1. INTRODUCTION

ZIURTAPEN ETA ZERBITZU ENPRESA-EMPRESA DE CERTIFICACION Y SERVICIOS IZENPE SA
Firmado digitalmente por ZIURTAPEN ETA ZERBITZU ENPRESA-EMPRESA DE CERTIFICACION Y SERVICIOS IZENPE SA
Fecha: 2026.10.30 09:50:39 +01'00'

This document sets out the certification policy corresponding to the certificates issued by *Ziurtapen eta Zerbitzu Enpresa - Empresa de Certificación y Servicios, Izenpe, S.A.* (hereinafter, Izenpe) for websites in their different variants.

Its purpose is to detail and complete for this type of certificate what is defined generically in the *Izenpe Certification Practice Statement*, in the specific documents of the *CA/Browser Forum Baseline Requirements (hereinafter BR), EV guidelines (hereinafter EVBR)* for issuing certificates for websites and in the ETSI specifications (www.etsi.org). Izenpe adheres to the latest published version of these standards.

Thus, Izenpe follows the following certification policies established by ETSI:

- DVCP (Domain Validation Certificates Policy): for 'DV SSL' certificates.
- OVCP (Organisational Validation Certificates Policy): in 'OV SSL' certificates.
- QEVCP-w (Qualified Extended Validation Certificates Policy): in 'Qualified SSL' certificates.

The Root Cas and Sub CA's covered in this document are detailed in section 1.3.1.

According to the validation conducted, Izenpe issues the following types of certificates:

- *SSL DOMAIN VALIDATED (SSL DV)*,

This certificate, considered as unqualified, will be used for the identification of the ownership of the domain hosting the website, providing reasonable assurance to the user of an Internet browser.

The validity of these certificates is 195 days.

- *SSL ORGANISATION VALIDATED (SSL OV)*,

This certificate, considered as unqualified, shall be used for the identification of domain ownership and accreditation of the organisation, providing reasonable assurance to the user of an Internet browser that the website being accessed is owned by the organisation identified in the certificate.

The validity of these certificates is 195 days.

- *SSL QUALIFIED EXTENDED VALIDATION(SSL EV)*,

This certificate is considered as qualified according to Regulation (EU) No 910/2014 4 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 as amended by Regulation (EU) 1183/2024 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS Regulation). It will be used for the identification of domain ownership and accreditation of the organisation, providing robust assurance to the user of an Internet browser that the website they are accessing is owned by the organisation identified in the certificate.

The validity of these certificates is 195 days.

1.1 Overview

The purpose of this document is to regulate the conditions and characteristics of the trust services applicable to users of the website authentication certificates issued by Izenpe and to establish the obligations that Izenpe undertakes to comply with in relation to:

- The management of the certificates and the conditions applicable to the request, issue, use and termination of their validity.
- The provision of the certificate validity status query service, as well as the conditions applicable to the use of the service and the guarantees offered.

In addition, it includes, either directly or with references to details of the liability regime applicable to the parties using and/or relying on the services described in the previous paragraph, the security controls applied to its procedures and facilities insofar as they can be published without impairing their effectiveness, and the rules of secrecy and confidentiality, as well as issues relating to the ownership of its property and assets, the protection of personal data, and other matters of an informative nature that it considers interesting to make available to the public.

IZENPE conforms to the latest published version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates published at https://www.cabforum.org, the CCADB policy, the Apple Root Program Policy, the Chrome Root Program Policy, the Mozilla Root Store Policy and the Microsoft Root Program Requirements. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

Effective as of 2026 15th April, this Certification Authority (CA) has ceased the issuance of new SSL/TLS certificates under the 2007 Root CA. This Certification Practice Statement (CPS) remains in effect solely to govern the management, revocation, and status validation services for certificates issued prior to the cessation date until their natural expiration.

1.2 Document name and identification

This document is called 'Certificate Policy - Certification Practices Statement for Website Authentication Certificates'.

- Version: 3.2
- Issuance date: 29 Oct 2026
- Location:https://www.izenpe.eus/contenidos/informacion/cps_ssl/en_def/adjuntos/cp_cps_3.2.pdf

In order to identify the certificates, Izenpe has assigned them the following object identifiers (OID).

ROOT 2007:

CERTIFICATE	POLICY OID
DV SSL	1.3.6.1.4.1.14777.1.2.4
OV SSL	1.3.6.1.4.1.14777.1.2.1
Qualified SSL	1.3.6.1.4.1.14777.6.1.3

ROOT 2024:

CERTIFICATE	POLICY OID
DV SSL	1.3.6.1.4.1.14777.50.1.2
OV SSL	1.3.6.1.4.1.14777.50.2.2
Qualified SSL	1.3.6.1.4.1.14777.50.3.2

Version Control

VERSION	CHANGE
1.0	- Requirements added to section 2.2 – Requirements updated in sections 2.1 and 2.2 – Requirements updated in section 2.2 – Index added. – Footer added. – Requirements deleted in sections 2.1 and 2.2 – Year deleted from cover page
1.1	– Updated requirements in domain validation, in section 2.2. – Figures deleted in sections 2.3 and 2.6
1.2	– Updated requirements in CAA validation, in section 2.2.
1.3	- 1. Introduction Within the scope of the Google Certificate Transparency project, the issued EV SSL and EV HQ certificates will be published in the CT service of the Log Servers providers with which Izenpe has an agreement. - 1.1. Certificate description. * Updating of the regulations concerning the regulation of the seal certificate. * Updating of the validity of the certificates to 1 or 2 years. - 1.2. Identification. * CA/B FORUM OIDs are included. * Certificate serial numbers shall have at least 64 bits of entropy. - Sections 1.3 and following. Adaptation of terminology to the issuance of EV certificates to private entities. - 14.General provisions, * Identification obligations. It is indicated that in all cases Izenpe checks the ownership or control of the domain. * Obligations of the certificate subscriber. Including those determined in the Public Key Disclosure Agreement (PDS). - Sections 1, 2, and 3. Inclusion of clarifications on compliance with BRs.
1.4	– The policy OID of EV SSL and EV HQ certificates has been updated. – It is stated in section '1.1 Description of certificates' that Qualified EV SSL and Qualified EV HQ certificates are considered qualified according to eIDAS. – It is stated in the introduction that ALL certificates will be published in the CTs. – All references to the HQ certificate have been removed.
1.5	- Qualified profiles have been added
1.6	The following domain ownership verification methods were added: - Email built to domain contact. - Email to DNS CAA contact. - Email to DNS TXT contact. - DNS Lookup. - Detailed revocation causes and deadlines in both end and sub CAs.
1.7	The following were added: - The test certificate paths (live, revoked, expired).

VERSION	CHANGE
	- checking of RSA key parameters. - Addition of the definition of 'pre-certificate'. - obligation to increment the version number, even if no changes have been made. The following were removed: - EVs from among the profiles currently issued by Izenpe. - Revocation procedure, and redirects to the CPS. – It is specified that Izenpe's public CAs do not issue for internal domains.
1.8	The document has been adapted to the structure of RFC 3647.
1.9	– The change control section was replaced with this version history table. – The lifetime of all profiles was updated to 395 days. – The DNS CAA method was removed. – The whois method was added for .eus
2.0	– Removal of references to qualified HQ and EV SSL certificates. – Update of Izenpe's postal and e-mail address. – Revision of the wording of the policy.
2.1	Sections, – 3.2.2.1 Identity: in relation to qualified SSL certificates. The list of entity verification sources according to CABFORUM is included. – Cover page: The footer of the document title is removed due to an error in the telephone number.
2.2	– Cover page: The footer of the document title is removed due to an error in the telephone number. Sections, -1 "Certificate Transparency" paragraph correction. - 3.1 Paragraph regarding RFC 6962 has been erased. - 3.2.2.1 Identity: the verification source list has been extended. – 3.2.2.1 Identity: in relation to qualified SSL certificates. The list of entity verification sources according to CABFORUM is included. - 3.2.2.2.4. Validation methods are correct but "c" description does not relate to anyone and CABFORUM 3.2.2.4.4 method description is missing. - 4.1.2 Erased references regarding entities that can not be checked their incorporation information. - 4.6 Translation mistake, stands for "revocation" when it should have been "renewal". - 4.4.3 Correction regarding "Certificate Transparency". - 4.9.6 Rewritten. - 6.3.2 Typo, it appears 395 when it must have been 398. - 6.1.5. ">=" added to 2048. - 9.1.3 Correction, "I" stands for Izenpe.
2.3	- Format homogenization. - 1., 1.2 and 1.3.1 modified to add new ROOT info. - Corrected references to CABFORUM. - 3.2.2.2. It was wrongly labeled as 3.2.2.2.2. - 3.2.2.4. It was wrongly labeled as 3.2.2.2.4.

VERSION	CHANGE
	- 3.2.2.4. Deleted reference to BR 3.2.2.4.1. - 7.1.8. Outdated reference to "UserNotice". - 6.1.5 and 7.1.3 modified to add new ROOT info.
2.4	- Rewriting of the following Sections:'1.6.1', '1.6.2','2.1','2.2','4.4.2' - New Sections included:'1.6.3','1.6.4','4.2.4','5.4.1.1','4.3.1.1','4.3.1.2','4.3.1.3','7.1.2.1','7.1.2.1.1', '7.1.2.2','7.1.3.1', '7.1.3.1.1','7.1.3.1.2','7.1.3.2','7.1.3.2.1','7.1.3.2.2','7.1.4.1','7.1.4.2', '7.1.4.3','7.1.4.4'
2.5	- CP and CPS have been merged. - All sections marked as "See the relevant section in the CPS." in the CP < have been replaced with the corresponding section of the CPS.
2.6	- 3.2.2.4 Modified to remove method 3.2.2.4.2. - 3.2.2.1 Modified to add a new verification sources.
2.7	- 7.2.2 Modified to set " Issuing Distribution Point" extension as critical.
2.8	- 5.7.1.2 Mass Revocationplan section included.
2.9	- SSL certificates duration set to 195 days.
3.0	- 1.1,4.3,5.8 Stop issuing TLS certificates on 15th April 2026 under 2007 Root CA.
3.1	- 1.1 Adherence to CCADB and Root programs.
3.2	- 7.2.2 "unspecified" CrlReaon will not be allowed for SubCAs.

1.3 PKI participants

Parties involved in the management and use of the trust services described:

1. Certification Authority
2. Registration Authority
3. Subscribers or Certificate holders
4. Relying Parties
5. Other participants

1.3.1 Certification authorities

Within the scope of this policy, Izenpe has the following Certification Authorities:

ROOT 2007

Type	CN	SHA1 Footprint
Root	Izenpe.com	2F783D255218A74A653971B52CA29C45156FE919
Subordinate	EAEko Herri Administrazioen CA - CA AAPP Vascas (2)	F79CDA11E7917419A0418DB84BA743C5313AD7F0
Subordinate	Certificate CA EV SSL	C68BADE5F069778A003074E619DAB2E7928342D5

ROOT CERTIFICATION AUTHORITY 2007

Field / extension	Content
version	Version 3
serialNumber	00B0B75A16485FBFE1CBF58BD719E67D
signature	sha256WithRSAEncryption
issuer	
CN	Izenpe.com
O	IZENPE S.A.
C	ES
validity	13 December 2037
subject	
CN	Izenpe.com
O	IZENPE S.A.
C	ES
subjectPublicKeyInfo	RSA 4096 bits
extensions	
subjectAltName	
rfc822Name	info@izenpe.com
directoryName	
STREET	Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz
O	IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
subjectKeyIdentifier	1D1C650EA8F2257BB491CFE4B1B1E6BD55746C05
keyUsage	Certificate signing, Offline CRL signing, Certificate revocation list (CRL) signing (06)

SUBORDINATE CERTIFICATION AUTHORITY: "EAEko Herri Administrazioen CA - CA AAPP Vascas (2)"

Field / extension	Content
version	Version 3
serialNumber	24C5C8AA566F8EE84CBEA7055CE164A4
signature	sha256WithRSAEncryption
issuer	
CN	Izenpe.com
O	IZENPE S.A.
C	ES
validity	13 December 2037
subject	

Field / extension	Content
CN	EAEko Herri Administrazioen CA - CA AAPP Vascas (2)
OU	AZZ Ziurtagiri publikoa - Certificado publico SCA
O	IZENPE S.A.
C	ES
subjectPublicKeyInfo	RSA 4096 bits
extensions	
subjectAltName	
rfc822Name	info@izenpe.com
directoryName	
STREET	Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz
O	IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
subjectKeyIdentifier	C0A94AF7472587FFBCB5A689CE82D246A889EBA3
authorityKeyIdentifier	1D1C650EA8F2257BB491CFE4B1B1E6BD55746C05
certificatePolicies	
policyIdentifier	All issuance directives
Directive certifier ID	CPS
cpsURI	http://www.izenpe.eus/cps
authorityInfoAccess	
Access method	Online certificate status protocol (1.3.6.1.5.5.7.48.1)
Alternative name	
URL address	http://ocsp.izenpe.com:8094
cRLDistributionPoints	http://crl.izenpe.com/cgi-bin/arl2
keyUsage	Certificate signing, Offline CRL signing, Certificate revocation list (CRL) signing (06)
Digital footprint	F79CDA11E7917419A0418DB84BA743C5313AD7F0

SUBORDINATE CERTIFICATION AUTHORITY: "Certificate CA EV SSL"

Field / extension	Content
version	Version 3
serialNumber	687DB7171744DA235B3F625A7393F8A5
signature	sha256WithRSAEncryption
issuer	
CN	Izenpe.com
O	IZENPE S.A.

