CERTIFICATE POLICY

SSL / TLS

October 2020

Version 1.8

TABLE OF CONTENTS

1. Introduction

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

Its purpose is to detail and complete what is generically defined in *Izenpe's Certification Practises Statement*, in the specific documents in the *CA/Browser Forum Baseline Requirements (hereinafter, BR) and EV guidelines (hereinafter, EVBR)* for issuing website certificates and in ETSI specifications (www.etsi.org). Izenpe follows the latest published version of said regulations.

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

- DVCP (Domain Validation Certificates Policy): for "SSL DV" certificates
- OVCP (Organizational Validation Certificates Policy): for "SSL OV" certificates
- EVCP (Extended Validation Certificates Policy): for "Office EV," "SSL EV," "SSL Qualified," and "Qualified Office" certificates

Within the scope of the Google Certificate Transparency project, all SSL certificates issued will be published on the log server providers' log service, with whom Izenpe has signed an agreement.

Izenpe holds testing websites so that software providers can test their products with SSL/TLS certificates in a production setting. Izenpe holds different websites with at least one final living, expired and revoked certificate:

- https://test-ev-qualified.izenpe.eus/
- https://test-expired-ev.izenpe.eus/
- https://test-revoked-ev.izenpe.eus/

Regarding the type of certificate that Izenpe issues,

SSL	ELECTRONIC OFFICE
SSL DV SSL OV SSL Qualified	Qualified Office

Depending on the validation made by Izenpe, the certificate may be,

- *SSL DOMAIN VALIDATED (**SSL DV**),*

  This certificate, deemed as non-qualified, will be used to identify the ownership of the domain hosting the website, providing a reasonable guarantee to the user of an Internet browser.

  These certificates may be valid for 1 or 2 years.

- *SSL ORGANISATION VALIDATED (**SSL OV**),*

This certificate, deemed as non-qualified, will be used to identify ownership of the domain and accreditation of the organisation, providing a reasonable guarantee to the user of an Internet browser that the website they are visiting is owned by the organisation identified in the certificate.

These certificates may be valid for 1 or 2 years.

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

  This certificate, deemed as non-qualified, will be used to identify ownership of the domain and accreditation of the organisation, providing a robust guarantee to the user of an Internet browser that the website they are visiting is owned by the organisation identified in the certificate.

  These certificates may be valid for 1 or 2 years.

  Izenpe currently does not issue this kind of certificate.

- *SSL QUALIFIED (**SSL QUALIFIED**),*

  This certificate is deemed qualified pursuant to (EU) REGULATION 910/2014 OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions on the domestic market, repealing Directive 1999/93/EC . It will be used to identify ownership of the domain and accreditation of the organisation, providing a robust guarantee to the user of an Internet browser that the website they are visiting is owned by the organisation identified in the certificate.

  These certificates may be valid for 1 or 2 years.

– *ELECTRONIC OFFICE CERTIFICATES*

Under *Spanish Law 40/2015 dated 1 October, on the Legal System for the Public Sector,* Izenpe issues the following certificates*:*

- ***ELECTRONIC OFFICE WITH EXTENDED VALIDATION EV (EV Office),***

  In addition to the characteristics defined in the *Electronic Office* certificate, extended validation's (EV) purpose is to provide a better level of authentication for the Public Administration, body or administrative entity, thanks to more exhaustive validation.

  According to the assurance levels defined in the *Identification and electronic signature system*, the *Electronic Office* certificate issued by Izenpe has a medium level.

  These certificates are valid for 2 years.

  Izenpe currently does not issue this kind of certificate.

- ***QUALIFIED ELECTRONIC OFFICE (QUALIFIED OFFICE),***

  This certificate is deemed qualified pursuant to (EU) REGULATION 910/2014 OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions on the domestic market, repealing Directive 1999/93/EC .

The extended validation's (EV) purpose is to provide a better level of authentication for the Public Administration, body or administrative entity, thanks to more exhaustive validation.

According to the assurance levels defined in the *Identification and electronic signature system*, the *Electronic Office* certificate issued by Izenpe has a medium level.

These certificates are valid for 2 years.

1.1. Purpose

The purpose of this document is to inform the public of the conditions and characteristics of trust services intended for users of website authentication Certificates from Izenpe, acting as Trusted Service Provider, specifically setting forth the obligations it undertakes to fulfil in relation to:

- management of said Certificates, the conditions applicable to the request, issue, use and expiry of validity of the certificates, and
- provision of the Certificate validity status consultation service, as well as the conditions applicable to use of the service and guarantees offered.

Moreover, this document also sets forth, either directly or by means of references to Izenpe's Certification Practises Statement (hereinafter, the CPS), under which this Statement falls, details on the liability system applicable to the users and/or parties who trust in the services mentioned in the paragraph above, security controls applied to procedures and facilities regarding what may be published, notwithstanding their efficacy, and secrecy and confidentiality standards, as well as issues bearing on ownership of goods and assets, personal data protection and other matters of an informational nature deemed of public interest.

These Certification Policies (hereinafter, CP) are part of the CPS. If there is a contradiction between this document and the CPS, this document shall prevail.

1.2. Name of document and identification

This document is called "Certification Policies and Practises Statement for website authentication certificates."

- Version: 1.8
- Date of issue: 01/10/2020
- Location: http://www.izenpe.eus/s15-content/es/contenidos/informacion/doc_especifica/es_def/index.shtml
- Related CPS: Izenpe's Certification Practises Statement
- Location: http://www.izenpe.eus/cps

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

CERTIFICATE	POLICY OID

SSL DV	1.3.6.1.4.1.14777.1.2.4
SSL OV	1.3.6.1.4.1.14777.1.2.1
SSL EV [1]	1.3.6.1.4.1.14777.6.1.1
SSL Qualified	1.3.6.1.4.1.14777.6.1.3
EV office[2]	1.3.6.1.4.1.14777.6.1.2
Qualified Office	1.3.6.1.4.1.14777.6.1.4

1.3. Intervening parties

The parties intervening in the management and use of the Trust Services described in this CP are:

1. Certification Authority
2. Registration Authority
3. Certificate Subscribers or Owners
4. Trusting parties
5. Other participants

1.3.1. Certification Authority

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

Type	CN	Print SHA1
Root	Izenpe.com	2f783d255218a74a653971b52ca29c45156fe919
Subordinate	EAEko Herri Administrazioen CA - Basque PA CA (2)	f79cda11e7917419a0418db84ba743c5313ad7f0
Subordinate	CA of EV SSL Certificates	6c484d0f4db295ec67ebb3e05e3dc214492a9ab8
Subordinate	CA of EV SSL Certificates	c68bade5f069778a003074e619dab2e7928342d5

ROOT CERTIFICATION AUTHORITY

This is the Certification Authority that issues certificates for subordinate Certification Authorities.

CA ROOT

[1]Although Izenpe no longer issues this type of certificate, it is maintained until the ones in force expire

[2]Although Izenpe no longer issues this type of certificate, it is maintained until the ones in force expire

Field/extension	Content
version	Version 3
serialNumber	00b0b75a16485fbfe1cbf58bd719e67d
signature	sha256WithRSAEncryption
issuer	
CN	Izenpe.com
O	IZENPE S.A.
C	ES
validity	30 years
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 (Spain)
O	IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
subjectKeyIdentifier	1d1c650ea8f2257bb491cfe4b1b1e6bd55746c05
keyUsage	Certificate signature, CRL signature without connection, Signature list of certificate revocation (CRL) (06)

SUBORDINATE CERTIFICATION AUTHORITY

EAEko Herri Administrazioen CA - Basque PA CA (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	
CN	EAEko Herri Administrazioen CA - Basque PA CA (2)
OU	AZZ Ziurtagiri publikoa - ACS Public certificate
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 (Spain)
O	IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
subjectKeyIdentifier	c0a94af7472587ffbcb5a689ce82d246a889eba3
authorityKeyIdentifier	Key ID=1d1c650ea8f2257bb491cfe4b1b1e6bd55746c05
certificatePolicies	
policyIdentifier	All issuance guidelines
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 signature, CRL signature without connection, Signature list of certificate revocation (CRL) (06)
Digital fingerprint	f79cda11e7917419a0418db84ba743c5313ad7f0

CA of SSL EV Certificates 2010	
Field/extension	**Content**
version	Version 3
serialNumber	6d71e25b7bb6b6364cbea848e3a4a981
signature	sha256WithRSAEncryption
issuer	
CN	Izenpe.com
O	IZENPE S.A.
C	ES
validity	20 October 2020
subject	
CN	CA of EV SSL Certificates
OU	Ziurtagiri publikoa - EV Public certificate
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 (Spain)
O	IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
subjectKeyIdentifier	a6ce69692ea621353b3acf0af12e3f15ac199027
authorityKeyIdentifier	Key ID=1d1c650ea8f2257bb491cfe4b1b1e6bd55746c05
certificatePolicies	
policyIdentifier	All issuance guidelines
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 signature, CRL signature without connection, Signature list of certificate revocation (CRL) (06)
Digital fingerprint	6c484d0f4db295ec67ebb3e05e3dc214492a9ab8

CA of SSL EV Certificates 2018	
Field/extension	**Content**
version	Version 3
serialNumber	687db7171744da235b3f625a7393f8a5
signature	sha256WithRSAEncryption
issuer	
CN	Izenpe.com
O	IZENPE S.A.
C	ES
validity	6 July 2028
subject	
CN	CA of EV SSL Certificates
OU	Ziurtagiri publikoa - EV Public certificate
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 (Spain)
O	IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8

subjectKeyIdentifier	c6edfe77fb51564dfcabd5e3b10c13a3bf54e39b
authorityKeyIdentifier	Key ID=1d1c650ea8f2257bb491cfe4b1b1e6bd55746c05
certificatePolicies	
policyIdentifier	All issuance guidelines
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 signature, CRL signature without connection, Signature list of certificate revocation (CRL) (06)
Digital fingerprint	c68bade5f069778a003074e619dab2e7928342d5

1.3.2. Registration Authority

Izenpe is the only Registration Authority that acts in the issue process for this type of Certificate. It conducts identification and verification tasks with the main objective of guaranteeing that the Certificate is issued to the Subscriber who holds control over the domain name incorporated into the Certificate. None of the verifications of identity of domain control are delegated to third parties.

