

SHA 256

Subject	CN = EAEko HAetako langileen CA - Basque PA personnel CA (2) OU = AZZ Ziurtagiri publikoa - ACS Public certificate O = IZENPE S.A. C = ES
SubjectAlternativeName	URL=http://www.izenpe.com Directory name: RFC822=info@izenpe.com Directory address: STREET= Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz O = IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8

Validity dates	From Wednesday, October 20 2010 9:22:40 until Sunday, December 13 2037 0:00:00
Thumbprint	93 a1 44 6b 61 99 4b 5b 0e 99 d0 5b 14 cd bb 32 2e 6c 17 64

CA NON-qualified public administrations

SHA1

Subject	CN = EAEko Herri Administrazioen CA - Basque PA CA (2) OU = AZZ Ziurtagiri publikoa - ACS Public certificate O = IZENPE S.A. C = ES
Subject alternative name	URL=http://www.izenpe.com Directory name: RFC822=info@izenpe.com Directory address: STREET= Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz O = IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
Validity dates	From Tuesday, February 24, 2009 9:00:23 until Sunday, December 13, 2037 0:00:00
SHA1 thumbprint	7f 58 bb 8f 87 11 c0 49 61 28 cf 71 63 4b 77 95 0a dd d3 2c

SHA 256

Subject	CN = EAEko Herri Administrazioen CA - Basque PA CA (2) OU = AZZ Ziurtagiri publikoa - ACS Public certificate O = IZENPE S.A. C = ES
SubjectAlternativeName	URL=http://www.izenpe.com Directory name: RFC822=info@izenpe.com Directory address: STREET= Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz O = IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
Validity dates	From Wednesday, October 20 2010 9:23:33 until Sunday, December 13 2037 0:00:00
Thumbprint	f7 9c da 11 e7 91 74 19 a0 41 8d b8 4b a7 43 c5 31 3a d7 f0

CA Basque Government Personnel

SHA1

Subject	CN = Eusko Jaurlaritzako langileen CA - CA Basque Government Personnel OU = Ziurtagiri publikoa - Public certificate O = IZENPE S.A. C = ES
Subject alternative name	URL=http://www.izenpe.com Directory name: RFC822=info@izenpe.com Directory address: STREET= Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz O = IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
Validity dates	From Thursday, February 11, 2010 11:43:40 until Tuesday, February 11, 2020 11:43:40
SHA1 thumbprint	4a 17 ed d4 9e d4 cc 39 24 3a be 74 b8 92 df aa 00 68 6a 80

SHA 256

Subject	CN = Eusko Jaurlaritzako langileen CA - CA Basque Government Personnel OU = Ziurtagiri publikoa - Public certificate O = IZENPE S.A. C = ES
SubjectAlternativeName	URL=http://www.izenpe.com Directory name: RFC822=info@izenpe.com Directory address: STREET= Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz O = IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
Validity dates	From Thursday, February 11, 2010 11:45:37 Until Tuesday, February 11 2020 11:45:37
Thumbprint	25 e9 d1 6d f8 d6 4a 60 73 40 8c be 24 8e 52 9c 23 9e 32 92

CA EV SSL

SHA1

This CA is obsolete and has been replaced by the following

Subject	CN = CA of EV SSL Certificates OU = BZ Ziurtagiri publikoa - EV Public certificate O = IZENPE S.A. C = ES
SubjectAlternativeName	URL=http://www.izenpe.com Directory name: RFC822=info@izenpe.com Directory address: STREET= Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz O = IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
Validity dates	From Wednesday, October 20 2010 9:27:24 Until Tuesday, February 20 2020 9:27:24
SHA1thumbprint	67 16 29 9c c4 c0 ca 25 52 ee 88 01 9a fc ee 49 b2 a1 63 34

SHA 256

Subject	CN = CA of EV SSL Certificates OU = BZ Ziurtagiri publikoa - EV Public certificate O = IZENPE S.A. C = ES
SubjectAlternativeName	URL=http://www.izenpe.com Directory name: RFC822=info@izenpe.com Directory address: STREET= Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz O = IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
Validity dates	From Wednesday, October 20 2010 9:28:56 Until Tuesday, February 20 2020 9:28:56
Thumbprint	6c 48 4d 0f 4d b2 95 ec 67 eb b3 e0 5e 3d c2 14 49 2a 9a b8

1.3.2 Registration Authorities

This Certification Practice Statement applies to the Registration Authorities used by IZENPE when issuing and managing certificates.

Registration Authorities identify applicants, subscribers and holders of certificate keys, verify the documentation accrediting the circumstances appearing in the certificates, and validate and approve requests to issue, revoke and renew certificates.

IZENPE or the user entities with which IZENPE signs the corresponding legal instrument are the registration authorities.

1.3.3 End entity users of certificates

Certificate end entities are individuals and organizations that utilise the services of issuance, management and use of digital certificates.

Certification system end entities are:

- Certificate applicants
- Certificate signer
- Certificate subscribers
- Key owners

The details for each type of certificate are defined in the *Specific documentation for each certificate.*

Certificate applicants, all certificates must be requested by an individual in his or her name or in the name of an organization.

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 subscribers, subscribers are the natural or legal persons identified in the certificate.

Key owners are the natural persons who own or are responsible for safeguarding the digital signature keys.

1.3.4 End entity users of timestamp services

End entity users of timestamp services are the individuals and organizations that benefit from the timestamp issuance services.

1.3.5 Relying parties

For the purposes of this Certification Practice Statement, the natural or legal persons who receive certificates and timestamps issued by IZENPE are third parties who trust in certificates and timestamps issued by IZENPE and, as such, are governed by the stipulations contained in this Certification Practice Statement when they decide to effectively trust the certificates or timestamps.

Third parties are understood to trust the certificates and timestamps in accordance with the use they make thereof in their relationships with subscribers.

When this use has been made, special consideration shall be given to the fact that the party has made no declarations expressing lack of reliance on the certificates or digital signatures attached to the messages, and therefore establishing that the party did effectively rely on the certificates and digital signatures, provided that certificates were valid, signatures were created during the validity period of the certificates and all other requirements determining the trustworthiness of a certificate have been met.

Third parties shall exercise due diligence in using each type of certificate and timestamp and shall keep to the principle of good faith and loyalty, abstaining from any fraudulent or neglectful conduct meant to repudiate messages issued within the level of trust attached to the category of certificate or timestamp.

1.4 Certificate uses

The permitted and prohibited usages of the certificates issued by IZENPE are described below.

1.4.1 Appropriate certificate uses

Qualified certificate

Usage of qualified certificates:

Qualified electronic signature certificates guarantee the identity of the subscriber and the private key holder. When they are used with secure signature creation devices they are suitable to offer support to the qualified electronic signature; in other words, an advanced electronic signature based on a qualified certificate that has been generated using a safe mechanism, and therefore, under Article 3.4 of the LFE, has the equivalent legal status of handwritten signatures without the need to meet any additional requirements.

Qualified electronic signature certificates can also 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 is used to guarantee the identity of the certificate subscriber.

Qualified certificates conform to technical standard TS 101 456 of the European Telecommunications Standards Institute ETSI.

Non-qualified certificate

Non qualified certificates guarantee the identity of the subscriber and, when appropriate, the private key holder; they should also be used in conjunction with a reasonably secure signature generation mechanism.

Non-qualified electronic signature certificates can also 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. In this case it is not equivalent to a handwritten signature. However, this digital signature is used to guarantee the identity of the certificate subscriber.

The Electronic main office and Electronic main office EV certificates are issued to reliably identify websites.

Electronic main office and stamp certificates are issued to public administrations for the identification of administrative headquarters and electronic stamping of documents, in accordance with *Law 11/2007 on electronic access of citizens to public services*.

The certificates can also provide support for multiple forms of authentication and advanced electronic signature when used in conjunction with software designed to offer reliable private key protection.

General usage certificates follow Technical Specification 102 042 from the European Telecommunications Standards Institute ETSI.

Computer security certification

Secure server certificates (SSL DV, SSL OV, SSL EV, Sede and Sede EV) and certificates for entities responsible for computer devices are issued.

This type of certificate follows the standards approved by the CA/Browser Forum and audited according to the technical specification TS 102 042, by ETSI both for its extended validation policy and the basic policy.

Code signing certificate

These certificates are issued to owner entities to guarantee the authentication and integrity of a software component.

Scope of use of certificates

There are two scenarios that illustrate certificate usage:

- Certificates issued by IZENPE to the general public are used by subscribers or, where applicable, key owners to conduct electronic transactions with Public Entity Users and public or private institutions that have accepted the use of the certificate system.

  Details on the scope of usage for each certificate are provided in the *Specific documentation for each certificate.*

- Certificates issued by IZENPE requested by user entities are used in the scope of competence of the particular organisation or post. However, key owners may also employ these certificates for other uses provided that they respect the usage limitations set forth in the paragraph a) above.

  Details on the scope of usage for each certificate are provided in the *Specific documentation for each certificate.*

1.4.2 Prohibited certificate uses

The certificates should be used exclusively for the specific purpose for which they were intended.

In the same way, the certificates should only be used in accordance with the applicable law.

No certificate regulated by this Certification Practice Statement can be used to conduct transactions as a Registration Authority.

The certificates are not designed, intended, or authorised for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation, communication, or control systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage.

1.5 Policies

1.5.1 Entity responsible for managing documentation

IZENPE, with its registered office at Avenida Mediterráneo, 14, Vitoria-Gasteiz and Tax ID no. A-01337260, is the Certification Authority which issues the certificates under this Certification Practice Statement.

1.5.2 Contact data

Name of service provider	Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, S.A.
Postal Address	c/ Beato Tomás de Zumárraga, nº 71, 1ª planta. 01008 Vitoria-Gasteiz
E-mail address	info@Izenpe.com.
Telephone	902 542 542

1.5.3 In charge of adapting the Certificate Practice Statement

The IZENPE Board of Directors is the body in charge of approving this Certificate Practice Statement and any possible changes to it.

1.5.4 Procedure to approve the Certificate Practice Statement

The final changes made to this document are approved by the IZENPE Board of Directors once it is determined that they meet the set requirements.

1.6 Definitions and acronyms

1.6.1 Definitions

- **Data Protection Agency (DPA):** a body under public law, with its own legal personality and unlimited public and private legal capacity, which acts fully independently of the public administrations in the performance of its tasks and whose main purpose is to ensure compliance with the legislation on data protection and ensure its application.
- **Certification Authority (CA):** the Certification Authority is the entity that automatically issues the necessary certificates requested by the Registration Authority following confirmation from the Local Registration Authority.
- **Registration Authority (RA):** the entity entrusted to process the registration (revocation and cancellation) of users in a public key infrastructure. The user must contact the registration authority to request a public key certificate with the guarantee of the certification authority associated with the registration authority.
- **Timestamping Authority (TSA):** authority that issues timestamp tokens

- Registration bodies identify applicants, subscribers and holders of certificate keys, verify the documentation accrediting the circumstances appearing on the certificates, and validate and approve requests to issue, revoke and renew certificates.
- **Certificate:** an electronic document signed electronically by a Certification Service Provider who links signature verification data to a signer and confirms his or her identity.
- **Root Certificate:** a certificate whose subscriber is a Certification Authority belonging to the IZENPE hierarchy, and which contains the CA's Signature Verification Data signed with the CA's Signature Creation Data as Certification Service Provider. The IZENPE issuing entities form a hierarchy by which there is one common root entity for any type of certificate and several subordinate entities for the different types of certificates.
- **Qualified certificate:** electronic certificates issued by a Certification Service Provider that complies with the requirements set forth in Electronic Signature Act 59/2003, dated 19th December, with regard to verification of the identity and other details of applicants and to the reliability and guarantees of the certification services rendered.
- **General usage certificates:** ordinary certificates, but without the legal effect of a qualified certificate, which guarantee the identity of the subscriber and the owner of the private key; they should also be used in conjunction with a reasonably secure signature creation mechanism.
- **Key:** sequence of symbols used for encrypting and decrypting operations.
- **Confidentiality:** confidentiality is the capacity to keep an electronic document inaccessible to all users except to a specific list of individuals. By doing so, communications are not disclosed to others and documents can only be read by the indicated recipient.
- **Cryptography:** cryptography is a branch of mathematics based on the transformation of legible data into data that cannot be read directly, e.g., information that must be decoded in order to be read.
- **Signature creation data (Private Key):** a private key is one single secret number that is held by only one person in such as way that the person can be identified by his or her private key. This key is asymmetric to the person's public key. One key can verify and decrypt what the other has signed or encrypted.
- **Signature Verification Data (Public Key):** a public key is one single number held by only one person but, as opposed to a private key, it is published. It is linked with a private key through mathematical methods and is used to encrypt and verify digital signatures.
- **Certification Practice Statement (CPS):** statement which IZENPE makes easily available through electronic means at no cost.
- The CPS is considered to be a security document which details, within the framework and provisions of Electronic Signature Act 59/2003, the obligations that Certification Service Providers pledge to undertake with regard to the management of signature creation and verification data and of electronic certificates; conditions applicable to the application, issuance, use, suspension and validity of certificates; technical and

organizational security measures; profiles and information mechanisms on certificate validity; and, where applicable, the procedures for coordinating with the corresponding public registers to allow the immediate exchange of information concerning the validity of the powers indicated in the certificates and which must necessarily be included in the registers.

