CERTIFICATE POLICY

SSL / TLS

June 2020

Version 1.7

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

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

TABLE OF CONTENTS

1 INTRODUCTION

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

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

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

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

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

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

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

1.1 Description of certificates

Izenpe issues these certificates in order to allow its subscribers to offer additional security in their web services.

Regarding the type of certificate that Izenpe issues,

SSL	ELECTRONIC OFFICE
SSL DV SSL OV SSL Qualified	Qualified Office

The purpose of this type of certificate is to establish data communications on web servers via SSL/TLS.

They provide for encrypting communications between the user and the website, facilitating the exchange of encryption keys needed to encrypt information on the Internet.

– *SSL CERTIFICATES*,

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

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

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

  These certificates may be valid for 1 or 2 years.

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

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

  These certificates may be valid for 1 or 2 years.

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

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

  These certificates may be valid for 1 or 2 years.

  Izenpe currently does not issue this kind of certificate.

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

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

  These certificates may be valid for 1 or 2 years.

– *ELECTRONIC OFFICE CERTIFICATES*

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

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

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

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

  These certificates are valid for 2 years.

  Izenpe currently does not issue this kind of certificate.

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

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

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

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

  These certificates are valid for 2 years.

1.2 Identification

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

CERTIFICATE	OID Izenpe	OID CA/B FORUM
SSL DV	1.3.6.1.4.1.14777.1.2.4	2.23.140.1.2.1
SSL OV	1.3.6.1.4.1.14777.1.2.1	2.23.140.1.2.2
SSL EV	1.3.6.1.4.1.14777.6.1.1	2.23.140.1.1
SSL Qualified	1.3.6.1.4.1.14777.6.1.3	2.23.140.1.1
EV office	1.3.6.1.4.1.14777.6.1.2	2.23.140.1.1
Qualified Office	1.3.6.1.4.1.14777.6.1.4	2.23.140.1.1

The certificates' serial numbers will have at least 64 bits of entropy.

1.3 Community and scope of use

The following are considered **users**,

- Certificate applicant, legal persona applying for a certificate. Once the certificate is issued, this individual is called a subscriber.
- Certificate subscriber, legal person identified on the certificate.

Scope of use. The certificates will be used within the scope of the responsibility of the organisation that owns the certificate.

1.4 General provisions

Identification obligations

Izenpe verifies the identity and any other personal circumstances of the certificate applicants and subscribers on its own or through the User Entities with which the subscriber subscribes to the corresponding legal instrument. Under no circumstances does Izenpe delegate verification of ownership or control over the domain.

The legal instrument between the parties shall include the requirement to comply with provisions in documents from the CA/*Browser Forum.*

Obligations of certificate subscribers

Subscriber obligations are set forth in the Certification Practises Statement and the Public Key Dissemination Agreement (PDS).

2 OPERATIONAL REQUIREMENTS

2.1 List of required documentation

- ✓ An application for issue must be provided, duly completed and electronically signed with a Representative or Izenpe Public Entity Personnel certificate, stating the position of the applicant. This signature shall not be necessary when the entity's legal representative delegates the ability to apply for SSL/TLS certificates. This delegation must be electronically signed by the legal representative, with a Representative or Izenpe Public Entity Personnel certificate, stating the position of the applicant.

- ✓ Except for SSL-DV certificate applications, non-public entities whose formation information is not available for consultation at the Commercial Registry must provide:

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

2.2 Application Procedure

- ➢ The Applicant shall send the issue application and required documentation,

    - Electronically to the email address certservidor@izenpe.net.
    - Or through the application designed to this end on Izenpe's website.

  With the signature of the Issue Application, the applicant accepts Public Key Infrastructure Dissemination Agreement Conditions (PDS).