1.3.3. Certificate Subscribers

Subscribers are legal persons to whom this type of Certificate are issued and who are legally bound by an agreement describing the terms of use for the Certificate.

For electronic office certificates, the Subscriber is the public administration, body, public body or public entity that holds control over the domain name of the electronic office.

1.3.4. Trusting parties

Trusting parties are Internet users who establish connections to websites through the use of TLS/SSL protocols incorporated into this kind of Certificate and decide to trust in them.

1.3.5. Other participants

Not stipulated.

1.4. Use of the certificates

1.4.1. Permitted certificate uses

Website authentication certificates authenticate a website and bind the website to the natural or legal person to whom the certificate was issued.

Additionally, qualified office certificates are a sub-set of website authentication certificates issued as electronic office identification systems that guarantee secure communication with it, pursuant to the terms defined in Law 40/2015 of 1 October, on the Legal System for the Public Sector and Law 18/2011 of 5 July, regulating the use of information and communication technologies in the Justice Administration.

All website authentication Certificates with Extended Validation (EV) policies issued under this Certification Policy are Qualified Certificates pursuant to EU Regulation 910/2014 of the European Parliament and the Council of 23 July 2014 on electronic identification and trust services for electronic transactions on the domestic market, repealing Directive 1999/93 (eIDAS regulation) and pursuant to requirements established in 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. Restrictions to the use of certificates

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

Furthermore, the certificates must only be used according to governing laws.

The certificates were not designed, nor can they be used, nor are they authorised to be used, or resold, as control equipment for dangerous situations, or for uses requiring fail-safe actions, such as operation of nuclear facilities, navigation systems or aerial communications, or armament control systems, where a failure could directly lead to death, personal harm or severe environmental damage.

If a user entity or third party wish to trust in these Certificates without accessing the Information and Consultation Service to view the validity status of the certificates issued under this Certification Policy, these Particular Policies and Certification Practises shall not provide coverage and there shall be no legal basis to claim or file legal action against Izenpe for damages, harm or conflicts stemming from the use of, or trust in, a Certificate.

Izenpe prohibits the use of Certificates issued under this CP for illegal interception or man-in-the-middle attacks (MITM), deep package inspection (DPI), etc.

1.5. Policy Administration

1.5.1. Responsible entity

IZENPE, with corporate headquarters at Avenida Mediterráneo 14 Vitoria-Gasteiz (Spain) and Tax ID Number A-01337260, is the Certification Authority that issues the certificates to which this Certification Practises Statement is applicable.

1.5.2. Contact information

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

To report security issues, such as suspicion of compromised keys, improper use of certificates, revocation requests, fraud or other issues, write to **incidencias@izenpe.eus**

1.5.3. Parties responsible for CPS adaptation

The IZENPE Security Committee is the body in charge of approving this CP and any possible changes to it.

1.5.4. CPS approval procedure

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

Izenpe manages its certification services and issues compliance certificates with the latest version of "Base requirements for the issue and management of trust certificates," requirements established by the CA entity/Browser forum that may be viewed at https://cabforum.org/baseline-requirements-documents/

Izenpe shall review its certification policies and practises and shall annually update this CP to keep it in line with the latest version of the aforementioned requirements, increasing the version number and adding an entry to record the changes with the date, even if no other changes are made to the document.

Updates, both for the CP and the for the CPS, are made available to the parties, with new versions published at www.izenpe.eus

1.6. Definitions and Acronyms

1.6.1. Definitions

- *Website authentication certificate*: This is a certificate to authenticate a website and bind the website to the natural or legal person to whom the certificate was issued.
- *Electronic office certificate*: EV certificate identifying an electronic office, guaranteeing secure communication with it under the terms set forth in Law 40/2015 of 1 October on the Legal System for the Public Sector.
- *EV Certificate*: Certificate of website authentication that contains validated information on its holder, pursuant to the exhaustive validation procedure in accordance with requirements from the "Guide for issue and management of Extended Validation Certificates" established by the CA entity/Browser forum that may be viewed at https://cabforum.org/extended-validation/
- *OV Certificate:* Website authentication certificate issued according to the organisation validation policy (OVCP), reasonably guaranteeing the Internet browser user that the holder of the website they are accessing matches the organisation identified by the OV Certificate. This Certificate complies with standard European requirements ETSI EN 319 411-1 “Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements."
- *Wildcard OV Certificate*: OV Certificate that incorporates an unlimited set of sub-domains, beginning at third level, with one unique website authentication certificate.
- *Certificate Transparency (CT):* this is an open framework for supervision of website authentication certificates, such that when one of these certificates is issued, it is published in CT registers, thus making it possible for domain owners to supervise issue of said certificates for their domains and to detect erroneously issued certificates.

- *Certification Practise Statement (CPS)*: Statement that Izenpe makes available to the public in an easily accessible fashion, electronically and free of cost. This is a security document which details, within the framework of eIDAS, the obligations that Trust Service Providers pledge to undertake with regard to the management of signature creation and verification data and of electronic certificates; conditions applicable to the request for and issuance, use and expiry of certificates; technical and organizational security measures; profiles and information mechanisms on certificate validity.
- *Certificate policy*: Particular CPS applicable to the issue of a determined set of certificates issued by Izenpe under the particular conditions set forth in said Statement and to which the Particular Policies defined therein are applicable.
- *Incident report with a certificate*: complaint of suspicion of a compromised key, improper certificate use or other types of fraud, compromise, improper use or inappropriate behaviour related to certificates.
- *Supervising Entity*: entity appointed by a Member State as responsible for supervision duties in provision of trust services, pursuant to article 17 of the eIDAS Regulation. In Spain, this is currently the Ministry of Energy, Tourism and Digital Agenda.
- *CAA Records:* Record of DNS resources (Domain Names System) for Certification Authority Authorisation (CAA). This allows a DNS domain name holder to specify the Certification Authorities (CA) authorised to issue certificates for that domain. The publication of CAA resource registers allows a domain name holder to implement additional controls to reduce the risk of unauthorised issue of a website authentication certificate for their domain name.
- *Subscriber Representative*: this is the legal representative natural person, or person authorised by them, for the website authentication Certificate Subscriber organisation, to request and use said Certificate.
- *Electronic office*: Electronic address available to citizens through telecommunications networks that is owned by a Public Administration or one or several public bodies or entities of Public Law in conducting their competencies.
- *Subscriber*: Legal person, body or public entity that is recipient of Izenpe's activities as Trust Service Provider, subscribing to the terms and conditions of the service. Under these Certification Policies, said service consists of issuing the website authentication certificates. The Subscriber is referenced in the Certificate's Subject field and is holder and responsible for its use and holds exclusive control and decision-making capacity over it.

1.6.2. Acronyms

For the purposes of provisions in this CP, the following acronyms are applicable. Their meaning matches the European standard ETSI EN 319 411 “Policy and security requirements for Trust Service Providers issuing certificates:”

CA: Certification Authority.
RA: Registration Authority.
ARL: Certification Authority Revocation List.
CN: Common Name.
CRL: List of revoked certificates.
DN: Distinguished Name.
CPS: Certification Practise Statement.

eIDAS: European Parliament and Council Regulation (EU) Num. 910/2014 dated 23 July 2014, on electronic identification and trust services for electronic transactions on the domestic market, repealing Directive 1999/93/EC.
EV: Extended Validation.
ETSI: European Telecommunications Standards Institute.
HSM: Hardware Security Module This is a security device that generates and protects cryptographic keys.
OCSP: Internet protocol used to obtain the status of an online certificate (Online Certificate Status Protocol).
OID Object Identifier.
OV: Organisational Validation.
PDS: PKI Disclosure Statement.
PIN: Personal Identification Number.
PKCS: Public Key Cryptography Standards developed by RSA laboratories.
TLS/SSL: Protocols that encrypt data and authenticate between applications and servers (Transport Layer Security/Secure Socket Layer protocol).
UTC: Coordinated Universal Time.

2. Publication and repositories

2.1. Repository

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

2.2. Publishing certificate information

Information on the issue of electronic certificates referenced in this CP, accessible through www.izenpe.eus, includes the following:

- ✓ Statements of certification practises and policies.
- ✓ Certificate profiles and revocation lists.
- ✓ PKI informative statements (PDS).
- ✓ Terms and conditions for use of the certificates as a binding legal instrument.
- ✓ Download of root certificates and Izenpe's subordinate CAs, as well as additional information.

2.3. Frequency of Publication

Izenpe shall review its certification policies and practises and shall annually update this CP, following the guidelines set forth in section “1.5.4. CPS approval procedure" of this document.
Any modification to the CPS or the CP shall be immediately published on the URL to access them.
Regarding CRL publication frequency, this is defined in section "4.9.7 Frequency of CRL generation" in the CPS.

2.4. Controlling access to repositories

IZENPE allows access to reading the information published in its repository and controls are put in place to prevent unauthorised individuals from adding, changing or deleting the registers provided by this service to protect the integrity and authenticity of the documents.
IZENPE uses reliable systems to access the information repository, so that:

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

3. Identification and authentication

3.1. Designation

Certificate encoding follows standard RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”. All fields defined in the certificate profile in the CPS and CP, except for fields where expressly stated otherwise, use UTF8String encoding.