- **Certificate Directory:** repository of information that conforms to standard X.500 of the ITU-T. Izenpe keeps an updated directory of certificates which includes all of the certificates issued and whether they are valid or have been suspended or expired.
- **Secure signature creation mechanism:** the device used to apply signature creation data which meets the requirements laid down in the specific rules of application in Spain, and in Directive 1999/93/CE by the European Parliament and Council, dated 13 December 1999, on a Community framework for electronic signatures.
- **Electronic signature:** a set of data in electronic form, attached to or associated with other data, used as a means of identifying the signer.
- **Advanced electronic signature:** the digital signature which allows identification of the signer and detection of any later modifications. It is also univocally bound to the signatory and to the referring data, and has been created by means under his or her exclusive control.
- **Qualified electronic signature:** a qualified electronic signature is an advanced electronic signature based on a qualified certificate and generated by means of a secure signature creation device.
- **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.
- **Hash or digital fingerprint:** a fixed-length output obtained by applying a hash function to a message, and which is associated only with the initial data.
- **HSM (hardware security module):** hardware-based security device that generates and protects cryptographic keys.
- **Public Key Infrastructure (PKI):** a PKI determines what entities form part of a certification system, the roles they play, the norms and protocols that must be followed in order to operate within the system, they way in which digital information is encoded and transmitted, and the information contained in the objects and documents managed by the infrastructure. All of this is based on Public Key technology (two keys).
- **Spanish Organic Law 15/1999 of 13 December on the Protection of Personal Data:** the purpose of the current law is to guarantee and safeguard the public freedoms and fundamental rights of individuals with regard to the processing of personal information, particularly in terms of personal and family honour and intimacy.
- **Certificate Revocation Lists (CRL):** the CRL is a list of the revoked or suspended certificates which Izenpe issues immediately when a certificate is revoked. A permanent Web service is also available to consult incremental updates of certificates revoked by IZENPE. As for publication of Certificate Revocation Lists, certificate users and subscribers are ensured secure and fast access.

- **Certificate serial number:** a whole unique value unmistakably associated with a certificate issued by any certification service provider.
- **OCSP (Online Certificate Status Protocol):** a computer protocol used to determine the status of a digital certificate.
- **OID (Object Identifier):** a unique sequence of non-negative integer values separated by dots, which can be assigned to registered objects.
- **PIN (Personal Identification Number):** a sequence of characters known only to the subject who has access to a resource protected by this mechanism.
- **PKCS (Public-Key Cryptography Standards):** the most widely-used standard for encoding different types of information, such as certificates of signed documents. Programmers and analysts refer to these conventions or standards as formats or layouts. PKCS stands for "Public Key Cryptography Standards".
- **PKCS#10 (Certification Request Syntax Standard):** Certification Request Syntax Standard. Describes the format for messages sent to a Certification Authority to request the certification of a public key.
- **PKCS #12 (Personal Information Exchange Syntax Standard):** Personal Information Exchange Syntax Standard. Describes a file format commonly used to store private keys and public key certificates protected by symmetric cryptography.
- **Certification Products:** an annex to the Certification Practice Statement which covers the scope of application, the technical characteristics of the different types of certificates, the rules indicating the procedures to be followed in rendering certification services, and the terms of use.
- **Key owners:** Key owners are the natural persons who own or are responsible for safeguarding the digital signature and decryption keys.
- **Certification Service Provider (CSP):** the individual or legal entity that issues certificates or provides other services related to electronic signatures.
- **Advanced Verification Program:** a program which enables user entities to benefit from the certificates issued by IZENPE by verifying the status of certificates based on the OCSP (Online Certificate Status Protocol).
- **PUK (Personal Unblocking Key):** sequence of characters known only to the subject who has access to a resource which is used to unblock access to that resource.
- **Publication Service:** the service that publishes all the documents associated with the certification system that should be made available to certificate users.
- **Time-Stamping Service:** this service provides user entities with proof of the existence of a certain piece of information at a particular time.
- **Secure Server:** a secure server is a Web server that uses encryption to safely transmit data from one point to another. In order to perform this operation, the server must hold a valid certificate.
- **Certificate applicant:** the individual who requests the issuance of a certificate in his or her own name or on behalf of an organization.

- **SSL (Secure Socket Layer):** a protocol that allows encrypted data to be transmitted between an Internet browser and a server.
- **Certificate Subscriber:** the individual whose personal identity is linked to the electronically signed data by means of a Public Key certified by the Certification Service Provider.
- **Cryptographic Card:** a card considered to be a Secure Signature Creation Device used by the Subscriber to: store private digital signature and encryption keys, generate electronic signatures and decrypt data messages.
- **Relying parties:** the natural or legal persons who are issued certificates by IZENPE. Upon making the decision to effectively rely on the certificates, relying parties are thus governed by the stipulations contained in this Certification Practice Statement.
- **Certificate Users:** Certificate end entities are individuals and organizations that utilise the services of issuance, management and use of digital certificates.

1.6.2 Acronyms

ARL: Certification Authority Revocation List

CA: Certification Authority

CA/B: CAs and Browser

CN: Common Name

CRL: Certificate Revocation List

DN: Distinguished Name

CPS: Certification Practice Statement

SSCD: Secure Signature Creation Device

ETSI: European Telecommunications Standards Institute

GN: Given Name

HSM: Hardware Security Module

LFE: Electronic Signature Law 59/2003 of 19 December.

LRA: Local Registration Authority

OCSP: Online Certificate Status Protocol (repository of revoked certificates based on a specific time and date)

OID: Object Identifier

PIN: Personal Identification Number

PKCS: Public Key Cryptography Standards (PKI standards developed by RSA Laboratories)

PKI: Public Key Infrastructure

CSP: Certification Service Provider

PUK: Personal Unblocking Key

RA: Registration Authority

SSL: Secure Socket Layer

TSA: Time Stamping Authority Server

2 Publication and supervisors of information repository

2.1 Information repository

IZENPE has a public information repository on http://www.Izenpe.com available 24 hours a day, 7 days a week.

2.2 Publishing certificate information

The IZENPE Repository is a system which publishes information about digital certification and related services.

Information is available at www.izenpe.com 24 hours a day, 7 days a week.

IZENPE

- guarantees on line information availability.
  However, if necessary for the purposes of auditing, inspection or cross-certification with other certification service providers, or if requested by a key owner or interested third party, IZENPE will provide a hard copy of the documents.
- facilitates the use of a fast and secure service by which relying parties can consult the register of certificates issued.
- maintains an updated directory of certificates which lists all certificates issued and whether they are valid or if their validity period has been suspended or expired.
- IZENPE also issues Certificate Revocation Lists (CRLs) and, if user accessible, real-time certificate verification services, using Online Certificate Status Protocol (OCSP).
- As for publication of Certificate Revocation Lists, certificate users and subscribers are ensured secure, fast access free of charge.

2.2.1 Publication and notification policies

IZENPE shall notify users of changes in specifications or in the terms and conditions of services via the IZENPE website home page www.izenpe.com.

For 30 days an announcement of changes made will be posted where users will find the original document, the document update and the new version.

After 30 days, the notice of amendment will be removed, as will the original version of the document. The original will be retained by IZENPE for at least 15 years and may be consulted by interested parties with justifiable cause.

2.2.2 Items not published in the Certification Practice Statement

The list of components, subcomponents and elements that exist but due to their confidential nature are not disclosed to the public are those included in section 9.3 of the present Certification Practice Statement.

2.3 Frequency of Publication

The Certificate Practice Statement is published as soon as it is approved. Changes to the Certification Practice Statement are governed by the provisions of this document.

Information concerning certification status is published in accordance with 4.9.6, 4.9.7 and 4.9.9 of this document.

2.4 Controlling access to the repository

IZENPE allows public read-only access to the information published in its Repository. However, controls are put in place to keep unauthorized individuals from adding, changing or deleting the registers provided by this service to protect the integrity and authenticity of the documents so that their content is not compromised.

IZENPE uses reliable systems to access the information repository, so that:

- Only authorized individuals can add additional information or make changes.
- The authenticity of the information can be validated.
- The certificates are available for consultation.
- Any technical change that affects the security requirements can be detected.

3 Identification and authentication

3.1 Names

3.1.1 Types of names

All end-entity user certificates contain a given name in the Subject Name field.

The attributes specified in the differentiated name in the subject field are contained in the section corresponding to the certificate profile.

The authenticated value in the *Common Name* field is the name of the key owner.

The s*ubjectAltName* field is also used on occasion to place a name that can be used to identify the subject, but different from the name that appears in the Subject Name field.

Issuer (Requisite of Article 11.2 c) LFE)

This field contains the identification of IZENPE, the Certification Authority that signed and issued the certificate.

The field cannot be left blank and must contain a differentiated number (DN) composed of a set of attributes, consistent in number or labels and an associated value.

The issuer field of the subordinate CAs coincides with the subject field of the CA that has issued the certificates.

Subject (Requisite of Article 11.2 e) LFE)

This field contains the identification of the subscriber or owner of the certificate issued by IZENPE (the CA identified in the Issuer field).

The field may not be left blank and must contain a distinguished name (DN). A distinguished name is a set of attributes consisting of a name or label and an associated value.

The detailed profile for each certificate issued by IZENPE is established in the *Specific documentation for each certificate.*

3.1.2 Rules for Interpreting name formats

No stipulation.

3.1.3 Uniqueness of names

Subscriber names and, where applicable, key owner names are unique for each type of certificate within the IZENPE Certification Practice Statement.

3.1.4 Resolving conflicts relating to names and processing trademarks

Certificate applicants are prohibited from using names in their certificate issue applications that infringe upon any third party intellectual property rights.

IZENPE does not verify whether a certificate applicant has intellectual property rights in the name appearing in a certificate application. IZENPE does not arbitrate, mediate, or otherwise

resolve any dispute concerning the ownership of any domain name of either individuals or organizations.

IZENPE reserves the right to reject any certificate application because of a name claim dispute.

Recognition, authentication, and role of trademarks

IZENPE does not determine whether a certificate applicant owns rights to any trademarks that may appear on a certificate application.

It does not act as arbitrator or mediator, or engage in any dispute resolution procedures concerning trademarks.

IZENPE reserves the right to reject a certificate application if there are any ongoing trademark claim disputes.

3.2 Validating identity

3.2.1 Methods to test private key ownership

When a pair of keys is generated,

- By a Registration Authority and the keys are stored on a cryptographic card, proof of possession of the private key is by virtue of the trusted procedure of delivery and acceptance of the cryptographic card and of the corresponding certificate and key pair stored within.
- By a Registration Authority and the keys are stored in a HSM, the key owner, possession of the private key is demonstrated by virtue of the reliable custody of the HSM and the trusted procedure for exclusive access to keys by the subscriber.
- By the key owner, possession of the private key is demonstrated by the proper use of the certificate.

3.2.2 Authentication of the Organization Identity

See *Specific Documentation for the Citizen Certificate.*

3.2.3 Authentication of the identity of a natural applicant

See Specific Documentation for the Citizen Certificate.

3.3 Identification and authentication for requests to reissue keys

In certificates in which Izenpe generates the keys, after revocation of the certificate and reissuance of a new certificate, the keys are always renewed.

3.4 Identification and authentication for revocation requests

The authentication conditions for a revocation request are explained in the *Specific documentation for each certificate*.

4 Operative requisites for the certificates' life cycle

This Certificate Practice Statement regulates the common operative requisites for the issued certificates.

The specific regulation for each type of certificate should be consulted in the *Specific documentation for each certificate*.

4.1 Certificate application

Consult *specific documentation for each certificate*

A new Issue Application will not be necessary for issues made as a result of a revocation due to a technical failure in the issuance and/or distribution of a certificate or associated documentation.

No more than one certificate can be issued with the same information on the same key owner.

For this purpose, before initiating the issuance process the Registration Authority verifies that the future key owner does not hold the same type of valid certificate for which he or she is submitting the application.

Therefore, subject to the length limitations determined by the technical factors established in the content of the certificate, the identification data are carefully taken from the identification documents.

4.1.1 Verification of application

Prior to issuing the certificate, IZENPE will check the data in the application.

4.1.2 Signing up process and responsibilities

The tasks to identify and validate the information in the certificate and validation and approval of the requests to issue, revoke and renew them will be carried out by the Registration Offices.

IZENPE's own Registration Offices or from the user entities with which IZENPE signs the corresponding legal instrument should assume the following obligations:

- To validate the identity and other personal details of the applicant, subscriber and key owner in the certificates or information relevant for the purpose of the certificates in accordance with these procedures.
- To keep all of the information and documentation concerning certificates, and manage their issuance, renewal, revocation or reactivation.
- To notify IZENPE of certificate revocation requests with due diligence and in a fast 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, reactivation requests and any other aspects related to the certificates issued by IZENPE.
- To validate, with due diligence, the circumstances for revocation that might affect certificate validity.
- To comply with the procedures established by IZENPE and with the current legislation in this area, in its management operations connected with the issuance, renewal and revocation of certificates.
- Where applicable, it can perform the function of making available to the key owner the technical procedures for signature creation data (private key) and electronic signature verification (public key).

4.2 Processing applications

4.2.1 Carrying out identification and authentication functions

It is IZENPE's responsibility to carry out the subscriber's identification properly. This process should be carried out prior to issuing the certificate.

In all cases, users should refer to the *Specific documentation for each certificate* for details regarding each.

