CERTIFICATION POLICY FOR WEBSITE AUTHENTICATION CERTIFICATES.

ZIURTAPEN ETA ZERBITZU ENPRESA-EMPRESA DE CERTIFICACION Y SERVIC

Firmado digitalmente por ZIURTAPEN ETA ZERBITZU ENPRESA-EMPRESA DE CERTIFICACION Y SERVIC
Fecha: 2021.10.18 09:41:02 +02'00'

Reference: Certification policy: Seal issued at the level of the administration.
Version No.: v 2.0

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

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

TRACK CHANGES

VERSION	CHANGE
1.0	– Requirements added to section 2.2 – Requirements updated in sections 2.1 and 2.2 – Requirements updated in section 2.2 – Index added. – Footer added. – Requirements deleted in sections 2.1 and 2.2 – Year deleted from cover page
1.1	– Updated requirements in domain validation, in section 2.2. – Figures deleted in sections 2.3 and 2.6
1.2	– Updated requirements in CAA validation, in section 2.2.

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

1.7	• checking of RSA key parameters • Addition of the definition of 'pre-certificate' • obligation to increment the version number, even if no changes have been made – The following were removed: • EVs from among the profiles currently issued by Izenpe • Revocation procedure, and redirects to the CPS – It is specified that Izenpe's public CAs do not issue for internal domains.
1.8	The document has been adapted to the structure of RFC 3647
1.9	– The change control section was replaced with this version history table – The lifetime of all profiles was updated to 395 days – The DNS CAA method was removed – The whois method was added for .eus
2.0	– Removal of references to qualified HQ and EV SSL certificates – Update of Izenpe's postal and e-mail address – Revision of the wording of the policy.

INDEX

1. INTRODUCTION

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

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

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

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

Within the scope of the Google Certificate Transparency project, all SSL certificates issued will be published on the CT service of the Log Servers providers with which Izenpe has an agreement.

Izenpe maintains test websites for software vendors to assess their products with SSL/TLS certificates in production environment. Izenpe maintains different sites with at least one live, expired and revoked final certificate:

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

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

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

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

  The validity of these certificates is 395 days.

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

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

- The validity of these certificates is 395 days. *SSL QUALIFIED (**SSL QUALIFIED**),*

  This certificate is considered as qualified according to Regulation (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS

Regulation). It will be used for the identification of domain ownership and accreditation of the organisation, providing robust assurance to the user of an Internet browser that the website they are accessing is owned by the organisation identified in the certificate.

The validity of these certificates is 395 days.

1.1. Purpose

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

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

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

This is part of the Izenpe CPS. In the event of any contradiction between this document and the provisions of the CPS, the provisions of this document shall take precedence.

1.2. Document name and identification

This document is called 'Certification Policy for Website Authentication Certificates.'

- Version: 2.0
- Issuance date: 06 October 2021
- Location:http://www.izenpe.eus/s15-content/es/contenidos/informacion/doc_especifica/es_def/index.shtml
- Related CPS: Izenpe Certification Practices Statement.

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

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

1.3. Parties involved

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

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

1.3.1. Certification Authority

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

Type	CN	SHA1 Footprint
Root	Izenpe.com	2f783d255218a74a653971b52ca29c45156fe919
Subordinate	EAEko Herri Administrazioen CA - CA AAPP Vascas (2)	f79cda11e7917419a0418db84ba743c5313ad7f0
Subordinate	Certificate CA EV SSL	6c484d0f4db295ec67ebb3e05e3dc214492a9ab8
Subordinate	Certificate CA EV SSL	c68bade5f069778a003074e619dab2e7928342d5

ROOT CERTIFICATION AUTHORITY

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

ROOT CA	
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
O	IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
subjectKeyIdentifier	1d1c650ea8f2257bb491cfe4b1b1e6bd55746c05
keyUsage	Certificate signing, Offline CRL signing, Certificate revocation list (CRL) signing (06)

SUBORDINATE CERTIFICATION AUTHORITY

EAEko Herri Administrazioen CA - CA AAPP Vascas (2)	
Field / extension	**Content**
version	Version 3
serialNumber	24c5c8aa566f8ee84cbea7055ce164a4
signature	sha256WithRSAEncryption
issuer	
CN	Izenpe.com
O	IZENPE S.A.
C	ES

validity	13 December 2037
subject	
CN	EAEko Herri Administrazioen CA - CA AAPP Vascas (2)
OU	AZZ Ziurtagiri publikoa - Certificado publico SCA
O	IZENPE S.A.
C	ES
subjectPublicKeyInfo	RSA 4096 bits
extensions	
subjectAltName	
rfc822Name	info@izenpe.com
directoryName	
STREET	Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz
O	IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
subjectKeyIdentifier	c0a94af7472587ffbcb5a689ce82d246a889eba3
authorityKeyIdentifier	Key ID=1d1c650ea8f2257bb491cfe4b1b1e6bd55746c05
certificatePolicies	
policyIdentifier	All issuance directives
Directive certifier ID	CPS
cpsURI	http://www.izenpe.eus/cps
authorityInfoAccess	
Access method	Online certificate status protocol (1.3.6.1.5.5.7.48.1)
Alternative name	
URL address	http://ocsp.izenpe.com:8094
cRLDistributionPoints	http://crl.izenpe.com/cgi-bin/arl2
keyUsage	Certificate signing, Offline CRL signing, Certificate revocation list (CRL) signing (06)
Digital footprint	f79cda11e7917419a0418db84ba743c5313ad7f0