Field / extension	Content
C	ES
validity	6 July 2028
subject	
CN	Certificate CA EV SSL
OU	BZ Ziurtagiri publikoa - Certificado publico EV
O	IZENPE S.A.
C	ES
subjectPublicKeyInfo	RSA 4096 bits
extensions	
subjectAltName	
rfc822Name	info@izenpe.com
directoryName	
STREET	Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz
O	IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
subjectKeyIdentifier	C6EDFE77FB51564DFCABD5E3B10C13A3BF54E39B
authorityKeyIdentifier	1D1C650EA8F2257BB491CFE4B1B1E6BD55746C05
certificatePolicies	
policyIdentifier	All issuance directives
Directive certifier ID	CPS
cpsURI	http://www.izenpe.eus/cps
authorityInfoAccess	
Access method	Online certificate status protocol (1.3.6.1.5.5.7.48.1)
Alternative name	
URL address	http://ocsp.izenpe.com
cRLDistributionPoints	http://crl.izenpe.com/cgi-bin/arl2
keyUsage	Certificate signing, Offline CRL signing, Certificate revocation list (CRL) signing (06)
Digital footprint	C68BADE5F069778A003074E619DAB2E7928342D5

ROOT 2024

Type	CN	SHA1 Footprint
Root	ROOT CA SSL IZENPE 2024	68E93296DEEB4254C18C49C4E80F5D8FA3D38A93
Subordinate	SUBCA SSL 2024	E3A0E57B82D88AE25E0A488C51C1E40E2AC0DB18

ROOT CERTIFICATION AUTHORITY 2024

Field / extension	Content
version	Version 3
serialNumber	1BE568F081EDFEEE7776604E73FA081E
signature	sha384ECDSA
issuer	
CN	ROOT CA SSL IZENPE 2024
O	IZENPE S.A.
C	ES
validity	24 September 2049
subject	
CN	ROOT CA SSL IZENPE 2024
O	IZENPE S.A.
C	ES
subjectPublicKeyInfo	ECC(384 Bits)
extensions	
subjectKeyIdentifier	EADC1AEECBD319D1B12B4FDB12CB56795DB2B0EA
keyUsage	Certificate signing, Offline CRL signing, Certificate revocation list (CRL) signing (06)

SUBORDINATE CERTIFICATION AUTHORITY: "SUBCA SSL 2024"

Field / extension	Content
version	Version 3
serialNumber	45C858662468EEA028BAEDB26E098D37
signature	sha384ECDSA
issuer	
CN	ROOT CA SSL IZENPE 2024
O	IZENPE S.A.
C	ES
validity	24 September 2049
subject	
CN	SUBCA SSL 2024
ORGANIZATIONIDENTIFIER	VATES-A01337260
O	IZENPE S.A.
C	ES
subjectPublicKeyInfo	ECC(384 Bits)

Field / extension	Content
extensions	
subjectKeyIdentifier	5730599CA33DA068ECB3DBCFD555C8AACC5D00A9
authorityKeyIdentifier	EADC1AEECBD319D1B12B4FDB12CB56795DB2B0EA
certificatePolicies	
policyIdentifier	All issuance directives
Directive certifier ID	CPS
cpsURI	http://www.izenpe.eus/cps
authorityInfoAccess	
`Access method`	calssuer
`URL address`	http://www.izenpe.eus/contenidos /informacion/cas_izenpe/es_cas/adjuntos/izenpe_root_ssl_2024.crt
cRLDistributionPoints	http://crl.izenpe.eus/2024/izsslroot.crl
keyUsage	Certificate signing, Offline CRL signing, Certificate revocation list (CRL) signing (06)
Digital footprint	E3A0E57B82D88AE25E0A488C51C1E40E2AC0DB18

1.3.2 Registration authorities

Izenpe is the only Registration Authority that acts in the process of issuing these certificates. It performs the identification and verification tasks in an automated manner, with the aim of guaranteeing that the certificate issued to the Subscriber has control of the domain name included in the Certificate. Controlled exclusively

None of the verifications on the identity or domain control will be delegated to third parties.

1.3.3 Subscribers

Subscribers are the legal entities to whom the certificates are issued, bound as determined in the Terms and Conditions document.

1.3.4 Relying parties

Relying parties are those Internet users who establish connections to websites using TLS/SSL protocols that incorporate such Certificates and choose to trust them.

1.3.5 Other participants

No stipulation.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

Website authentication certificates authenticate a website and link it to the legal person to whom it has been issued.

All qualified website authentication certificates issued under this Policy are qualified certificates in accordance with the eIDAS Regulation and the requirements set out in the European standards ETSI EN 319 411-2 'Requirements for trust service providers issuing EU qualified certificates' and ETSI EN 319 412-4 'Certificate profile for web site certificates'.

1.4.2 Prohibited certificate uses

The certificates must be used for their own function and established purpose and may not be used in other functions and for other purposes.

Likewise, certificates must only be used in accordance with the applicable legislation.

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

If a user entity or third party relies on these certificates without accessing the information and consultation service on the validity status of the certificates issued under this Certification Policy, it will not be covered by these Particular Certification Policies and Practices and will not have any legitimacy to claim or take legal action against Izenpe for damages, loss or conflicts arising from the use of or reliance on a Certificate.

Izenpe prohibits the use of certificates issued under this policy for unlawful interception or decryption of encrypted communications (MITM), deep packet inspection (DPI), etc.

1.5 Policy administration

1.5.1 Organization administering the document

Izenpe, with registered office at c/ Beato Tomás de Zumárraga, nº 71, 1ª planta, 01008 Vitoria-Gasteiz and holding NIF A-01337260, is the Certification Authority that issues the certificates to which this Certification Policy applies.

1.5.2 Contact person

Provider name	**Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, S.A.**
Address	c/ Beato Tomás de Zumárraga, nº 71, 1ª planta. 01008 Vitoria-Gasteiz
Email	izenpe@izenpe.eus

To report security problems, such as suspected key compromise, certificate misuse, fraud, revocation requests or other issues, please contact **incidencias@izenpe.eus**.

1.5.3 Person determining CPS suitability for the policy

The Izenpe Security Committee is the body responsible for the approval of this Policy.

1.5.4 CPS approval procedures

Izenpe manages its certification services and issues certificates in accordance with the latest version of the Basic requirements for the issuance and management of trust certificates requirements established by the CA/Browser forum, which can be consulted at the following address https://cabforum.org/baseline-requirements-documents/

Izenpe annually reviews and updates this Policy by identifying, publishing new versions in www.izenpe.eus

1.6 Definitions and acronyms

1.6.1 Definitions

- ***Applicant:*** The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate is issued, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request.
- ***CAA:*** From RFC 8659 (http://tools.ietf.org/html/rfc8659): "The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify one or more Certification Authorities (CAs) authorized to issue certificates for that domain name. CAA Resource Records allow a public CA to implement additional controls to reduce the risk of unintended certificate mis-issue."
- ***CA Key Pair:*** A Key Pair where the Public Key appears as the Subject Public Key Info in one or more Root CA Certificate(s) and/or Subordinate CA Certificate(s).
- ***Certificate:*** An electronic document that uses a digital signature to bind a public key and an identity.
- ***Certificate Policy:*** A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.
- ***Certificate Incident Report:*** Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.
- ***Certificate Profile:*** A set of documents or files that defines requirements for Certificate content and Certificate extensions in accordance with Section 7, e.g. a Section in a CA's CPS or a certificate template file used by CA software.
- ***Certificate Revocation List:*** A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.
- ***Certificate Transparency (CT):*** is an open framework for the supervision of website authentication Certificates, so that when one of these Certificates is issued, it is published in CT records, thus making it possible for domain owners to supervise the issuance of the same for their domains and detect erroneously issued certificates.
- ***Certification Authority:*** An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Root C?s and Subordinate CAs.
- ***Certification Practice Statement (CPS/DPC):*** One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.
- ***Domain Contact:*** The Domain Name Registrant, technical contact, or administrative contact (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record, or as obtained through direct contact with the Domain Name Registrar.
- ***Domain Label:*** From RFC 8499 (http://tools.ietf.org/html/rfc8499): "An ordered list of zero or more octets that makes up a portion of a domain name. Using graph theory, a label identifies one node in a portion of the graph of all possible domain names."
- ***Domain Name:*** An ordered list of one or more Domain Labels assigned to a node in the Domain Name System.
- ***eIDAS Regulation:*** Refers to Regulation (EU) 910/2014 as amended by Regulation (EU) 1183/2024.
- ***Issuing CA:*** In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.
- ***Key Compromise:*** A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, or an unauthorized person has had access to it.
- ***Key Pair:*** The Private Key and its associated Public Key.
- ***Object Identifier:*** A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.
- ***OCSP Responder:*** An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.
- ***Private Key:*** The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

- ***Public Key:*** The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.
- ***Public Key Infrastructure:*** A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.
- ***Random Value:*** A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.
- ***Registration Authority (RA):*** Any Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.
- ***Reliable Data Source:*** An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.
- ***Relying Party:*** Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate.
- ***Repository:*** An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.
- ***Root CA:*** The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.
- ***Root Certificate:*** The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.
- ***Subject:*** The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.
- ***Subject Identity Information:*** Information that identifies the Certificate Subject. Subject Identity Information does not include a Domain Name listed in the subjectAltName extension or the Subject commonName field.
- ***Subordinate CA:*** A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.
- ***Subscriber:*** A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.
- ***WHOIS:*** Information retrieved directly from the Domain Name Registrar or registry operator via the protocol defined in RFC 3912, the Registry Data Access Protocol defined in RFC 7482, or an HTTPS website.
- ***Wildcard Certificate:*** A Certificate containing at least one Wildcard Domain Name in the Subject Alternative Names in the Certificate.

1.6.2 Acronyms

- **CA:** Certification Authority
- **CAA:** Certification Authority Authorization
- **CN:** Common Name
- **CP:** Certificate Policy
- **CPS:** Certification Practice Statement
- **CRL:** Certificate Revocation List
- **CT:** Certificate Transparency
- **DNS:** Domain Name System
- **DN:** Distinguished Name
- **EIDAS:** eIDAS Regulation
- **ETSI:** European Telecommunications Standards Institute
- **EV:** Extended Validation
- **FQDN:** Fully-Qualified Domain Name
- **HSM:** Hardware Security Module. A security device that generates and protects cryptographic keys.
- **HTTP:** Hyper Text Transfer Protocol
- **ISO:** International Organization for Standardization
- **OCSP:** Online Certificate Status Protocol
- **OID:** Object IDentifier
- **OV:** Organisational Validation.
- **PDS:** PKI Disclosure Statement.
- **PKI Public Key:** Infrastructure
- **PKCS:** Public Key Cryptography Standards.
- **RA:** Registration Authority
- **TLS/SSL:** Transport Layer Security/Secure Socket Layer protocol.
- **UTC:** Coordinated Universal Time.

1.6.3 References

Document	Title
ETSI EN 319 401	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
ETSI EN 319 403	Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers
ETSI EN 319 411-1	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
ETSI EN 319 411-2	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part2: Requirements for Trust Service Providers issuing EU qualified certificates
ETSI EN 319 421	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing Time-Stamps
RFC 2119	Key words for use in RFCs to Indicate Requirement Levels
RFC 3492	Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA)
RFC 3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

Document	Title
RFC 3986	Punycode: Uniform Resource Identifier (URI): Generic Syntax
RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
RFC 6962	Certificate Transparency
RFC 8737	Automated Certificate Management Environment (ACME) TLS Application-Layer Protocol Negotiation (ALPN) Challenge Extension

1.6.4 Conventions

The key words “must”, “must not”, “required”, “shall”, “shall not”, “should”, “should not”, “recommended”, “may”, and “optional” in these documents shall be interpreted in accordance with RFC 2119.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

Izenpe has a public information repository at www.izenpe.eus, available 24 hours a day, 7 days a week where information about CP/CPS, Root Certificates and subCA certificates can be found.

2.2 Publication of certification information

The information relating to the issuance of electronic certificates covered by this Policy is accessible via www.izenpe.eus and includes the following information:

- Certification policy and practice statements.
- Certificate profiles and revocation lists.
- PKI Information Statements (PDS).
- The terms and conditions of use of the Certificates, as a binding legal instrument.
- Download of Izenpe's root Certificates and subordinate CAs, as well as additional information.

IZENPE will take all the measurements needed to make this repository available all the time.

Application Software Suppliers can test their software with the following addresses:

ROOT 2007

Status	URL
Valid	https://test-ev-qualified.izenpe.eus
Expired	https://test-expired-ev.izenpe.eus
Revoked	https://test-revoked-ev.izenpe.eus

ROOT CA SSL IZENPE 2024

Status	URL
Valid	https://test-valid-ev-2024.izenpe.eus
Expired	https://test-expired-ev-2024.izenpe.eus
Revoked	https://test-revoked-ev-2024.izenpe.eus

2.3 Time or frequency of publication

Izenpe reviews its certification policies and practices and updates this document annually following the guidelines set out in the '1.5.4. Approval procedure' section of this document.

Any changes to the CP/CPS will be published immediately.

The frequency of publication of CRLs is defined in section '4.9.7 Frequency of CRL generation' of this document.

2.4 Access controls on repositories

Izenpe allows read access to the information published in its repository and establishes controls to prevent unauthorised persons from adding, modifying, or deleting records from this Service and to protect the integrity and authenticity of the deposited information. Izenpe employs reliable systems for access to the information repository so that:

- Only authorised persons can make annotations and modifications.
- The authenticity of the information can be verified.
- Certificates are available for consultation.
- Any technical changes affecting security requirements can be detected.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

The encoding of the certificates follows the RFC 5280 standard 'Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile'. All fields defined in the Certificates profile in the CPS and in the policy, except in the fields that specifically state otherwise, use UTF8String encoding.