- ➢ Validation of following documentation,

SSL DV SSL OV SSL Qualified Qualified Office	➢ Ownership or right to use the domain. This may be done in any of the following ways: a) Email the domain contact (BR 3.2.2.4.2): Izenpe shall send the applicant a unique, random code by email to the address in the whois contact (Registrant, administrative or technical). Any individual from the applicant organisation can answer, providing the random code. b) Constructed email to the domain contact (BR 3.2.2.4.4): Izenpe sends an email to one or more of the following addresses: "admin," "administrator," "webmaster," "hostmaster," or "postmaster," followed by the @ symbol and the domain name for which the SSL certificate is being applied for. The email includes a random and unique code. Anyone at the applicant organisation may respond to the email, providing the random code. c) Change agreed upon in DNS (BR 3.2.2.4.7): The applicant makes a change in the domain's DNS registration, so they apply for the SSL certificate. The applicant must add the random and unique code sent by Izenpe in a CNAME, TXT or CAA field in the DNS register. Once the change has been made by the applicant, Izenpe verifies it. d) IP Address (BR 3.2.2.4.8): Izenpe carries out a DNS lookup of the domain and extracts the IP address from the A field or the AAAA field. After, it is verified that the applicant has assigned the obtained IP address by searching on Internet Assigned Numbers Authority (IANA) or Regional Internet Registry

	(RIPE, APNIC, ARIN, AfriNIC, LACNIC). Izenpe sends the contact an email with a unique and random code. Any individual from the applicant organisation can answer, providing the random code. This method CANNOT be used to validate wildcards. e) Email to contact DNS CAA (BR 3.2.2.4.13): Izenpe shall send the applicant a unique, random code by email to the address in the DNS CAA register. To this end, there should be a "contactemail" CAA entry with an email address: CAA 0 contactemail "contacto@example.com" Any individual from the applicant organisation can answer, providing the random code. f) Email to contact DNS TXT (BR 3.2.2.4.14): Izenpe shall send the applicant a unique, random code by email to the address in the DNS TXT register. There should be a TXT entry in the subdomain "_validation-contactemail" with an email address: _validation-contactemail.izenpe.eus. 299 IN TXT "contacto@example.com" Any individual from the applicant organisation can answer, providing the random code. g) Change agreed upon on website (BR 3.2.2.4.18): The applicant must publish the file with the random and unique code sent by Izenpe on the route "/.well-known/pki-validation" Once the change has been made by the applicant, Izenpe verifies it. ➢ Prior to issuing all SSL certificates, Izenpe validates the existence of a CAA register for each DNS name of CN extensions and subjectAltName of the certificate, according to RFC 6844 specifications. If the certificate is issued, the validation is conducted before the CAA registration TTL, and in any event before 8 hours have passed. Izenpe processes the "issue" and "issuewild" tags. The CAA registers that identify the domains for which Izenpe authorises the issue are "izenpe.com" and "izenpe.eus." ➢ With SSL DV and SSL OV certificates, wildcards are permitted in sub-domains or host names, as long as the applicant entity can prove their legitimate control over the complete domain. Otherwise, the application shall be denied. For example, * co.uk or *.local cannot be issued, but *.example.com for the company Example S.A. shall be issued. ➢ Izenpe validates the list of rejected applications in its internal database ➢ Izenpe verifies high-risk applications in MacAfee TrustedSource
SSL OV SSL Qualified Qualified Office	➢ Verification of the organisation's official name: – Public entity: Certification issued by the Secretary/Attorney, registry certification/simple informative note or reference in Official Gazette in the 13 months prior to the issue application

	– Private entity: original certification of pertinent registration or simple informative note. ➢ Verification of the organisation's commercial name: in the event that the applicant has a commercial name, the same sources will be used for verification as for the official name ➢ Email verification that the applicant is aware of the certificate's processing. The entity representative must indicate the authorised applicants. ➢ Verification of the entity's post address in: – Data Protection Agencies. – Eudel for municipalities in the Basque Country. – Official Register. ➢ Country verification: ➢ Data Protection Agency ➢ Eudel ➢ Pertinent Public Registry
SSL Qualified Qualified Office	➢ Verification of the entity's Tax Identification Number: – Public entity: Data Protection Agencies, Official State Gazette or pertinent official registry. – Private entity: Data Protection Agencies, original registry certification or simple informative note. – Company: Data Protection Agencies or Commercial Register – Non-commercial/not-for-profit international entity: verification that the entity is a recognised International Organisation ➢ Verification of operational existence: All methods described in the sections "Verification of official name," "Verification of commercial name" and "Verification of postal address" verify that the organisation is in active status. If not possible, QIIS will be consulted online (e.g., einforma, DUN & BRADSTREET, etc.). ➢ Verification of name, position and capacity of the person authorising the Application, the Certificate Applicant and the Application Signatory. ➢ Dual signature of documentation verification
Qualified Office	➢ Verification of the official publication of the electronic office in the pertinent Official Gazette