Certificate CA EV SSL 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	Certificate CA EV SSL
OU	BZ Ziurtagiri publikoa - Certificado publico EV
O	IZENPE S.A.
C	ES
subjectPublicKeyInfo	RSA 4096 bits
extensions	
subjectAltName	
rfc822Name	info@izenpe.com
directoryName	
STREET	Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz
O	IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
subjectKeyIdentifier	a6ce69692ea621353b3acf0af12e3f15ac199027
authorityKeyIdentifier	Key ID=1d1c650ea8f2257bb491cfe4b1b1e6bd55746c05
certificatePolicies	
policyIdentifier	All issuance directives
Directive certifier ID	CPS
cpsURI	http://www.izenpe.eus/cps
authorityInfoAccess	
Access method	Online certificate status protocol (1.3.6.1.5.5.7.48.1)
Alternative name	
URL address	http://ocsp.izenpe.com
cRLDistributionPoints	http://crl.izenpe.com/cgi-bin/arl2
keyUsage	Certificate signing, Offline CRL signing, Certificate revocation list (CRL) signing (06)
Digital footprint	6c484d0f4db295ec67ebb3e05e3dc214492a9ab8

Certificate CA EV SSL 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	Certificate CA EV SSL
OU	BZ Ziurtagiri publikoa - Certificado publico EV
O	IZENPE S.A.
C	ES
subjectPublicKeyInfo	RSA 4096 bits
extensions	
subjectAltName	
rfc822Name	info@izenpe.com
directoryName	
STREET	Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz
O	IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
subjectKeyIdentifier	c6edfe77fb51564dfcabd5e3b10c13a3bf54e39b
authorityKeyIdentifier	Key ID=1d1c650ea8f2257bb491cfe4b1b1e6bd55746c05
certificatePolicies	
policyIdentifier	All issuance directives
Directive certifier ID	CPS
cpsURI	http://www.izenpe.eus/cps
authorityInfoAccess	
Access method	Online certificate status protocol (1.3.6.1.5.5.7.48.1)
Alternative name	

URL address	http://ocsp.izenpe.com
cRLDistributionPoints	http://crl.izenpe.com/cgi-bin/arl2
keyUsage	Certificate signing, Offline CRL signing, Certificate revocation list (CRL) signing (06)
Digital footprint	c68bade5f069778a003074e619dab2e7928342d5

1.3.2. Registration Authority

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

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

1.3.3. Certificate Subscribers

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

I

1.3.4. Relying Parties

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

1.3.5. Other participants

Not provided

1.4. Certificate uses

1.4.1. Permitted uses of the certificates

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

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

1.4.2. Restrictions on the use of certificates

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

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

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

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

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

1.5. Policy Management

1.5.1. Responsible entity

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

1.5.2. Contact details

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

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

1.5.3. Adaptation managers

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

1.5.4. Approval procedure

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

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

1.6. Definitions and Acronyms

1.6.1. Definitions

- Website authentication certificate: certificate that allows authenticating a website and linking the website to the natural or legal person to whom the Certificate has been issued.
- OV Certificate: website authentication certificate issued in accordance with the Organisation Validation Policy (OVCP), providing reasonable assurance to the Internet browser user that the owner of the website being accessed is the same as the Organisation identified by the OV Certificate. This Certificate complies with the requirements of the European standard 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 subdomains, starting from the third level, with a single Website Authentication Certificate.
- Qualified Web Authentication Certificate: This certificate is considered qualified according to eIDAS. It will be used for domain ownership identification and organisation accreditation, providing a strong assurance to an Internet browser user that the website they are accessing is owned by the organisation identified in the certificate.
- *Certificate Transparency (CT):* is an open framework for the supervision of website authentication Certificates, so that when one of these Certificates is issued, it is published in CT records, thus making it possible for domain owners to supervise the issuance of the same for their domains and detect erroneously issued certificates.
- *Declaration of Certification Practices (DPC*): declaration made available to the public by Izenpe that is easily accessible electronically and free of charge. It is considered a security document that details, within the eIDAS framework, the obligations that Trusted Service Providers undertake to comply with in relation to the management of signature creation and verification data and electronic certificates, the conditions applicable to the request, issue, use and termination of the validity of the Certificates, the technical and organisational security measures, the profiles and the information mechanisms on the validity of the Certificates.

- *Certificate policy*: policy that applies to the issuance of a specific set of certificates issued by Izenpe under the specific conditions set out therein.
- *Certificate Incident Report*: a complaint of suspected key compromise, certificate misuse or other types of fraud, compromise, misuse, or misconduct related to certificates.
- *Supervisory Body*: Body designated by a Member State as responsible for the supervisory functions in relation to the provision of trust services, in accordance with Article 17 of the eIDAS Regulation. In Spain, it is currently the Ministry of Economic Affairs and Digital Transformation.
- *CAA registry (CAA records)*: DNS (Domain Name System) resource registry of Certification Authority Authorisation (CAA). It allows a DNS domain name holder to specify the Certificate Authorities (CAs)

authorised to issue certificates for that domain.

Publication of CAA resource records allows a domain name registrant to implement additional controls to reduce the risk of unauthorised issuance of a Website Authentication Certificate for their domain name.

- *Subscriber Representative*: natural person authorised by the subscriber to process the certificate.
- *Subscriber*: legal person, public body or organisation receiving Izenpe's activities as a Trusted Service Provider, which subscribes to the terms and conditions of the service. Under this Certification Policy, this service consists of the issuing of website authentication Certificates. The Subscriber is referred to in the Subject field of the Certificate and is the holder and responsible for its use and has exclusive control and decision-making power over it.