Additionally, for qualified SSL certificates, Izenpe will comply with the requirements established in the 'latest extended validation guidelines' which can be consulted at https://cabforum.org/working-groups/server/extended-validation/guidelines/.

3.1.1 Types of names

The end-entity electronic certificates covered by this Policy contain a distinguished name (DN) in the Subject Name field, consisting of the information relating to the Certificate profile (section 7.1 of this document). Izenpe complies with X.500, RFC 5280, and CA/Browser Forum (BRs and EVGs) requirements in this respect.

The Common Name field defines the certificate subscriber.

3.1.2 Need for names to be meaningful

All distinguished names (DNs) in the Subject Name field are meaningful. The description of the attributes associated with the certificate subscriber is human readable (see section 7.1.4 Name format of this document).

The Subject Distinguished Name field will also be subject to the requirements established in section 9.2 of CABForum in its 'guide for the issuance and management of Extended Validation Certificates' and which can be consulted at https://cabforum.org/extended-validation/. Izenpe does not issue Wildcard Certificates with EV policies.

3.1.3 Anonymity or pseudonymity of subscribers

Under this Certification Policy Izenpe does not allow the use of pseudonyms.

3.1.4 Rules for interpreting various name forms

The requirements defined by the X.500 reference standard in ISO/IEC 9594 apply.

3.1.5 Uniqueness of names

The distinguished name (DN) assigned to the certificate subscriber within the Trusted Service Provider's domain shall be unique.

3.1.6 Recognition, authentication, and role of trademarks

Certificate applicants must not include names in applications for issuance that may involve infringement of third-party rights by the future subscriber.

Izenpe does not determine whether a certificate applicant has any rights to the name appearing in a certificate application. Izenpe does not act as an arbitrator or mediator, nor does it otherwise resolve any dispute concerning the ownership of names of persons or organisations or domain names.

Izenpe reserves the right to reject a certificate application due to name conflict.

3.2 Initial identity validation

Izenpe performs the validation process of the information included in the website authentication certificate in accordance with the 'Basic requirements for issuing and managing trusted certificates', requirements established by the CA/Browser forum and which can be viewed at https://cabforum.org/working-groups/server/baseline-requirements/requirements/ .

Additionally, Izenpe, before issuing a qualified SSL Certificate, ensures that all the information included in these types of certificates regarding the subscriber, is in accordance with (and verified according to) the requirements defined by the CA/Browser forum entity in its 'guide for the issuance and management of Extended Validation Certificates', (section 11) and which can be viewed at https://cabforum.org/working-groups/server/extended-validation/guidelines/ .

Izenpe records all confirmations made in this section for the periodic internal and independent audit processes.

3.2.1 Method to prove possession of private key

Izenpe receives a certificate request, in PKCS#10 format, digitally signed by the Private Key generated by the subscriber's representative in its environment wich includes the Public Key related to the Private one.

3.2.2 Authentication of organization identity

Before requesting any certificate for the first time, Izenpe will force to enroll the Organization into its system with the authorization of a Representative. In this process, the Organization and Representative information will be validated against a reliable source as stated in the 3.2.2.1 section and this info will be used when OV and EV certificates are issued.

3.2.2.1 Identity

Izenpe does not issue authentication certificates for websites whose subscriber is a natural person.

- In the case of DV certificates,

Izenpe does not check the identity or any type of information about the organisation.

- In the case of OV certificates
    - Izenpe verifies the postal address and the identity of the subscribing organisation depending on the type of organisation (private or public).
    - When the subscriber is a private sector organisation, Izenpe verifies its address and identity by consulting the corresponding official register.

In the case of public entities, verification is conducted by consulting the corresponding Official Gazette and other consulted registers.

Izenpe verifies that the name and postal address of the organisation subscribing the certificate included in the certificate application coincides with the name and address formally entered in the consulted registers as described in the previous sections.

- In the case of qualified SSL certificates

Izenpe verifies the existence, address, and identity of the organisation, depending on the type of organisation.

- When the subscriber is a private sector organisation, Izenpe verifies its address and identity by consulting the corresponding official register.
- In the case of public entities, verification is conducted by consulting the corresponding Official Gazette and other consulted registers.

The verification sources that Izenpe will use in these cases are the following:

VERSION	DATE
3	2025/06/19

DESCRIPTION	URL	COUNTRY	PROVINCE
OFFICIAL BULLETIN OF THE BASQUE COUNTRY	https://www.euskadi.eus/y22-bopv/es/bopv2/datos/Ultimo.shtml	ES	EUSKADI
OFFICIAL BULLETIN OF THE GENERALITAT OF CATALONIA	https://dogc.gencat.cat/es/inici/index.html	ES	CATALUNYA
LOCAL ENTITIES REGISTRY OF THE	https://www.euskadi.eus/registro-de-entidades-locales/web01-a2tokiad/es/	ES	EUSKADI

DESCRIPTION	URL	COUNTRY	PROVINCE
BASQUE COUNTRY			
Ministry of Justice for Religious Entities	https://maper.mjusticia.gob.es/Maper/buscarRER.action	ES	
TAX AGENCY	https://www10.agenciatributaria.gob.es/wlpl/BURT-JDIT/ws/VNifV2SOAP	ES	
COMMERCIAL REGISTRY	https://sede.registradores.org/site/invitado/mercantil/busqueda#/	ES	
INVENTORY OF PUBLIC ENTITIES	https://www.pap.hacienda.gob.es/invente2/pagMenuPrincipalV2.aspx/	ES	
BANK OF SPAIN	www.bde.es	ES	
OFFICIAL BULLETIN OF SPAIN	https://www.boe.es/buscar/boe.php	ES	
OFFICIAL BULLETIN OF BIZKAIA	https://apps.bizkaia.eus/BT00/	ES	BIZKAIA
GIPUZKOA OFFICIAL BULLETIN	https://egoitza.gipuzkoa.eus/es/bog	ES	GIPUZKOA
ARABA/ALAVA OFFICIAL BULLETIN	https://www.araba.eus/botha/	ES	ALAVA/ARABA
OFFICIAL BULLETIN OF THE BASQUE COUNTRY	https://www.euskadi.eus/y22-bopv/es/p43aBOPVWebWar/buscarAvanzada.do?idioma=es&tipoBusqueda=2	ES	EUSKADI
REGISTRATION ASSOCIATIONS OF THE BASQUE COUNTRY	https://www.euskadi.eus/registro-asociaciones-buscador/web01-a2aderre/es/	ES	EUSKADI
ASSOCIATIONS REGISTRY	https://www.pap.hacienda.gob.es/invente2/pagMenuPrincipalV2.aspx/	ES	
LOCAL ENTITIES OF NAVARRA	https://www.navarra.es/es/buscador-de-entidades-locales	ES	NAVARRA
TRADE UNIONS AND BUSINESS ORGANIZATIONS	https://expinterweb.mites.gob.es/deose/publico/expedientes	ES	

Izenpe verifies that the name, address, and tax identification number of the subscribing organisation of the certificate incorporated in the certificate application coincide with the name, address and tax identification number formally registered in the records consulted as described in the previous sections.

Izenpe will comply with the requirements defined by the CA/Browser forum entity in its 'guide for the issuing and management of Extended Validation Certificates,' which can be consulted at https://cabforum.org/extended-validation/.

3.2.2.2 Trade name or registered trademark

If the subject identity information includes a trade name or trademark, Izenpe will use the same verification procedures and criteria as in Section 3.2.2.1 to verify the Applicant's right to use the trade name or trademark.

In the case of qualified SSL Certificates, a comprehensive identity verification is required as defined in section 11.3 of CABForum's 'Guide to the Issuance and Management of Extended Validation Certificates'.

3.2.2.3 Country Verification

The country shall be verified using any of the methods listed in Section 3.2.2.1.

3.2.2.4 Validation of authorisation and domain control

To validate the domain for website authentication certificates, Izenpe uses one of the following methods described in the CA/Browser Forum's Baseline Requirements document:

- 3.2.2.4.4 Constructed Email to Domain Contact
- 3.2.2.4.7 DNS Change
- 3.2.2.4.14 Email to DNS TXT Contact
- 3.2.2.4.18 Agreed-Upon Change to Website v2
- 3.2.2.4.19 Agreed-Upon Change to Website - ACME

For each of the methods used, Izenpe will follow a documented process and maintain records indicating the methods used for each issue. The other methods described in CA/Browser Forum's Baseline Requirements are not used for domain validation.

- Constructed Email to Domain Contact (BR 3.2.2.4.4).

  An email with a Random value will be sent to one or more of the following recipients “admin”,”administrator”, “webmaster”, “hostmaster” o “postmaster” of the requested domain.

- Agreed DNS change (BR 3.2.2.4.7): The applicant makes a change to the DNS record of the domain for which it is requesting the SSL certificate. The applicant must add the random and unique code sent by Izenpe in a CNAME, TXT or CAA field in its DNS record. Once the change is made by the applicant, Izenpe verifies it.

  Izenpe will provide a unique random code for the certificate request and will not use the random code after 30 days.

  For this there must be a CAA type ‘contactmail’ entry with an email address: CAA 0 contactemail contacto@example.com

  Izenpe will provide a unique random code for the certificate request and will not use the random code after 30 days.

- Email to DNS TXT contact (BR 3.2.2.4.14): Izenpe sends the applicant a unique and random code by email to the address that appears in the DNS TXT record. There must be a TXT entry in the subdomain ‘_validation-contactemail’ with an email address:

  _validation-contactemail.izenpe.eus. 299 IN TXT ‘contacto@example.com’

  Izenpe will provide a unique random code for the certificate request and will not use the random code after 30 days.

- Agreed website change (BR 3.2.2.4.18): The applicant must publish in the path ‘/. well-known/pki-validation’ the file with a random and unique code sent by Izenpe. Once the change is made by the applicant, Izenpe verifies it.

- Agreed-Upon Change to Website - ACME:
  Confirming the Applicant's control over a FQDN by validating domain control of the FQDN using the ACME HTTP Challenge method defined in section 8.3 of RFC 8555. The following are additive requirements to RFC 8555.
  IZENPE must receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received). The token (as defined in RFC 8555, Section 8.3) MUST NOT be used for more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values, in which case the CA MUST follow its CPS. IZENPE does not follow redirects.

Izenpe confirms that the subscriber's representative has control over the full domain names or FQDN (Fully Qualified Domain Name) that are incorporated into the website authentication certificates it issues. To do this, Izenpe checks, through the application that registers the requests for these certificates, the identity of the subscriber's representative and the name of the FQDN. It then verifies that the request comes from the contact that has control over said domain (according to the methods defined in the previous section) or is authorised by said contact. In addition, it checks that the certificate request has been made after the registration in said registers.

Additionally, before issuing a website authentication certificate, it is verified that the domain to be included in the certificate is public (it is not an internal domain) and public registries are consulted to verify that it is not a high-risk domain (Google Safe Browsing).

3.2.2.5 Authentication for an IP address

Izenpe does not issue certificates to identify IP addresses.

3.2.2.6 Wildcard Domain Validation

The RA will verify that the entire domain namespace in the OV Wildcard Certificates is legitimately controlled by the Subscriber.

If in a wildcard certificate the asterisk is within the label immediately to the left of a public suffix or controlled record, Izenpe will refuse to issue such a certificate unless the applicant demonstrates legitimate control of the entire domain name space.

For this purpose, it will consult the 'Public Suffix List' available at https://publicsuffix.org/, which will be downloaded from time to time.

3.2.2.7 Data Source Accuracy

Prior to using any data source as a Reliable Data Source, Izenpe shall evaluate the source for its reliability, accuracy, and resistance to alteration or falsification. Izenpe will consider the following during its evaluation:

1. The age of the information provided,
2. The frequency of updates to the information source,
3. The data provider and purpose of the data collection,
4. The public accessibility of the data availability, and
5. The relative difficulty in falsifying or altering the data.

3.2.2.8 CAA Registration

As part of the Certificate issuance process, IZENPE shall retrieve and process CAA records in accordance with RFC 8659 for each dNSName in the subjectAltName extension that does not contain an Onion Domain Name.

When processing CAA records, IZENPE shall process the issue, issuewild, and iodef property tags as specified in RFC 8659, although they are not required to act on the contents of the iodef property tag. Additional property tags MAY be supported, but MUST NOT conflict with or supersede the mandatory property tags set out in this document. IZENPE SHALL respect the critical flag and not issue a certificate if they encounter an unrecognized property tag with this flag set.

If IZENPE issues a certificate after processing a CAA record, it MUST do so within the TTL of the CAA record, or 8 hours, whichever is greater.

3.2.3 Authentication of individual identity

Izenpe checks that the subscriber's representative coincides with the natural person requesting a website authentication certificate, by electronically signing the application form using a Qualified Electronic Signature Certificate, thus guaranteeing the authenticity of their identity.

In the case of DV or OV certificates, the Subscriber's representative may delegate the application capacity to authorised applicants. The representative must electronically sign this delegation through the SSL certificate management application.

3.2.4 Non-verified subscriber information

All the information included in the electronic certificate is verified by the Registration Authority, therefore, no unverified information is included in the 'Subject' field of the issued certificates.