4.2.2 Approve or deny applications

Once the certificate has been requested, the RA should verify the information provided by the applicant, including the validation of the subscriber identity.

If the information is not correct, the RA will deny the request and contact the applicant to explain why. If it is correct, the certificate will be issued.

When this request is for a certificate that includes a domain name for the authentication of a server, Izenpe will examine the Certification Authority Authorization (CAA) register, in accordance with RFC 6844. If the CAAs are present but do not allow Izenpe to issue the certificates because the server is not registered, Izenpe will not issue the certificate but will allow applicants to make another request after Izenpe has resolved the incident.

In all cases, users should refer to the *Specific documentation for each certificate* for details regarding each.

4.3 Issuance of certificate

All applications must be fully approved before certificates can be issued.

IZENPE will issue the certificate and deliver it

- In the event of delivery in person, at the time of issue, Izenpe will hand over the PIN, the personal unblocking key (PUK) and the sheet featuring the telephone identification password.

- At this point, the applicant should sign, through the Issue Application, the certificate delivery receipt.

- If the application is not in person, the certificate will be sent to the postal address given in the Issue Application, in two stages

  - Sending the certificate

  - Sending the PIN, personal unblocking key (PUK) and the sheet featuring the telephone identification password.

No unlock codes (PIN or PUK) will be delivered in the case of certificates for which Izenpe does not generate the keys.

If the applicant has not received the certificate within 1 month of applying for issue, they should contact Izenpe.

The applicant should sign and return the Receipt and Acceptance Sheet to Izenpe.

4.3.1 CA actions during issuance

Certificates can be issued either on a smartcard, HSM, or a software mechanism.

I. Issuance procedure for certificates issued on a smartcard:

- The Registration Authority authenticates the validity of the documentation submitted by the applicant.

- Following authentication, the Registration Authority requests a certificate from IZENPE.

- After verifying that the request has come from an authorized Registration Authority, IZENPE issues the certificate according to the established procedures and sends it to the Registration Authority.

- After the Registration Authority has ascertained that the request comes from IZENPE, it then downloads the certificate to the signature creation device using a secure cryptographic device management process.

- For security reasons (confidentiality of the certificate private key), a random PIN and PIN unblocking code (PUK) are generated in such a way as to remain confidential, and are delivered to the subscriber or the key owner if the two are different people.

- The certificate and envelopes containing the PIN and PUK are delivered securely in person to the certificate subscriber/key owner.

- Should IZENPE decide not to issue the certificate (even when authentication procedures are correct), the applicant will be notified of the reasons for the decision.

II. "Issuance procedure for certificates issued on HSM:

- The Registration Authority authenticates the validity of the documentation submitted by the applicant.
- Following authentication, the Registration Authority requests a certificate from IZENPE.
- After verifying that the request has come from an authorized Registration Authority, IZENPE issues the certificate according to the established procedures and sends it to the Registration Authority.
- After the Registration Authority has ascertained that the request comes from IZENPE, it then downloads the certificate to the signature creation device using a secure cryptographic device management process.
- Should IZENPE decide not to issue the certificate (even when authentication procedures are correct), the applicant will be notified of the reasons for the decision."

III. Issuance procedure for certificates issued using a software mechanism:

- The Registration Authority authenticates the validity of the documentation submitted by the applicant.
- Together with the application form, the applicant generates a key pair in the server itself giving IZENPE the technical request.
- After receiving the documentation IZENPE then issues the certificate.

Check details for each type of certificate in the *Specific documentation for each certificate*.

4.3.2 Notification to the issuance subscriber

IZENPE notifies the subscriber about the certificate emission.

4.4 Certificate acceptance

The acceptance of a certificate constitutes the subscriber's acceptance of the terms and conditions of the contract which determines the rights and obligations of IZENPE and the subscriber's understanding of the provisions of this Certification Practice Statement, which governs the technical and operational aspects of the digital certification services provided by IZENPE.

The subscriber/ key owner has 15 days from when the certificate has been delivered to ensure that it functions properly and, if necessary, return it to the Registration Authority.

If a certificate is returned due to technical defects (e.g. malfunction of certificate media storage, problems with program compatibility, technical error in certificate, etc.) or to errors in the data contained in the certificate, IZENPE shall revoke the issued certificate and issue a new one.

4.4.1 Certificate acceptance process

Depending on the certificate application document, acceptance of conditions for use and the subscriber's contract are indicated, both of which must comply. As evidence, the subscriber should sign a receipt and acceptance sheet.

4.4.2 CA publishes the certificate

Once the certificate has been accepted by the subscriber and generated, the certificate will be published in the certificate repositories that are considered necessary.

4.4.3 Notification of certificate issuance by the CA and other entities

IZENPE does not notify other entities of issuing your certificates, except for EV certificates published on the Izenpe Certificate Transparency Log Server.

4.5 Pair of keys and uses of the certificate

4.5.1 Private subscriber's key and use of the certificate

The subscriber who has custody of the keys:

- Will guarantee the proper usage and maintenance of certificate media storage.
- Will make proper use of the certificate and in particular, comply with the usage limitations thereof.
- Will diligently safeguard the private key to prevent unauthorized use in accordance with sections 6.1, 6.2 and 6.4 of 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:
    - The subscriber's private key has been lost, stolen or potentially compromised.
    - Control over the subscriber's private key has been lost due to compromised activation data (e.g., cryptographic device PIN code) or due to other reasons.

- Inaccuracy or changes to the certificate content, as notified to or suspected by the subscriber, calling for the revocation of the certificate when such changes constitute a cause for revocation.

- Will cease using the private key at the end of the certificate validity period.
- Will transfer specific obligations to key owners.
- Will refrain from monitoring, interfering with, or reverse engineering the technical implementation of certification services without prior written approval from the Certification Authority.
- Will refrain from intentionally compromising the security of certification services.
- Will 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.
- Subscribers of qualified certificates who generate digital signatures using the private key corresponding to the public key listed in the certificate must acknowledge in the appropriate legal instrument that such electronic signatures are equivalent to handwritten signatures, provided that a cryptographic device is used, pursuant to the provisions of article 3.4 of the LFE.

The subscriber whose keys are hosted on Izenpe:

- Will make proper use of the certificate and, in particular, comply with the usage limitations thereof.
- Will diligently safeguard the private key to prevent unauthorized use in accordance with sections 6.1, 6.2 and 6.4 of 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:
    - Control over the subscriber's private key has been lost due to compromise of activation data or for any other reason.
    - Inaccuracy or changes to the certificate content, as notified to or suspected by the subscriber, calling for the revocation of the certificate when such changes constitute a cause for revocation.
- Will cease using the private key at the end of the certificate validity period.
- Will transfer specific obligations to key owners.
- Will 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.
- Will 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.

- Subscribers of qualified certificates who generate digital signatures using the private key corresponding to the public key listed in the certificate must acknowledge in the appropriate legal instrument that such electronic signatures are equivalent to handwritten signatures, provided that a cryptographic device is used, pursuant to the provisions of article 3.4 of the LFE.

4.5.2 Use of the public key and the certificate by relying parties

Certificate verifiers agree to the following obligations:

- Independently assess the appropriateness of the use of a certificate and determine that it will, in fact, be used for an appropriate purpose.
- Be aware of the conditions for using the certificates in compliance with what is set forth in the Certificate Practice Statement.
- Verify the validity, suspension or revocation of the certificates issued, using information on certificate status.
- Verify all certificates in the certificate hierarchy before relying on a digital signature or on any of the certificates in the hierarchy.
- Bear in mind any usage limitations on certificates, whether contained in the certificate itself or in the verifier contract.
- Bear in mind any precautions included in a contract or other instrument, regardless of legal nature.
- Notify IZENPE of any inaccuracy or defect in a certificate which may be considered cause for revocation.
- 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.
- Users of qualified certificates must acknowledge in the appropriate legal instrument that electronic signatures are equivalent to handwritten signatures, pursuant to article 3.4 of the LFE.

4.6 Renewal of certificate without changing keys

IZENPE does not consider this option.

4.7 Renewal of certificate with change of keys

To renew a user certificate, either because it has been revoked or the validity period has expired, a new certificate should be requested by following the certificate issuance process described in the *Specific documentation for each certificate*.

Subscribers can request renewal of certificates issued on a cryptographic device up to sixty days prior to the expiration date. The validity period of the new certificate begins immediately upon the expiration date of the previous certificate.

For security reasons, renewing a certificate requires rekey, or a new key pair to be generated, except in the case of encryption certificates.

4.7.1 Circumstances to renew the certificate

The certificate can be renewed if the certificate has not expired or less than 5 years have passed since their last appearance and identification before the RA.

4.7.2 Who can request it

Any subscriber can ask for their certificate to be renewed if they meet the circumstances described in the previous point.

4.7.3 Processing renewal requests

The subscriber can contact IZENPE and request its renewal. IZENPE will inform you how to formalise your application.

4.7.4 Notification to the subscriber

The following steps will be taken:

- IZENPE will be able to check that a certificate is about to expire.
- The subscriber will be informed that they can renew their certificate.
- The subscriber will request an appointment either by phone or through the website and can even sign the application by using their certificate, signing the renewal of their certificate.
- The certificate will then be generated following the usual issuance procedure.
- The generated certificate will be delivered to the subscriber.

4.7.5 Renewed certificate acceptance procedure

The certificate will be accepted by signing the renewal electronically (in the event that it is done this way) or signing the delivery form and acceptance.

4.7.6 Publishing the certificate

Once the certificate has been renewed, the new certificate can be published in the certificate repositories considered necessary, replacing the previous certificate.

4.7.7 Notifying other entities

As recorded in point 4.4.3.

4.8 Modifying the certificate

When necessary to modify any information on the certificate, IZENPE will revoke the certificate and issue a new one.

4.9 Revocation

4.9.1 Circumstances for revocation

IZENPE will revoke certificates if any of the following events occur:

- A revocation request is made by the signer, the natural or legal person represented by the signer, an authorized third party, or a natural person who applied for a digital certificate for a legal person.
- The signature creation data of the signer or the certification service provider has been compromised or if the signer or a third party has misused the data.
- When a legal or administrative order has been issued to this effect.
- The death or termination of the signer's legal person, death or termination of the legal person represented by the signer, total or partial unforeseeable incapacity of the signer or person represented by the signer, termination of the representation, dissolution of the legal person represented, change in the circumstances of the safekeeping or use of the signature creation data included in the certificates issued to a legal person.
- IZENPE terminates its activity, except in cases where the signer has given his or her consent for electronic certificate management services to be transferred to another certification service provider.
- Change in the data supplied in order to obtain the certificate or modification in the circumstances verified for certificate issuance.
- The certificate is lost, stolen or rendered useless due to damage to the certificate media, or when the support has been changed to another support not envisaged in the certification policy.
- One of the parties breaches its obligations.
- An error is detected in the certificate issuance procedure, either because one of the prerequisites has not been satisfied or due to technical problems during the certificate issuance process.
- There is a potential threat to the security of the systems and the reliability of certificates issued by IZENPE for reasons other than the compromise of signature creation data.

- Technical failure in the issuance and/or distribution of certificates or associated documentation.
- Three months have elapsed from the time the certification is requested to time it is collected.
- If IZENPE receives an application for issuance of certificate, and a valid certificate of the same class and uniqueness already exists, the valid certificate will be revoked upon revocation request from the applicant.

4.9.2 Who can request revocation

See Specific *Documentation for the Citizen Certificate*.

4.9.3 Processing revocation requests

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 authenticated revocation request and the information justifying revocation is recorded and archived.

If revocation is requested by someone other than the applicant, subscriber or key owner, either before or concurrent with revocation, IZENPE shall inform the certificate key owner and subscriber of the revocation of its certificate and specifying the reason for revocation.

The applicant can revoke the certificate through the following channels:

- In person, on IZENPE premises
- Over the phone, by calling 902 542 542.
- Online, at the address www.izenpe.com or by email with electronically signed request using a qualified certificate.
- Or by post, sending the certificate revocation application signed and validated before a notary.

Consult the Specific Documentation on the particular type of certificate for identification requirements.

4.9.4 CA deadline to process the revocation

Once what is set forth in section 4.9.3 has been completed, and the revocation duly processed by the RA, the revocation will be made effective in accordance with current legislation.

4.9.5 Obligation to verify revocations by relying parties

The verification of the state of the certificates is compulsory for each certificate use, either by consulting the certificate revocation list (CRL) or the OCSP service.

IZENPE supplies information to verifiers on how and where to find the corresponding CRL and/or OCSP.

4.9.6 Frequency of generating CRLs

IZENPE immediately issues a Certificate Revocation List (hereinafter CRL) the moment a certificate is revoked.

The CRL contains the stipulated time for issuance of a new CRL, although a CRL may be issued prior to the time indicated on the previous CRL. If there are no revocations, the Certificate Revocation List is regenerated on a daily basis.

The CRL for the end entity certificates is issued at least every 24 hours or when a revocation occurs, valid for 10 days.

The CRL for the CA certificates (ARLs) is issued every 12 months or when a revocation occurs.

Revoked certificates which expire are removed from the CRL. They are then retained in IZENPE's internal register for a period of 15 years.

4.9.7 Time passing between generation and publication of the CRLs

Maximum latency time is set at 30 seconds from generating the CRL.

4.9.8 Availability of the online verification system for certificate status

IZENPE provides its User Entities with a real-time certificate checking service based on OCSP (Online Certificate Status Protocol). This allows them to verify certificate status.