1.6.2. Acronyms

For the purposes of this CP, the following acronyms apply, the meaning of which is in accordance with the European standard ETSI EN 319 411 'Policy and security requirements for Trust Service Providers issuing certificates':

CA: Certification Authority

RA: Registration Authority

ARL: Authority Revocation List

CN: Common Name

CRL: Certificate Revocation List

DN: Distinguished Name

DPC: Certification Practices Statement

eIDAS: Regulation 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

EV: Extended Validation.

ETSI: European Telecommunications Standards Institute

HSM: Hardware Security Module. A security device that generates and protects cryptographic keys.

OCSP: Online Certificate Status Protocol

OID: Object IDentifier

OV: Organisational Validation.

PDS: PKI Disclosure Statement.

PIN: Personal Identification Number.

PKCS: Public Key Cryptography Standards.

TLS/SSL: Transport Layer Security/Secure Socket Layer protocol.

UTC: Coordinated Universal Time.

2. PUBLICATION AND REPOSITORIES

2.1. Repository

Izenpe has a public information repository at www.izenpe.eus, available 24 hours a day, 7 days a week.

2.2. Publication of certification information

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

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

2.3. Frequency of publication

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

Any changes to the CPS or to this document will be published immediately.

The frequency of publication of CRLs is defined in section '4.9.7 Frequency of CRL generation' of the CPS.

2.4. Access control to the repositories

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

Izenpe employs reliable systems for access to the information repository so that:

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

3. IDENTIFICATION AND AUTHENTICATION

3.1. Name

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

Additionally, for qualified SSL certificates, Izenpe will comply with the requirements established in section 9.2 of CABForum in its 'guide for the issuance and management of Extended Validation Certificates,' which can be consulted at https://cabforum.org/extended-validation/.

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

3.1.1. Types of names

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

The Common Name field defines the certificate subscriber.

3.1.2. Meaning of names

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

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

3.1.3. Pseudonyms

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

3.1.4. Rules used to interpret various name formats

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

3.1.5. Uniqueness of names

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

3.1.6. Trademark recognition and authentication

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

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

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

3.2. Initial identity validation

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

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

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

3.2.1. Methods for proving possession of the private key

Izenpe receives a certificate request, in PKCS#10 format, digitally signed by the private key generated by the subscriber's representative in its environment.

Before issuing the certificate, Izenpe verifies this signature, guaranteeing that the public key included in the request corresponds to the private key generated by the person responsible for the certificate.

3.2.2. Authentication of the Organisation's Identity

3.2.2.1 Identity

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

– In the case of DV certificates

– Izenpe does not check the identity or any type of information about the organisation. In the case of OV certificates

Izenpe verifies the postal address and the identity of the subscribing organisation depending on the type of organisation (private or public).

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

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

– In the case of qualified SSL certificates

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

- When the subscriber is a private sector organisation, Izenpe verifies its address and identity by consulting the corresponding official register.
- In the case of public entities, verification is conducted by consulting the corresponding Official Gazette and other consulted registers.
- If the nature of the subscriber is different from the two previous cases, the verifications relating to existence, address and identity will be conducted by consulting the corresponding official source.

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

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

3.2.2.2.2 Trade name or registered trademark

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

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

3.2.2.3 Country Verification

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

3.2.2.2.4 Validation of authorisation and domain control

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

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

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

a) Email to Domain Contact (BR 3.2.2.4.2): Izenpe sends the applicant a unique, random code by email to any of the addresses listed in the whois contact (Registrant, administrative or technical). The reply must include the random number.

   Each email can confirm control of multiple domain names.

   Izenpe may resend the email in its entirety, including the reuse of the random code, as long as the full content of the communication and the recipients remain valid.

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

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

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

c) Email to DNS CAA contact (BR 3.2.2.4.13): Izenpe sends the applicant a unique and random code by email to the address that appears in the DNS CAA record.

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

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

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

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

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

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

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

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

3.2.2.5 Authentication for an IP address

Izenpe does not issue certificates to identify IP addresses.

3.2.2.6 Wildcard Domain Validation

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

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

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

3.2.2.7 Reliability of data sources

Before using any data source as a reliable data source, the RA shall evaluate the source for reliability, accuracy and resistance to alteration or falsification.

3.2.2.8 CAA Registration

Prior to the issuance of any SSL certificate, Izenpe validates the existence of a CAA record for each DNS name of the CN and subjectAltName extensions of the certificate, as specified in RFC 6844. In case the certificate is issued, the validation will be done before the TTL of the CAA record, and in any case no longer than 8 hours. Izenpe processes the 'issue' and 'issuewild' tags.

The CAA records that identify domains for which Izenpe is authorised to issue certificates are 'izenpe.com' and 'izenpe.eus.'

3.2.3. Authentication of the identity of the natural person applicant

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

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

3.2.4. Unverified Subscriber information

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

3.2.5. Validation of representative capacity

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

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

For requests for qualified SSL certificates, Izenpe will comply with the requirements defined by the CA/Browser Forum entity in its 'guide for the issuance and management of Extended Validation Certificates' (sections 11.8 and 11.11).

3.2.6. Interoperability criteria

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

3.3. Identification and authentication for key renewal requests

3.3.1. Identification and authentication for routine key renewal

Certificate subscribers should request the renewal of their certificates before their period of validity expires.