3.2.5 Validation of authority

Izenpe verifies that the applicant has sufficient representative capacity by electronically signing the customer registration application form, as described in section 3.2.3 of this policy, accepting the use of an Izenpe Representative certificate. When the aforementioned form is signed using a qualified certificate other than those mentioned in the previous section, the Izenpe RA verifies the representative capacity of the signatory of the application by consulting official registers (Companies Register, Official Gazettes, etc., depending on the nature of the representation). If the results of these consultations do not provide evidence of sufficient representation, Izenpe will contact the subscriber to obtain such evidence.

Through the online application for requesting SSL certificates, the entity's representative will be able to create the associated users to allow the request for DV and OV certificates for said entity.

For requests for qualified SSL certificates, Izenpe will comply with the requirements defined by the CA/ Browser Forum entity in its 'guide for the issuance and management of Extended Validation Certificates'.

3.2.6 Criteria for interoperation

There are no interoperability relationships with Certification Authorities external to Izenpe.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Subscribers may request re-key of any certificate via IZENPE's web application. This new request may require new validations if any of them hava expired.

The authentication conditions for a renewal request are described in the section of this CP corresponding to the Certificate renewal process (see section 4.6 of this document).

3.3.2 Identification and authentication for re-key after revocation

The certificate renewal process after revocation of the certificate shall be the same as the one followed for the initial issuance of the certificate.

3.4 Identification and authentication for revocation request

IZENPE may revoke any certificate covered by this CP at its sole discretion. The conditions for authentication of a revocation request are developed in section 4.9 of this document.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

Only Subscriber Representatives, or persons duly authorised to apply for the certificate on behalf of the Subscriber, who have accredited that they have control over the domain name to be included in the certificate, may request website authentication certificates. The aforementioned control over the domain name will be verified by Izenpe as described in section '3.2 Initial validation of identity' of this Policy.

Additionally, for qualified certificates, Izenpe will comply with the requirements of the 'Guide for the issuance and management of Extended Validation Certificates' established by the CA/Browser forum.

4.1.2 Enrollment process and responsibilities

Prior to the issuance of a Certificate, IZENPE SHALL gather the following documentation from the Applicant:

- Submission of the application for issuance and acceptance of the applicable terms and conditions. With this acceptance, subscribers guarantee that all information contained in the certificate request is correct.
- Submission of the technical request (PKCS#10).
- Payment, if applicable, of the applicable fees.

The Izenpe RA will verify the Subscriber's subscribing organisation and the Subscriber's representative, and check that the Certificate application is correct, complete, and duly authorised, in accordance with the requirements defined in section '3.2 Initial validation of identity' of this document. Izenpe may conduct additional checks to the validation processes described in the aforementioned section.

Izenpe will compile and keep the evidence corresponding to the checks conducted.

Section 9.6 'Obligations and guarantees' of this document sets out the responsibilities of the parties in this process.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

The Subscriber's Representative will send the Izenpe RA an electronically signed form with a qualified electronic certificate, which contains all the information to be included in the website authentication certificate. Based on this information, the Izenpe RA will carry out the checks described in section '3.2 Initial validation of identity' of this Policy.

Izenpe will check the veracity of the data included in the application and, where applicable, the capacity of the representative through the corresponding verifications, keeping the appropriate evidence.

The electronic signature generated for the conclusion of the contract will be verified by Izenpe.

The use of pre-validation data or documentation, obtained from a source specified in section 3.2, may not be used more than 12 months after the validation of such data or documentation.

4.2.2 Approval or rejection of certificate applications

The RA that acts in the process of issuing website authentication certificates is always Izenpe itself and, therefore, does not delegate the validation of domain ownership to any other RA.

Izenpe's RA performs the checks relating to proof of possession of the private key by the Subscriber Representative, authentication of the identity of the organisation and of the person requesting the certificate, as well as validation of the domain, as described in section '3.2 Initial validation of identity' of this CP, which will result in the approval or rejection of the request for the same.

Izenpe maintains an internal database of all revoked certificates, and all previously rejected certificate applications due to suspected phishing or other fraudulent use. This information is considered to identify subsequent suspicious certificate requests before proceeding with the approval of certificate issuance.

Additionally, Izenpe develops, maintains, and implements documented procedures that identify and require additional verification activity for high-risk certificate requests prior to approval of certificate issuance, as reasonably necessary to ensure that such requests are adequately verified against these requirements.

If any such validation could not be confirmed, Izenpe shall reject the certificate application, reserving the right not to disclose the reasons for such rejection. The Subscriber Representative whose application has been rejected may reapply at a later date.

Any application for an OV certificate or qualified certificate shall be processed by Izenpe personnel with the role of trusted personnel for this purpose. The approval system for issuing qualified certificates requires the action of at least two people belonging to the Izenpe RA with the role of trusted personnel, one to validate the application and the other to approve it.

Additionally, Izenpe checks if there is a CAA record for each domain name included in an issued website authentication certificate, according to the procedure set out in RFC 8659 and following the processing instructions set out in RFC 8659 for any records found.

If such a CAA Record exists, it will not issue such a Certificate unless it determines that the Certificate request is consistent with the applicable CAA resource record set.

4.2.3 Time to process certificate applications

The time taken to process the application for a certificate depends to a large extent on the Subscriber Representative providing the necessary information and documentation in the manner provided for in the procedures approved by Izenpe for this purpose. However, Izenpe will make every effort to ensure that the validation process resulting in the acceptance or rejection of the application does not exceed five working days.

This period of time may occasionally be exceeded for reasons beyond Izenpe's control. In such cases, it will endeavour to keep the Subscriber Representative who made the request informed of the causes of such delays.

4.2.4 Certificate Authority Authorization (CAA)

iZENPE supports CAA for the issuance of TLS and Verified Mark Certificates as described in Section 3.2.2.8.

Subscribers who wish to authorize IZENPE to issue TLS Certificates for their FQDNs should include a CAA record property issue or issuewild, including the value "izenpe.com" or "izenpe.eus" in their respective DNS zone.

4.3 Certificate issuance

As of April 15, 2026, Izenpe will no longer perform TLS certificate issuance functions under 2007 ROOT CA. No new certificates, including renewals or re-keys, will be issued under this CA. All automated and manual issuance systems have been decommissioned or restricted to prevent further production of publicly-trusted certificates.

4.3.1 CA actions during certificate issuance

Once the Certificate application has been approved by the Izenpe RA, the certificate generation system has a series of controls, prior to issuing the certificate, which verify compliance with the requirements of RFC 5280 and CA/Browser Forum (BRs and EVGs). After this verification, the Certificate is issued in accordance with the approved profile for each type of Certificate.

Likewise, Izenpe periodically monitors deviations in the certificates issued.

The processes related to the issuing of electronic Certificates guarantee that all the accounts involved in them have multi-factor authentication.

4.3.1.1 Manual authorization of certificate issuance for Root Cas

Certificate issuance by the Root CA SHALL require an individual authorized by IZENPE (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation.

4.3.1.2 Linting of to-be-signed Certificate content

Due to the complexity involved in implementing Certificate Profiles that conform to these Requirements, it is considered best practice for the CA to implement a Linting process to test the technical conformity of each to-be-signed artifact prior to signing it. When a Precertificate has undergone Linting, it is not necessary for the corresponding to-be-signed Certificate to also undergo Linting, provided that the CA has a technical control to verify that the to-be-signed Certificate corresponds to the to-be-signed Precertificate in the manner described by RFC 6962, Section 3.2. Effective 2024-09-15, the CA SHOULD implement such a Linting process. Effective 2025-03-15, the IZENPE SHALL implement such a Linting process.

IZENPE SHOULD use the Linting tools that have been widely adopted by the industry (see https://cabforum.org/resources/tools/). Specifically, zlint and pkimetal.

4.3.2 Notification to subscriber by the CA of issuance of certificate

Once the Certificate has been issued, Izenpe sends a communication to the e-mail address given in the customer registration form signed by the Subscriber's Representative, informing that the certificate is available for download.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

In the Certificate application process, the Subscriber's Representative accepts the conditions of use and expresses his/her willingness to obtain the certificate, as necessary requirements for the generation of the certificate.

4.4.2 Publication of the certificate by the CA

Root and Sub CAs are published in the Izenpe general repository (Section 2.2 of this document).

Izenpe generates a precertificate for each certificate issued according to RFC6962 (Certificate Transparency). This precertificate contains the same information of the intended-to-issue certificate and shall be considered as it was issued (even if it was not). These certificates can be retrieved by anyone quering the Certificate Transparency servers.

4.4.3 Notification of certificate issuance by the CA to other entities

Prior to the issuance of Website Authentication Certificates, a pre-certificate is sent to the Certificate Transparency service registers of those providers where Izenpe Root Certificate has been included.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

Izenpe does not generate or store the private keys associated with the Certificates issued under this Certification Policy. The status of custodian and control of the certificate keys corresponds to the Subscriber's Representatives who have accredited control over the domain name to be included in the certificate. Therefore, the private key associated with the public key shall be under the responsibility of said custodian.

4.5.2 Relying party public key and certificate usage

User entities and relying third parties shall use software that is compatible with the standards applicable to the use of electronic certificates (X.509, IETF, RFCs, etc.). If the connection to the website requires additional security measures, these measures must be obtained by the user entities.

Third parties relying on the establishment of a secure connection guaranteed by a Website Authentication Certificate must ensure that said connection was created during the period of validity of the Certificate, that said Certificate is being used for the purpose for which it was issued in accordance with this CP, as well as verifying that the Certificate is currently active, by checking its revocation status in the manner and conditions set out in section ‘4.10 Certificate status information services’ of this document.

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

To renew a certificate, the applicant shall follow the certificate issuance process set out in this document.

4.6.2 Who may request renewal

To renew a certificate, the applicant shall follow the certificate issuance process set out in this document.

4.6.3 Processing certificate renewal requests

To renew a certificate, the applicant shall follow the certificate issuance process set out in this document

4.6.4 Notification of new certificate issuance to subscriber

To renew a certificate, the applicant shall follow the certificate issuance process set out in this document.

4.6.5 Conduct constituting acceptance of a renewal certificate

To renew a certificate, the applicant shall follow the certificate issuance process set out in this document.

4.6.6 Publication of the renewal certificate by the CA

To renew a certificate, the applicant shall follow the certificate issuance process set out in this document.

4.6.7 Notification of certificate issuance by the CA to other entities

To renew a certificate, the applicant shall follow the certificate issuance process set out in this document.

4.7 Certificate re-key

The renewal with key regeneration of website authentication certificates is always performed by issuing new public and private keys, following the same process as described for the issuance of a new Certificate.

4.7.1 Circumstance for certificate re-key

Certificate keys will be renewed under the following circumstances:

- Due to the imminent expiry of the current keys at the request of the renewal applicant.
- Due to compromise of the keys or any other circumstance listed in section '4.9 Revocation and suspension of the certificate' of this CP.

4.7.2 Who may request certification of a new public key

The same process as described for the issuance of a new Certificate shall be followed.

4.7.3 Processing certificate re-keying requests

The same process as described for the issuance of a new Certificate shall be followed.

4.7.4 Notification of new certificate issuance to subscriber

The same process as described for the issuance of a new Certificate shall be followed.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

The same process as described for the issuance of a new Certificate shall be followed.

4.7.6 Publication of the re-keyed certificate by the CA

The same process as described for the issuance of a new Certificate shall be followed.

4.7.7 Notification of certificate issuance by the CA to other entities

The same process as described for the issuance of a new Certificate shall be followed.

4.8 Certificate modification

It is not possible to make modifications to issued Certificates. Therefore, any need for modification entails the issuance of a new Certificate.

4.8.1 Circumstance for certificate modification

Modification is not stipulated.

4.8.2 Who may request certificate modification

Modification is not stipulated.

4.8.3 Processing certificate modification requests

Modification is not stipulated.

4.8.4 Notification of new certificate issuance to subscriber

Modification is not stipulated.

4.8.5 Conduct constituting acceptance of modified certificate

Modification is not stipulated.

4.8.6 Publication of the modified certificate by the CA

Modification is not stipulated.

4.8.7 Notification of certificate issuance by the CA to other entities

Modification is not stipulated.

4.9 Certificate revocation and suspension

Website authentication certificates issued by Izenpe will be revoked in the following cases:

1. Termination of the validity period of the certificate.
2. Cessation of activity as a Trusted Service Provider of Izenpe, unless, with the express consent of the subscriber, the certificates issued by Izenpe have been transferred to another Trusted Service Provider. In cases a) and b), the loss of effectiveness of the certificates will take place as soon as these circumstances arise.
3. Revocation of the certificate for any of the reasons listed in this document.

The expiry of the validity of the certificate will take effect from the date on which Izenpe becomes aware of any of the determining events and so states in its Information and Consultation Service on the status of the certificates.

Izenpe makes available to subscribers, trusting third parties, software providers and third parties a communication channel via incidencias@izenpe.eus, to allow them to report any issue related to this type of certificate, regarding an alleged compromise of the Private Key, improper use of the Certificates or other types of fraud, compromise, misuse or inappropriate conduct.

Izenpe, as a Trusted Service Provider, reserves the right not to issue or revoke this type of certificate if the subscriber who has control of the domain name of the website included in the certificate does not use it appropriately, infringing the industrial or intellectual property rights of third parties over the applications, websites or electronic sites that it wishes to protect with such certificates, or its use is misleading or confusing as to the ownership of such applications, websites or electronic sites and, therefore, of its content.

Izenpe shall be held harmless by the owners or persons responsible for the equipment, applications, websites, or electronic sites that do not comply with the provisions of this section and that are related to the certificate and shall be exonerated from any claim or demand for the improper use of such certificates.