NOTES

– If there is a discrepancy between the documentation provided and the documentation verified, Izenpe shall verify that the address on the Application matches a location where the Applicant Entity stably operates.

- The entity's validity and application competency is not required for a valid recognised corporate certificate, entity or stamp issued by Izenpe to the applicant, as long as the certified was issued in the past 825 days (13 months for EVs or qualified).
- The validity of tokens and random values used to verify ownership of the domain is 30 days.
- Through Izenpe's online application to apply for SSL certificates, the entity may create users associated with employees who are permitted the issue of certificates for said entity.
- Izenpe will always be responsible for verifying ownership or right to use the domain.
- Izenpe may conduct additional verifications, such as: the organisation's confirmation of application or of authorisation for the applicant to process the certificate on behalf of the organisation, and the annual revision of compliance by means of an external audit.
- When the validation cannot be conducted as determined, this will be justified in the documentation verification document.
- Once the documentation is verified, Izenpe shall leave proof of the verifications conducted with the documentation verification document.
- Validation is only dual for EV and qualified certificates.
- Izenpe does NOT contemplate issues to IP addresses
- Izenpe shall always verify that CSRs are not reused
- Izenpe's public subCAs do not issue certificates for internal domains.
- Izenpe considers the following reliable sources:
    - Data Protection Agencies.
    - Eudel
    - Pertinent Official Registry
    - Official Gazettes.
    - Certification issued by the Town Hall Secretary/Attorney.
    - ICANN.
    - Whois for each ccTLD

  If not on this list, the following criteria will be considered to consider a source as reliable:
    - The age of the information.
    - Frequency of updating.
    - Data provider and purpose of data collection.
    - Public accessibility and availability.
    - Relative difficulty of data falsification or alteration.
- Before issuing the certificate, Izenpe verifies that the RSA keys meet the following requirements:
    - Minimum key size of 2048 bits
    - The public exponent is odd and greater than or equal to 3
    - The public exponent is in the range 2^16 < and < 2^256
    - The module is odd, not a prime number power and does not have factors under 752
    - The public key is not on CVE-2008-0166's blacklist
    - The public key is not vulnerable to ROCA CVE-2017-15361 threat
- Izenpe does not consider that a "pre-certificate" as defined in the RFC 6962 (Certificate Transparency) is considered a "certificate," and consequently should not be subject to the RFC 5280-Internet X.509 PKI and CRL Profile requirements.

2.3 Certificate issue and delivery

Izenpe will contact the Technical Manager indicated in the *Issue Application* to generate the technical application and send it to Izenpe via email.

If Izenpe's application for placing the application is used, the Technical Manager will be in charge of entering the technical application.

Izenpe shall send the certificate to the Technical Manager via email or the application.

2.4 Cost amount

Once the certificate is issued, the cost will be paid according to the applicable rate.

On an annual basis, Izenpe publishes applicable rates on its website www.izenpe.com , and on the application, as well.

2.5 Certificate verification

The Applicant shall have 15 working days as of certificate issue to verify proper operation, and if necessary, communicate operational defects to Izenpe.

Only if operational defects are due to technical causes or errors in the data contained on the certificate that are attributable to Izenpe, shall Izenpe revoke the certificate and issue a new one, bearing the costs derived therefrom.