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

The validity of the applicant's entity and competence will not be required if it has been verified by Izenpe in the last 13 months.

3.3.2. Identification and authentication for key renewal after revocation

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

3.4. Identification and authentication for revocation requests

The conditions for authentication of a revocation request are developed in section 4.9 of this document.

4. OPERATIONAL REQUIREMENTS FOR THE LIFECYCLE OF CERTIFICATES

4.1. Certificate Application

4.1.1. Who can apply for a Certificate?

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

Additionally, for qualified certificates, Izenpe will comply with the requirements of section 11 of the 'Guide for the issuance and management of Extended Validation Certificates' established by the CA/Browser forum.

4.1.2. Registration process and responsibilities

Each applicant must apply for a certificate and the required information before a certificate can be issued.

The registration process includes the following phases:

- ✓ Submission of the application for issuance and acceptance of the applicable terms and conditions.

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

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

Those non-public entities whose incorporation information is not available for consultation in the Companies Register must provide:

- ✓ Copy of the publication in the corresponding register
- ✓ Copy of the CIF

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

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

4.2. Certificate application procedure

4.2.1. Carrying out the identification and authentication functions

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

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

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

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

4.2.2. Approval or rejection of the certificate request

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

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

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

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

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

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

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

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

4.2.3. Application processing time

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

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

4.3. Certificate issuance

4.3.1. CA actions during issuance

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

Likewise, Izenpe periodically monitors deviations in the certificates issued.

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

4.3.2. Notification of certificate issue

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

4.4. Certificate acceptance

4.4.1. Acceptance process

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

4.4.2. Publication of the certificate by the CA

The generated Certificates are stored in a secure repository belonging to Izenpe.

4.4.3. Notification of issuance to other entities

Prior to the issuance of Website Authentication Certificates, a pre-certificate is sent to the Certificate Transparency service registers of those providers with whom Izenpe has an agreement for this purpose.

4.5. Key pair and certificate use

4.5.1. Subscriber's private key and use of the certificate

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

4.5.2. Use of the certificate and the public key by trusted third parties

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

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

4.6. Certificate revocation

4.6.1. Circumstances for certificate renewal

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

4.6.2. Who may apply for certificate renewal?

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

4.6.3. Processing of certificate renewal applications

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

4.6.4. Notification of certificate renewal

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

4.6.5. Conduct constituting acceptance of the renewal of the certificate

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

4.6.6. Publication of the renewed certificate

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

4.6.7. Notification of certificate renewal to other entities

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

4.7. Renewal with certificate key regeneration

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

4.7.1. Circumstances for renewal with key regeneration

Certificate keys will be renewed under the following circumstances:

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

4.7.2. Who can apply for renewal with key regeneration?

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

4.7.3. Processing of renewal applications with key regeneration

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

4.7.4. Notification of renewal with key regeneration

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

4.7.5. Conduct constituting acceptance of renewal with key regeneration

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

4.7.6. Publication of the renewed certificate

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

4.7.7. Notification of renewal with key regeneration to other entities

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

4.8. Modification of the certificate

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

4.8.1. Circumstances for certificate modification

Modification is not stipulated.

4.8.2. Who may apply for certificate modification?

Modification is not stipulated.

4.8.3. Processing of certificate modification applications

Modification is not stipulated.

4.8.4. Notification of certificate modification

Modification is not stipulated.

4.8.5. Conduct constituting acceptance of the certificate modification

Modification is not stipulated.

4.8.6. Publication of the modified certificate

Modification is not stipulated.

4.8.7. Notification of certificate modification to other entities

Modification is not stipulated.

4.9. Revocation and suspension of the certificate

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

a) Termination of the validity period of the certificate.

b) Cessation of activity as a Trusted Service Provider of Izenpe, unless, with the express consent of the subscriber, the certificates issued by Izenpe have been transferred to another Trusted Service Provider.

In cases a) and b), the loss of effectiveness of the certificates will take place as soon as these circumstances arise.

c) Revocation of the certificate for any of the reasons listed in this document.

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

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

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

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

4.9.1. Circumstances for revocation

4.9.1.1 Grounds for revocation of an End Entity Certificate

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

a) The request for revocation by authorised persons. In any case, this request must be made:

- The loss of the certificate medium.
- The use by a third party of the private key associated with the certificate.
- The violation or compromise of the secrecy of the private key associated with the certificate.
- Non-acceptance of the new conditions that may imply the issuing of new Certification Practice Statements, during the period of one month after their publication.

b) Judicial or administrative resolution ordering it.

c) Extinction, dissolution, or closure of the website identified by the certificate.

d) Extinction or dissolution of the subscriber's legal personality.

e) Termination of the form of representation of the certificate subscriber's representative.

f) Total or partial incapacity of the Subscriber's representative.

g) Inaccuracies in the data provided by the Subscriber's Representative to obtain the certificate, or alteration of the data provided to obtain the certificate or modification of the circumstances verified for the issuance of the certificate, such that the certificate no longer conforms to reality.

h) Contravention of a substantial obligation of this Certification Practice Statement by the subscriber, the subscriber's representative, or a Registration Entity if, in the latter case, it could have affected the procedure for issuing the Certificate.

i) Using the certificate for the purpose of generating doubts among users about the origin of the products or services offered, making it appear that their origin is different from that actually offered. To this end, the criteria on infringing activity of the regulations on consumers and users, trade, competition, and advertising will be followed.

j) Termination of the contract signed between the subscriber or their representative and Izenpe, or non-payment of the services provided.

k) Violation or endangerment of the secrecy of Izenpe's signature/seal creation data, with which it signs/seals the certificates it issues.

l) Non-compliance with the requirements defined by the audit schemes to which the Certification Authority issuing the certificates covered by this Policy is subject, with special attention to those of algorithm and key sizes, which entail an unacceptable risk for the parties that trust these Certificates.