Additionally, for qualified SSL certificates, Izenpe shall comply with requirements set forth in section 9.2 of CABForum in the "guide for issue and management of Extended Validation Certificates" that may be viewed at https://cabforum.org/extended-validation/

Izenpe does not consider that a "pre-certificate" as defined in the RFC 6962 (Certificate Transparency) is considered a "certificate," and consequently should not be subject to the RFC 5280-Internet X.509 PKI and CRL Profile requirements.

3.1.1. Types of names

The end entity's electronic certificates referenced in this CP have a distinctive name (DN) in the Subject Name field, composed as described in information on the certificate profile (section 7.1 of this document). Izenpe fulfils requirements X.500, RFC 5280 and CA/Browser Forum (BRs and EVGs) in this regard.
The Common Name field defines the Certificate holder.

3.1.2. Meaning of names

All distinctive names (DN) in the Subject Name field are significant. The description of the attributes associated with the Certificate Subscriber is legible to humans (see section 7.1.4 Format of names in this document).

The Subject Distinguished Name field is also subject to requirements set forth in section 9.2 of CABForum in the "guide for issue and management of Extended Validation Certificates" and may be viewed at https://cabforum.org/extended-validation/ Izenpe does not issue Wildcard Certificates with EV policies.

3.1.3. Pseudonyms

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

3.1.4. Rules used to interpret several name formats

The requirements defined by standard X.500 of reference in standard ISO/IEC 9594 are applicable.

3.1.5. Uniqueness of names

The distinctive name (DN) assigned to the Certificate Subscriber within the Trust Service Provider name shall be unique.

3.1.6. Recognition and authentication of registered marks

Certificate applicants are prohibited from using names in their certificate issue requests that infringe upon any third-party intellectual property rights..
IZENPE does not verify whether a certificate applicant has intellectual property rights in the name appearing in a certificate request. Furthermore, IZENPE does not arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any domain name of either individuals or organizations or domain names.
IZENPE reserves the right to reject any certificate request because of a name claim dispute.

3.2. Initial identity validation

Izenpe conducts the validation process for the information included in the website authentication certificate pursuant to the "Baseline requirements for the issue and management of trust certificates," requirements established by the CA entity/Browser Forum and that may be viewed at https://cabforum.org/baseline-requirements-documents/
Additionally, before issuing an SSL Qualified or Qualified Office Certificate, Izenpe ensures that all information included in this type of Certificate on the Subscriber is compliant with (and is verified pursuant to) the requirements defined by the CA entity/Browser forum in the "guide for the issue and management of Extended Validation Certificates" (section 11) and that may be viewed at https://cabforum.org/extended-validation/
Izenpe registers all confirmations in this section for periodical auditing processes, both internal and independent.

3.2.1. Methods to test private key ownership

Izenpe receives a certificate request in PKCS#10 format, digitally signed by the private key generated by the Subscriber Representative in their setting. Before issuing the Certificate, Izenpe verifies the signature, guaranteeing that the public key included in the request matches the private key generated by the Certificate Manager.

3.2.2. Authentication of the Organisation Identity

3.2.2.1 Identity

Izenpe does not issue website authentication certificates for a Subscriber who is a natural person.

In the event of DV certificates

Izenpe does not verify identity or any type of information on the organisation in the event of SSL DV certificates.

In the event of OV certificates

Izenpe verifies the postal address and the identity of the certificate subscribing organisation with different methods, depending on the type of organisation (private, public or company).
When the Subscriber is a private entity or company, its address and identity is verified by consulting the Commercial Register.
Public entities are verified by consulting the pertinent Official State Gazette.

If the subscriber type is one other than the two cases above, post address and identity are verified by consulting the pertinent official register.

Izenpe verifies that the certificate subscriber organisation's name and post address in the request for the certificate match the name and address formally registered with the registers consulted as described in the sections above.

For qualified SSL and qualified Office certificates

Izenpe verifies the legal existence, postal address and the identity of the certificate subscribing organisation with different methods, depending on the type of organisation (private, public or company).
When the Subscriber is a private entity or company, its existence, address and identity, which is legally recognised, active at that time and formally registered, shall be verified by consulting the Commercial Register.
Public entities are verified by consulting the pertinent Official State Gazette.
If the subscriber type is one other than the two cases above, the legal existence, post address and identity are verified by consulting the pertinent official register.

Izenpe verifies that the certificate subscriber organisation's name, tax identification number and post address in the request for the certificate match the name, tax identification number and address formally registered with the registers consulted as described in the sections above.

If the request refers to an EV certificate, Izenpe shall comply with the requirements defined by the CA entity/Browser forum in its "guide for the issue and management of Extended Validation Certificates" that can be viewed at https://cabforum.org/extended-validation/

3.2.2.2 Commercial name or registered mark

If the subject's identity information includes a commercial name or registered mark, Izenpe shall use the same procedures and criteria for verification as in Section 3.2.2.1 to verify the Applicant's right to use the commercial name or registered mark.

For EV Certificates, exhaustive identity verification is required, as defined in section 11.3 of CABForum in its "guide for the issue and management of Extended Validation Certificates."

3.2.2.3 Country verification

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

3.2.2.4 Validation of authorisation and control over the domain

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

- ✓ 3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact
- ✓ 3.2.2.4.7 DNS Change
- ✓ 3.2.2.4.13 Email to DNS CAA Contact
- ✓ 3.2.2.4.14 Email to DNS TXT Contact
- ✓ 3.2.2.4.18 Agreed-Upon Change to Website v2

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

a) **Email the domain contact (BR 3.2.2.4.2):** Izenpe shall send the applicant a unique, random code by email to any of the addresses in the whois contact (Registrant, administrative or technical). The response must include the random number.

   Each email can confirm the control of several domain names.

   Izenpe may forward the email in its entirety, including reuse of the random code, provided that the complete content of the communication and the recipients remain in force.

   Izenpe shall provide an exclusive random code to request the certificate and shall not use the random code after 30 days.

b) **Change agreed upon in DNS (BR 3.2.2.4.7):** The applicant makes a change in the domain's DNS registration, so they apply for the SSL certificate. The applicant must add the random and unique code sent by Izenpe in a CNAME, TXT or CAA field in the DNS register. Once the change has been made by the applicant, Izenpe verifies it.

   Izenpe shall provide an exclusive random code to request the certificate and shall not use the random code after 30 days.

c) **Email to contact DNS CAA (BR 3.2.2.4.13):** Izenpe shall send the applicant a unique, random code by email to the address in the DNS CAA register. To this end, there should be a "contactemail" CAA entry with an email address :

   CAA 0 contactemail contacto@example.com.

   Izenpe shall provide an exclusive random code to request the certificate and shall not use the random code after 30 days.

d) **Email to contact DNS TXT (BR 3.2.2.4.14):** Izenpe shall send the applicant a unique, random code by email to the address in the DNS TXT register. There should be a TXT entry in the subdomain "_validation-contactemail" with an email address:

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

   Izenpe shall provide an exclusive random code to request the certificate and shall not use the random code after 30 days.

e) **Change agreed upon on website (BR 3.2.2.4.18):** The applicant must publish the file with the random and unique code sent by Izenpe on the route "/.well-known/pki-validation" Once the change has been made by the applicant, Izenpe verifies it.

Izenpe confirms that the Subscriber Representative holds control over the complete names of the domains or FQDN (Fully Qualified Domain Name) that are incorporated into the website authentication certificates being issued. To this end, Izenpe consults the identity of the Subscriber Representative and the name of the aforementioned FQDN through the application that records requests for these Certificates. It then verifies that the request has come from a contact with control over said domain (according to the methods defined in the section above) or has been

authorised by said contact. Additionally, it is verified that the certificate request was made after the date of said registrations.

Moreover, before issuing a website authentication certificate, it is verified that the domain to be included in the certificate is public (not an internal domain) and public registers 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 shall verify that all domain name space in Wildcard OV Certificates is legitimately controlled by the Subscriber.

If a wildcard certificate falls into the tag immediately to the left of a public suffix or controlled register, Izenpe shall reject the issue of said certificate unless the Applicant demonstrates legitimate control over all the domain name space. To this end, they shall consult the "Public Suffix List" available at https://publicsuffix.org/, which shall be periodically downloaded.

3.2.2.7 Reliability of data sources

Before using any data source as a reliable data source, the RA shall assess the source insofar as reliability, precision and resistance to alteration or falsification are concerned.

3.2.2.8 CAA Register

Prior to issuing all SSL certificates, Izenpe validates the existence of a CAA register for each DNS name of CN extensions and subjectAltName of the certificate, according to RFC 6844 specifications. If the certificate is issued, the validation is conducted before the CAA registration TTL, and in any event before 8 hours have passed. Izenpe processes the "issue" and "issuewild" tags.

The CAA registers that identify the domains for which Izenpe authorises the issue are "**izenpe.com**" and "**izenpe.eus.**"

3.2.3. Authentication of the applying natural person

Izenpe's RA shall verify that the Subscriber Representative matches the natural person requesting a website authentication certificate by means of electronic signature of the request form, using a qualified electronic signature certificate, thus guaranteeing the authenticity of their identity.

For DV or OV certificates, the subscriber representative may delegate request capacity to authorised applicants. The representative must electronically sign this delegation through the SSL certificate management application.

3.2.4. Unverified subscriber information

All information incorporated into the electronic certificate is verified by the Registration Authority; therefore, unverified information is not included in the "Subject" field of issued certificates.

3.2.5. Validation of representation capacity

Izenpe's RA verifies that the Applicant holds sufficient representation capacity by means of the electronic signature of the client's registration request form, as described in section 3.2.3 of this CP, accepting the use of a qualified Izenpe representative certificate by a legal subscriber person or a Qualified Public Entity Personnel Certificate, for whose issue the representative capacity has been accredited.