2.6 Revoking the certificate

Revocation application

See section "4.9.2 Who can apply for revocation" in the Certification Practises Statement (CPS).

Procedure

See section "4.9.3 Processing revocation applications" in the Certification Practises Statement (CPS).

Reasons for revocation

For final certificates, see section "4.9.1 Circumstances for revocation" in the Certification Practises Statement (CPS).

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

1. The subCA requests it in writing
2. The subCA notifies the issuer CA that the application for the original certificate was not authorised and does not admit retroactive authorisation
3. The issuer CA obtains evidence that the private key for the subCA for the certificate's public key has been subject to key compromise or has ceased to comply with requirements in sections 6.1.5 and 6.1.6 of the BRs
4. The issuer CA obtains evidence that the certificate was issued incorrectly

5. The issuer CA detects that the certificate was not issued pursuant to the Certificate Policy or the CPS
6. The issuer CA determines that data on the certificate is imprecise or incorrect
7. The issuer CA or the subCA ceases operations for any reason and agreements have not been entered into with another CA to provide the revocation service
8. The issuer CA or subCA's right to issue certificates under BR's requirements finalises or is revoked, unless the issuer CA has enabled agreements to continue maintaining the CRL/OCSP repository
9. The issuer CA and/or CPS policy requires revocation
10. The content or technical format of the certificate bears a risk that is unacceptable to software providers or third parties
11. Providers or third parties (e.g.: the CA/Browser Forum may determine that an algorithm/encryption signature of key size bear an unacceptable risk and that these certificates must be revoked and replaced within a specific period of time)

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

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

2.7 Certificate renewal

To renew a certificate, the applicant must follow the established certificate issue process, bearing in mind that the verifications are valid for 13 months for EVs and 39 months for the rest.

2.8 Audits and incidents

Criteria regarding audits and incident analysis,

☐ Channels to file complaints or suggestions,

- Telephone: 902 542 542
- Email: info@izenpe.com
- Filling out the complaint and suggestion form, available at www.izenpe.eus
- Filling out the complaint and suggestion form, available at registration desks.

☐ Internal record of incidents occurred.

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

- ☐ Annual audit planning is conducted according to BR criteria. Izenpe also conducts the internal audits set forth in section 8.7 of the BRs
- ☐ Izenpe reports cases it considers to be incidents (fraud, phishing, etc.) to the Anti-PhishingWorkGroup website (www.apwg.org) and verifies prior to issue that the applicant or representatives are not in Izenpe's internal security incident database. In any event, the right to issue certificates in suspicious situations is reserved.
- ☐ Audits will be based on ETSI EN 319 411-1

3 CHANGE MANAGEMENT

Modifications to this document shall be approved by Izenpe's Security Committee. Said Committee reviews the CPS on an annual basis or when any change occurs. This review includes all Certificate Policies. The version number is increased, and the changes made are recorded, even if no changes have been made.

Amendments in the CPS will be set out in a document entitled Specific Documentation Update, the maintenance of which is guaranteed by Izenpe.

Updated versions of specific documentation may be viewed at www.izenpe.eus.

4 CHANGE TRACKING

4.1 From version 0 to 1.0

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

4.2 From version 1.0 to 1.1

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

4.3 From version 1.1 to 1.2

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

4.4 From version 1.2 to 1.3

	SECTION / CLARIFICATION

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

4.5 From version 1.3 to 1.4

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

4.6 From version 1.4 to 1.5

Updates to the previous version	Qualified profiles were added

4.7 From version 1.5 to 1.6

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

4.8 From version 1.6 to 1.7

Change	Section
The test certificate routes were added (living, revoked, expired)	1 Introduction
The EVs were deleted from the profiles that Izenpe currently issues	1.1 Certificate description
It is specified that Izenpe's public CAs are not issued for internal domains Verification of RSA key parameters was added The definition of "pre-certificate" was added	2.2 Application Procedure
The revocation procedure is eliminated, and one is rerouted to the CPS	2.6 Certificate revocation
The obligation to increase in the version number even if there are no changes is added	3 Change management