Under no circumstances should it be understood that Izenpe assumes any obligation to check the points mentioned in letters c) to i) of this section.

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

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

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

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

4.9.1.2 Causes for revocation of a Sub CA certificate

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

a) The Sub CA requests it in writing

b) The Sub CA notifies the issuing CA that the original certificate request was not authorised and does not allow retroactive authorisation.

c) The issuing CA obtains evidence that the Sub CA's private key corresponding to the certificate's public key has been compromised or no longer meets the requirements of sections 6.1.5 and 6.1.6 of the BRs.

d) The issuing CA obtains evidence that the certificate was incorrectly issued.

e) The issuing CA detects that the certificate was not issued in accordance with the Certificate Policy or the CPS.

f) The issuing CA determines that information in the certificate is inaccurate or incorrect

g) The issuing CA or sub CA ceases operations for any reason and has not enabled arrangements with another CA to provide the revocation service.

h) The right to issue certificates by the issuing CA or sub CA under the BR requirements is terminated or revoked, unless the issuing CA has enabled arrangements to continue to maintain the CRL/OCSP repository.

i) Revocation is required by the issuing CA's policy and/or by the CPS.

j) The content or technical format of the certificate presents an unacceptable risk to software vendors or third parties.

k) Providers or third parties (e.g., the CA/Browser Forum may determine that a cryptographic algorithm/signature or key size presents an unacceptable risk and that such certificates should be revoked and replaced within a specified period of time).

4.9.2. Who can request revocation?

The CA, RA and Subscribers can initiate the revocation of a certificate.

The revocation of a Website Authentication Certificate may only be requested by the person authorised to represent the Subscriber to whom the Certificate has been issued.

In addition, they shall be entitled to request the revocation of said certificate:

- The governing body, body or entity subscribing the certificate, or the person delegated by it.
- The Registration Office–through its manager–designated for this purpose by the Administration, body or entity under public law, Subscriber of the Certificate to be revoked, when it detects that any of the data contained in the certificate
  - ✓ is incorrect, inaccurate or has changed with respect to what is stated in the Certificate, or
  - ✓ the natural person, the custodian of the Certificate, does not correspond to the person responsible or designated for the management and administration of the electronic address stated in the Certificate that is the subject of the revocation

  always within the framework of the terms and conditions applicable to the revocation of this type of Certificate.

Additionally, Subscribers, relying parties, application software providers and other third parties may inform the issuing CA of reasonable cause to revoke the Certificate by submitting a Certificate Incident Report.

However, Izenpe may revoke ex officio Website Authentication Certificates in the cases set out in this Certification Policy and Practice Statement.

Furthermore, in the case of the certificates regulated in this specific documentation, Izenpe,

1. Will provide the Subscriber, third parties and Internet browsers with clear instructions for the submission of complaints or suspicions of compromise of the private key, misuse of certificates or other types of fraud, compromise, misuse, or improper conduct in relation to the certificates.

2. Will investigate problem reports within twenty-four hours of receipt and decide on revocation, based on the following criteria:

    - The nature of the alleged problem;
    - The number of problem reports received for a certificate or web page.
    - The identity of the complainants.
    - The legislation in force.

4.9.3. Revocation application procedure

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

The applicant may revoke the certificate through the following channels,

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

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

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

4.9.4. Grace period for the revocation request

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

4.9.5. Time period for processing the revocation request

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

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

4.9.6. Obligation to verify revocations by relying parties

Third parties who trust and accept the use of certificates issued by Izenpe are obliged to verify:

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

4.9.7. Frequency of CRL generation

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

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

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

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

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

4.9.8. Maximum latency period for CRLs

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

4.9.9. Availability of the online verification system for the status of certificates

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

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

4.9.10. On-line revocation verification requirements

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

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

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

The use of the freely available OCSP service will require:

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

4.9.11. Other forms of revocation notice available

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

4.9.12. Special requirements for revocation of compromised keys

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

4.9.13. Circumstances for suspension

Suspension of certificates is not contemplated.

4.9.14. Who can request suspension?

Suspension of certificates is not contemplated.

4.9.15. Procedure for requesting suspension

Suspension of certificates is not contemplated.

4.9.16. Limits on the period of suspension

Suspension of certificates is not contemplated.

4.10. Certificate status information services

4.10.1. Operational characteristics

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

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

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

4.10.2. Service availability

Izenpe provides the User Entities with a 24x7 (24 hours a day, 7 days a week) revocation service.

4.10.3. Optional characteristics

Not stipulated.

4.11. Termination of subscription

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

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

4.12. Custody and recovery of keys

4.12.1. Key custody and recovery practices and policies

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

4.12.2. Session key protection and recovery practices and policies

Not stipulated.