4.9.1 Circumstances for revocation

4.9.1.1 Grounds for revocation of an End Entity Certificate

In addition to the provisions of the previous section, the following shall be causes for revocation of a website authentication certificate:

1. The request for revocation by authorised persons. In any case, this request must be made:
    - The loss of the certificate medium.
    - The use by a third party of the private key associated with the certificate.
    - The violation or compromise of the secrecy of the private key associated with the certificate.
    - Non-acceptance of the new conditions that may imply the issuing of new Certification Practice Statements, during the period of one month after their publication.
2. Judicial or administrative resolution ordering it.
3. Extinction, dissolution, or closure of the website identified by the certificate.
4. Extinction or dissolution of the subscriber's legal personality.
5. Termination of the form of representation of the certificate subscriber's representative.
6. Total or partial incapacity of the Subscriber's representative.
7. Inaccuracies in the data provided by the Subscriber's Representative to obtain the certificate, or alteration of the data provided to obtain the certificate or modification of the circumstances verified for the issuance of the certificate, such that the certificate no longer conforms to reality.
8. Contravention of a substantial obligation of this Certification Practice Statement by the subscriber, the subscriber's representative, or a Registration Entity if, in the latter case, it could have affected the procedure for issuing the Certificate.
9. Using the certificate for the purpose of generating doubts among users about the origin of the products or services offered, making it appear that their origin is different from that actually offered. To this end, the criteria on infringing activity of the regulations on consumers and users, trade, competition, and advertising will be followed.
10. Termination of the contract signed between the subscriber or their representative and Izenpe, or non-payment of the services provided.
11. Violation or endangerment of the secrecy of Izenpe's signature/seal creation data, with which it signs/seals the certificates it issues.
12. Non-compliance with the requirements defined by the audit schemes to which the Certification Authority issuing the certificates covered by this Policy is subject, with special attention to those of algorithm and key sizes, which entail an unacceptable risk for the parties that trust these Certificates.

Under no circumstances should it be understood that Izenpe assumes any obligation to check the points mentioned in numbers "3." to "9." of this section.

Izenpe will only be responsible for the consequences of not having revoked a Certificate in the following cases:

- That the revocation has been requested by the Subscriber's Representative following the procedure established for this type of Certificate.
- The revocation should have been carried out due to the termination of the contract signed with the Subscriber.
- That the revocation request or the cause for revocation has been notified to the Subscriber by means of a judicial or administrative resolution.
- That in cases "3." to "7." of this section, the aforementioned points have been reliably accredited, after identification of the Applicant for revocation.

Actions constituting a crime or misdemeanour of which Izenpe is unaware that are carried out on the data or the Certificate, inaccuracies in the data or lack of diligence in communicating them to Izenpe, will exonerate Izenpe from liability.

All requests for revocation of end-entity certificates are processed within a maximum period of 24 hours from receipt of the request.

4.9.1.2 Causes for revocation of a Sub CA certificate

Sub CA certificates shall be revoked within a maximum period of 7 days for the following reasons:

1. The Sub CA requests it in writing
2. The Sub CA notifies the issuing CA that the original certificate request was not authorised and does not allow retroactive authorisation.
3. The issuing CA obtains evidence that the Sub CA's private key corresponding to the certificate's public key has been compromised or no longer meets the requirements of sections 6.1.5 and 6.1.6 of the BRs.
4. The issuing CA obtains evidence that the certificate was incorrectly issued.
5. The issuing CA detects that the certificate was not issued in accordance with the Certificate Policy or the CPS.
6. The issuing CA determines that information in the certificate is inaccurate or incorrect
7. The issuing CA or sub CA ceases operations for any reason and has not enabled arrangements with another CA to provide the revocation service.
8. The right to issue certificates by the issuing CA or sub CA under the BR requirements is terminated or revoked, unless the issuing CA has enabled arrangements to continue to maintain the CRL/OCSP repository.
9. Revocation is required by the issuing CA's policy and/or by the CPS.
10. The content or technical format of the certificate presents an unacceptable risk to software vendors or third parties.
11. Providers or third parties (e.g., the CA/Browser Forum may determine that a cryptographic algorithm/ signature or key size presents an unacceptable risk and that such certificates should be revoked and replaced within a specified period of time).

4.9.2 Who can request revocation

The Subscriber, RA, or Issuing CA can initiate revocation. Additionally, Subscribers, Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Reports informing the issuing CA of reasonable cause to revoke the certificate.

4.9.3 Procedure for revocation request

The revocation applicant shall submit the revocation request to Izenpe. In the event that the revocation is requested by a person other than the applicant, the subscriber, or the key holder, prior to or at the same time as the revocation, Izenpe will inform the key holder and the subscriber of the certificate of the revocation of their certificate and the reason it has been carried out.

The applicant may revoke the certificate through the following channels,

- In person before,
    - Izenpe via prior appointment at www.izenpe.eus
    - Or to the subscribing organisation with which Izenpe has signed the relevant legal instrument.
- Online, at www.izenpe.eus
- By e-mail, by sending the revocation request form signed with the electronic ID card or a qualified certificate issued by Izenpe.

The authenticated revocation request, as well as the information justifying the revocation, is registered, and archived.

Once Izenpe has proceeded to the revocation of the website authentication certificate, the corresponding List of Revoked Certificates will be published in the Secure Directory, containing the serial number of the revoked Certificate, as well as the date, time, and cause of revocation. The Subscriber's Representative will receive, via the e-mail address specified in the application, notification of the change in the Certificate's validity status.

4.9.4 Revocation request grace period

There is no grace period associated with this process, as revocation takes place immediately upon verified receipt of the revocation request.

4.9.5 Time within which CA must process the revocation request

All requests for revocation of end-entity certificates are processed within a maximum period of 24 hours from the acknowledgement of receipt of the request.

Izenpe proceeds to the immediate revocation of the website authentication certificate at the time of carrying out the checks described above or, where appropriate, once the veracity of the request has been verified by judicial or administrative resolution.

4.9.6 Revocation checking requirement for relying parties

Third parties who trust and accept the use of certificates issued by Izenpe may verify:

- that the certificate is still valid and active, and
- the status of the certificates included in the certification chain.

4.9.7 CRL issuance frequency (if applicable)

Izenpe immediately issues a Certificate Revocation List (hereinafter CRL) as soon as a revocation occurs.

The scheduled time for issuing a new CRL is indicated in the CRL, although a CRL may be issued before the deadline indicated in the previous CRL. If no revocations occur, the Certificate Revocation List is regenerated daily.

The CRL for end-entity certificates is issued at least every 24 hours, or when a revocation occurs, with a validity of 10 days.

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

Revoked certificates that expire are removed from the CRL. The record of the revocation is then kept in Izenpe's internal register for a period of 15 years.

4.9.8 Maximum latency for CRLs (if applicable)

The maximum latency time is set at 30 seconds from the generation of the CRL.

4.9.9 On-line revocation/status checking availability

Izenpe provides User Entities with a real-time certificate verification service using the OCSP protocol (Online Certificate Status Protocol), so that the user applications will verify the status of the certificate.

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

4.9.10 On-line revocation checking requirements

The use of the CRLs service, which is freely accessible, shall require,

- To check in any case the last CRL issued, which can be downloaded from the URL address contained in the certificate itself in the extension 'CRL Distribution Point.'
- For the user to additionally check the relevant CRL(s) of the hierarchy's certification chain.
- For the user to ensure that the revocation list is signed by the authority that has issued the certificate to be validated.
-

Revoked certificates that expire will be removed from the CRL, however, information on the status of the certificate will still be provided via the online check, regardless of whether it is expired.

The use of the freely available OCSP service will require:

- Checking the URL address contained in the certificate itself in the 'Authority Info Access' extension.
- The user must ensure that the response is signed by the CA that issued the certificate to be validated.

4.9.11 Other forms of revocation advertisements available

Izenpe sends an informative email to the certificate subscriber when a certificate is revoked.

4.9.12 Special requirements re key compromise

There are no special requirements in the case of certificate revocation caused by a key compromise, and the requirements described for the rest of the causes of revocation apply.

4.9.13 Circumstances for suspension

Suspension of certificates is not contemplated.

4.9.14 Who can request suspension

Suspension of certificates is not contemplated.

4.9.15 Procedure for suspension request

Suspension of certificates is not contemplated.

4.9.16 Limits on suspension period

Suspension of certificates is not contemplated.

4.10 Certificate status services

4.10.1 Operational characteristics

The operation of the Certificate Status Information and Query Service is as follows: the OCSP server receives the OCSP request made by an OCSP Client and checks the validity status of the certificates included in the request. If the request is valid, an OCSP response is issued informing about the current status of the Certificates included in the request. This response is signed/sealed with the Signature Creation Data /Izenpe Seal, thus guaranteeing the integrity and authenticity of the information provided on the revocation status of the Certificates consulted.

It is the responsibility of the User Entity to have an OCSP Client to operate with the OCSP server made available by Izenpe.

Izenpe operates and maintains its CRL and OCSP service maintenance capabilities with sufficient resources to provide a sufficient response time under normal operating conditions.

4.10.2 Service availability

IZENPE performs all the necessary actions for the uninterruptible - as possible - availability of its OCSP service. IZENPE SHALL operate and maintain its CRL and OCSP capability with resources sufficient to provide a response time of ten (10) seconds or less under normal operating conditions.

4.10.3 Optional features

Not stipulated.

4.11 End of subscription

The certificate is no longer valid for use after the end of the validity period or when it has been revoked.

The expiry of each certificate is indicated in the specific Policy.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

Izenpe does not generate the private keys of website authentication certificates and, therefore, does not keep them and cannot recover them.

4.12.2 Session key encapsulation and recovery policy and practices

Not stipulated.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

5.1.1 Site location and construction

The facilities where information is processed fulfils the following requirements:

- The building with the information processing facilities is physically solid, 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

Data Processing Centre.

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 is kept.
- 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.

Registration Authorities (RAs)

RAs meet necessary security criteria, defined both in Izenpe's Security Policy and its Provider Security Policy.

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 organisation. The roles and responsibilities are defined for each one of them.

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 Roles requiring separation of duties

IZENPE follows the security policy CWA 14167 (Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures) and it is defined in the security model.

5.3 Personnel controls

5.3.1 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

With its Human Resource procedures, Izenpe carries out pertinent research before hiring anyone. Due to legal limitations, a criminal background check is not included.

5.3.3 Training requirements

IZENPE provides its personnel with the training needed to perform their job responsibilities competently and satisfactorily. Training is carried out at least once per year, which includes at least the following points:

- 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. • Incident management procedures.

Specific awareness-raising and training shall be given to RA operators at least when beginning, and then with the frequency defined by Izenpe.

5.3.4 Retraining frequency and requirements

Any significant change in IZENPE's operation will call for a training plan and implementation of the plan will be documented. "Trusted Role" staff must receive training at least once per year to maintain their skill levels. This training must always include a review of content.

5.3.5 Job rotation frequency and sequence

Employees are rotated according to the needs of the role itself, or at the behest of the employee.

5.3.6 Sanctions for unauthorized actions

Information security incidents

IZENPE has a security incident management plan.

Punitive process

There is an internal disciplinary regime which defines sanctions against personnel.

5.3.7 Independent contractor requirements

All personnel subcontracted by Izenpe to carry out roles related to operating Izenpe services is subject to the same requirements from Izenpe's Provider Security Policy.

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 logging procedures

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 Types of events recorded

The following logs are stored:

- New certificate applications
- Rejected certificate applications
- Account access violation
- Certificate signature
- Revoking the certificate
- Account logon
- CRLs signature
- CA modifications
- Certificate expiry

This list is not inclusive and is limited to events that are directly related to managing certificates or administrative roles. Particularly, technical events registered at other sites are not included.

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

5.4.1.1 Router and firewall activities logs

No stipulation.

5.4.2 Frequency of processing log

The logs are continuously processed and audited on a quarterly basis by the technical area. The audit report includes the following aspects:

- List of unauthorised access attempts
- Errors generated in each CA

5.4.3 Retention period for audit log

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 Protection of audit log

Access to log information is assigned to all personnel who require access as part of their role. The Auditor role may access it. The log is stored in the database, and access is protected at different levels.

Unauthorised deletion and modification of log records is blocked. There are contingency methods to prevent log data from being lost.

5.4.5 Audit log backup procedures

The logs are hosted in the database, so they are included in the daily database backup, according to the security copy policy.

5.4.6 Audit collection system (internal vs. external)

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

5.4.7 Notification to event-causing subject

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

5.4.8 Vulnerability assessments

Both external and internal vulnerabilities in IZENPE's internal systems are assessed on a quarterly basis. A penetration test is also performed annually.

5.5 Records archival

5.5.1 Types of records archived

The following data or files, in addition to others, are recorded:

- Data related to the certificate registration and application procedure:
- The audit logs described in the previous section;
- Key record.

5.5.2 Retention period for archive

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 Protection of archive

The Archive Management Procedure indicates the protective measures taken so that both paper registers and electronic registers cannot be handled or have their content destroyed.

5.5.4 Archive backup procedures

There is a security copy policy and contingency plan that define 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 Requirements for time-stamping of 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 for the date and time. All of the systems synchronise their time based on this source.