This service is available 24 hours a day, 7 days a week.

4.9.9 Online revocation checking requisites

Use of the CRL free access service will require:

- In all cases, checking the latest CRL issued that can be downloaded at the URL address contained in the action certificate in the “CRL Distribution Point” extension.
- The user also checking the CRL(s) relevant to the hierarchy certificate chain.
- The user making sure that the revocation list is signed by the authority that has issued the certificate requiring validation.

Revoked certificates which expire will be removed from the CRL.

Use of the OCSP free access service will require:

- Checking the URL address contained in the actual certificate in the “Authority Info Access” section.
- That the user is sure that the answer has been signed by the CA issuing the certificate they wish to validate.

4.9.10 Other revocation notifications available

Izenpe sends an email to notify the certificate subscriber when a qualified certificate has been revoked.

4.9.11 Special committed key requisites

If the private key associated with the certificate is compromised, the subscriber/key owner shall notify IZENPE to request certificate revocation and cease using the certificate.

If the IZENPE CA private key is compromised, the procedure shall be in accordance with section 5.7.3 of the present document.

4.10 Certificate status services

4.10.1 Operative characteristics

IZENPE offers a free service to publish the Certificate Revocation Lists (CRL) without restricting access. Additionally, it offers certificate validation services by means of the OCSP protocol (Online Certificate Status Protocol)

4.10.2 Service availability

IZENPE provides the user entities with a 24x7 revocation service.

4.11 Finalising the subscription

When it expires or when has been revoked, the certificate is not valid for use.

Check the expiry of the different certificates in the species documentation.

4.12 Custody and recovery of keys

IZENPE does not offer this service.

5 Physical, procedural and personnel security controls

5.1 Physical controls

Controls are in place at all locations where IZENPE provides its services.

5.1.1 Site location and construction

The site where information is processed fulfils the following requirements:

- The building housing the information processing facility provides physically security. The exterior walls are solidly built, the site is continuously monitored by video cameras and only duly authorized personnel are allowed access to the site.
- All of the doors and windows are locked and protected to prevent unauthorized access.

5.1.2 Physical access

IZENPE facility

The IZENPE facility has a complete physical access control system consisting of:

- Perimeter security which extends from true floor to ceiling to prevent unauthorized access.
- Control over physical access to the facility,
    - Only authorized personnel are allowed access.
    - The rights to access the security area are reviewed and updated periodically.
    - All personnel are required to wear or carry some type of visible identification, and employees are encouraged to question anyone who does not comply with this requirement.
    - Personnel not on the IZENPE access list who may be working on the site are properly supervised.

A secure site access log.

Access mechanisms on the building's perimeter doors at the IZENPE site.

A system of closed circuit television which monitors the components IZENPE uses in providing its certification services.

RAs

The RAs comply with the necessary security criteria defined in the registration site securitization document.

5.1.3 Power and air conditioning

The data processing centre is provided with power and air conditioning sufficient to create a reliable operating environment.

The IZENPE facilities are also provided with an uninterrupted power supply (UPS and electro-power unit) which keeps the equipment running for the time needed to shut down the

systems in an orderly fashion in the event of a power failure or if the air-conditioning system causes a shutdown.

5.1.4 Water exposures

IZENPE has taken the necessary precautions to minimize the impact of water exposure.

5.1.5 Fire prevention and protection

The IZENPE data processing centre has physical barriers which extend from the true floor to the true ceiling, as well as automatic fire detection systems for the purposes of:

- Notifying surveillance and IZENPE personnel of the onset of a fire.
- Disconnecting the ventilation system, closing the fireproof gates, turning off the power supply and triggering the automatic fire extinction facility.

5.1.6 Media storage

Media containing backup information is stored in a safe and secure manner.

5.1.7 Waste disposal

A policy is in place to regulate the procedures governing the destruction of information media.

Storage media that contains confidential information is destroyed to ensure that data is no longer readable or recoverable after disposal.

5.1.8 Off-site backup

IZENPE keeps backup copies of storage media in a safe and secure environment protected against accidents and at a sufficient distance to prevent damage in the event of a disaster at the primary site.

5.2 Procedural controls

5.2.1 Trusted roles

A "trusted role" is defined as a person assigned responsibilities than can lead to security problems if not performed satisfactorily, whether accidentally or maliciously.

To ensure that trusted persons perform their corresponding duties properly, the following considerations are addressed:

- The first is that the technology is designed and configured so as to prevent errors and improper conduct.
- The second is that duties are distributed among several individuals so that any improper conduct would require the complicity of a number of them.

IZENPE has full definitions of all of the roles carried out in the organization. The duties and responsibilities associated with every role are defined, and each has a set of documented procedures which regulate the practical attached to each.

5.2.2 Number of persons required per task

To reinforce system security, more than one person is assigned to each role, with the exception of the role of operator, which can be fulfilled by the administrator.

Several individuals may also be assigned to the same role.

5.2.3 Identification and authentication for each role

Trusted roles require verification of identity by secure means; all trusted roles are performed by individuals.

IZENPE has specific documentation giving further details of each role.

5.2.4 Separating tasks among the different roles

IZENPE follows the CIMC (Certificate Issuing and Management Component) security policy which is defined in its security model.

5.3 Personnel controls

5.3.1 Background, qualifications, experience, and clearance requirements

IZENPE employs personnel with the experience and qualifications needed to perform their job responsibilities.

All personnel with trusted roles are free from any interests that may affect their impartiality regarding IZENPE operations.

5.3.2 Background check procedures

Not applicable under Spanish law.

5.3.3 Training requirements

IZENPE provides its personnel with the training needed to perform their job responsibilities competently and satisfactorily. Personnel training includes following:

- A copy of the Certification Practice Statement.
- Awareness-raising on security
- Software and hardware operation for each specific role.
- Security procedures for each specific role.
- Management and operation procedures for each specific role.
- Disaster recovery procedure.

5.3.4 Retraining frequency and requirements

Any significant change in IZENPE PKI operations will call for a training plan and implementation of the plan will be documented.

5.3.5 Job rotation frequency and sequence

Not applicable.

5.3.6 Sanctions for unauthorized actions

Information security incidents

IZENPE has a security incident management plan.

Sanctions for unauthorized actions

There is an internal disciplinary regime which defines sanctions against personnel

5.3.7 Contracting personnel requirements

IZENPE maintains a policy for contracting personnel and assigning roles and responsibilities.

5.3.8 Documentation supplied to personnel

All personnel with trusted roles receive:

- A copy of the Certification Practice Statement
- Documentation which defines the obligations and procedures associated with each role.
- Personnel also have access to the operations manuals on the various components of the system.

5.4 Audit

Audit logs are used to reconstruct significant events recorded in the IZENPE or Registration Authority software, and the user or event that gave rise to the log. Logs will also be used in arbitration to resolve any possible disputes by checking the validity of a signature at a given time.

5.4.1 Type of events recorded

The logs store:

- All events associated with the life cycle of the cryptographic keys.
- All events associated with the life cycle of the certificates.
- All events related to issuing cryptographic mechanisms.
- All events associated with the administration of accounts for IZENPE operators and administrators.

The time and date is recorded for each event using a reliable time basis.

5.4.2 Frequency of log processing

Audit logs are revised regularly by the IZENPE auditor.

5.4.3 Period for audit log retention

The information generated in the log file is retained online until it is archived. After they are archived, log files are retained for 7 years.

5.4.4 Protecting the audit log

Auditors are entitled to view audit logs.

Unauthorized deletion or modification of log entries is prevented by writing audit logs using non-writable media such as a CD-ROM or others.

5.4.5 Audit log backup procedure

Backup copies of the audit log are generated online based on the same planning and controls as for the rest of the IZENPE system.

5.4.6 Compiling logs

CA and RA log files are stored in IZENPE's internal systems.

5.4.7 Notifying the action causing the logs

There is no provision for notification regarding the subject giving rise to the log.

5.4.8 Vulnerability assessments

Regular security vulnerability assessments are performed in the IZENPE internal systems.

5.5 Registration archiving

5.5.1 Type of records archived

The following data or files, among others, are recorded:

- Data connected with the certificate registration and application procedure:
- The audit logs described in the previous section;
- Key history

5.5.2 Archive retention period

All of the information and documentation related to qualified certificates is retained for 15 years (from date of issuance); documents related to other types of certificates are retained for 7 years (from certificate end date).

5.5.3 Protecting the archive

Measures will be adopted to protect archives from manipulation or from any of the content being destroyed.

5.5.4 Archive backup procedures

A security copy policy, contingency plan and business continuity plan are in place, each of which defines the criteria and strategies for action should an incident occur. The design of the strategy for action in the case of incidents is based on the corresponding assets inventory and risk analysis.

5.5.5 Requisites for time stamping the records

The information systems used by IZENPE ensure that a record is kept of the exact time each logged event occurs. The exact time used by the systems comes from a reliable time source as to date and hour. All of the systems synchronize their time based on this source.

5.5.6 Archive system

The archive collection system is located on-site at IZENPE and at the facilities of the entities taking part in rendering of services.

5.5.7 Procedures to obtain and verify the archive information

Access to this information is limited to authorized personnel and is therefore protected against physical and logical access in accordance with sections 5 and 6 of this Certification Practice Statement.

5.6 Change of keys

To renew a user certificate, either because it has been revoked or the validity period has expired, a new certificate should be requested by following the certificate issuance process described in the *Specific documentation for each certificate*.

Key changeover entails certificate renewal.

5.7 Contingency plan

5.7.1 Incident management procedures

A Contingency Plan describes all of the actions carried out and the resources and personnel used should an incident, whether intentional or accidental, damage or render unusable the certification resources or services provided by IZENPE.

The main objectives of the Contingency Plan are:

- To maximise the effectiveness of recovery operations by establishing three phases:
    - Notification/Evaluation/Activation phase to detect and assess the damage and set the plan in motion.
    - Recovery phase aimed at temporarily and partially reestablishing services until the damage to the original system has been repaired.
    - Reconstitution phase to restore regular operations and processes.
- Identify the activities, resources and procedures needed to provide partial certification services in an alternate CPD during prolonged interruptions in regular operations.
- Assign responsibilities to personnel designated by IZENPE and provide a guide for the recovery of regular operations during long periods of interruption.
- Ensure coordination among all stakeholders (departments of the entity, external points of contact and salespeople) taking part in the planned contingency strategy.

The IZENPE Contingency Plan applies to all of the functions, operations and resources needed to restore the provision of certification services. The plan applies to IZENPE personnel associated with the provision of certification services.

The Contingency Plan establishes the participation of certain groups in the recovery of IZENPE operations.

Assessments of damages and the plan of action are described in the Contingency Plan.

Should the algorithm, combination of key sizes used or any other technical circumstance significantly reduce the technical security of the system, the Contingency Plan shall be applied. An economic impact analysis will be conducted. The analysis will address the critical nature of the security problem, its scope and the recovery strategy to manage the incident. The following points must be defined in the impact analysis report:

- Detailed description of the contingency, timeframe, etc.
- Critical nature, field
- Proposed solution or solutions
- Deployment plan for the chosen solution, which shall include at least the following aspects:
    - Notification of users by whatever means are considered most effective. Certificate requesters, subscribers and verifiers (trusted third parties) shall be included.

- The contingency will be posted on the website
- Revocation of affected certificates
- Renewal strategy

5.7.2 Action plan to deal with corrupt data and software

The strategy for dealing with problems of this type is provided in the IZENPE Contingency Plan.

5.7.3 Procedure to deal with compromised private key

The Root CA will revoke the certificate of an issuing CA if the CA's private key has been compromised.

In the event that the Root CA must revoke the issuing CA certificate, it shall immediately notify:

- The issuing CA.
- All of the RAs authorized for the registration of the issuing CA.
- All holders of certificates issued by that CA.

The Root CA will also publish the revoked certificate in the ARL (Certification Authority Revocation List).

After addressing the factors that led to revocation, the Root CA can:

- Generate a new certificate for the issuing CA.
- Make sure that all of the new certificates and the CRL issued by the CA are signed using the new key.

The issuing CA may issue certificates to all of the affected end entities.

In the event of the compromise of a root CA's key, the certificate of all the applications will be eliminated and a new certificate re-issued.

5.7.4 Business continuity after a disaster

The operation of the CA will be suspended until the disaster recovery procedure has been finalised and secure operations are re-established at the primary site location or an alternative facility.

The IZENPE Business Contingency and Continuity Plan will put into action.

5.8 Termination of the CA or RA

5.8.1 Certification Authority

IZENPE has a Termination of CA Service Plan which specifies the procedure to be carried out should such an event occur.

IZENPE must notify subscribers at least two months prior to the termination of operations, by any means that will ensure the proper transmission and reception of its intent to cease its activity as a certification service provider.

CSPs, browser manufacturers and any entity with which IZENPE has entered into a contractual relationship for the use of its certificates shall also be notified.

The IZENPE General Directorate is responsible for such notification and shall determine the most appropriate mechanism to do so.

If IZENPE decides to transfer its operations to another certification service provider, it shall notify the Ministry of Industry, Energy and Tourism and the subscribers of its certificates of the transfer agreements. In such an event, IZENPE will send a document explaining the terms and conditions of transfer and the terms and conditions of use which will govern the relationship between the subscriber and the new CSP. Notification will be made by any means that will ensure the proper transmission and reception thereof at least two months prior to the cessation of its operations.