5. PHYSICAL SECURITY, PROCEDURAL AND PERSONNEL CONTROLS

5.1. Physical Security Controls

5.1.1. Location of facilities

See the relevant section in the CPS

5.1.2. Physical Access

See the relevant section in the CPS

5.1.3. Electricity and Air Conditioning

See the relevant section in the CPS

5.1.4. Exposure to water

See the relevant section in the CPS

5.1.5. Fire Prevention and Protection

See the relevant section in the CPS

5.1.6. Media Storage

See the relevant section in the CPS

5.1.7. Waste Disposal

See the relevant section in the CPS

5.1.8. Off-site backups

See the relevant section in the CPS

5.2. Procedure Controls

5.2.1. Roles of Trust

See the relevant section in the CPS

5.2.2. Number of people per task

See the relevant section in the CPS

5.2.3. Identification and authentication for each role

See the relevant section in the CPS

5.2.4. Roles requiring segregation of duties

See the relevant section in the CPS

5.3. Personnel Controls

5.3.1. Knowledge, qualifications, experience, and accreditation requirements

See the relevant section in the CPS

5.3.2. Background check procedures

See the relevant section in the CPS

5.3.3. Training requirements

See the relevant section in the CPS

5.3.4. Training requirements and frequency

See the relevant section in the CPS

5.3.5. Sequence and frequency of job rotation

See the relevant section in the CPS

5.3.6. Penalties for unauthorised actions

See the relevant section in the CPS

5.3.7. Recruitment requirements

See the relevant section in the CPS

5.3.8. Provision of documentation to staff

See the relevant section in the CPS

5.4. Audit procedures

5.4.1. Types of registered events

See the relevant section in the CPS

5.4.2. Record processing frequency

See the relevant section in the CPS

5.4.3. Record retention period

See the relevant section in the CPS

5.4.4. Record protection

See the relevant section in the CPS

5.4.5. Procedures for backing up audited records

See the relevant section in the CPS

5.4.6. Record collection systems

See the relevant section in the CPS

5.4.7. Notification to the subject causing the events

See the relevant section in the CPS

5.4.8. Vulnerability analysis

See the relevant section in the CPS

5.5. Archiving of records

5.5.1. Types of archived records

See the relevant section in the CPS

5.5.2. File retention period

See the relevant section in the CPS

5.5.3. File protection

See the relevant section in the CPS

5.5.4. Archive backup procedures

See the relevant section in the CPS

5.5.5. Requirements for the timestamping of Records

See the relevant section in the CPS

5.5.6. Filing system

See the relevant section in the CPS

5.5.7. Procedures for obtaining and verifying archived information

See the relevant section in the CPS

5.6. CA key change

See the relevant section in the CPS

5.7. Incident and vulnerability management

5.7.1. Incident and vulnerability management

See the relevant section in the CPS

5.7.2. Dealing with corrupted data and software

See the relevant section in the CPS

5.7.3. Procedure in case of compromise of the CA's private key

See the relevant section in the CPS

5.7.4. Business continuity after a disaster

See the relevant section in the CPS

5.8. Termination of the Trusted Service Provider's activity

See the relevant section in the CPS

6. TECHNICAL SAFEGUARDS

6.1. Generation and installation of Keys

6.1.1. Key pair generation

6.1.1.1 CA Key pair generation

See the relevant section in the CPS

6.1.1.2 RA Key Pair Generation

Not provided

6.1.1.3 Subscriber Key Pair Generation

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

6.1.2. Sending the private key to the subscriber

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

6.1.3. Sending the public key to the certificate issuer

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

6.1.4. Distribution of the CA's public key to relying parties

The public keys of the IZENPE CAs are distributed through various means, including the IZENPE website www.izenpe.eus. In the CPS, sections 1.3.1.1 and 1.3.1.2, the different footprints of the root CAs and issuing CAs are also published.

6.1.5. Key sizes and algorithms used

The algorithm used in all cases is RSA with SHA2.

As for the size of the keys, 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 and Quality Assurance Parameters

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

6.1.7. Supported Key Usages (KeyUsage field X.509v3)

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

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

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

6.2. Private key protection and cryptographic module controls

6.2.1. Standards for cryptographic modules

See the relevant section in the CPS.

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

See the relevant section in the CPS.

6.2.3. Private key custody

See the relevant section in the CPS.

6.2.4. Private key backup

See the relevant section in the CPS.

6.2.5. Private key archiving

See the relevant section in the CPS.

6.2.6. Private key transfer to/from the cryptographic module

See the relevant section in the CPS.

6.2.7. Storage of the private key in the cryptographic module

See the relevant section in the CPS.

6.2.8. Private key activation method

See the relevant section in the CPS.

6.2.9. Private key deactivation method

See the relevant section in the CPS.

6.2.10. Private key destruction method

See the relevant section in the CPS.

6.2.11. Classification of cryptographic modules

See the relevant section in the CPS.

6.3. Other aspects of key pair management

6.3.1. Public key archiving

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

6.3.2. Certificate operating periods and key pair usage periods

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

- Root CA Certificate and its key pair: see section '1.3.1.

  Certification Authority' of this CP.

- The Certificate of the Sub CA issuing the Web Site Authentication Certificates and its key pair: see section '1.3.1.

  Certification Authority' of this CP.

- The Web Site Authentication Certificates and their key pair: the maximum period of validity is 395 days.

6.4. Activation data

6.4.1. Generation and installation of activation data

See the relevant section in the CPS.

6.4.2. Activation data protection

See the relevant section in the CPS.

6.4.3. Other aspects of the activation data

See the relevant section in the CPS.

6.5. Computer security controls

6.5.1. Specific technical requirements for computer security

See the relevant section in the CPS.

6.5.2. Assessment of the level of IT security

See the relevant section in the CPS.