5.5.6 Archive collection system (internal or external)

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 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 Key changeover

To minimise the risk of compromising a CA private key, the key must be changed according to the security level of the algorithms used. Once changed, the new key should only be used for signature purposes. The old key, although still valid, should be available to verify old signatures until all of the certificates signed with it have expired. The private key should only be kept if used to sign CRLs that have certificates signed with this key and shall be protected with the same protection level as the new one. The procedure to generate a new CA key is defined in the Generation Ceremony Document for new CAs and migration from old CAs. Section 6.1.5 defines key sizes and algorithms used.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

5.7.1.1 Incident Response and Disaster Recovery Plans

There is a Contingency Plan that 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 re-establishing 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 to 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 action plan 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 applicants, subscribers and verifiers (trusted third parties) shall be included.
    - The contingency will be posted on the website
    - Revocation of affected certificates
    - Renewal strategy

5.7.1.2 Mass Revocation Plans

Since September 1, 20025, Izenpe maintains a comprehensive and actionable plan for mass revocation events to ensure a rapid, consistent, and reliable response to large-scale certificate revocation events.

This plan will be tested, reviewed, and updated annually. It will also be made available to Izenpe's auditors.

5.7.2 Computing resources, software, and/or data are corrupted

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

5.7.3 Entity private key compromise procedures

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

This contingency will be included in Izenpe's Business Continuity Plan, and shall determine, amongst others, the following actions to take:

1. Cease providing the affected service.
2. Revoke certificates that may be affected.
3. Notify subscribers, users and third parties. In the same fashion, a notification to TSPs shall be included with trust agreements, browser manufacturers and in general, any entity with which Izenpe holds any contractual use-of-service relationship.
4. Study the need to execute the TSP Activity Termination Plan according to the CPS and laws in force.

5.7.4 Business continuity capabilities 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 CA or RA termination

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

In the event of IZENPE activity termination, IZENPE must notify subscribers at least two months prior to the termination of operations, by any means that will ensure the proper communication and reception of its intent to cease its activity as a certification service provider. This notification shall indicate that all certificates in force will be revoked within a 2-month period.

In the event that a CA finalises due to expiry or revocation, consultations on the status of the certificate shall still be responded to through the OCSP service. Once the CA is finalised, OCSP responses on certificates issued by that CA shall be signed by another one of Izenpe's CAs in force of Izenpe.

Izenpe's CRLs do not include expired certificates, as indicated in section 4.9.7 Frequency of CRLs under this document.

In the event that Izenpe ceases activity, information on certificate revocation shall be provided through a last CRL, with a nextUpdate of "99991231235959Z" according to specifications in section 6.3.9 of ETSI EN 319 411-1.

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

For as long as necessary according to specifications in this CP/CPS, Izenpe shall keep all information on registration, status of revocation and log archives. If transferred to another entity, measures shall be taken so that said transfer is conducted with all guarantees necessary.

The party responsible for this notification is the IZENPE Directorate General or individual(s) appointed by the Board of Administrators, who shall decide on the most appropriate mechanism.

Izenpe shall inform the Supervising Entity of termination of its activity, including information on Certificates whose validity will expire. This communication will be made through the notification-sending platform of the electronic headquarters of the Ministry responsible for the provision of trust services, with a minimum of 3 months' notice prior to cessation of its activity.

Any authorisation with a thirty party with whom Izenpe holds a service provision contract (identification, issue, hosting, etc.) shall be deemed as terminated.

Izenpe or the entity with whom Izenpe agrees to transfer the service shall offer validity information on all its qualified certificates, even when the certificate has expired (until the expiry date for the subordinate CA that issued the certificate).

Izenpe has initiated a formal termination process regarding its SSL/TLS issuance services under 2007 ROOT CA. The following provisions apply:

- Cessation of Issuance: New certificate issuance was terminated on 2026/04/15.
- Continuous Revocation Services: The CA shall maintain its Repository, CRL issuance, and OCSP responder services in accordance with the timelines specified in the CA/B Forum Baseline Requirements until the last issued certificate has expired or has been revoked.
- Record Retention: All audit logs and evidence of certificate validation will be archived and retained for a minimum period of seven (7) years following the expiration of the last certificate issued by this CA."

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

6.1.1.1 CA Key pair generation

The root and subordinate CA cryptographic keys must be generated in a cryptographic hardware module (HSM) that meets with FIPS 140-2 level 3 (or later) and Common Criteria EAL 4+ for the corresponding protection profile. All cryptographic keys must be generated pursuant to minimum algorithm and key length recommendations stipulated in ETSI TS 119 312.

6.1.1.2 RA Key Pair Generation

Not provided

6.1.1.3 Subscriber Key Pair Generation

The private keys of website authentication certificates are generated and held by the certificate subscriber.

6.1.2 Private key delivery to subscriber

There is no generation or delivery of the private key by the CA to the Subscriber.

6.1.3 Public key delivery to certificate issuer

The Public Key, generated together with the Private Key on the key generation and custody device, is delivered to the Certification Authority by sending a certification request in PKCS#10 format.

6.1.4 CA public key delivery to relying parties

The public keys of the IZENPE CAs are distributed through various means, including the IZENPE website www.izenpe.eus. In the CP/CPS, section 1.3.1, the different footprints of the root CAs and issuing CAs are also published.

6.1.5 Key sizes

The algorithm used are as listed:

ROOT 2007 HIERARCHY

As for the size of the keys, depending on each case, it is:

TYPE OF CERT	KEY TYPE
Root CA	RSA 4096 bits
Subordinate CA	RSA 4096 bits
Website Authentication Certificate	RSA >=2048 bits

ROOT 2024 HIERARCHY

As for the size of the keys, depending on each case, it is:

TYPE OF CERT	KEY TYPE
Root CA	ECC 384 bits
Subordinate CA	ECC 384 bits
Website Authentication Certificate	ECC 256,384 bits

6.1.6 Public key parameters generation and quality checking

The Public Keys of the Web Site Authentication Certificates are encrypted according to RFC5280 and PKCS#1.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

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

The Root CA keys are used to sign the certificates of the Sub CAs, the ARLs and the TSA certificate. Sub CA or issuing CA keys are only used to sign end-user certificates and CRLs.

The supported key uses for end certificates are defined in the certificate profiles document available at www.izenpe.eus.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

A hardware security module (HSM) is a security device that generates and protects cryptographic keys. It is required that the HSM meet FIPS 140-2 Level 3 criteria at minimum, or Common Criteria EAL 4+ for the corresponding protection profile.

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 qualified 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.

In the event that these devices lose the secure device certification and this entails the loss of the condition of qualified signature, Izenpe will proceed to revoke the certificate; always as determined by the supervisory body and/or current regulations.

The European reference standard for subscriber devices used is Commission Implementing Decision (EU) 2016/650 dated 25 April 2016.

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 Private key escrow

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 as explained above.

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

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 event of contingency.

There is a procedure for recovering subscriber cryptographic module keys under Izenpe's custody which can be applied in the cases defined in the respective.

In both cases, the same controls are applied as those indicated in point 6.2.2.

6.2.5 Private key archival

Izenpe may make a backup copy of the Private Keys, ensuring that the security of the duplicated data is of the same level as that of the original data and that the amount of duplicated data does not exceed the minimum necessary to guarantee the continuity of the service. Signature creation data is not duplicated for any other purpose.

6.2.6 Private key transfer into or from a cryptographic module

The root CA private key, subordinate CAs, VA and TSA are generated in an HSM pursuant to point 6.2.1 and exportation is not possible. As a contingency measure, it is possible to recover private keys as indicated in section 6.2.4.

6.2.7 Private key storage on cryptographic module

There is a CA root and subordinate 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 EN 319 411-1, and CABForum Baseline Requirement Guidelines.

To generate subscriber keys in the cryptographic card, Izenpe follows European Commission recommendations (eIDAS) and EN 319 411-1.

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.

6.2.8 Method of activating private key

Private Keys of Certification Authorities are generated and held in custody by a cryptographic device that meets the security requirements of FIPS 140-2 Level 3.

Activation and use mechanisms of Private Keys of End Entity Certificates are described in the Specific Policy for each certificate.

6.2.9 Method of deactivating private key

A person with the administrator role may deactivate the Certification Authorities key by stopping the system. To reactivate it, action must be taken as described in section "6.2.8 Private key activation method".

Regarding deactivation of Private Keys of End Entity Certificates, this is described in the Specific Policy for each certificate.

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, the established procedure shall be followed.

This procedure is not applied to user signature or authentication keys issued on a cryptographic card or secure container, except in the case of key changeovers using the same cryptographic device.

6.2.11 Cryptographic Module Rating

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 Website Authentication Certificates and, therefore, their associated Public Keys, are kept by Izenpe for the period of time required by current legislation, which is currently 15 years.

6.3.2 Certificate operational periods and key pair usage periods

The operational periods of the Certificates and their associated Keys are:

- Root CA Certificate and its key pair: see section '1.3.1.Certification Authority' of this CP.
- The Certificate of the Sub CA issuing the Web Site Authentication Certificates and its key pair: see section '1.3.1. Certification Authority' of this CP.
- The Web Site Authentication Certificates and their key pair: the maximum period of validity is 195 days.

6.4 Activation data

6.4.1 Activation data generation and installation

Activation data, both for root CA keys and for subordinate CA keys issued by End Entity Certificates, are generated during the creation key ceremony of said Certification Authorities.

Regarding activation data of Keys of End Entity Certificates, they are described, if necessary, in the Specific Policy for each certificate.

6.4.2 Activation data protection

The root CA key activation data are distributed between several different physical cards, and at least two people are needed to perform any operation. The card keys are kept in custody in different safes.

The subordinate CA key activation data are distributed between several different physical cards, and at least two people are needed to perform any operation. The card keys are kept in custody in different safes.

The TSA and VA keys are generated and managed in the same HSM as the subordinate CA keys. The same rules apply.

Subscribers are compelled to keep their activation data secret.

6.4.3 Other aspects of activation data

See specific policy for each certificate type.

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.
    - There is 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 possesses the functions necessary to be 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 organisation.
    - 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.
    - There are quality guidelines for passwords
    - All operator accounts with capacity to issue certificates have double factor- based access control.

Izenpe has a security policy and specific procedures to guarantee security at different levels.

6.5.2 Computer security rating

The products used for the provision of certification services have the international certificate based on 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:

- Izenpe's policy includes rules to securely develop applications and systems.
- There is a formal procedure to track changes. Changes are limited to those necessary, and undergo thorough control.
- When operational systems are changed, the business applications deemed critical according to the Business Continuity Plan are reviewed.
- Secure system engineering principles are established.
- The development setting is duly protected.
- Outsourced development is supervised and controlled by Izenpe.
- Operational security tests are performed during development.
- Acceptance testing programmes are established for new information systems, updates and versions.
- Test data are selected, protected and controlled.

6.6.2 Security management controls

Izenpe constantly monitors to ensure that systems and communications operate according to Izenpe's Security Policy. All processes are logged and audited according to valid legislation and regulations.

6.6.3 Life cycle security controls

In order to conduct test, a large volume of data as similar as possible to production data is required. The use of production databases containing personal information is avoided.

6.7 Network security controls

The network's security is based on the concept of multi-level zoning with multiple redundant firewalls. The confidential information transferred by insecure networks is encrypted by using SSL/TLS protocols. There are IPS systems for internal and external traffic.

6.8 Time-stamping

IZENPE obtains the time from their systems by means of a connection with the Royal Navy Observatory by following the NTP protocol. . A description of the NTP protocol may be found in the IETF RFC 5905 standard.

Based on this internal service, Izenpe offers a time stamp service (TSA) that can be used to create time stamps on arbitrary documents, according to IETF RFC 3161 and ETSI EN 319 421. More information in Izenpe's Timestamp Practice Statement.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

The Website Authentication Certificates are in accordance with the European standard ETSI EN 319 412-4 'Certificate profile for web site certificates'.

They include the following CABForum policy identifiers:

CERTIFICATE	OID CA/B FORUM
DV SSL	2.23.140.1.2.1

CERTIFICATE	OID CA/B FORUM
OV SSL	2.23.140.1.2.2
EV SSL	2.23.140.1.1
Qualified SSL	2.23.140.1.1

7.1.1 Version number(s)

Certificates MUST be of type X.509 v3

7.1.2 Certificate extensions

On the following website https://www.izenpe.eus/contenidos/informacion/doc_juridica/es_def/adjuntos/Perfiles_de_Certificados.pdf the document describing the profile of the Website Authentication Certificates, including all its extensions, is published.

7.1.2.1 Root CA Certificate

- basicConstraints
  - This extension MUST appear as a critical extension. The cA field MUST be set true. The pathLenConstraint field SHOULD NOT be present
- keyUsage
  - This extension MUST be present and MUST be marked critical. Bit positions for keyCertSign and cRLSign MUST be set. If the Root CA Private Key is used for signing OCSP responses, then the digitalSignature bit MUST be set.
- certificatePolicies
  - This extension SHOULD NOT be present.
- extKeyUsage
  - This extension MUST NOT be present.