When the aforementioned form is signed with a qualified certificate other than those mentioned in the section above, Izenpe's RA shall verify the request's signatory's authorisation for representation by consulting official registers (Commercial Register, Official State Gazettes, etc., depending on the type of representation). If these consultations do not bear evidence of sufficient representation, Izenpe's RA shall contact the Subscriber to collect said evidence.

Through the online request to apply for SSL certificates, the entity representative may create users associated with employees who are permitted to request of DV or OV certificates for said entity.

For SSL qualified certificate requests, Izenpe shall comply with the requirements defined by the entity CA/Browser forum in its "guide for the issue and management of Extended Validation Certificates" (sections 11.8 and 11.11).

3.2.6. Inter-operation criteria

There are no interactivity relations with Certification Authorities outside Izenpe.

3.3. Identification and authentication for requests to renew keys

3.3.1. Identification and authentication for requests for routine renewal of keys

Certificate Subscribers must request renewal of said certificates before their validity period expires. Conditions to authenticate a renewal request are set forth in this CP's section on the certificate renewal process (see section 4.6 of this document).

The validity of the entity and competence of the applicant shall not be required if verified by Izenpe in the past 13 months.

3.3.2. Identification and authentication for renewal of keys after revocation

The Certificate renewal process after revocation of the certificate is the same as the process followed for the initial issue of said certificate.

3.4. Identification and authentication for revocation requests

Conditions to authenticate a revocation request are set forth in this CP's section on the certificate revocation process (see section 4.9 of this document).

4. Operative requisites for the certificates' life cycle

4.1. Certificate request

4.1.1. Who may request a Certificate

Only Subscriber Representatives may request website authentication certificates, or individuals duly authorised to solicit the certificate on behalf of the subscriber who have proven control over the domain name to be included in the certificate. Control over the domain name shall be verified by Izenpe as described in section "3.2 Initial identity validation" of this CP.

Additionally, for Qualified Certificates, Izenpe shall fulfil the requirements of section 11 of the "Guide for the issue and management of Extended Validation Certificates" set forth by the entity CA/Browser forum.

4.1.2. Registration and liabilities process

Each applicant must file a certificate request and the information required before issuing a certificate.

The registration process includes the following phases:

- ✓ Send a complete certificate request and accept the applicable terms and conditions. With this acceptance, Subscribers guarantee that all information in the certificate request is correct.
- ✓ Send technical request (PKCS#10).
- ✓ When applicable, pay applicable rates.

Izenpe's RA verifies the subscriber organisation and the subscriber representative's identity and verifies that the certificate request is correct, complete and duly authorised, pursuant to the requirements defined in section "3.2 Initial identity validation" in this document. Izenpe may conduct verifications in addition to the validation processes described in the aforementioned section.

Non-public entities whose formation information is not available for consultation at the Commercial Registry must provide:

- ✓ Copy of the publication in the pertinent registry
- ✓ Copy of the Tax ID Code

Izenpe shall collect evidence for the verifications conducted, which shall be stored in a repository.

Section 9.6 "Obligations and guarantees" of this document sets forth the parties' liabilities in this process.

4.2. Certificate request procedure

4.2.1. Carrying out identification and authentication functions

The Subscriber Representative sends Izenpe's RA a form, electronically signed, with a qualified electronic certificate that includes all the information to be incorporated into the website authentication certificate. Based on this information, Izenpe's RA conducts the verifications described in section "3.2 Initial identity validation" of this CP.
Izenpe shall verify the veracity of the data included in the request and, if applicable, the Representative's capacity through pertinent verifications, storing applicable evidence.
The Electronic Signature generated for the subscription of the contract shall be verified by Izenpe.
The data or documentation for previous validation obtained from one of the sources set forth in section 3.2 cannot be used more than 12 months after validation of said data or documentation.

4.2.2. Approval or rejection of the certificate request

The RA acting in the website authentication certificate issue process is always Izenpe itself and, therefore, it does not delegate validation of ownership of the domain to any other RA.

Izenpe's RA conducts verifications associated with proving the Subscriber Representative's ownership of the private key, authentication of the identity of the Organisation and the individual applying for the Certificate, as well as validation of the domain, as set forth in section "3.2 Initial identity validation" of this CP, which shall lead to the approval or rejection of the request for the certificate.

Izenpe keeps an internal database with all revoked certificates and all previous rejected certificates due to suspicion of phishing or other fraudulent use. This information is considered to identify later suspicious certificate requests before approving their issue.

Additionally, Izenpe conducts, maintains and implements documented procedures that identify and require additional verification activity for high-risk certificate requests before approval of issue of the certificate, as is reasonably necessary to guarantee that said requests are suitably verified according to these requirements.

If any of these validations were unable to be confirmed, Izenpe shall reject the certificate request and reserves the right to not reveal the grounds for said denial. The Subscriber Representative whose request was rejected may request it again later.

All OV Certificate or Qualified Certificate requests shall be processed by Izenpe's personnel with a trust role to this end. The Qualified Certificate issue approval system requires the action of at least two people belonging to Izenpe's RA with a trust role, one to validate the request and another to approve it.

Additionally, Izenpe verifies whether there is a CAA Register for reach domain name included on an issued website authentication certificate, pursuant to the procedure set forth in RFC 8659 and following the processing instructions established in RFC 8659 for all registers found. If said CAA Register exists, said certificate shall not be issued unless it is determined that the certificate request is consistent with the applicable set of CAA appeals.

4.2.3. Time to process request

The time period to process the request for a certificate largely depends on the Subscriber Representative providing the information and documentation necessary as set forth in the procedures approved by Izenpe to this end. Notwithstanding, this Entity shall make the efforts necessary for the validation process to bear a result of acceptance or rejection for the request in no longer than 5 working days.

Occasionally, this time period may be exceeded due to reasons beyond Izenpe's control. In these cases, it shall do everything possible to keep the Subscriber Representative who made the request informed of the reasons for such delays.

4.3. Issuance of certificate

4.3.1. CA actions during issuance

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

Moreover, Izenpe periodically monitors possible deviations in issued certificates.

Processes related to the issue of electronic certificates guarantee that all accounts related thereto have multi-factor authentication.

4.3.2. Notification of certificate issue

Once the certificate is issued, Izenpe sends a communication to the email address provided on the client registration form signed by the Subscriber Representative, informing that said certificate is available for download.

4.4. Certificate acceptance

4.4.1. Acceptance process

In the Certificate request process, the Subscriber Representative accepts the conditions for use and states their desire to obtain the certificate as requirements necessary to generate it.

4.4.2. CA publishes the certificate

The generated certificates are stored in a secure Izenpe repository.

4.4.3. Notification of issuance to other entities

Before issuing website authentication certificates, a pre-certificate is sent to the Certificate Transparency service registers owned by the providers with whom Izenpe has an agreement to this end.

4.5. Pair of keys and certificate use

4.5.1. Private subscriber's key and use of the certificate

Izenpe does not generate or store private keys associated with the certificates issued under this Certification Policy. Custody and control over the certificate keys falls on the Subscriber Representatives who have accredited control over the domain name to be included in the certificate. Therefore, the private key associated with the public key is under the responsibility of said custody.

4.5.2. Use of the public key and the certificate by trusting parties

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

Third parties who trust in the establishment of a secure connection guaranteed by a website authentication certificate must ensure that said connection was created during the certificate's validity period, that this certificate is being used with the purpose for which it was issued pursuant to this CP, and verify that the Certificate is active at that moment, by verifying its revocation status in the fashion and under the conditions set forth in section "4.10 Certificate status information services" in this document.

4.6. Certificate renewal

4.6.1. Certificate renewal circumstances

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

4.6.2. Who may request the modification of the certificate

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

4.6.3. Processing requests to renew the certificate

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

4.6.4. Certificate renewal notification

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

4.6.5. Conduct constituting acceptance of certificate renewal

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

4.6.6. Publishing the renewed certificate

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

4.6.7. Notifying other entities of renewal of the certificate

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

4.7. Renewal with certificate key regeneration

Renewal with regeneration of keys for website authentication certificates is always done by issuing new public and private keys, following the same process as the one described for the issue of a new certificate.

4.7.1. Circumstances for renewal with regeneration of keys

The certificate keys shall be renewed in the following cases:

- ✓ Upcoming expiry of current keys, at the request of the renewal applicant.
- ✓ The keys are compromised, or another circumstance as set forth in section "4.9 Certificate revocation and suspension" in this CP.

4.7.2. Who may request renewal with key regeneration

The same process as the one set forth to issue a new certificate must be followed.

4.7.3. Processing requests for renewal with key regeneration

The same process as the one set forth to issue a new certificate must be followed.

4.7.4. Notification of renewal with regeneration of keys

The same process as the one set forth to issue a new certificate must be followed.

4.7.5. Conduct constituting acceptance of renewal with key regeneration

The same process as the one set forth to issue a new certificate must be followed.

4.7.6. Publishing the renewed certificate

The same process as the one set forth to issue a new certificate must be followed.

4.7.7. Notification of renewal with regeneration of keys to other entities

The same process as the one set forth to issue a new certificate must be followed.

4.8. Modifying the certificate

It is not possible to make modifications to issued certificates. Therefore, any need for modification shall entail issuance of a new certificate.

4.8.1. Circumstances to modify the certificate

Modification not stipulated.

4.8.2. Who may request modification of the certificate

Modification not stipulated.

4.8.3. Processing requests to modify the certificate

Modification not stipulated.

4.8.4. Notification of certificate modification

Modification not stipulated.

4.8.5. Conduct constituting acceptance of certificate modification

Modification not stipulated.

4.8.6. Publishing the modified certificate

Modification not stipulated.