6.6. Life cycle engineering controls

6.6.1. System development controls

See the relevant section in the CPS.

6.6.2. Security management controls

See the relevant section in the CPS.

6.6.3. Life cycle security controls

See the relevant section in the CPS.

6.7. Network security controls

See the relevant section in the CPS.

6.8. Time source

See the relevant section in the CPS.

7. CERTIFICATE, CRL AND OCSP PROFILES

7.1. Certificate profile

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

They include the following CABForum policy identifiers:

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

7.1.1. Version number

Website Authentication Certificates are compliant with the X.509 version 3 standard.

7.1.2. Certificate extensions

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

7.1.3. Algorithm object identifiers

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

7.1.4. Name Formats

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

7.1.5. Name restrictions

Sub CAs issuing 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 the one defined in section '1.2 Document name and identification' of this document.

7.1.7. Use of extension policy restrictions

No policy restrictions are used.

7.1.8. Syntax and semantics of policy qualifiers

The Certificate Policies extension contains the following policy qualifiers:

- **CPS Pointer**: contains a pointer to the IZENPE Certification Practice Statement,http://www.Izenpe.com/cps
- **User notice:** Text note that is displayed on the screen, at the request of an application or user, when a third party verifies the certificate.
- **Policy Identifier**: Indicates the OID of the certificate

User Notice common to all certificates (except SSL certificates):

USER NOTICE	Kontsulta www.izenpe.com-en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consult www.izenpe.com for terms and conditions before using or relying on the certificate.

7.1.9. Semantic treatment for the 'Certificate policy' extension.

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

7.2. CRL Profile

The certificates issued by IZENPE conform to the following standards:

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

7.2.1. Version number

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

7.2.2. CRL and extensions

The extensions used are as follows:

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

7.3.1. Version number

Version 2.0

7.3.2. OCSP Extensions

See the relevant section in the CPS

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

8. COMPLIANCE AUDITS

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

- European standards ETSI EN 319 401 'General Policy Requirements for Trust Service Providers' and ETSI EN 319 411-1 'Policy and security requirements for Trust Service Providers issuing certificates'.

- ETSI EN 319 411-2 'Requirements for trust service providers issuing EU qualified certificates'.

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

- ✓ Audit of the Information Security Management System in accordance with UNE-ISO/IEC 27001 'Information Security Management Systems (ISMS) Requirements'.

- ✓ Audit in accordance with the National Security Scheme (Royal Decree 3/2010, of 8 January, which regulates the National Security Scheme in the field of e-Government).

- ✓ Audit in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC, and Organic Law 3/2018, of 5 December, on the Protection of Personal Data and guarantee of digital rights (RGPD/LOPD-GDD).

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

8.1. Audit frequency

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

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

8.2. Auditor qualifications

See the relevant section in the CPS.

8.3. Relationship of the auditor with the audited company

See the relevant section in the CPS.

8.4. Elements to be audited

See the relevant section in the CPS.

8.5. Decision-making when deficiencies are detected

See the relevant section in the CPS.

Security incidents are managed by the Izenpe Security Committee.

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

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

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

8.6. Communication of results

See the relevant section in the CPS.

8.7. Self-assessment

See the relevant section in the CPS.

9. OTHER LEGAL AND BUSINESS MATTERS

9.1. Fees

See the relevant section in the CPS.

9.1.1. Fees for the issue or renewal of certificates

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

9.1.2. Fees for access to certificates

Not stipulated.

9.1.3. Fees for access to status or revocation information

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

9.1.4. Fees for other services

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

9.1.5. Refund policy

Izenpe does not have a refund policy.

9.2. Financial responsibility

See the relevant section in the CPS.

9.2.1. Liability insurance

See the relevant section in the CPS.

9.2.2. Other assets

See the relevant section in the CPS.

9.2.3. Insurance and guarantees for end entities

See the relevant section in the CPS.

9.3. Information confidentiality

See the relevant section in the CPS.

9.3.1. Scope of confidential information

See the relevant section in the CPS.

9.3.2. Information not included in the scope

See the relevant section in the CPS.

9.3.3. Responsibility to protect confidential information

See the relevant section in the CPS.

9.4. Personal data protection

See the relevant section in the CPS.

9.4.1. Privacy Plan

See the relevant section in the CPS.

9.4.2. Information treated as private

See the relevant section in the CPS.

9.4.3. Information not considered private

See the relevant section in the CPS.

9.4.4. Responsibility to protect private information

See the relevant section in the CPS.

9.4.5. Notice and consent to use private information

See the relevant section in the CPS.

9.4.6. Disclosure pursuant to judicial or administrative process

See the relevant section in the CPS.

9.4.7. Other disclosure circumstances

See the relevant section in the CPS.

9.5. Intellectual property rights

See the relevant section in the CPS.

9.6. Obligations and guarantees

9.6.1. Obligations of the CA

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

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

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

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

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

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

- ✓ Check the identity and personal circumstances of the certificate applicant and the subscriber and/or its Representative and collect the statement that the applicant is authorised by the subscriber to make the application.

- ✓ In the registration process, check the data relating to the subscriber's legal personality and the Representative's capacity. All these checks shall be conducted in accordance with the provisions of this document and Izenpe's registration protocols and procedures.