7.1.2.1.1 Root CA Validity

FIELD	MINIMUN	MAXIMUN
notBefore	One day prior to the time of signing	The time of signing
notAfter	2922 days (approx. 8 years)	9132 days (approx. 25 years)

7.1.2.2 Intermediate CA Certificate

1. ***basicConstraints***
   This extension SHALL be present and SHALL be marked critical. The cA field SHALL be set true. The pathLenConstraint field MAY be present.
2. ***authorityKeyIdentifier***
   This extension SHALL be present and SHALL NOT be marked critical. It SHALL contain a keyIdentifier field and it SHALL NOT contain a *authorityCertIssuer* or *authorityCertSerialNumber* field.
3. ***subjectKeyIdentifier***
   This extension SHALL be present and SHALL NOT be marked critical. It identifies a particular CA Key uniquely. It contains the ID of the CA Certificate key.
4. ***keyUsage***
   This extension SHALL be present and SHALL be marked critical. Bit positions for keyCertSign and cRLSign SHALL be set. If the Subordinate CA Private Key is used for signing OCSP responses, then the digitalSignature bit SHALL be set.
5. ***certificatePolicies***
   This extension must be present and should not be marked critical. It MUST contain at least one PolicyInformation.
6. ***extKeyUsage***
   This extension SHALL be present and SHOULD NOT be marked critical.
   For Subordinate CA Certificates that will be used to issue TLS server certificates, the value id-kp-serverAuth [RFC5280] SHALL be present. The value id-kp-clientAuth [RFC5280] MAY be present. The values id-kp-emailProtection [RFC5280], id-kp-codeSigning [RFC5280], id-kp-timeStamping [RFC5280], id-kp-OCSPSigning [RFC5280] and anyExtendedKeyUsage [RFC5280] SHALL NOT be present. Other values SHOULD NOT be present.
7. ***authorityInformationAccess***
   This extension MUST be present and MUST NOT be marked critical. It MUST contain a keyIdentifier field and it MUST NOT contain a authorityCertIssuer or authorityCertSerialNumber field.
8. ***cRLDistributionPoints***
   This extension SHALL be present and SHALL NOT be marked critical. It SHALL contain the HTTP URL of the CA's CRL service.

7.1.3 Algorithm object identifiers

Izenpe SHALL use one of the following signature algorithms and encodings.

ROOT CN	Algorithmidentifier	Encoding
Izenpe.com (2007)	RSASSA-PKCS1-v1_5 with SHA-256	300D06092A864886F70D01010B0500
ROOT CA SSL IZENPE 2024	ecdsaWithSHA384	300A06082A8648CE3D040303

7.1.3.1 SubjectPublicKeyInfo

The following requirements apply to the ***subjectPublicKeyInfo*** field within a Certificate or Precertificate. No other encodings are permitted.

7.1.3.1.1 RSA

IZENPE SHALL indicate an RSA key using the rsaEncryption (OID: 1.2.840.113549.1.1.1) algorithm identifier. The parameters MUST be present, and MUST be an explicit NULL. IZENPE SHALL NOT use a different algorithm, such as the id-RSASSA-PSS (OID: 1.2.840.113549.1.1.10) algorithm identifier, to indicate an RSA key.

When encoded, the ***AlgorithmIdentifier*** for RSA keys MUST be byte-for-byte identical with the following hex-encoded bytes: ***300d06092a864886f70d0101010500***

7.1.3.1.2 ECDSA

The CA SHALL indicate an ECDSA key using the id-ecPublicKey (OID: 1.2.840.10045.2.1) algorithm identifier. The parameters MUST use the ***namedCurve*** encoding.

- For P-256 keys, the ***namedCurve*** MUST be secp256r1 (OID: 1.2.840.10045.3.1.7).
- For P-384 keys, the ***namedCurve*** MUST be secp384r1 (OID: 1.3.132.0.34).
- For P-521 keys, the ***namedCurve*** MUST be secp521r1 (OID: 1.3.132.0.35).

When encoded, the ***AlgorithmIdentifier*** for ECDSA keys MUST be byte-for-byte identical with the following hex-encoded bytes:

- For P-256 keys, 301306072a8648ce3d020106082a8648ce3d030107
- For P-384 keys, 301006072a8648ce3d020106052b81040022
- For P-521 keys, 301006072a8648ce3d020106052b81040023

7.1.3.2 Signature AlgorithmIdentifier

All objects signed by a CA Private Key MUST conform to these requirements on the use of the ***AlgorithmIdentifier*** or ***AlgorithmIdentifier-derived*** type in the context of signatures.

7.1.3.2.1 RSA

IZENPE SHALL use one of the following signature algorithms and encodings. When encoded, the AlgorithmIdentifier MUST be byte-for-byte identical with the specified hex-encoded bytes.

- RSASSA-PKCS1-v1_5 with SHA-256:
  Encoding: 300d06092a864886f70d01010b0500
- RSASSA-PKCS1-v1_5 with SHA-384:
  Encoding: 300d06092a864886f70d01010c0500
- RSASSA-PKCS1-v1_5 with SHA-512:
  Encoding: 300d06092a864886f70d01010d0500
- RSASSA-PSS with SHA-256, MGF-1 with SHA-256, and a salt length of 32 bytes:
  Encoding: 304106092a864886f70d01010a3034a00f300d060960864801650304020l
  0500a11c301a06092a864886f70d010108300d060960864801650304020l 0500a203020120
- RSASSA-PSS with SHA-384, MGF-1 with SHA-384, and a salt length of 48 bytes: Encoding:
  304106092a864886f70d01010a3034a00f300d060960864801650304020202
  0500a11c301a06092a864886f70d010108300d060960864801650304020202 0500a203020130
- RSASSA-PSS with SHA-512, MGF-1 with SHA-512, and a salt length of 64 bytes: Encoding:
  304106092a864886f70d01010a3034a00f300d060960864801650304020203
  0500a11c301a06092a864886f70d010108300d060960864801650304020203 0500a203020140

7.1.3.2.2 ECDSA

IZENPE SHALL use the appropriate signature algorithm and encoding based upon the signing key used.

If the signing key is P-256, the signature MUST use ECDSA with SHA-256. When encoded, the AlgorithmIdentifier MUST be byte-for-byte identical with the following hex-encoded bytes: ***300a06082a8648ce3d040302***.

If the signing key is P-384, the signature MUST use ECDSA with SHA-384. When encoded, the AlgorithmIdentifier MUST be byte-for-byte identical with the following hex-encoded bytes: ***300a06082a8648ce3d040303***.

If the signing key is P-521, the signature MUST use ECDSA with SHA-512. When encoded, the AlgorithmIdentifier MUST be byte-for-byte identical with the following hex-encoded bytes: ***300a06082a8648ce3d040304***.

7.1.4 Name forms

The encoding of the Web Site Authentication Certificates follows the RFC 5280 'Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile' recommendation. All fields defined in the profile of these Certificates, except for fields specifically expressed otherwise, use UTF8String encoding.

7.1.4.1 Name Encoding

For every valid Certification Path (as defined by RFC 5280, Section 6):

- For each Certificate in the Certification Path, the encoded content of the Issuer Distinguished Name field of a Certificate SHALL be byte-for-byte identical with the encoded form of the Subject Distinguished Name field of the Issuing CA certificate.
- For each CA Certificate in the Certification Path, the encoded content of the Subject Distinguished Name field of a Certificate SHALL be byte-for-byte identical among all Certificates whose Subject Distinguished Names can be compared as equal according to RFC 5280, Section 7.1, and including expired and revoked Certificates.

7.1.4.2 Subject Attribute Encoding

No stipulation.

7.1.4.3 Subscriber Certificate Common Name Attribute

No stipulation.

7.1.4.4 Other Subject Attributes

No stipulation.

7.1.5 Name constraints

Sub CAs issuing certificates under this CP/CPS are not technically restricted.

7.1.6 Certificate policy object identifier

The object identifier (OID) of the Website Authentication Certificate policy is the one defined in section '1.2 Document name and identification' of this document.

7.1.7 Usage of Policy Constraints extension

No policy restrictions are used.

7.1.8 Policy qualifiers syntax and semantics

The Certificate Policies extension contains the following policy qualifiers:

- CPS Pointer: contains a pointer to the IZENPE Certification Practice Statement, http://www.lzenpe.com/cps
- Policy Identifier: Indicates the OID of the certificate

7.1.9 Processing semantics for the critical Certificate Policies extension

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

7.2 CRL profile

The certificates issued by IZENPE conform to the following standards:

- 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(s)

Version 2 (populate version field with integer '1').

7.2.2 CRL and CRL entry extensions

The extensions used are as follows:

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

The CRLReason unspecified (0) MUST NOT be used for revoked CA certificates included in Authority Revocation Lists (ARLs). A specific and appropriate revocation reason MUST be assigned to each revoked CA certificate listed in an ARL.

7.3 OCSP profile

Izenpe OCSP responses are compliant with RFC 6960 (X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP) and are signed by the OCSP Responder whose certificate has been signed by the same CA with which the certificate being queried was issued.

7.3.1 Version number(s)

7.3.2 OCSP extensions

Field	Mandatory	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. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The system for issuing website authentication certificates is audited annually in accordance with,

- European standards ETSI EN 319 401 'General Policy Requirements for Trust Service Providers' and ETSI EN 319 411-1 'Policy and security requirements for Trust Service Providers issuing certificates'.
- ETSI EN 319 411-2 'Requirements for trust service providers issuing EU qualified certificates'.

In addition, the certificate issuing system is subject to the following audits,

- Audit of the Information Security Management System in accordance with UNE-ISO/IEC 27001 'Information Security Management Systems (ISMS) Requirements'.
- Audit in accordance with the National Security Scheme (Royal Decree 3/2010, of 8 January, which regulates the National Security Scheme in the field of e-Government).
- Audit in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC, and Organic Law 3/2018, of 5 December, on the Protection of Personal Data and guarantee of digital rights (RGPD/LOPD-GDD).

Risk analyses are also carried out, in accordance with the provisions of the Information Security Management System.

8.1 Frequency or circumstances of assessment

In the case of certificates considered as qualified, the audit additionally guarantees compliance with the requirements of the European standards ETSI EN 319 411-2 'Requirements for trust service providers issuing EU qualified certificates' and ETSI EN 319 412-4 'Certificate profile for web site certificates'.

The frequency of the remaining additional audits shall be in accordance with the stipulations of the corresponding regulations in force.

8.2 Identity/qualifications of assessor

Auditors are qualified and have demonstrated proficiency in auditing secure systems of production, especially digital certification systems. The auditor must be accredited as per ETSI EN 319 403.

8.3 Assessor's relationship to assessed entity

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

8.4 Topics covered by assessment

The compliance audit will cover the following topics:

- PKI processes,
- Information systems.
- Protection of the data processing centre.
- Documents.

Details on how each of these topics is audited are provided in the IZENPE Auditing Plan.

8.5 Actions taken as a result of deficiency

Security incidents are managed by the Izenpe Security Committee.

Izenpe will open an investigation within a maximum of 24 hours of receipt, and will decide on the action to be taken, considering the criteria in section 4.9.5 of the BRs.

In addition, Izenpe reports cases that it considers to be incidents (cases of fraud, phishing, etc.) on the Anti-PhisingWorkGroup website (www.apwg.org) and verifies prior to issuance that the applicant or representatives do not appear in Izenpe's internal database of security incidents.

In any case, it reserves the right to issue certificates in suspicious situations.

8.6 Communication of results

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

8.7 Self-Audits

IZENPE shall monitor adherence to this CP/CPS and control its service quality by performing self-audits on at least a quarterly basis against a randomly selected sample of the greater of one certificate or at least three percent (3%) of the Publicly Trusted Certificates issued for SSL/TLS, including EV Certificates.

IZENPE SHALL complete and submit an annual self-assessment to the CCADB covering requirements of at least version of the following:

- CCADB Policy.
- Chrome Root Program Policy.
- Mozilla Root Store Policy.
- Network and Certificate System Security Requirements.
- Baseline Requirements for Publicly-Trusted TLS Certificates.
- Extended Validation Guidelines for Publicly-Trusted TLS Certificates.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

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

9.1.1 Certificate issuance or renewal fees

The determination of fees applicable to the issue or renewal of certificates shall follow the provisions of section '9.1 Fees' of this document.

9.1.2 Certificate access fees

Not stipulated.

9.1.3 Revocation or status information access fees

Izenpe offers certificate status information services via CRL and OCSP protocol free of charge.

9.1.4 Fees for other services

The rates applicable to other services are approved annually by the Board of Directors of Izenpe.

9.1.5 Refund policy

Izenpe does not have a refund policy.

9.2 Financial responsibility

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

9.2.1 Insurance coverage

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.

9.2.2 Other assets

Not stipulated.

9.2.3 Insurance or warranty coverage for end-entities

Not stipulated.

9.3 Confidentiality of business information

9.3.1 Scope of 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's 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.

9.3.2 Information not within the scope of confidential information

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.
- The name and surname of the certificate subscriber, in the case of certificates in which the subscriber and signer is a natural person, or of the signers, in the case ofcertificates in which the subscriber is a legal person or administrative body, as well as any other circumstance or personal data of the holder, in the event that it is significant based on the purpose of the certificate.
- If included, the email address of the certificate subscriber in the case of certificates whose subscriber and signatory 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 expiry 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.

9.3.3 Responsibility to protect 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.

The certificates shall be published in accordance with the provisions of the eIDAS1 and eIDAS2 Regulation and Law 6/2020, of 11 November, regulating certain aspects of electronic trust services.

9.4 Privacy of personal information

Izenpe publishes its Processing Activity Recording and other information on personal data so that interested parties may view it at the following website: www.izenpe.eus/datos.

9.4.1 Privacy plan

Izenpe's personal data processing is aligned with provisions in EU Regulation 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and their free circulation and which repeals Directive 95/46/EC (General Data Protection Regulation, hereinafter, GDPR), as well as requirements applicable due to specific national regulations in this regard.

9.4.2 Information treated as private

Izenpe considers personal information on all individuals using the Trusted Services that must not be incorporated into certificates and the mechanisms using the Information and Certificate Validity Status Consultation Service as private.

In any event, all personal information collected during request, renewal and revocation processes for electronic certificates (with the exception set forth in the section below), the Private Keys in the possession of the Trusted Service Provider and all information clearly identified as private, are considered private.

Izenpe applies suitable safeguards to protect private information.