Subscribers shall express their express consent to the transfer of certificates, thus accepting the terms and conditions put forward by the new CSP. If the two-month period has elapsed with no transfer agreement or the subscriber has not given his or her express consent, the certificates shall be revoked.

If the two-month period has elapsed and no agreement has been reached with another CSP, all of the certificates will be automatically revoked.

Any authorisation with a thirty party with whom Izenpe holds a service provision contract (identification, issue, hosting, etc.) will be taken as finalised.

5.8.2 Registration Authority

After the Registration Authority ceases to perform its operations, it shall transfer to IZENPE any records it is required to retain; any other information will be cancelled and destroyed.

6 Technical security controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

Components where the key pair is generated for each of the different entities comprising or collaborating with IZENPE:

- Root CA: the machine where the root CA resides has a specific cryptographic device (HSM) for root CA key generation.
- Issuing CAs: there is a cryptographic module in every machine used by CAs.
- User certificates issued on a cryptographic card or HSM: keys are generated by the cryptographic device
- User certificate issued in the cryptographic software medium: keys are generated by the server where the service resides
- Time Stamping Authority (TSA) server and OCSP validation server: general keys in the cryptographic module associated with the system in which both servers reside.
- In the case of keys generated by the actual holder, they should be generated following the algorithm and minimum key length recommendations defined in ETSI TS 102 176

6.1.2 Private key delivery to subscriber

Method for private key delivery to the different entities that comprise or collaborate with IZENPE:

- Certificates issued on a cryptographic card: private keys for authentication and signature are delivered on a cryptographic device.
- Certificates issued on HSM: private keys for authentication and signature are hosted on a cryptographic device
- Certificates issued on a software mechanism: the private key is generated by the server. It does not need to be delivered.

6.1.3 Public key delivery to certificate issuer

The method used by the different entities that comprise or collaborate with IZENPE for delivering the public key to the corresponding certificate issuer is as follows:

- Issuing CAs: the public key is sent to the root CA in X.509 or PKCS#10 format.
- Certificates issued on a cryptographic device: they are read from the cryptographic device.

- Certificate software mechanism: the public key is sent to the IZENPE CA in X.509 or PKCS#10 format.

6.1.4 Certification Authority public key delivery to certificate users

IZENPE CA public keys are delivered by different means, including via the IZENPE website. Section 1.3.1.1 and 1.3.1.2 of this Certification Practice Statement also contains the root CA and issuing CA footprints.

6.1.5 Key size and algorithms used

The algorithm used in all cases is RSA with SHA-2.

Key size, depending on each case, is:

- Not less than 2048 bits for keys for natural or legal persons or for device keys, OCSP Server and TSA Server and technical certificates.
- Not less than 2048 bits for CA keys issued until 2006, and 4096 bits for certificates issued as of the new root CA 2007

6.1.6 Certificate signature algorithms

The algorithm identifier (AlgorithmIdentifier) used by IZENPE to sign the certificates is SHA-2 (hash algorithm) with RSA (signature algorithm) which corresponds to "Identifier for SHA-2 checksum with RSA encryption for use with Public Key Cryptosystem One defined by RSA Inc." The padding scheme used is emsa-pkcs1-v2.1 (according to RFC 3447 section 9.2).

End user certificates are signed with RSA with SHA-2. Izenpe recommends that end users employ RSA with SHA-2 or higher when signing a certificate.

IZENPE uses an algorithm qualified by the industry and appropriate for the qualified signature proposal. For this the certificate expiry date will be taken into account in addition to following the recommendations indicated by the CA/B Forum and by the different ETSI standards.

Should the algorithm, combination of key sizes used or any other technical circumstance significantly reduce the technical security of the system, the Contingency Plan shall be applied. An economic impact analysis will be conducted. The analysis will address the critical nature of the security problem, its scope and the recovery strategy to manage the incident. The following points must be defined in the impact analysis report:

- Detailed description of the contingency, timeframe, etc.
- Critical nature, field
- Proposed solution or solutions
- Deployment plan for the chosen solution, which shall include at least the following aspects:
    - Notification of users by whatever means are considered most effective. Certificate requesters, subscribers and verifiers (trusted third parties) shall be included.
    - The contingency will be posted on the website

- Revocation of affected certificates
- Renewal strategy

6.1.7 Admissible key uses (KeyUsage field X.509v3)

All certificates include the Key Usage and Extended Key Usage extension, indicating the enabled key uses.

Digital signature, key and data encryption and no repudiation are mainly used for the former whilst the latter usually uses customer or server authentication, smartcard logon or email protection.

The root CA keys will only be used to sign subordinate CA certificates and ARLs and the keys for the subordinate CAs or issuers will only be used to sign end user certificates and CRLs

The uses admitted for each certificate's key are defined in the *Specific documentation for each certificate.*

6.2 Private key protection

6.2.1 Standards for cryptographic modules

A hardware security module (HSM) is a security device that generates and protects cryptographic keys. HSMs must comply with a minimum of FIPS 140-2 Level 3 or equivalent.

IZENPE holds protocols to check that an HSM has not been manipulated during transport and storage

Cryptographic devices with qualified electronic signature certificates, suitable as secure signature creation devices (DSCF), meet the requirements of security level CC EAL4+, although certifications complying with a minimum of ITSEC E3 or FIPS 140-2 Level 2 security criteria or equivalent are also acceptable.

The European reference standard for the subscriber devices used is CEN CWA 14169.

IZENPE, in any case, maintains control over the preparation, storage and distribution of the subscriber devices where IZENPE generates keys.

6.2.2 Private key (n out of m) multi-person control

The use of CA private keys requires the approval of at least two persons.

6.2.3 Custody of the private key

The root CA private key is held by a cryptographic hardware device certified with the FIPS 140-2 level 3 and/or CC EAL4+ standard, guaranteeing that the private key is never outside the cryptographic device. The activation and use of the private key requires multi-person control explained above.

The Subordinate CA private keys are held in secure cryptographic devices certified with the FIPS 140-2 level 3 standard.

In the case of “cloud certificates” the private keys for end user certificateswill be stored on secure cryptographic devices under standard FIPS 140-2, security level 3.

In cases where subscribers keep the private key, it will be their responsibility to keep it under their exclusive control.

6.2.4 Private key backup

There is a procedure for the recovery of cryptographic module keys of the CA (root or subordinate) which can be applied in the case of contingency. The same controls are applied as those indicated in point 6.2.2.

6.2.5 Private key archiving

IZENPE will not archive the certificate signature private key after it has expired.

Private keys for internal certificates that use the different CA system components to communicate with each other, sign and encrypt the information will be archived, after issuing the last certificate.

The subscribers' private keys can be archived by themselves, by means of preserving the signature creation device or other methods, due to the fact that they might be necessary to decrypt the historical information encrypted with the public key, as long as the custody device allows this.

6.2.6 Transfer of the private key to or from the cryptographic module

Only in the case of contingency will the procedure described in 6.2.4 be used to recover private keys in the cryptographic modules.

6.2.7 Storage of the private key in the cryptographic module

There is a CA key ceremony document describing the processes for generating the private key and the use of cryptographic hardware.

In generating CA keys, Izenpe follows the recommendations of ETSI TS 102 042, 7.2.1 g), and Baseline Requirement Guidelines 17.7.

For generating the keys for end user certificated stored "in the cloud", Izenpe follows the recommendations of the European Commission (eIDAS) and the European Technical Specification CEN/TS 419241.

In cases where private keys are stored outside the cryptographic modules, they will be protected so as to ensure the same level of protection as if they were physically inside the cryptographic modules. All HSMs used by IZENPE to store private keys for Certification Authorities have level 3 FIPS 140-2 certification.

6.2.8 Method of activating private key

The Root CA and subordinate CA keys are activated by a process that requires the simultaneous use of n out of m cryptographic devices (cards).

The subscriber's private key is accessed using a PIN. The device has a system protecting it against access attempts that block it when the wrong code is entered more than three times. The subscriber has a device unlocking code. If it is entered wrongly three times, the device is definitively locked and cannot be used.

Access of the subscriber's private key in the case of certificates stored "in the cloud" will have a second authentication factor, which may vary depending on the type of certificate.

6.2.9 Method of deactivating private key

Removal of the cryptographic card from the reader will deactivate any action in operation.

6.2.10 Method of destroying private key

There is a procedure for the destruction of CA keys.

In the event of withdrawing the HSM that houses the CA keys, they will be destroyed.

Private keys of certificates stored "in the cloud" will be eliminated once the relationship with Izenpe has ended or the certificates have expired.

This procedure is not applied to user signature or authentication keys issued on a cryptographic card, except in the case of key changeover using the same cryptographic device. In such cases the previous key will be destroyed and new keys will be generated on the same media.

6.2.11 Qualifying the cryptographic module

As indicated in section 6.2.1 of this document

6.3 Other aspects of key pair management

6.3.1 Public key archival

The certificates generated by the CA, and therefore the public keys, are stored by the CA for the period of time stipulated under current law.

6.3.2 Usage periods for the public and private keys

Usage periods shall constitute the validity period for each of the certificates.

6.4 Activation data

6.4.1 Activation data generation and installation

- Certificates issued on a cryptographic device: Activation data (PIN) or a password is needed to operate the private key associated with each certificate.

The activation data (PIN) or password:

- randomly generated by the IZENPE software and stored in the cryptographic device supported by the certificate,
- is generated and printed upon certificate issuance.
- is delivered to the user through a system which ensures confidentiality.
- IZENPE provides subscribers with an option to change the PIN code on the card.
- The PIN is never stored.

- Certificates issued on a software mechanism: the installation and activation of the private key associated with a certificate requires the use of security systems defined by the user.
- Certificates issued "in the cloud": the use of the private key associated with each certificate requires a second authentication factor.

6.4.2 Activation data protection

With regard to signature activation data, certificate users are required to:

- Memorize the data.
- Exercise the utmost care to safeguard data.
- Refrain from storing data next to the cryptographic device or sharing it with other people.
- Change the PIN and PUK before using them.

6.4.3 Other aspects of activation data

The lifetime of the activation data is not stipulated. However, they should be changed periodically to decrease the possibility of being revealed.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

A series of controls are in place in the different components making up the IZENPE certification service system (CAs, IZENPE databases, IZENPE Internet Services, CA Operation and Network Management):

- Operational controls
  - All of the operations procedures are duly documented in the corresponding operations manuals. IZENPE maintains a Contingency Plan
  - Tools have been implemented to protect against viruses and malicious codes.
  - The equipment is maintained on an ongoing basis to ensure uninterrupted availability and integrity.

- A procedure exists for saving, deleting and safely eliminating storage media, removable media and obsolete equipment.

- Data exchange. The following data exchanges are encrypted to ensure confidentiality.
  - Transmission of registration data between RAs and the registration database.
  - Transmission of pre-registration data.
  - Communication between RAs and CAs.
- The revocation publication service is available on a 24x7 basis.
- Access control.
  - Unique user IDs are used in such a way that users are associated with, and can be held responsible for, their actions.
  - Rights are assigned according to the principal of providing users with the least amount of system privileges they need to do their jobs.
  - Access rights are immediately cancelled whenever users change jobs or leave the organization.
  - The access level assigned to users is revised every three months.
  - System privileges are assigned on a case-by-case basis and terminated once the reason for their assignation is no longer valid.
  - IZENPE maintains password quality guidelines.

6.5.2 Computer security rating

The products used for the provision of certification services have the international "Common Criteria" security rating or ISO standard ISO/IEC 15408

6.6 Life cycle technical controls

6.6.1 System development controls

Implementation of the software for the production systems is controlled.

To prevent possible problems with these systems, the following controls should be considered:

- There is a formal authorization procedure for updating software libraries (including patches) in production. Authorization is granted only after making sure it functions correctly.
- A testing system is kept separate from the production system to make sure it functions correctly before moving on to production.
- A log file is retained on all library updates.
- Earlier versions of software are retained.
- The software acquired is kept at the level supported by the supplier.

6.6.2 Security management checks

The products used for the provision of certification services have the international "Common Criteria" security rating or ISO standard ISO/IEC 15408

6.6.3 Life cycle security checks

In order to conduct tests a large volume of data as similar as possible to production data is required. IZENPE avoids using production databases with personal information.

6.7 Network security controls

All security measures and controls specified for the rest of systems are applied to network devices.

A security policy for the use of networks and network services is described in the network security policy.

Users may only access the services they are authorized for.

6.8 Time source

IZENPE obtains the time from their systems by means of a connection with the Royal Navy Observatory by following the NTP protocol through the connection established with the Basque Government. The description of the NTP protocol can be found in the IETF RFC 5905 standard.

7 Certificate and CRL profiles

7.1 CRL profile

The certificates issued by IZENPE meet the following norms:

- Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 5280) April 2002
- Internet X.509 Public Key Infrastructure Authority Information Access Certificate Revocation List (CRL) Extension (RFC 4325) December 2005
- Update to DirectoryString Processing in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 4630) August 2006
- ITU-T Recommendation X.509 (2005): Information Technology - Open Systems Interconnection – The Directory: Authentication Framework.
- ETSI TS 101 867 Qualified Certificate Profile.
- RFC 3739: Internet X.509 Public Key Infrastructure – Qualified Certificate Profile.

7.1.1 Version number

The certificates issued under this Certification Practice Statement use the X509 standard, version 3.