4.8.7. Notifying other entities of modification of the certificate

Modification not stipulated.

4.9. Certificate revocation and suspension

Website authentication certificates issued by Izenpe shall be rendered invalid in the following cases:

a) Termination of the Certificate's validity period.
b) Izenpe's cessation of activity as Trust Service Provider, subject to the Subscriber's express consent, with the certificates issued by Izenpe transferred to another Trust Service Provider.
   In these two cases a) and b), the Certificates shall lose efficacy as soon as these circumstances occur.
c) Revocation of the Certificate for any of the reasons set forth in this document.

The Certification's revocation shall be effective, meaning its validity expires, as of the date when Izenpe has certain knowledge of any of the determining events and leaves a record of this in its Certificate Status Information and Consultation Service.

Izenpe provides Subscribers, trusting third parties, software providers and third parties with a communication channel through incidencias@izenpe.eus so they can report any issue related to this type of certificate regarding supposed compromise of a Private Key, undue use of the Certificates or other kinds of fraud, compromise, improper use or inappropriate conduct.

Izenpe, as a Trusted Service Provider, reserves the right to not issue or revoke this type of Certificate if the Subscriber who holds control over the website domain name included on the Certificate does not make appropriate use of it, violating third-party industrial or intellectual property rights over applications, websites or electronic offices whose protection is intended with these Certificates, or if their use lends itself to deceit or confusion regarding the ownership over these applications, websites or electronic offices and, therefore, their contents.

Izenpe shall be held blameless by the holders or those responsible for the equipment, applications, websites or electronic offices that fail to comply with provisions in this section and that are related to the certificate and shall be held exempt from any claim for inappropriate use of said certificates.

4.9.1. Circumstances for revocation

4.9.1.1 Grounds for revoking an end entity certificate

In addition to provisions in the section above, the following shall be grounds to revoke a website authentication certificate:

a) A request for revocation from authorised individuals. In any event, the following shall lead to this request:
   - Loss of certificate media.
   - A third party's use of the Private Key associated with the certificate.
   - Violation or endangering of the Private Key associated with the certificate.
   - Failure to accept new conditions that may be set forth by the issue of new Certification Practise Statements during the period of one month after publication.
b) A legal or administrative ruling ordering to do so.
c) Termination, dissolution or closure of the website identified by the certificate.
d) Termination or dissolution of the subscriber's legal personality.
e) Termination of the Certificate Subscriber's representative's representation status.

f) Total or partial supervening incapacity of the Subscriber representative.
g) Inaccuracies in the data provided by the Subscriber Representative to obtain the Certificate, or alteration in the data provided to obtain the Certificate or modification of the circumstances verified to issue the certificate, such that it is no longer compliant with reality.
h) The Subscriber, Subscriber Representative or Registration Office contravening a substantial obligation in this Certification Practises Statement, if in the latter case, this may have affected the Certificate issue process.
i) Use of the Certificate with the purpose of creating doubt in users regarding the origin of the products or services offered, showing that the origin is different than the one truly offered. To this end, criteria on activity infringing standards for consumers and users, trade, competition and advertising will be followed.
j) Termination of the contract entered into between the Subscriber or the Representative and Izenpe or non-payment of services provided.
k) Violation or endangering of secrecy of Izenpe's Signature Creation/Stamp Data with which it signs/stamps the Certificates it issues.
l) Failure to comply with the requirements defined by the auditing systems to which the Certification Authority that issues the Certificates covered by this CP is subject, especially algorithm and key size, which entail an unacceptable risk to the parties who trust in these certificates.

Under no circumstances shall Izenpe assume any obligation to verify the cases mentioned in letters c) through i) of this section.

Izenpe shall only be held liable from the consequences of not revoking a certificate in the following cases:

- When the revocation was requested by the Subscriber Representative, following the procedure established for this type of certificate.
- When the revocation should have been completed because the contract subscribed with the Subscriber was terminated.
- When the request for revocation or the grounds for doing so was notified to Izenpe by means of a legal or administration ruling.
- When causes c) through g) of this section are reliably proven to Izenpe, subject to identification of the revocation applicant.

Actions constituting a crime or misdemeanour of which Izenpe is not aware that are taken on data or the Certificate, inaccuracies in data or lack of diligence in communication with Izenpe shall exempt Izenpe from liability.

All requests for end-entity certificate revocation are processed within a maximum period of 24 hours after reception.

4.9.1.1 Grounds for revoking a subordinate CA certificate

For subordinate CA certificates, they shall be revoked within 7 days at the latest for the following reasons:

a) The subCA requests it in writing
b) The subCA notifies the issuing CA that the request for the original certificate was not authorised and does not admit retroactive authorisation

c) The issuing CA obtains evidence that the private key for the subCA for the certificate's public key has been subject to key compromise or has ceased to comply with requirements in sections 6.1.5 and 6.1.6 of the BRs
d) The issuing CA obtains evidence that the certificate was issued incorrectly
e) The issuing CA detects that the certificate was not issued pursuant to the Certificate Policy or the CPS
f) The issuing CA determines that data on the certificate is imprecise or incorrect
g) The issuing CA or the subCA ceases operations for any reason and agreements have not been entered into with another CA to provide the revocation service
h) The issuing CA or subCA's right to issue certificates under BR's requirements finalises or is revoked, unless the issuing CA has enabled agreements to continue maintaining the CRL/OCSP repository
i) The issuing CA and/or CPS policy requires revocation
j) The content or technical format of the certificate bears a risk that is unacceptable to software providers or third parties
k) Providers or third parties (e.g.: the CA/Browser Forum may determine that an algorithm/encryption signature of key size bear an unacceptable risk and that these certificates must be revoked and replaced within a specific period of time)

4.9.2. Who may request revocation

The CA, the RA and Subscribers may initiate certificate revocation.

Revocation of a website authentication certificate may only be requested by the individual with authorisation to represent the Subscriber to whom the Certificate was issued.

Additionally, the following shall be authorised to request revocation of said certificate:

- The management body, entity or Certificate Subscriber entity or the person delegated by the Subscriber.

- The Registration Office (through its responsible party) who has been appointed to this end by the Administration, body or entity of public law that is the Subscriber of the Certificate to be revoked when it detects that any of the data in the Certificate:
  - ✓ is incorrect or imprecise or has varied from what is contained in the Certificate, or
  - ✓ the natural person, custodian of the Certificate, does not match the highest responsible party or party designated for management and administration of the email address contained in the Certificate to be revoked,

  always under the terms and conditions applicable to revocation of this type of certificate.

Additionally, subscribers, trustworthy parties, application software providers and other third parties may inform the issuing CA of reasonable grounds to revoke the certificate by sending an incident report with a certificate.

Notwithstanding, Izenpe may revoke ex officio the website authentication certificates under the circumstances set forth in this Certification Policies and Practises Statement.

Moreover, for certificates regulated in this specific documentation, Izenpe ,

1. Shall provide clear instructions to file reports or suspicions of private key compromise, improper use of certificates or other kinds of fraud and improper use or behaviour, regarding the certificates to third parties and Internet browsers.
2. Shall investigate reports on problems within twenty-four hours after reception, and shall decide regarding revocation, under the following criteria:
    - The type of alleged problem
    - The number of reports received on problems with a certificate or webpage
    - The identity of the claimants
    - Current legislation

4.9.3. Procedure to request revocation

The revocation applicant will process the Revocation Request through IZENPE. If revocation is requested by someone other than the applicant, subscriber or key owner, either before or concurrent with revocation, IZENPE shall inform the certificate key owner and subscriber of the revocation of its certificate and specify the reason for revocation.

The applicant can revoke the certificate through the following channels:

- In person,
    - At Izenpe, requesting a prior appointment at www.izenpe.com
    - Or with the subscriber organisation with which Izenpe entered into the pertinent legal instrument.
- Online, at the website www.izenpe.com
- By email, sending the revocation request form, signed with a qualified certificate

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

Once Izenpe has proceeded to revoke the website authentication certificate, this shall be published on the pertinent Revoked Certificate List in the Secure Directory, containing the serial number of the revoked certificate, as well as the date, time and cause for revocation. Through the email address provided in the request, the Subscriber Representative shall receive notification in the change of the Certificate's validity status.

4.9.4. Grace period for request for revocation

There is no grace period associated with this process, given that the revocation occurs immediately upon verified reception of the request for revocation.

4.9.5. Deadline to process the revocation request

All requests for end-entity certificate revocation are processed within a maximum period of 24 hours after reception.

Izenpe proceeds to immediately revoke the website authentication certification when making the aforementioned verifications or, if applicable, after verifying the veracity of the request made by means of a legal or administrative ruling.

4.9.6. Trusting parties' obligation to verify revocations

Third parties who trust and agree to the use of Certificates issued by Izenpe are bound to verify:

- ✓ the Advanced Electronic Signature or the Advanced Electronic Stamp of the Trust Service Provider issuing the Certificate,
- ✓ that the Certificate is still in force and active, and
- ✓ the status of the Certificates included in the Certification Chain.

4.9.7. Frequency of generating CRLs

IZENPE immediately issues a Certificate Revocation List (hereinafter CRL) the moment a certificate is revoked.
The CRL contains the stipulated time for issuance of a new CRL, although a CRL may be issued prior to the time indicated on the previous CRL. If there are no revocations, the Certificate Revocation List is regenerated on a daily basis.
The CRL for the end entity certificates is issued at least every 24 hours or when a revocation occurs, valid for 10 days.
The CRL for the CA certificates (ARLs) is issued every 12 months or when a revocation occurs.
Revoked certificates which expire are removed from the CRL. They are then retained in IZENPE's internal register for a period of 15 years.