9.4.3 Information not deemed private

Information incorporated into electronic certificates, information on the validity status of certificates, the start date of said status (active, revoked, expired, etc.), as well as the reason behind the change in status is not considered private information. Therefore, electronic certificates, lists of revoked certificates and all of their content is not deemed private information.

9.4.4 Responsibility to protect private information

Izenpe adopts the security measures required by the GDPR regarding access and processing for Certificate applicant and subscribers' personal data.

The technical and organisational measures shall be established considering the cost of the technique, costs of application, as well as the nature, scope, context and purposes of processing and the risks to rights and liberties.

9.4.5 Notice and consent to use private information

Obtaining private information from natural persons during processes related to the life cycle of the Certificates (request, identity accreditation, renewal, revocation, etc.) shall always be subject to unequivocal consent from said individuals, meaning a statement from the interested party or by means of a clear affirmative action.

9.4.6 Disclosure pursuant to judicial or administrative process

Izenpe shall not share personal data, barring a request from administrative or legal authorities.

9.4.7 Other information disclosure circumstances

Not stipulated.

9.5 Intellectual property rights

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.

Property rights in certification practice

IZENPE retains all property rights to this Certification Practice Statement.

Property rights in names

The subscriber, and where applicable the key owner, retains all rights (if any), to 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.

Property rights in keys and key material

Key pairs are the property of certificate subscribers.

9.6 Representations and warranties

9.6.1 CA representations and warranties

The obligations and responsibilities of Izenpe, as a Trusted Service Provider, with the certificate subscriber and, where applicable, with user parties and relying third parties, will be determined in the document relating to the conditions of use or the contract for issuing the certificate, and, alternatively, by this Declaration of Certification Practices and Policies.

Izenpe complies with the requirements of the technical specifications of the ETSI EN 319 411 standard for the issue of certificates and undertakes to continue to comply with this standard or those that replace it.

Izenpe issues website authentication certificates in accordance with the 'Basic requirements for the issuance and management of trusted certificates,' requirements established by the CA/Browser Forum, which can be consulted at https://cabforum.org/. It will also adapt its certificate issuance practices to the current version of these requirements.

In the event of any inconsistency with this Policy, said requirements shall prevail over this document.

In addition, Izenpe undertakes to comply, in relation to the issue of qualified certificates, with the requirements established by the CA/Browser Forum entity for this type of Certificates (EV SSL Certificate Guidelines), which can be consulted at the following address https://cabforum.org/extended-validation/. In the event of any inconsistency with this Policy, such requirements shall prevail over this document.

Notwithstanding the provisions of the regulations applicable to this type of certificate, as well as the obligations described in the corresponding section of the CPS, the Trusted Service Provider undertakes, prior to issuing the certificate, to:

- Check the identity and personal circumstances of the certificate applicant and the subscriber and/or its Representative and collect the statement that the applicant is authorised by the subscriber to make the application.
- In the registration process, check the data relating to the subscriber's legal personality and the Representative's capacity. All these checks shall be conducted in accordance with the provisions of this document and Izenpe's registration protocols and procedures.
- In the aforementioned verification processes, Izenpe may conduct verifications through the intervention of third parties with notarial powers or competent Registries.
- Verify that all the information contained in the certificate application corresponds to that provided by the applicant.
- Check that the applicant is in possession of the Private Key associated with the Public Key that is included in the certificate to be issued.
- Guarantee that the procedures followed ensure that the Private Keys corresponding to the website authentication certificates are generated without copies being made or stored by Izenpe.
- Communicate information to the subscriber, representative and applicant in such a way as to guarantee their confidentiality.
- Make available to the applicant, subscriber, Representative and other interested parties (Izenpe's Certification Practices Statement and any other relevant information for the development of the procedures related to the life cycle of the certificates covered by this Certification Policy in accordance with the applicable regulations.

9.6.2 RA representations and warranties

The activities related to the RA will be conducted exclusively by Izenpe for all website authentication certificates.

The RA has the following obligations:

- In general, to follow the procedures established by Izenpe in the Certification Policy and Practices applicable to the performance of its Certificate management, issuance, and revocation functions and not to alter this framework.
- In particular, verify the identity, and any relevant personal circumstances for the determined purpose, of the certificate applicants, subscribers, and their Representatives, by any means permitted by law and in accordance with the general provisions of this Policy.
- Check that the ownership of the domain name corresponds to the identity of the Subscriber or, if applicable, obtain the Subscriber's authorisation, which shall be associated with the
- Website Authentication Certificate, by the means at its disposal that allow such ownership to be accredited, in accordance with the state of the art.
- Expressly state the subscriber's power of decision regarding the ownership of the domain of the website authentication certificate.
- Keep all the information and documentation relating to the certificates whose application, renewal, or revocation it manages for 15 years.
- Receive and manage applications via the application management application published at www.izenpe.eus.
- Diligently check the causes of revocation that may affect the validity of the certificates.

9.6.3 Subscriber representations and warranties

For website authentication certificates, Subscribers must have control of the website domain name included in such Certificates and keep the associated Private Keys under their exclusive use. The applicant and the Subscriber of Certificates issued under this CP are obliged to:

- Not use the certificate outside the limits specified in this particular Certification Policy and Practices.
- Not use the certificate in the event that the Trusted Service Provider has ceased its activity as the Certificate Authority that issued the certificate in question, especially in cases where the provider's Seal Creation Data may have been compromised, and this has been communicated.
- Provide truthful information when applying for Certificates and keep it updated, subscribing the contracts by a person with sufficient capacity.
- Not request for the Subject of the certificate distinctive signs, names or industrial or intellectual property rights of which it is not the owner, licensee or has demonstrable authorisation for their use.
- Act with diligence with regard to the custody and conservation of the Signature/Seal creation Data or any other sensitive information such as Keys, Certificate activation codes, access words, personal identification numbers, etc., as well as the Certificate media, which includes, in any case, not disclosing any of the aforementioned data.
- Be aware of and comply with the conditions of use of the Certificates foreseen in the conditions of use and in the Declaration of Certification Practices and, in particular, the limitations of use of the Certificates.
- Be aware of and comply with the modifications made to the Certification Practice Statement.
- Request the revocation of the corresponding Certificate, according to the procedure described in this document, diligently notifying Izenpe of the circumstances for the revocation or suspicion of loss of Confidentiality, disclosure, modification, or unauthorised use of the associated private Keys,
- Review the information contained in the Certificate and notify Izenpe of any errors or inaccuracies.
- Verify, prior to trusting the Certificates, the advanced electronic Signature or electronic Seal of the Trust Service Provider issuing the Certificate.
- Diligently notify Izenpe of any modification to the data provided in the application for the Certificate, requesting, when appropriate, the revocation of the same.

The Subscriber shall be responsible for the proper use and diligent custody of the Certificate, according to the purpose and function for which it has been issued, as well as for informing Izenpe of any change in the status or information with respect to what is reflected in the Certificate, for its revocation and reissuance.

Likewise, the Subscriber shall be liable, in all cases, to Izenpe, the User Entities and, where applicable, to third parties, for improper use of the Certificate, or for falsehoods or errors in the statements contained therein or acts or omissions that cause damage or harm to Izenpe or third parties.

It shall be the Subscriber's responsibility and, therefore, obligation not to use the Certificate in the event that the Trusted Service Provider has ceased its activity as the Certificate Issuer that issued the Certificate in question and the subrogation provided for by law has not taken place. In any case, the Subscriber shall not use the Certificate in cases in which the Provider's Signature Creation Data may be threatened and/or compromised, and this has been communicated by the Provider or, where applicable, the Subscriber has become aware of these circumstances.

The relationship between Izenpe and the Subscriber will be determined for the purposes of the regime of use of the Certificates, through the document relating to the conditions of use or, where applicable, the contract of issue of the Certificate and in accordance with the agreements, conventions, or relationship document between Izenpe and the corresponding Entity.

9.6.4 Relying party representations and warranties

The certificate verification user undertakes to:

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

9.6.5 Representations and warranties of other participants

Not stipulated.

9.7 Disclaimers of warranties

Not stipulated.

9.8 Limitations of liability

Certification Authority liabilities

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.
- IZENPE shall not be liable for any direct, indirect, special, incidental, consequential damages, lost profits, loss of data, punitive damages, whether foreseeable or not, arising in connection with the use, delivery, licencing, operation or non-operation of the Certificates, digital signatures, or any other transaction or service offered or contemplated in the Certification Practices Statement in case of 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.

IZENPE shall be held liable for harm and damage caused to any individual, due to a lack of or delay in inclusion in the consulting service for the validity of certificates or expiry of certificate validity.

Furthermore, it shall be held liable to third parties for actions of individuals to whom it has delegated the roles necessary to provide certification services. In this regard, a civil liability insurance policy has been taken out to cover the risk of liability for harm and damage that may arise in using the certificates.

Registration authority liabilities

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

When the identification functions are carried out by the Public Administrations that subscribe to the certificates, the patrimonial responsibility of the Public Administrations will apply, as established by the Law on the Legal Regime of Public Administrations and the Common Administrative Procedure.

Subscriber liabilities

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 or revocation thereof, when inaccuracies in the information have not been detected by the service provider.
- Promptly notify IZENPE or the Registration Authority of any changes in the information submitted for the certificate.
- Diligently save signature creation data in order to ensure confidentiality and protect the data from any access or revelation.
- Apply for certificate revocation if there is any doubt regarding maintaining the confidentiality of signature creation data.
- Abstain from using the signature creation data from the time the certificate's validity period expires, or the service provider notifies that it is no longer valid.
- Follow the limits on the certificate regarding its possible uses, and using it as per the established conditions communicated to the certification services signatory.

Relying third party liability

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

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

- Verifying and bearing in mind the restrictions on the certificate regarding its possible uses and the itemised amount of transactions that can be made with it.
- Ensuring the validity of the certificate.
- Check the digital identifier of the qualified certificate in the Trusted Service List (TSL).

9.9 Indemnities

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

9.9.1 Indemnification of the CA

Not stipulated.

9.9.2 Indemnification of Subscribers

Not stipulated.

9.9.3 Indemnification of the relying parties

Not stipulated.

9.10 Term and termination

9.10.1 Term

This Certification Policy shall enter into force at the time of its publication.

9.10.2 Termination

This Certification Policy shall be repealed when a new version of the document is published.

The new version will replace the previous document in its entirety. Izenpe undertakes to subject this Policy to an annual review process.

9.10.3 Effect of termination and survival

For current certificates issued under this Certification Policy, the new version shall prevail over the previous version in all that does not conflict with it.

9.11 Individual notices and communications with participants

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

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

9.12 Amendments

9.12.1 Procedure for amendment

Modifications to this Certification Policy shall be approved by the Izenpe Security Committee, which shall be reflected in the corresponding minutes, in accordance with the approved internal procedure.

9.12.2 Notification mechanism and period

Any modification to this Certification Policy will be published immediately on the URL of access to the same.

If the modifications to be made do not entail significant changes in terms of the system of obligations and responsibilities of the parties or relating to a modification of the policies for the provision of services, Izenpe will not inform users in advance, but will simply publish a new version of the affected statement on its website.

9.12.3 Circumstances under which OID must be changed

Significant modifications to the conditions of services, regime of obligations and responsibilities or limitations of use may lead to a change in the service policy and its identification (OID), as well as the link to the new service policy statement. In this case, Izenpe may establish a mechanism for informing of the proposed changes and, where appropriate, for collecting the opinions of the parties concerned.

9.13 Dispute resolution provisions

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

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

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

9.14 Governing law

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

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

- Law 6/2020, of 11 November, regulating certain aspects of electronic trust services.
- Regulation 910/2014 on electronic identification and trust services for electronic transactions on the domestic market, repealing Directive 1999/93/EC.
- Regulation 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation 910/2014 as regards the establishment of the European digital identity framework.
- Public Administration Common Administrative Procedural Law 39/2015.
- Public Sector Legal Scheme Law 40-2015.
- Organic Law 3/2018 of 5 December on Personal Data Protection and guarantee of digital rights.
- (EU) Regulation 2016/679 on the protection of natural persons regarding personal data processing and the free circulation of these data, repealing Directive 95/46/EC (GDPR).

Additionally, the practice for trust services intended by Izenpe follow these standards:

- ETSI EN 319 401: General Policy Requirements for Trust Service Providers.
- General Statement of Trust Service and Electronic Certification Practices Version 5.7.
- ETSI EN 319 411-1: Policy and security requirements for Trust Service Providers issuing certificates. General requirements.
- ETSI EN 319 411-2: Requirements for trust service providers issuing EU qualified certificates.
- ETSI EN 319 412: Electronic Signatures and Infrastructures (ESI); Certificate Profiles.
- ETSI EN 319 421: Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
- ETSI EN 319 422: Time-stamping protocol and time-stamp token profiles.
- CABForum Baseline Requirements.
- CABForum EV Certificate Guidelines.

9.15 Compliance with applicable law

Izenpe declares its commitment to comply with the regulations and requirements applicable to each type of Website Authentication Certificate, including the considerations set out in section ‘1.5.4. CPS approval procedure’ of this CP document.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

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.

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.

9.16.2 Assignment

Izenpe shall not be held liable for lack of service of anomalies therein, nor for damages and harm that may be directly or indirectly caused when the failure or disaster is caused by force majeure, terrorist attack, sabotage or wildcat strikes; all this notwithstanding conducting the actions necessary to remedy and/or re-initiate the service as quickly as possible.

9.16.3 Severability

Not stipulated.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Not stipulated.

9.16.5 Force Majeure

Not stipulated.

9.17 Other provisions

No stipulation