7.1.2 Certificate extensions

The extensions used are:

- Authority key Identifier
- subjectKeyIdentifier
- basicConstraints
- keyUsage
- certificatePolicies
- subjectAltName
- issuerAltName
- extKeyUsage
- cRLDistributionPoint
- netscapeCertType
- Subject Directory Attributes
- Authority Information Access

For generic profiles of electronic signature certificates, encryption and mechanisms, see the *Specific documentation for each certificate*.

Individual profiles of each can be requested from IZENPE.

Generic profile of electronic signature certificate

Field	Contents	Required	Critical
1. X.509v1 Field			
1.1. Version	v3	YES	
1.2. Serial Number	Automatically assigned by issuing CA	YES	
1.3. Signature Algorithm	SHA-1 or higher, with RSA signature	YES	
1.4. Signature Value	Signature encoded as string of bits	YES	
1.5. Issuer Distinguished Name	Subject of the issuing CA	YES	
1.6. Validity		YES	
1.6.1. Not Before	Initial validity date of the certificate	YES	
1.6.2. Not After	Validity end date of certificate	YES	
1.7. Subject		YES	
1.7.1. CountryName (C)	ES	No1	
1.7.2. Organization (O)	Full name or Registered Name of organization of subscriber	Yes/No1	
1.7.3. Organizational Unit (OU)	Post and/or department		
1.7.4. Organizational Unit (OU)	Indication of whether certificate is qualified, where applicable	No	
1.7.5. Organizational Unit (OU)	Indication of type of certificate	YES	
1.7.6. Organizational Unit (OU)	Indication of authority	Yes/No	
1.7.7. Organizational Unit (OU)	"Terms and conditions of use " + URL reference + legal notice	Yes	
1.7.8. dnQualifier	NIF or NIE (Tax ID numbers) of subscriber (natural person) or key owner and the possibility of the Health ID card number (TIS) (*) (*) format: -dni nnnnnnnnL o -nie XnnnnnnnnL and optionally –TIS nnnnnnnn	Yes/No1	
1.7.9. Common Name (CN)	Full name of subscriber (natural person) or key owner. Registered Name for entity certificates	Yes/No	
1.7.10. GivenName	Given name of subscriber (natural person) or key owner. Given name of representative for entity certificates.	Yes	
1.7.11. Surname	Surname of subscriber (natural person) or key owner. Surname of representative for entity certificates.	Yes	

[1] Does not appear in all certificates

1.7.12. SerialNumber	Tax ID number (NIF, NIE) (*) of subscriber (natural person) or key owner. NIF or CIF of legal entity for entity certificates.	Yes	
1.7.13. 1.3.6.1.4.1.18838.1.1	Tax ID number (NIF, NIE) of person responsible for entity. Not present in others.	Yes1	
1.8. Subject Public Key Info	2048-Bit encoded public key in compliance with RFC5280 & PKCS#1	Yes	
2. X.509v3 Extensions			
2.1. Authority Key Identifier			
2.1.1. Key Identifier	Identifier of issuer's public key		
2.1.2. AuthorityCertIssuer	Name of the CA corresponding to the key identified ubkeyIdentifier		
2.1.3. AuthorityCertSerialNumber	CA certificate serial number		
2.2. Subject Key Identifier			
2.2.1. Key Identifier	Identifier of Public Key of subscriber or key owner		
2.3. Key Usage		Yes	Yes
2.3.1. Digital Signature	Selected "1"	Yes	
2.3.2. Non Repudiation	Not selected "0"		
2.3.3. Key Encipherment	Selected/Not Selected "1"/"0"2	Yes	
2.3.4. Data Encipherment	Not Selected "0" 1		
2.3.5. Key Agreement	Not selected "0"		
2.3.6. Key Certificate Signature	Not selected "0"		
2.3.7. CRL Signature	Not selected "0"		
2.4. Qualified Certificate Statements		Yes	
2.4.1. qCStatement OID		Yes	
2.5. Certificate Policies		Yes	
2.5.1. Policy Identifier	Certificate policy OID	Yes	
2.5.2. Policy Qualifier ID		Yes	
2.5.2.1. CPS Pointer	URL to the CPS	Yes	
2.5.2.2. User Notice	Field explicitText	Yes	
2.6. Subject Alternate Names			
2.6.1. rfc822Name	E-mail of subscriber or key holder		
2.7. Issuer Alternative Name			
2.7.1. dNSName	DNS address of certificate issuer		
2.8. Extended Key Usage			

[2] Depending on certificate type

2.8.1. emailProtection	OID emailProtection		
2.8.2. clientAuth	OID clientAuth		
2.9. cRLDistributionPoint			
2.9.1. distributionPoint	CRL address		
2.10. netscapeCertType	SSL client, SMIME client		
2.11. Subject Directory Attributes		Yes	
2.11.1. Date of Birth	Date of birth of subscriber (natural person) or key holder3		
2.12. Authority Information Access		Yes	
2.12.1. Access Description		Yes	
2.12.1.1. Access Method	OID of On-line Certificate Status Protocol	Yes	
2.12.1.2. accessLocation	URL of On-line Certificate Status Protocol	Yes	

7.1.3 Algorithm object identifiers

The algorithm identifier (AlgorithmIdentifier) used by IZENPE to sign the certificate is SHA-2/RSA which corresponds to "Identifier for SHA-2 checksum with RSA encryption for use with Public Key Cryptosystem One defined by RSA Inc."

7.1.4 Name forms

As indicated in section 3.1 and 3.2 of the Certification Practice Statement.

7.1.5 Name constraints

No name constraints are used.

7.1.6 Certificate policy object identifier

As indicated in section 1.2 of the Certification Practice Statement.

7.1.7 Usage of policy constraints extension

Policy constraints are not used.

7.1.8 Policy qualifiers syntax and semantics

The Certificate Polices extension contains the following policy qualifiers:

CPS Pointer: contains a pointer to the IZENPE Certificate Practice Statement http://www.Izenpe.com/cps

[3] Except for entity certificates where there is no key owner.

User notice: A drop-down text notice that appears on the screen, with an application or user request, when a third party verifies the certificate.

Policy Identifier: Indicates the certificate's OID

User Notice common to all certificates:

USER NOTICE	Bermeen mugak ezagutzeko www.Izenpe.com Ziurtagirian konfiantza izan aurretik kontratua irakurri. Limitations of liability at www.Izenpe.com Consult the contract before relying on the certificate.

7.1.9 Semantic processing for the certificate policy extension

The Certificate Policy extension can identify the policy that IZENPE associates with the certificate and where these policies can be found.

7.2 Profile of the certificate revocation list

The certificates issued by IZENPE meet the following norms:

Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 5280) April 2002

Internet X.509 Public Key Infrastructure Authority Information Access Certificate Revocation List (CRL) Extension (RFC 4325) December 2005

Update to DirectoryString Processing in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 4630) August 2006.

7.2.1 Version number

Version 2.

7.2.2 CRL and CRL entry extensions components

The following extensions are used:

Field	Required	Critical
X.509v2 Extensions		
1. Authority key Identifier	No	No
2. CRL Number	Yes	No
3. Issuing Distribution Point	Yes	No
4. Reason Code	Yes	No
5. Invalidity Date	Yes	No

7.3 OCSP Profile

The certificates issued by IZENPE meet the following norms:

7.3.1 Version number

Version 3.

7.3.2 OCSP Extensions

Field	Required	Critical
1. Issuer Alternative Name	No	No
2. Authority/Subject key Identifier	No	No
3. CRL Distribution Point	No	No
4. Key Usage	Yes	Yes
5. Enhanced Key usage	Yes	Yes

8 Timestamping Authority (TSA) Practices Statement

The Timestamping Authority (TSA) Practices Statement defines the requirements for the service provided by Izenpe. The procedures and their correct implementation are audited by an external entity, in accordance with the ETSI standard, TS 102 023 v1.2.2.

8.1 Timestamp Authority Disclosure Statement

The terms and conditions in this document are binding on all subscribers and parties who trust in the use of Izenpe timestamp services.

- For contact information, consult point 1.5.2 of this document
- All timestamp tokens issued by Izenpe include the policy object identifier (OID) 1.3.6.1.4.1.14777.3.3
- The certificate that is used to sign is generated with sha256WithRSAEncryption, with a 4096 bit key
- The hash algorithm for the token is SHA-1
- The TSA ensures a minimum UTC time accuracy of ± 1 second. The Izenpe TSA will not issue timestamp tokens if the time accuracy is not ensured
- The obligations of the timestamping authority are defined in point 10.6.11 of this document
- The obligations of the subscriber are defined in point 10.6.12 of this document
- The obligations of third parties are defined in point 10.6.13 of this document
- The responsibilities of the Timestamping authority are defined in point 10.7.2 of this document
- The cost of the service is contained in the Izenpe price catalogue
- Izenpe keeps logs of all TSA operation, as indicated in point 5.4 of this document
- Izenpe's responsibilities are defined in point 10.7.1 of this document and in the subscriber contract
- For claims and dispute resolution, consult point 10.12 of this document

Subscribers and third parties accept the terms of use defined by Izenpe

9 Compliance audits

Verification of conformity with security requirements, also known as a security audit or security review, is an activity performed to ensure compliance with and suitability of the security plan of the IZENPE certification service. The compliance audit is defined in the IZENPE Audit Plan.

On-site verification is conducted to determine whether IZENPE personnel follow the specified procedures and safeguards.

9.1 Audit frequency

Verification of conformity with security requirements is performed regularly and planned and integrated into other activities.

9.2 Auditor qualification

Auditors are qualified and have demonstrated proficiency in auditing secure systems of production, especially digital certification systems.

9.3 Auditor's relationship to audited company

Both internal and external auditors are used, but in all cases they are independent of the production service being audited.

9.4 Audit focus elements

The compliance audit will cover the following topics:

- PKI processes
- Information systems
- Data processing centre security.
- Documents

Details on how each of these topics is audited are provided in the Izenpe, S.A. Auditing Plan.

9.5 Decision making as the result of deficiencies

When it is determined that safeguards do not meet the requirements, a corrective action plan will implemented and the results of the plan reviewed.

9.6 Communicating results

Audit results reports will be delivered to the Security Committee for study.

If it is determined that certificates must be revoked as a result of a compliance audit, the report will be published by the IZENPE Repository as proof of revocation.

10 Other legal and activity matters

10.1 Fees

IZENPE will receive the corresponding economic remuneration in accordance with the fees approved by its Board of Directors.

10.1.1 Certificate issuance or renewal fees

The fees that users must pay for issuance or renovation of certificates appear in section 9.1.

10.1.2 Certificate status information access fees

IZENPE offers certificate status information services through CRLs or the OCSP free of charge.

10.1.3 Fees for other services

The fees applicable for other services will be agreed on between IZENPE and the customers of these services.

10.1.4 Refund policy

IZENPE does not have a refund policy.

10.2 Financial responsibility

IZENPE, the Registration Authorities and the User Entities shall have sufficient financial resources to maintain their operations and perform their duties.

IZENPE maintains a liability insurance policy for any errors and omissions resulting from the generation of certificates, which exclusively covers the activities performed by IZENPE. The relationship between IZENPE and the Registration Authorities, when intervening, and certificate subscribers and users is neither mandatory nor fiduciary. Certificate subscribers and users cannot compel IZENPE or the Registration Authorities to provide any services whatsoever, either by contract or any other means.

10.3 Information confidentiality

10.3.1 Scope of the confidential information

In order to provide services, IZENPE and the Registration Authorities need to collect and store certain types of data including personal information. This information is gathered directly from the affected parties with their express consent, or without consent from the affected parties in cases where the law on personal data protection provides for the collection of this type of information.

IZENPE and the Registration Authorities only collect data needed for the issuance and management of certificates and for providing other electronic signature services; data may not be used for any other purpose without the express written consent of the signatory.

IZENPE privacy policy has been developed in accordance with the current law on personal data protection.

IZENPE and the Registration Authorities shall not disclose or share personal information except those situations described in the sections of this Certification Practice Statement and in the section on the termination of services provided by IZENPE and the Registration Authorities.

The following information is kept confidential by IZENPE and the Registration Authorities:

- Certificate applications, whether approved or disapproved, and all other personal information obtained from the issuance and maintenance of certificates, except for the information indicated in the corresponding section.
- Private keys generated and/or stored by IZENPE.
- Transactional records, including full records and the audit trail of transactions.
- Internal and external audit trail records created and/or retained by IZENPE or the Registration Authorities and their respective auditors.
- Business continuity and disaster recovery plans.
- Security policy and plans.
- Records on operations and other operational plans, such as archival, monitoring and other analogous plans.

10.3.2 Information not within the scope

The following information is not considered confidential and is thus acknowledged by the affected parties in the legal instrument signed with IZENPE:

- Certificates that have been or are in the process of being issued.
- Information linking the natural person subscriber to a certificate issued by IZENPE.
- Given name and surname of the certificate subscriber in the case of certificates whose subscriber and signer are a natural person, or the full name of the key owner in the case of certificates whose subscriber is a legal person or government agency, and any other circumstance or personal detail of the certificate holder when significant to the purpose of the certificate.
- If included, the e-mail address of the certificate subscriber in the case of certificates whose subscriber and signer are a natural person, or the e-mail address of the key owner in the case of certificates whose subscriber is a legal person or government agency, or the e-mail address assigned by the subscriber for device certificates.
- The usages and financial limitations included in the certificates.
- The validity period, the date of issuance and the expiration date of the certificate.
- The certificate serial number.
- The different situations or status dates of the certificate and the commencement date for each, specifically: pending generation and/or issuance, valid, revoked, suspended or expired, and the reason for the change in status.