4.9.8. Maximum CRL latency period

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

4.9.9. Availability of the online verification system for certificate status

IZENPE provides its User Entities with a real-time certificate checking service based on OCSP (Online Certificate Status Protocol), so that user applications verify the certificate status.
This service is available 24 hours a day, 7 days a week.

4.9.10. Online revocation verification requisites

Use of the CRL free access service will require:

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

Revoked certificates that expire shall be removed from the CRL; however, information will still be offered on the status of the certificate through online verification, even if it is expired.
Use of the OCSP free access service will require:

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

4.9.11. Other revocation notifications available

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

4.9.12. Special requirements for revocation of compromised keys

There are no special requirements for revoking certificates due to compromised keys; provisions described for the rest of grounds for revocation are applicable.

4.9.13. Circumstances for suspension

Certificate suspension is not provided for.

4.9.14. Who may request the suspension

Certificate suspension is not provided for.

4.9.15. Procedure to request suspension

Certificate suspension is not provided for.

4.9.16. Limits on suspension period

Certificate suspension is not provided for.

4.10. Certificate status information services

4.10.1. Operative characteristics

Operation of the certificate status consultation and information system is as follows: the OCSP server receives the OCSP request made by an OCSP Client and verifies the validity status of the Certificates included therein. In the event that the request is valid, an OCSP response shall be issued, reporting on the status of the Certificates included in the petition at that time. Said response is signed/stamped with Izenpe's Signature Creation/Signature Data, thus guaranteeing the integrity and authenticity of the information supplied on the revocation status of the consulted certificates.

It will be the User Entity's responsibility 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 capacities with sufficient resources to provide sufficient response time under normal operating conditions.

4.10.2. Service Availability

IZENPE provides the user entities with a 24x7 revocation service (24 hours a day, 7 days a week).

4.10.3. Optional characteristics

Not stipulated.

4.11. Finalising the subscription

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

The expiry for each certificate is stipulated in the Specific policy.

4.12. Custody and recovery of keys

4.12.1. Practises and policies for custody and recovery of keys

Izenpe does not generate private keys for the website authentication certificates, and therefore, does not keep custody over them nor can it retrieve them.

4.12.2. Session key protection and recovery practises and policies

Not stipulated.

5. Physical, procedural and personnel security controls

5.1. Physical security controls

5.1.1. Location at facilities

See the pertinent section in the CPS

5.1.2. Physical access

See the pertinent section in the CPS

5.1.3. Power and air conditioning

See the pertinent section in the CPS

5.1.4. Water exposure

See the pertinent section in the CPS

5.1.5. Fire prevention and protection

See the pertinent section in the CPS

5.1.6. Media storage

See the pertinent section in the CPS

5.1.7. Waste removal

See the pertinent section in the CPS

5.1.8. Backup copies outside the facilities

See the pertinent section in the CPS

5.2. Procedural controls

5.2.1. Trusted roles

See the pertinent section in the CPS

5.2.2. Number of persons required per task

See the pertinent section in the CPS

5.2.3. Identification and authentication for each role

See the pertinent section in the CPS

5.2.4. Roles that require function segregation

See the pertinent section in the CPS

5.3. Personnel controls

5.3.1. Knowledge, qualification, experience and accreditive requirements

See the pertinent section in the CPS

5.3.2. Background check procedures

See the pertinent section in the CPS

5.3.3. Training requirements

See the pertinent section in the CPS

5.3.4. Training frequency and requirements

See the pertinent section in the CPS

5.3.5. Job rotation frequency and sequence

See the pertinent section in the CPS

5.3.6. Sanctions for unauthorised actions

See the pertinent section in the CPS

5.3.7. Personnel hiring requirements

See the pertinent section in the CPS

5.3.8. Documentation supplied to personnel

See the pertinent section in the CPS

5.4. Auditing procedures

5.4.1. Type of events recorded

See the pertinent section in the CPS

5.4.2. Frequency of record processing

See the pertinent section in the CPS

5.4.3. Record storage period

See the pertinent section in the CPS

5.4.4. Record protection

See the pertinent section in the CPS

5.4.5. Procedures for backup copies of audited records

See the pertinent section in the CPS

5.4.6. Record collection systems

See the pertinent section in the CPS

5.4.7. Notification to the subject causing the events

See the pertinent section in the CPS

5.4.8. Vulnerability assessments

See the pertinent section in the CPS

5.5. Record archiving

5.5.1. Type of records archived

See the pertinent section in the CPS

5.5.2. Archive retention period

See the pertinent section in the CPS

5.5.3. Protecting the archive

See the pertinent section in the CPS

5.5.4. Archive backup copy procedures

See the pertinent section in the CPS

5.5.5. Requisites for time stamping the record registrations

See the pertinent section in the CPS

5.5.6. Archive system

See the pertinent section in the CPS

5.5.7. Procedures to obtain and verify the archived information

See the pertinent section in the CPS

5.6. CA key change

See the pertinent section in the CPS

5.7. Incident and Vulnerability Management

5.7.1. Incident and Vulnerability Management

See the pertinent section in the CPS

5.7.2. Action plan to deal with corrupt data and software

See the pertinent section in the CPS

5.7.3. Procedure to deal with compromised private CA key

See the pertinent section in the CPS

5.7.4. Business continuity after a disaster

See the pertinent section in the CPS

5.8. Cessation of Trust Service Provider activity

See the pertinent section in the CPS

6. Technical security controls

6.1. Key generation and installation

6.1.1. Key pair generation

6.1.1.1 CA key pair generation

See the pertinent section in the CPS

6.1.1.2 RA key pair generation

Not stipulated

6.1.1.3 Subscriber key pair generation

The private keys for website authentication certificates are generated and with custody held over them by the Certificate Subscriber.

6.1.2. Sending the private key to the subscriber

The CA does not generate or deliver the Private Key to the holder.

6.1.3. Sending the public key to the certificate issuer

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

6.1.4. Distribution of the CA public key to trusting parties

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

6.1.5. Key size and algorithms used

The algorithm used in all cases is RSA with SHA2.

Regarding key size, depending on each case, it is:

- Root CA keys: RSA 4096 bits.
- Subordinate CA Keys: RSA 4096 bits.
- Website authentication certificate keys: RSA 2048 bits.

6.1.6. Public key generation parameters and quality verification

The public keys for website authentication certificates are encoded according to RFC5280 and PKCS#1.

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

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

Root CA keys are used to sign subordinate CA certificates, ARLs and the TSA certificate. Subordinate CA or issuer keys are only used to sign end user certificates and CRLs

Admitted key uses for end certificates are defined in the certificate profile document, available at www.izenpe.eus.

6.2. Private key protection and cryptographic module controls

6.2.1. Standards for cryptographic modules

See the pertinent section in the CPS.

6.2.2. Multi-person (n of m) control over the private key

See the pertinent section in the CPS.

6.2.3. Custody of the private key

See the pertinent section in the CPS.

6.2.4. Private key backup copy

See the pertinent section in the CPS.

6.2.5. Private key archiving

See the pertinent section in the CPS.

6.2.6. Transfer of the private key to/from the cryptographic module

See the pertinent section in the CPS.

6.2.7. Storage of the private key in the cryptographic module

See the pertinent section in the CPS.

6.2.8. Method of activating private key

See the pertinent section in the CPS.

6.2.9. Method of deactivating private key

See the pertinent section in the CPS.

6.2.10. Method of destroying private key

See the pertinent section in the CPS.

6.2.11. Classification of cryptographic modules

See the pertinent section in the CPS.

6.3. Other aspects of key pair management

6.3.1. Public key archival

Website authentication certificates, and therefore their associated public keys, are stored by Izenpe for the period of time required by applicable law, which is currently 15 years.

6.3.2. Operational periods of the certificate and key-pair use periods

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

- Root CA certificate and key pair: see section "1.3.1. Certification Authority" in this CP.
- The subordinate CA certificate that issues the website authentication certificates and their key pair: see section "1.3.1. Certification Authority" in this CP.
- The website authentication certificates and their key pair: the maximum validity period is 395 days.

6.4. Activation data

6.4.1. Activation data generation and installation

See the pertinent section in the CPS.

6.4.2. Activation data protection

See the pertinent section in the CPS.

6.4.3. Other aspects of activation data

See the pertinent section in the CPS.

6.5. IT security controls

6.5.1. Specific computer security technical requirements

See the pertinent section in the CPS.

6.5.2. IT security rating

See the pertinent section in the CPS.

6.6. Life cycle technical controls

6.6.1. System development controls

See the pertinent section in the CPS.

6.6.2. Security management checks

See the pertinent section in the CPS.

6.6.3. Life cycle security checks

See the pertinent section in the CPS.

6.7. Network security controls

See the pertinent section in the CPS.

6.8. Time source

See the pertinent section in the CPS.

7. CRL and OCSP certificate profiles

7.1. Certificate profile

The website authentication certificates comply with European standard ETSI EN 319 412-4 "Certificate profile for website certificates."

They include CABForum's following policy identifiers:

CERTIFICATE	OID CA/B FORUM
SSL DV	2.23.140.1.2.1
SSL OV	2.23.140.1.2.2
SSL EV	2.23.140.1.1
SSL Qualified	2.23.140.1.1
EV office	2.23.140.1.1
Qualified Office	2.23.140.1.1

7.1.1. Version number

The website authentication certificates comply with standard X.509 version 3.

7.1.2. Certificate extensions

The page https://www.izenpe.eus/contenidos/informacion/doc_juridica/es_def/adjuntos/Perfiles_de_Certificados.pdf publishes the document describing the website authentication certificate profile, including all extensions.

7.1.3. Algorithm object identifiers

The algorithm identifier (AlgorithmIdentifier) used by IZENPE to sign the certificate is SHA-256/RSA which corresponds to "Identifier for SHA-2 checksum with RSA encryption for use with Public Key Cryptosystem One defined by RSA Inc."