- ✓ In the aforementioned verification processes, Izenpe may conduct verifications through the intervention of third parties with notarial powers or competent Registries.
- ✓ Verify that all the information contained in the certificate application corresponds to that provided by the applicant.
- ✓ Check that the applicant is in possession of the Private Key associated with the Public Key that is included in the certificate to be issued.
- ✓ Guarantee that the procedures followed ensure that the Private Keys corresponding to the website authentication certificates are generated without copies being made or stored by Izenpe.
- ✓ Communicate information to the subscriber, representative and applicant in such a way as to guarantee their confidentiality.
- ✓ Make available to the applicant, subscriber, Representative and other interested parties (Izenpe's Certification Practices Statement and any other relevant information for the development of the procedures related to the life cycle of the certificates covered by this Certification Policy in accordance with the applicable regulations.

9.6.2. Obligations of the RA

See the relevant section in the CPS.

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

The RA has the following obligations:

- ✓ In general, to follow the procedures established by Izenpe in the Certification Policy and Practices applicable to the performance of its Certificate management, issuance, and revocation functions and not to alter this framework.
- ✓ In particular, verify the identity, and any relevant personal circumstances for the determined purpose, of the certificate applicants, subscribers, and their Representatives, by any means permitted by law and in accordance with the general provisions of the CPS and, in particular, this Policy.
- ✓ Check that the ownership of the domain name corresponds to the identity of the Subscriber or, if applicable, obtain the Subscriber's authorisation, which shall be associated with the

- ✓ Website Authentication Certificate, by the means at its disposal that allow such ownership to be accredited, in accordance with the state of the art.

- ✓ Expressly state the subscriber's power of decision regarding the ownership of the domain of the website authentication certificate.

- ✓ Keep all the information and documentation relating to the certificates whose application, renewal, or revocation it manages for 15 years.

- ✓ Receive and manage applications via the application management application published at www.izenpe.eus.

- ✓ Diligently check the causes of revocation that may affect the validity of the certificates.

9.6.3. Obligations of subscribers

See the relevant section in the CPS.

For website authentication certificates, Subscribers must have control of the website domain name included in such Certificates and keep the associated Private Keys under their exclusive use.

The applicant and the Subscriber of Certificates issued under this CP are obliged to:

- ✓ Not use the certificate outside the limits specified in this particular Certification Policy and Practices.

- ✓ Not use the certificate in the event that the Trusted Service Provider has ceased its activity as the Certificate Authority that issued the certificate in question, especially in cases where the provider's Seal Creation Data may have been compromised, and this has been communicated.

- ✓ Provide truthful information when applying for Certificates and keep it updated, subscribing the contracts by a person with sufficient capacity.

- ✓ Not request for the Subject of the certificate distinctive signs, names or industrial or intellectual property rights of which it is not the owner, licensee or has demonstrable authorisation for their use.

- ✓ Act with diligence with regard to the custody and conservation of the Signature/Seal creation Data or any other sensitive information such as Keys, Certificate activation codes, access words, personal identification numbers, etc., as well as the Certificate media, which includes, in any case, not disclosing any of the aforementioned data.

- ✓ Be aware of and comply with the conditions of use of the Certificates foreseen in the conditions of use and in the Declaration of Certification Practices and, in particular, the limitations of use of the Certificates.

- ✓ Be aware of and comply with the modifications made to the Certification Practice Statement.

- ✓ Request the revocation of the corresponding Certificate, according to the procedure described in this document, diligently notifying Izenpe of the circumstances for the revocation or suspicion of loss of Confidentiality, disclosure, modification, or unauthorised use of the associated private Keys,

- ✓ Review the information contained in the Certificate and notify Izenpe of any errors or inaccuracies.

- ✓ Verify, prior to trusting the Certificates, the advanced electronic Signature or electronic Seal of the Trust Service Provider issuing the Certificate.

- ✓ Diligently notify Izenpe of any modification to the data provided in the application for the Certificate, requesting, when appropriate, the revocation of the same.

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

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

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

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

9.6.4. Obligations of the relying parties

It is the responsibility of the User Entity and the third parties that trust the certificates to verify and check the status of the certificates, and under no circumstances may they assume the validity of the certificates without such checks.

Likewise, it shall be the responsibility of the User Entity to observe the provisions of the Certification Practices Statement and its possible future modifications, with special attention to the limits of use established for the certificates in this Certification Policy.

See the relevant section in the CPS.

9.6.5. Obligations of other participants

Not stipulated.

9.7. Waiver of guarantees

Not stipulated.

9.8. Limits of liability

See the relevant section in the CPS.

9.9. Compensation

9.9.1. Indemnification of the CA

Not stipulated.

9.9.2. Indemnification of Subscribers

Not stipulated.

9.9.3. Indemnification of the relying parties

Not stipulated.

9.10. Validity of this document

9.10.1. Term

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

9.10.2. Termination

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

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

9.10.3. Effects of termination

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

9.11. Individual notifications and communication with participants

See the relevant section in the CPS.

9.12. Amendments to this document

9.12.1. Procedure for modifications

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

9.12.2. Notification period and mechanism

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

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

9.12.3. Circumstances under which an OID must be changed

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

9.13. Complaints and dispute resolution

See the relevant section in the CPS.

9.14. Applicable legislation

See the relevant section in the CPS.

9.15. Compliance with applicable legislation

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

9.16. Various stipulations

9.16.1. Full agreement

See the relevant section in the CPS.

9.16.2. Allocation

See the relevant section in the CPS.

9.16.3. Severability

See the relevant section in the CPS.

9.16.4. Compliance

See the relevant section in the CPS.

9.16.5. Force Majeure

See the relevant section in the CPS.

9.17. Other stipulations

See the relevant section in the CPS.