- Certificate Revocation Lists (CRLs), and other information regarding revocation status.
- The information contained in the IZENPE Repository.
- Any other information that is not indicated in the section on confidential information in this Certification Practice Statement

10.3.3 Responsibility to protect the confidential information

IZENPE or the Registration Authorities shall be entitled to disclose confidential information to the extent required by law.

Specifically, records that certify the trustworthiness of the information included on the certificate will be disclosed if required as evidence of certification in judicial proceedings, even without consent from the certificate subscriber.

Certificates are subject to publication in accordance with the provisions of article 18.c) of Electronic Signature Act 59/2003, dated 19th December.

10.4 Protection of personal information

10.4.1 Introduction

As a certification service provider, IZENPE protects its personal data files in accordance with Spanish Organic Law 15/1999, dated 13th December, on Personal Data Protection, and Royal Decree 1720/2007, dated 21st December, approving the ruling on security measures for automated files containing personal data and other development standards.

Taking into account what appears in the LFE, this Certification Practice Statement is considered a security document for the purposes of legislation relating to personal data protection, and meets the legal requirements.

10.4.2 Scope of application

In the security document for the protection of files containing personal data IZENPE establishes the security measures required to ensure that the personal information in their files is protected. Guarantees centre on the installations, media platforms and information systems used for processing personal data, whether automated, non-automated or a combination of the two.

The following aspects are covered in the security document:

- Organization of security for the protection of personal data
- Structure of the personal data files and security levels
- Safety procedures and standards

The effective protection of personal data against unauthorized processing or access, change or loss of information is done by controlling all of the ways in which information can be accessed.

Thus, the resources that serve as a direct or indirect means of accessing IZENPE files containing personal data and which must therefore be governed by the standard are as follows:

- The processing installations or centres and premises where the files are located and where the media and documents they contain are stored.
- The servers and the operating system and communications environment in which the servers are located and in which the automated files operate.
- The non-automated documentation and information files.
- The systems, whether automated, manual or combination, established to access the data.

10.4.3 Organization of security for the protection of personal data

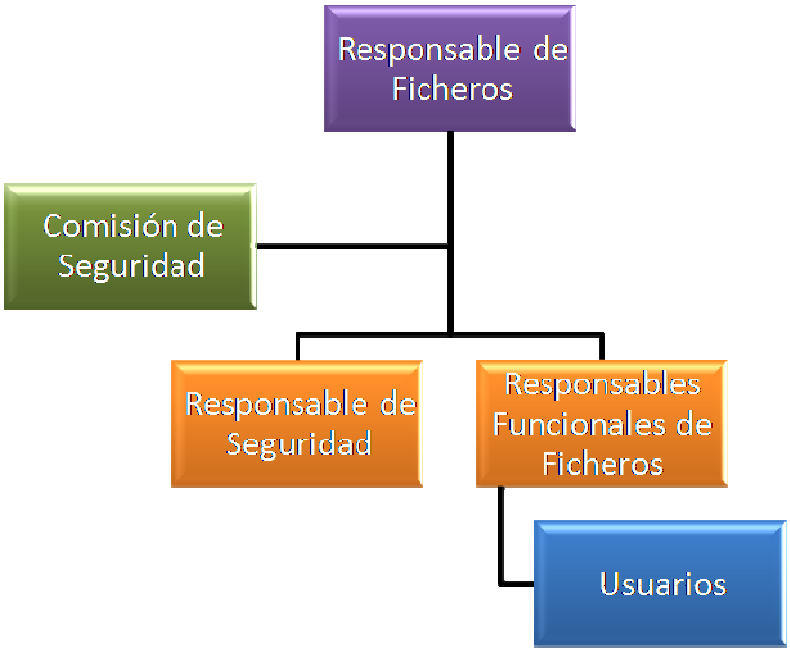
This section describes the organization of security established by IZENPE to guarantee the security of personal data.

The organizational model for security is represented, identifying and showing the units implied and the hierarchical or functional dependency between them.

The IZENPE security document specifically defines the functions to be developed by each of the security organization units.

10.4.4 Organizational model for security

The organization chart below shows a simplified security structure designed to manage and control the security of personal data at IZENPE. It shows the units in charge of organizing the security and the hierarchical or functional relations between them, namely the file managers, security committee, security manager, functional managers of Izenpe files, and users.



10.4.5 Classification of units for security organization

In accordance with the above, the units and personnel associated with the security document for the organization of security are classified into the following categories:

- File supervisor, natural or legal person who decides on the file's purpose, content and use.

  This person is in charge of file security; he/she adopts and implements the necessary security measures so that the personnel who are governed by this document learn about the standards which affect how each of their functions is developed.

  He/she keeps this document updated and must adapt its content at all times to the regulations in force relating to data security.

- Security supervisor, the person named by the file supervisor who formally assigns them the functions of coordinating and checking the security measures which can be applied to the data contained in the file.

  He/she collaborates with the file supervisor in distributing the security document and helps to maintain its compliance.

- Security Commission, the highest consultative body created to provide support for the different units of organization for making decisions on data security and data protection. In carrying out its duties, the Committee acts by delegation and with support from the Management, maximum representation of IZENPE, and as such responsible for files containing personal data, and for the various executive bodies to which the files are ascribed, as internal bodies responsible for the files.

- Functional file supervisor, this is the person in charge of making decisions regarding operational aspects of the information systems from the perspective of service functionality. Functional file supervisors are authorized by IZENPE to act by delegation as File Supervisor. The IZENPE personnel in this role are basically those responsible for running the particular service, or in other words, responsible for each area.

- File user, persons who, in performing their duties, process or have access to personal data. With regard to personal information, file users are bound to obey the rules and procedures laid down in the security document, and the rules and procedures under applicable law.

10.4.6 Structure of files containing personal data

For the purposes of the present Certification Practice Statement, IZENPE is responsible for the following personal data files (hereafter FILES) registered with the Spanish Data Protection Agency:

- Users: basic security level
- Administrative management: basic security level
- Human Resources: basic security level
- CV: basic security level
- Log file on documentation input and output: basic security level

- Transactions: basic security level
- Relationships with Third Parties: basic security level

The files contain personal data; therefore, in accordance with Article 81 of Royal Decree 1720/2007, all of the corresponding security measures shall be applied.

The description of the structure of the files is detailed in the security document of the organization.

10.4.7 Security rules and procedures

There are measures, rules and procedures in place to guarantee the security of personal data.

The security document places particular emphasis on the operating system environment and on the physical settings and workstations with computers that contain the FILES protected by the security document.

Rules

IZENPE sets rules to guarantee the protection of the personal data contained in the files it processes in carrying out its responsibilities, and thus comply with the law regarding data of this type.

The rules apply to all IZENPE services, facilities, and information systems, and to all personal data contained therein in any format (computer, paper, video, etc.), and to any person (internal or external) who makes use of these elements.

These rules are listed below:

- Regulation on the communication of files to the security supervisor
- Procedure for user administration
- Regulation on recording access to high-level files
- Regulation to authorise supports and/or documents with personal data
- Regulation on recording media input/output and documents with personal data
- Regulation on identification and auditing of media and/or documents
- Regulation on the reutilization and destruction of media and/or documents that contain personal data
- Regulation on processing temporary files
- Regulation on verification of the provisions laid down in the security document
- Regulation on making regular audits
- Regulation on the use of real personal data for testing
- Regulation on controlling physical access to the facilities and outbuildings of izenpe and cpd
- Regulation on the creation, modification and deletion of personal data files
- Regulation on security measures in the development and implementation of files
- Regulation on the creation of backup copies
- Regulation on the classification of personal data files
- Regulation on the management and custody of non-automated media and/or documents
- Regulation on storing non-automated files
- Regulation on storage devices in non-automated files

- Regulation on copying or reproducing documents from non-automated files
- Regulation on accessing non-automated documentation
- Regulation on security measures in communications

Procedures

Izenpe has also established the necessary procedures to guarantee the protection of the personal data it handles.

The procedures apply to all IZENPE services, facilities, and information systems, and to all personal data contained therein in any format (computer, paper, video, etc.), and to any person (internal or external) who makes use of these elements.

The procedures in place are listed below:

- Procedure for user administration
- Procedure for incident notification and management
- Procedure for backup copies
- Procedure for data recovery
- Procedure for exercising the right to access personal data
- Procedure for exercising the right to rectify and cancel personal data
- Procedure for exercising the right to oppose personal data

10.5 Intellectual property rights

10.5.1 Property rights in certificates

IZENPE is the only entity that retains the intellectual property rights to the certificates it issues.

Intellectual and industrial property rights derived from software used in the digital certification system and owned by third parties are excluded.

The same rules apply to the certificate revocation data system.

10.5.2 Property rights in certification practice

IZENPE retains all property rights to this Certification Practice Statement.

10.5.3 Property rights in names

The subscriber, and where applicable the key owner, retains all rights (if any), in any trademark, product or trade name contained in the certificate.

The subscriber, and where applicable the key owner, is the owner of the distinguished name of the certificate, consisting of the information specified in section 3 of the Certification Practice Statement.

10.5.4 Property rights in keys and key material

Key pairs are the property of certificate subscribers.

10.6 Obligations and guarantees

As the Certification Authority responsible for issuing the certificates in accordance with this Certification Practice Statement, IZENPE undertakes the following obligations:

10.6.1 Obligations concerning the rendering of services

IZENPE renders certification services in accordance with this 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. The Certification Authority undertakes the following obligations:

- It will not copy the signature creation data of the person to whom it has administered services.
- It will maintain a system which indicates whether a certificate is issued, revoked, suspended or expired.
- It will use a secure method to retain a record of all of the information and documentation connected with qualified certificates and valid certification practice statements for at least 15 years from the time of issuance, so that the signatures can be verified; information relative to other types of certificates shall be retained for 7 years.
- It will make sure that the signer is in possession of the signature creation data corresponding to the verification data contained in the certificate.
- It will ensure the complementary nature of signature creation and verification data, provided that both are generated by the certification service provider.
- It will meet the security standards and rules (Data Protection Act, ISO, ETSI and Izenpe Security Policy).
- It will demand that hosting suppliers meet the security standards and rules (Data Protection Act, ISO, ETSI and Izenpe Security Policy).
-

10.6.2 Obligations concerning trusted operations

IZENPE guarantees the following:

- That the identity contained in the certificate is uniquely linked to the public key.
- The speed and security of its services. In particular, it provides a fast and secure service aimed at checking certificate validity and ensures secure and immediate notification of the termination of effectiveness of the certificates in agreement with this Certification Practice Statement. The service is available 24 hours a day, 7 days a week.
- Compliance of the technical and personnel requirements as established by current legislation on electronic signature:

    1. Demonstrate the reliability necessary for providing certification services.
    2. Ensure that the date and time when a certificate is issued, terminated or expired can be determined precisely.
    3. Employ trusted personnel who possess the expert knowledge, experience, and qualifications necessary to carry out the duties associated with the

certification services provided and who have competence in security and management procedures in the area of electronic signature.

4. Use trustworthy systems and products which are protected against modification and ensure the technical and, where applicable, cryptographic security of the processes supported by them in accordance with the Security Policy.

5. Take measures against the forgery of certificates and guarantee confidentiality during the generation process in conformity with section 6 and ensure secure delivery of the certificate to the signer.

6. Use trustworthy systems to store certificates in a verifiable form so that only authorized persons can make entries and changes, information can be checked for authenticity, certificates are publicly available for retrieval in only those cases for which the certificate-holder's consent has been obtained, and any technical changes compromising these security requirements are apparent.

- The correct management of its security through implementation of an Information Security Management System in accordance with the requirements established in ISO/IEC 27001, which includes but is not limited to the following measures:

1. Perform regular security checks to verify conformity with the established security requirements.

2. A comprehensive security incident management procedure to ensure detection, resolution and optimization.

3. Maintain contacts and appropriate relationships with special interest groups in the area of security, including specialists, security forums and professional associations devoted to information systems security.

4. Properly plan the maintenance and evolution of systems in order to guarantee good performance at all times and provide service that complies with the expectations of users and clients.

10.6.3 Obligations concerning identification

In the case of qualified certificates, IZENPE identifies the certificate subscriber in compliance with articles 12 and 13 of Electronic Signature Act 19/2003, dated 19th December, and this Certification Practice Statement.

10.6.4 Obligations concerning information provided to users

- Prior to issuance and delivery of a certificate to a subscriber, IZENPE informs the potential subscriber of the terms and conditions regarding certificate use and fees – when established – as well as usage limitations and the binding legal instruments referred to in section 2.1.1.6 of this Certification Practice Statement.

The requirement is met by a "Terms and conditions of use of certificates" document through a durable (i.e. with integrity over time) means of communication, which may be transmitted electronically, and in readily understandable language.

- 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.
- IZENPE shall give signers two months' notification of the termination of service and, where applicable, will inform them of the characteristics of the service provider to which it proposes to transfer the management of certificates. Notification to signers will be conducted in accordance with the stipulations of this document.
- IZENPE has a termination of service plan which specifies the conditions under which such an event would take place.
- All of this public information connected to certificates is included in the IZENPE Repository, section 2.6 of this Certification Practice Statement.