7.1.4. Name formats

Website authentication certificate encoding follows standard RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.” All fields defined in the profile of these certificates, except for fields where expressly stated otherwise, use UTF8String encoding.

7.1.5. Name constraints

The subordinate CAs that issue certificates under this CP are not technically restricted.

7.1.6. Certificate policy object identifier

The object identifier (OID) of the website authentication certificate policy is defined in section "1.2 Document name and identification" of this document.

7.1.7. Usage of policy constraints extension

Policy constraints are not 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 Certificate Practice Statement http://www.Izenpe.com/cps
- **User notice:** A drop-down text notice that appears on the screen, with a request or user request, when a third party verifies the certificate.
- **Policy Identifier**: Indicates the certificate's OID

User Notice for all certificates (except for SSL certificates):

USER NOTICE	Kontsulta www.izenpe.com-en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - See terms and conditions at www.izenpe.com before using or trusting the certificate

7.1.9. Semantic processing for the "certificate policy" extension

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

7.2. CRL profile

The certificates issued by IZENPE meet the following norms:

- ✓ Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 5280) April 2002
- ✓ Internet X.509 Public Key Infrastructure Authority Information Access Certificate Revocation List (CRL) Extension (RFC 4325) December 2005
- ✓ Update to DirectoryString Processing in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 4630) August 2006

7.2.1. Version number

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

7.2.2. CRL and extensions

The following extensions are used:

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

7.3. OCSP profile

Izenpe's OCSP responses are compliant with standard RRC 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 whom the certificate being consulted was issued.

7.3.1. Version number

Version 3.

7.3.2. OCSP Extensions

See the pertinent section in the CPS

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

8. Compliance audits

The website authentication certificate issue service is subject to an annual auditing process, pursuant to 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.”

Additionally, certificates considered qualified undergo an audit to guarantee compliance with requirements set forth in the European standard ETSI EN 319 411-2 “Requirements for trust service providers issuing EU qualified certificates.”

The certificate issuance system is subjected to other additional audits:

- ✓ Information Security Management System audit, pursuant to UNE-ISO/IEC 27001 "Information Security Management Systems (SGSI). Requirements."
- ✓ Audit as set forth in the National Security System (Royal Decree 3/2010 of 8 January, regulating the National Security System in the scope of Electronic Administration).
- ✓ Audit pursuant to (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, and Organic Law 3/2018 of 5 December on Personal Data Protection and the guarantee of digital rights (GDPR/LOPD-GDD).

Risk analysis is also conducted, pursuant to the Information Security Management System.

8.1. Frequency of audits

The ETSI audits mentioned in the previous section are conducted on an annual basis. For certificates considered qualified (qualified SSL, qualified office), the audit additionally guarantees compliance with requirements from 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 rest of additional audits is pursuant to stipulations in pertinent applicable regulations.

8.2. Auditor qualification

See the pertinent section in the CPS.

8.3. Auditor’s relationship to audited company

See the pertinent section in the CPS.

8.4. Audit focus elements

See the pertinent section in the CPS.

8.5. Decision-making when deficiencies are detected

See the pertinent section in the CPS.

Security incidents are managed by Izenpe's Security Committee. Izenpe will open up an investigation within 24 hours at the latest after reception and decide upon the actions to take, considering the criteria in section 4.9.5 of the BRs.

Additionally, Izenpe reports cases it considers to be incidents (fraud, phishing, etc.) to the Anti-PhishingWorkGroup website (www.apwg.org) and verifies prior to issue that the applicant or representatives are not in Izenpe's internal security incident database. In any event, the right to issue certificates in suspicious situations is reserved.

8.6. Communicating results

See the pertinent section in the CPS.

8.7. Self-assessment

See the pertinent section in the CPS.

9. Other legal and activity matters

9.1. Fees

See the pertinent section in the CPS.

9.1.1. Certificate issuance or renewal fees

Fees applicable to the issue or renewal of Certificates are determined according to provisions in section "9.1 Fees" in this document.

9.1.2. Fees to access certificates

Not stipulated

9.1.3. Fees to access status or revocation information

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

9.1.4. Fees for other services

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

9.1.5. Refund policy

IZENPE does not have a refund policy.

9.2. Financial liability

See the pertinent section in the CPS.

9.2.1. Civil liability insurance

See the pertinent section in the CPS.

9.2.2. Other assets

See the pertinent section in the CPS.

9.2.3. Insurance and guarantees for end entities

See the pertinent section in the CPS.

9.3. Information confidentiality

See the pertinent section in the CPS.

9.3.1. Scope of the confidential information

See the pertinent section in the CPS.

9.3.2. Information not included in the scope

See the pertinent section in the CPS.

9.3.3. Responsibility to protect the confidential information

See the pertinent section in the CPS.

9.4. Personal data protection

See the pertinent section in the CPS.

9.4.1. Privacy plan

See the pertinent section in the CPS.

9.4.2. Information processed as private

See the pertinent section in the CPS.

9.4.3. Information not considered private

See the pertinent section in the CPS.

9.4.4. Responsibility to protect the private information

See the pertinent section in the CPS.

9.4.5. Notification and consent to use private information

See the pertinent section in the CPS.

9.4.6. Sharing according to the legal or administrative process

See the pertinent section in the CPS.

9.4.7. Other circumstances to share information

See the pertinent section in the CPS.

9.5. Intellectual property rights

See the pertinent section in the CPS.

9.6. Obligations and guarantees

9.6.1. CA obligations

Izenpe's obligations and responsibilities, as Trust Service Provider, toward the Certificate Subscriber and, if applicable, trusting users and third parties, shall be mainly determined by the document on conditions for use or the Certificate issuance contract and, alternatively, by this Certification Practises and Policy Statement.

Izenpe fulfils the requirements of technical specifications from standard ETSI EN 319 411 to issue Certificates and binds itself to continue to fulfil said standard or standards that replace it.

Izenpe issues website authentication certificates pursuant to the "Baseline requirements for the issue and management of trust certificates," requirements established by the CA entity/Browser Forum and that may be viewed at https://cabforum.org/. Moreover, it adapts its issuance practises for said certificates to the current version of the aforementioned requirements. In the event of any lack of coherence between this CP and the aforementioned version, said requirements shall prevail over this document.

Additionally, Izenpe undertakes to fulfil, in relation to issuing EV certificates (qualified SSL and qualified office), the requirements set forth by the CA entity/Browser forum for this type of certificate (EV SSL Certificate Guidelines), which may be viewed at https://cabforum.org/extended-validation/. In the event of any lack of coherence between this CP and the aforementioned version, said requirements shall prevail over this document.

Notwithstanding provisions in regulations applicable to this type of certificate, as well as the obligations described in the pertinent CPS section, the Trust Service Provider undertakes to:

Before issuing the certificate:

- ✓ Verify the identity and personal circumstances of the Certificate Applicant and the Subscriber and/or their Representative and collect a statement that the Applicant is authorised by the Subscriber to make the request.

- ✓ In the registration process, verify data on the legal personality of the Subscriber and the Representative's authorisation. All these verifications shall be conducted pursuant to the Particular Certification Practises set forth in this document and based on Izenpe's registration protocols and procedures.

- ✓ During processes to verify the cases mentioned above, Izenpe may verify through the action of third parties who hold authorisation to do so or from public or private registers.

- ✓ Verify that all the information contained in the Certificate request matches the information provided by the Applicant.

- ✓ Verify that the Applicant holds the Private Key associated with the Public Key incorporated into the Certificate to be issued.

- ✓ Guarantee that the procedures followed ensure that the Private Keys for the website authentication Certificates are generated without Izenpe making copies or storing them.

- ✓ Communicate information to the Subscriber, Representative and Applicant such that it remains confidential.

- ✓ Provide the Applicant, Subscriber, Representative and other interested parties (www.izenpe.eus/cps) with the Certification Practises Statement and all other relevant information to conduct the procedures related to the life cycle of the certificates referenced in this Particular Certification Practises and Certification Policy, pursuant to applicable regulations.

9.6.2. RA obligations

See the pertinent section in the CPS.

Activities related to the RA shall be exclusively conducted by Izenpe through its Registration Area for all website authentication certificates.

Through Izenpe's Registration Area, the RA has the following obligations:

- ✓ In general, to follow the procedures established by Izenpe in the applicable Certification Practises and Policy in conducting its certificate management, issuance and revocation roles, and to not alter this framework for action.
- ✓ In particular, verify the identity, and all relevant personal circumstances for the assigned purpose, of the Certificate Applicants, Subscribers and their Representatives, using any of the means permitted by Law and pursuant, in general, to the provisions in the CPS, and particularly, in this CP.
- ✓ Verify that ownership of the domain name matches with the Subscriber's identity or, if applicable, obtain the Subscriber's authorisation, which shall be associated with the
- ✓ website authentication Certificate, by the means within their reach which would reasonably provide for verification of said ownership, pursuant to the state of the art.
- ✓ Expressly collect the Subscriber's statement regarding ownership of the domain from the website authentication certificate, stating that they hold decision-making power over it.
- ✓ Store all information and documentation related to the Certificates, whose request, renewal or revocation it manages for 15 years.
- ✓ Receive and manage requests and contracts for issue (PDF form) of Certificates with their Subscriber.
- ✓ Diligently verify the reasons for revocation that may affect the validity of the certificates.

9.6.3. Subscriber Obligations

See the pertinent section in the CPS.

Regarding website authentication certificates, Subscribers must hold control over the domain name of the website included on said Certificates and keep the associated private keys for their exclusive use.