10.6.5 Obligations concerning verification programs

IZENPE provides the public with verification mechanisms to check the validity of certificates through systems described in this Certification Practice Statement.

10.6.6 Obligations concerning legal regulations of the certification service

IZENPE assumes all of the obligations directly incorporated in the certificate or incorporated by reference. Incorporation by reference is made by including an object identifier or other form of link in a certificate.

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, and contains, at least, the following content:

- Provisions set forth to comply with sections 2.1.4, 2.1.5, 2.1.6, 2.2, 2.3 and 2.4 of this Certification Practice Statement.
- Indication of the applicable Certification Practice Statement and indication, where applicable, as to whether the certificates are issued to the public and the need to utilise a secure signature creation device or message decryption.
- Clauses concerning the issuance, suspension, revocation, renewal and, where applicable, recovery of private keys.
- Declaration stating that the information contained in the certificate is correct unless otherwise notified 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.
- Usage limitations, including those put forth in section 1.3.2.

- Information on how to validate a certificate, including the requirement of checking certificate status, and the conditions in which parties can reasonably rely on a certificate.
- Applicable limitations of liability, including the usages for which IZENPE accepts or excludes liability.
- Retention period for certificate application information.
- Retention period for audit log.
- Applicable dispute resolution procedures.
- Governing law and jurisdiction
- Whether IZENPE has been declared in conformity with the certification policies of other public entities and, if so, with what system.
- The way in which IZENPE guarantees liability for damages.

10.6.7 Registration Authority obligations

The Registration Authority undertakes the following obligations:

- To validate the identity and other personal details of the applicant, subscriber and key owner in the certificates or information relevant for the purpose of the certificates in accordance with these procedures.
- To keep all of the information and documentation concerning certificates, and manage their issuance, renewal, revocation or reactivation.
- To notify IZENPE of certificate revocation requests with due diligence and in a fast 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, reactivation requests and any other aspects related to the certificates issued by IZENPE.
- To validate, with due diligence, the circumstances for revocation that might affect certificate validity.
- To comply with the procedures established by IZENPE and with the current legislation in this area, in its management operations connected with the issuance, renewal, revocation and reactivation of certificates.
- To meet the security standards and rules (Data Protection Act, ISO, ETSI and Izenpe Security Policy).

  Where applicable, it can perform the function of making available to the key owner the technical procedures for signature creation data (private key) and electronic signature verification (public key).

10.6.8 Certificate applicant obligations

Certificate applicants agree to the following obligations:

- Ensure that the required information included in the certificate application is true, complete and current.
- Comply with the application procedure defined in the specific documentation.

10.6.9 Obligations of certificate subscribers

- 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.
- Ensure that the information provided in the certificate is true, complete and current.
- Understand and accept the terms and conditions of use of the certificate, and any changes that may be made to the terms and conditions.
- Give prior consent to the issuance and delivery of a certificate.
- Will guarantee the proper usage and maintenance of certificate media storage.
- Make proper use of the certificate and in particular, comply with the usage limitations thereof.
- Will diligently safeguard the private key to prevent unauthorized use in accordance with sections 6.1, 6.2 and 6.4 of 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:
    1. The subscriber's private key has been lost, stolen or potentially compromised.
    2. Control over the subscriber's private key has been lost due to compromise of activation data (e.g., cryptographic device PIN code) or due to other reasons.
    3. Inaccuracy or changes to the certificate content, as notified to or suspected by the subscriber, calling for the revocation of the certificate when such changes constitute a cause for revocation.
- Cease using the private key at the end of the certificate validity period.
- Will transfer specific obligations to key owners.
- Will refrain from monitoring, interfering with, or reverse engineering the technical implementation of certification services without prior written approval from the Certification Authority.
- Will refrain from intentionally compromising the security of certification services.
- Will 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.

Subscribers of qualified certificates who generate digital signatures using the private key corresponding to the public key listed in the certificate must acknowledge in the appropriate legal instrument that such electronic signatures are equivalent to handwritten signatures, provided that a cryptographic device is used, pursuant to the provisions of article 3.4 of Electronic Signature Act 59/2003, dated 19th December.

10.6.10 Obligations of certificate verifiers

Certificate verifiers agree to the following obligations:

- Independently assess the appropriateness of the use of a certificate and determine that it will, in fact, be used for an appropriate purpose.
- Understand the terms and conditions of use of the certificates in accordance with the Certification Practice Statement and the certification service contract signed by the certificate verifier and IZENPE.
- Verify the validity or revocation of the certificates issued, using information on certificate status.
- Verify all certificates in the certificate hierarchy before relying on a digital signature or on any of the certificates in the hierarchy.
- Bear in mind any usage limitations on certificates, whether contained in the certificate itself or in the verifier contract.
- Bear in mind any precautions included in a contract or other instrument, regardless of legal nature.
- Notify IZENPE of any inaccuracy or defect in a certificate which may be considered cause for revocation.
- 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.

Users of qualified certificates must acknowledge in the appropriate legal instrument that electronic signatures are equivalent to handwritten signatures, pursuant to article 3.4 of Electronic Signature Act 59/2003, dated 19th December.

10.6.11 Obligations of the Timestamp Authority

The Izenpe Timestamping Authority issues secure timestamp tokens (TST) to users of timestamp services (including subscribers and third parties)

The Izenpe Timestamping Authority has the responsibility for providing timestamp services. Izenpe Timestamping Authority can operate with different identifiable timestamping units (TSUs). Each TSU can have its own signature key.

The Izenpe Timestamping Authority is identified in the digital certificate used for timestamp services.

10.6.12 Timestamp subscriber obligations

The timestamp subscriber can use timestamp services only in compliance with ETSI TS 101 861, section 4: “Requirements of a TSP client”.

The subscriber must verify that the timestamp token has been correctly signed by the timestamping authority and that the private key used to sign the timestamp token has not been revoked.

10.6.13 Obligations of third party timestamp verifiers

When a timestamp token is received, the third party must verify that the timestamp token has been correctly signed and that the private key used to sign the timestamp token has not been revoked.

During the validity period of the certificate used to generate the timestamp, the validity of the signature key can be verified in the corresponding CRL.

If verification is done after the expiration date of the certificate, the third party shall make sure that the hash function being used, algorithms and length of the cryptographic keys are considered secure.

10.6.14 Repository obligations

Not applicable since the Repository is not an independent entity.

10.7 Responsibilities

10.7.1 Certification Authority responsibilities

IZENPE is liable for negligence or a lack of due diligence exercised in providing the certification services described in this Certification Practice Statement, and for a failure to meet any of the legal obligations set forth in electronic signature legislation, except in the following cases:

- In no event shall IZENPE be held liable for damages caused by the information contained in the certificates provided that the content thereof substantially complies with the Certification Practice Statement.
- In no event shall IZENPE be held liable for damages caused by certificate expiration, provided that it substantially complies with the publication obligations set forth in this Certification Practice Statement.
- In no event shall IZENPE 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.

- In no event shall IZENPE be held liable 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, notarized or otherwise authorized document, except in the case of documents supplied by the Registration Authority.
- IZENPE shall not be held liable for damages to subscribers or bona fide third parties for failure to comply with the duties attached to subscribers or relying parties.

Pursuant to article 22 of the LFE, IZENPE shall be held responsible for damages to any person due to a failure to include or to a delay in including in the certification query service information on the validity, expiration or suspension of a certificate.

Additionally, IZENPE shall assume full liability for the actions of persons to which it has delegated authority to perform the functions necessary for rendering certification services. Thus, IZENPE maintains insurance coverage liability of 3,500,000 euros for damages incurred as a result of the use of the certificates.

10.7.2 Responsability of the Timestamping Authority

Izenpe operates its TSA in accordance with the Izenpe TSA policy, the Izenpe CPS and the terms of any other binding agreement between Izenpe and timestamp services users. Izenpe strives to deliver services with high availability, but does not guarantee 100% availability or timestamp precision. Izenpe is not liable for any loss of profit, any indirect or consequential loss or damage, or loss of data, to the extent permitted under the legislation in force. Izenpe is not liable for damage resulting from infringements committed by the subscriber or third parties with regard to the applicable terms and conditions. Under no circumstances shall Izenpe be held responsible for damages as a result of an event of force majeure, including natural disasters, loss of power supply or telecommunications, fire, unpredictable external interactions such as viruses, hackers' attacks, governmental actions or strikes. In any event, Izenpe will make all reasonable endeavours to minimize the effects of any such event. Any claims for damages resulting from delay due to an event of force majeure shall not accepted by Izenpe.

10.7.3 Registration Authority responsibilities

Any organization 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, in the terms established in the corresponding legal agreement.

When identification functions are carried out by government agencies that have subscribed to certificates, liability for damages shall be governed pursuant to the Law on Public Administration and the Common Administrative Procedure.

10.7.4 Subscriber responsibilities

The Subscriber shall be held liable for all of the authenticated electronic transactions using a digital signature generated with the Subscriber's private key when the certificate has been validated through the verification services provided by IZENPE.

If no notification of loss or theft of the certificate is received, as laid down in this Certificate Practice Statement, any liability resulting from the unauthorized 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 unauthorized 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, and
- 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, revocation or suspension 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 safeguard signature creation data to keep it strictly confidential and protect it from unauthorized access or disclosure.
- Request the suspension or revocation of a certificate if the Subscriber becomes aware of or suspects the compromise of signature creation data.
- Refrain from using the signature creation data when the validity period has expired or when the service provider notifies the Subscriber that such data is no longer valid.
- Observe the limitations listed in the certificate with regard to possible uses and employ the certificate in conformance with the terms and conditions set forth and communicated to the signer of the certificate services.

10.7.5 Relying party liability

A relying party who vests trust in a certificate that has not been verified assumes all of the risks associated thereto 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, neither shall IZENPE 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 obligations:

- Confirm and take account of any limitations on the usage of the certificate and the fee for each of the transactions that can be performed with the certificate.
- Make sure the certificate is valid.

10.8 Compensation

Should IZENPE fail to meet its obligations or breach the requirements of the law, indemnification clauses are included in the legal instruments which link IZENPE to the subscriber and verifier.

10.9 Validity period

10.9.1 Deadline

The CPS comes into force as soon as it is published.

10.9.2 Termination

The current CPS will be revoked as soon as a new version of the document is published.

The new version will fully substitute the previous document.

10.9.3 Finalisation effects

For the valid certificates issued under a previous CPS, the new version will prevail over the former in everything not opposed to it.

10.10 Individual notifications and communication with the participants

IZENPE establishes the media and deadlines for notifications in the binding legal instrument.

In general, the IZENPE website www.izenpe.com will be used to make any type of notification and communication.

10.11 Amendments

10.11.1 Procedure for changes

The modifications made to this document will be approved by the IZENPE Board of Directors. Amendments will be set out in a document entitled Certification Practice Statement Update, the maintenance of which is guaranteed by IZENPE.

The updated versions of the Certification Practice Statement, together with the list of amendments made, can be consulted online at http://www.izenpe.com

IZENPE may unilaterally amend the Certification Practice Statement provided that the following procedure is observed:

- Any amendment must be justified from a technical, legal or commercial perspective, and must be attested by IZENPE management.
- All of the technical and legal implications should be considered of the new version of specifications.
- An amendment control procedure shall be established to ensure that the resultant specifications meet the requirements they set out to fulfil and which brought about the change.
- The implications of the change in specifications on the user should be established, the user should be notified of such changes.

10.11.2 Notification period and mechanism

The IZENPE Security Committee will annually review the CPS and in any case when it has to be modified. This review will be performed jointly among responsible areas and participants in drawing it up and maintaining it.

IZENPE could make modifications to this document without having to previously inform users for example:

- Typographical corrections made in the document
- Changes in contact details

Modifications that could require informing users such as:

- Changes in the specifications or service conditions.
- Changes in URLs

10.11.3 Circumstances in which an OID must be changed

The OID will be changed when one of the procedures described in this document is changed.

10.12 Complaints and resolving disputes

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 citizens 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.

10.13 Applicable regulations

The implementation, elaboration, 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:

- Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.
- Electronic Signature Law 59/2003 of 19 December.
- Law 11/2007, of 22 June, on citizens' electronic access to Public Services
- Spanish Organic Law 15/1999 of 13 December on the Protection of Personal Data.
- Royal Decree 1720/2007 of 21 December, which approves the Regulation implementing Organic Law 15/1999 of 13 December on the Protection of Personal Data.
- EU Regulation 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS).

10.14 Meeting applicable regulations

The parties shall submit to the competent jurisdiction governed by Spanish procedural law.

In any case, IZENPE demonstrates meeting the standards given in section 9.13

10.15 Diverse stipulations

Each clause contained in this Certification Practice Statement is valid in itself and does not impair the remainder of the clauses. The invalid or incomplete clause can be substituted for another equivalent clause.

The rules contained in sections 8 and 9 will remain in force after the end of the life of this Certificate Practice Statement.

None of the terms and provisions of this Certification Practice Statement which directly affect the rights and obligations of IZENPE and do not affect the remaining parties may be amended, waived, supplemented, modified or eliminated without authorized written consent from

IZENPE; in no case does such a change effect a novation but rather a modification which does not affect the remainder of the rights and obligations of the other parties.

Written communications for IZENPE should be sent to the following address:

IZENPE, S.A.
c/ Beato Tomás de Zumárraga, nº 71, 1ª planta.
01008 Vitoria-Gasteiz