The Applicant and the Subscriber of the Certificates issued under this CP have the obligation to:

- ✓ Not use the Certificate beyond the limits set forth in this Particular Certification Practises and Policy.
- ✓ Not use the certificate if the Trust Service Provider has ceased activity as issuing entity of certificates that issued the certificate in question, especially when the supplier's Stamp Creation Data may be compromised, and this has been communicated.
- ✓ Provide truthful information on the certification request and keep it updated, with duly authorised individuals signing the contracts.
- ✓ Not request distinctive signs, designations or industrial or intellectual property rights for the object of the certificate over which they do not hold ownership, license or demonstrable authorisation to use.
- ✓ Act diligently regarding custody and storage of Signature Creation/Stamp Data and all other sensitive information, such as keys, certificate activation codes, login words, PINs, etc., as well as certificate media, which under all circumstances includes not revealing any of the aforementioned data.
- ✓ Be aware of, and comply with, the conditions for use of certificates set forth in the conditions for use and in the Certification Practises Statement and, particularly, limitations on use of certificates
- ✓ Be aware of, and comply with, the modifications made to the Certification Practises Statement.
- ✓ Request revocation of the pertinent Certificate, pursuant to the procedure described in this document, diligently notifying Izenpe of the circumstances for revocation or suspicion of loss of confidentiality, revelation, modification or unauthorised use of the associated private keys.
- ✓ Review the information contained in the certificate and notify Izenpe of all errors or inaccuracies.
- ✓ Before trusting the certificates, verify the advanced electronic signature or electronic stamp of the Trust Service Provider issuing the certificate.
- ✓ Diligently notify Izenpe of all modifications to the data provided in the Certificate request and, when as a consequence it is pertinent to do so, requesting that it be revoked.

In any event, it shall be the Subscriber's responsibility to appropriately use and diligently keep custody over the certificate, based on the purpose and role for which it was issued, and to inform Izenpe of all variations to the status or information on the Certificate for revocation and new issuance.

Moreover, the Subscriber, under all circumstances, shall be held liable to Izenpe, user entities and, if applicable, third parties, for undue certificate use or falsehood or errors in statements included in the certificate, or actions or omissions that lead to harm and damages to Izenpe or third parties.

It shall be the responsibility, and consequently the obligation of the Subscriber to not use the Certificate in the event that the Trust Service Provide has ceased activity as Certificate Issuing Entity that issued the Certificate in question and the subrogation set forth by law has not occurred. In any event, the Subscriber shall not use the Certificate in cases where the Supplier Signature Creation Data may be threatened and/or compromised, and the Supplier has communicated this situation or, if applicable, news has been had of these circumstances.

Regarding Electronic Office Certificates, Public Subscriber Entities, represented through the different competent bodies, acting through the Head of Registration Operations for the issuance of this type of Certificate, they have the obligation to:

- ✓ Not register or process requests for Certificates issued under this policy and whose Applicant is a natural person who does not provide their services to the Certificate Subscriber entity and/or has not been authorised by the individual acting as Entity Representative.
- ✓ Reliably verify the identifying and authorisation data of the Certificate Subscriber (the Entity that owns the electronic address, domain or URL used to access) and the Applicant (the natural person with sufficient authorisation to request a qualified certificate) of the Certificate and verify that it matches the owner and contacts in the pertinent databases, to manage and administer the electronic address used to access the electronic office to identify the certificate being requested.
- ✓ Request revocation of the certificate issued under this policy when any of the data referring to the Subscriber or the electronic address included in the Certificate are incorrect, inaccurate or have varied in comparison with the Certificate, or do not match the owner and contacts established in the pertinent databases to manage and administer the electronic address on the certificate to be revoked.

Relations between Izenpe and the Subscriber shall be mainly determined, for the purposes of the certificate use system, through the document on conditions for use or, if applicable, the certificate issuance contract, heeding to the agreements, pacts or document stipulating the relationship between Izenpe and the pertinent entity.

9.6.4. Obligations of trusting parties

It shall be the responsibility of the user entity and third parties trusting in the certificates to verify and guarantee the certificates' status, and under no circumstances may the validity of the certificates be presumed without said verifications.

If circumstances indicate the need for additional guarantees, the User Entity may obtain additional guarantees, so that said trust is reasonable.

Moreover, it shall be the User Entity's responsibility to fulfil provisions in the Certification Practises Statement and its possible future amendments, paying special attention to the limits to use set forth for Certificates in this Certification Policy.

See the pertinent section in the CPS.

9.6.5. Obligations of other participants

Not stipulated

9.7. Waiving guarantees

Not stipulated

9.8. Liability limits

See the pertinent section in the CPS.

9.9. Compensation

9.9.1. CA compensation

Not stipulated

9.9.2. Subscriber compensation

Not stipulated

9.9.3. Trusting party compensation

Not stipulated

9.10. This document's validity period

9.10.1. Enforcement

This Certification Policies and Practises Statement enters in force the moment it is published.

9.10.2. Termination

This Certification Policy will be revoked as soon as a new version of the document is published. The new version will fully substitute the previous document. Izenpe commits to submit said Statement to a revision process on an annual basis.

9.10.3. Finalisation effective

For the valid certificates issued under a previous Certification Policies and Practises Statement, the new version will prevail over the former in everything not opposed to it.

9.11. Individual notifications and communication with the participants

See the pertinent section in the CPS.

9.12. Modifications to this document

9.12.1. Procedure for modifications

Modifications to this Certification Policy shall be approved by Izenpe's Security Committee and shall be set forth in the pertinent minutes, pursuant to the approved internal procedure.

9.12.2. Notification period and mechanism

Any modification to this Certification Policy shall be immediately published on the URL to access them.

If the modifications do not entail significant changes to the system of obligations and responsibilities of the parties or regarding a modification to the service provision policies, Izenpe shall not inform users in advance and shall merely publish a new version of the affected statement on its website.

9.12.3. Circumstances under which an OID must be changed

Significant modifications to service conditions, system of obligations and responsibilities or limitations of use may lead to a change in service policy and identification (OID), as well as the link to a new service policy statement. In this case, Izenpe may establish a mechanism to inform of proposed changes and, if applicable, to collect opinions from affected parties.

9.13. Complaints and resolving disputes

See the pertinent section in the CPS.

9.14. Applicable regulations

See the pertinent section in the CPS.

9.15. Meeting applicable regulations

Izenpe states its commitment to meet applicable regulations and requirements for each type of website authentication certificate, including the considerations set forth in section "1.5.4. CPS approval procedure" of this CP document.

9.16. Miscellaneous stipulations

9.16.1. Comprehensive agreement

See the pertinent section in the CPS.

9.16.2. Assignation

See the pertinent section in the CPS.

9.16.3. Severability

See the pertinent section in the CPS.

9.16.4. Compliance

See the pertinent section in the CPS.

9.16.5. Force Majeure

See the pertinent section in the CPS.

9.17. Other stipulations

See the pertinent section in the CPS.

CHANGE TRACKING

From version 0 to 1.0

	SECTION / CLARIFICATION
Updates to the previous version	Requirements in section 2.2 added Requirements in sections 2.1 and 2.2 updated
Clarifications	Requirements in sections 2.2
Format updates.	Table of contents added. Footnote added.
Eliminations.	Requirements in sections 2.1 and 2.2 eliminated Year eliminated on cover page

From version 1.0 to 1.1

	SECTION / CLARIFICATION
Updates to the previous version	Domain validation requirements updated, in section 2.2
Eliminations.	Graphs in sections 2.3 and 2.6 eliminated.

From version 1.1 to 1.2

	SECTION / CLARIFICATION
Updates to the previous version	CAA validation requirements updated, in section 2.2.

From version 1.2 to 1.3

	SECTION / CLARIFICATION
Updates to the previous version	– 1. Introduction. Within the scope of the Google Certificate Transparency project, all SSL EV and Office EV certificates issued will be published on the log server providers' CT service, with whom Izenpe has signed an agreement. – 1.1. Description of certificates. ▪ Updated standards regarding stamp certificate regulation. ▪ Updated certificate validity, which may be 1 or 2 years – 1.2. Identification ▪ OID CA/B FORUM are included ▪ The certificates' serial numbers will have at least 64 bits of entropy – Sections 1.3 and following. Adaptation of terminology to issue of EV certificates to private entities. – 14. General Provisions, ▪ Identification obligations. It is stated that all Izenpe cases verify ownership or control over the domain. ▪ Obligations of certificate subscribers. Those determined in the Public Key Dissemination Agreement (PDS) are included. – Sections 1, 2, 3 and 3. Inclusion of clarifications regarding BR compliance.

From version 1.3 to 1.4

Updates to the previous version	The SSL-EV and Office-EV certificate policy OID was updated In section "1.1 Certificate description," it is stated that the qualified SSL EV and qualified Office EV certificates are considered qualified, according to eIDAS The introduction states that ALL certificates will be published in the CTs

Eliminations.	All references to office certificate were eliminated

From version 1.4 to 1.5

Updates to the previous version	Qualified profiles were added

From version 1.5 to 1.6

Change	Section
The following domain ownership verification methods have been added: • Constructed email to the domain contact • Email to DNS CAA contact • Email to DNS TXT contact • DNS Lookup	2.2
Causes and deadlines for revocation set forth both for final and subCAs	2.6

From version 1.6 to 1.7

Change	Section
The test certificate routes were added (living, revoked, expired)	1 Introduction
The EVs were deleted from the profiles that Izenpe currently issues	1.1 Certificate description
It is specified that Izenpe's public CAs are not issued for internal domains Verification of RSA key parameters was added The definition of "pre-certificate" was added	2.2 Request Procedure
The revocation procedure is eliminated, and one is rerouted to the CPS	2.6 Certificate revocation

The obligation to increase in the version number even if there are no changes is added	3	Change management

From version 1.7 to 1.8

Change	Section
The document was adapted to the RFC 3647 structure	The entire document