CERTIFICATE POLICY

SECURE SERVER (SSL)

March 2017

Version 1.1

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 *Specific Documentation* (or 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 and EV guidelines* for issuing website certificates) and in ETSI specifications (www.etsi.org), for this type of certificate.

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" and "Office" certificates
- EVCP (Extended Validation Certificates Policy): for "Office EV" and "SSL EV" certificates

Within the scope of the Google Certificate Transparency project, SSL EV and Office EV certificates issued will be published on Izenpe's CT Log service, and other log server providers' log service, with whom Izenpe has signed an agreement, in order to meet Google's requirements.

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	**Office**
SSL OV	**EV Office**
SSL EV	

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

This provides 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, 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, 2 or 3 years.

- *SSL ORGANIZATION 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, 2 or 3 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.

– *ELECTRONIC OFFICE CERTIFICATES*

Pursuant to *Spanish Law 11/2007, dated 22 June, on electronic access for citizens to public services,* Izenpe issues the following certificates*,*

- ***ELECTRONIC OFFICE**,*

  This certificate is considered non-qualified, and identifies the Public Administration, body or administrative entity that owns the website.

  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 3 years.

- ***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.

1.2 Identification

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

CERTIFICATE	OID
SSL DV	1.3.6.1.4.1.14777.1.2.4
SSL OV	1.3.6.1.4.1.14777.1.2.1
SSL EV	1.3.6.1.4.1.14777.6.1.1
Electronic office	1.3.6.1.4.1.14777.1.1.3
Electronic office EV	1.3.6.1.4.1.14777.6.1.2

1.3 Community and scope of use

The following are considered **users,**

- Certificate applicant, person applying for the certificate on behalf of the organisation.
- Certificate subscriber, organisation identified on the certificate.

Scope of use. The certificates will be used within the scope of the responsibility of the organisation, Public Administration, body or administrative entity that owns the certificate.

1.4 General stipulations

Obligations concerning identification

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 the corresponding legal instrument.

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

The subscriber's obligations are stipulated in the Certification Practises Statement, in the section on *Subscriber Obligations.*

2 OPERATIONAL REQUIREMENTS

2.1 List of required documentation

- **Issue application** duly completed and signed with:
  - Handwritten signature
  - Electronic signature: with a recognised certificate from Izenpe or National Identity Document that identifies the applicant

  The applicant shall thus accept the *Conditions for Use* and *the Subscriber Contract* applicable on the date when the Application is signed, published on www.izenpe.com.
- **Tax ID Number** of the organisation.
- **Accreditation of the identity and validity of the applicant entity** (see section 2.2 Application Procedure)
- **Accreditation of power of the Applicant to use the entity's name** (see section 2.2 Application Procedure)

2.2 Application Procedure

- The APPLICANT shall send the issue application and required documentation to,
  - The address IZENPE, S.A.- C/ BEATO TOMAS DE ZUMARRAGA, 71 -1ª PLANTA – 01008 VITORIA-GASTEIZ (Spain).
  - Electronically to the email address certservidor@izenpe.net.
  - Or through the application designed to this end on Izenpe's website.

  By signing the Issue Application, the applicant accepts the Conditions for Use and the Subscriber Contract.

- Document validation,

SSL DV **SSL OV** **SSL EV** **Office** **EV Office**	➢ Verification of ownership of the domain: This may be done in any of the following ways: a) Domain use authorisation document: issued by the domain-registering entity b) Change agreed upon on website: publication on the path <;domain>;/.well-known/pki-validation of a file with a challenge sent by Izenpe. c) TLS using a random number: confirm the presence of a file generated by Izenpe in a certificate published in the domain applied for that is accessible to Izenpe by using TLS d) Email to the Registrant's contact, obtained through a whois consultation, including a random value ➢ Verification of CAA if registered, and under all circumstances following RFC 6844 guidelines. ➢ With SSL DV, SSL OV and Office 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.

SSL OV **SSL EV** **Office** **EV Office**	➢ Whois verification. The registrant must match the applicant organisation. Otherwise, the applicant must accredit the subscriber's right to use. Verification that the applicant has the right to use the domain or sub-domain: • Domains .es: www.nic.es • Domains .eu: www.eurid.eu • Domain .eus: whois.nic.eus • Rest domains: whois.icann.org ➢ Verification of applicant entity's identity and validity in: • Public entity: ▪ Name*: Official Gazette, certificate from secretary or Commercial Registry ▪ Tax ID Number*: AGPD (Spanish Data Protection Agency), Official Gazette or Commercial Registry • Private entity: ▪ Name*: original certification of pertinent registration or simple informative note ▪ Tax ID Number*: AGPD (Spanish Data Protection Agency), original certification of pertinent registration or simple informative note ➢ Verification of Applicant's power to use the entity's name in: • Public entity:*: Certification issued by the Secretary/Attorney, 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 * 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 39 months (13 months for EVs). ➢ Email verification that the applicant is aware of the certificate's processing. ➢ Verification of post address in: ➢ Data Protection Agencies. ➢ Telephone operator pages. ➢ Eudel for municipalities in the Basque Country. ➢ Commercial Registry 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 Organisation stably operates. ➢ Country verification: ○ AGPD (Spanish Data Protection Agency), Eudel, Yellow Pages or Commercial Registry ➢ Verification of list of denials in Izenpe's internal databases. ➢ Verification of high-risk applications in MacAfee TrustedSource.
SSL EV **EV Office**	➢ Verification that the landline telephone (not mobile) number belongs to the applicant entity. Verification sources: ➢ Telephone operator pages, Data Protection Agencies or Eudel, for municipalities in the Basque Country. ➢ Later verification by calling. ➢ Verification of operational existence. Private entities must accredit that they perform bank

	operations with a regulated financial institution. ➢ Dual signature of documentation verification by, ➢ Legal Assessment ➢ and the Technical Department ➢ Validation of verifications made by the Technical Department Manager.

NOTE.

- 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 certificates.
- The previous verifications shall not be necessary if the information has already been validated within a maximum timeframe of 13 months for EVs, and 39 months for the rest.
- Izenpe does NOT contemplate issues to IP addresses (e.g.: 1.2.3.4)

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.

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

2.4 Cost

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

The following my apply for certificate revocation,

- The subscriber.
  The following are authorised to request certificate revocation: the Legal Representative of the subscriber entity, the Personnel Chief or third party authorised by either of the aforementioned.
- The applicant.
- Izenpe is authorised to apply for revocation of end entity subscriber certificates for the technical reasons stipulated in the CPS.

Procedure

The revocation applicant will process the *Revocation Application through Izenpe.*
The certificate may be revoked at any time.
The applicant can revoke the certificate through the following channels:

- In person,
  - At Izenpe, requesting a prior appointment at www.izenpe.com
  - Or with the subscriber organisation with which Izenpe entered into the pertinent legal instrument.
- Over the phone, by calling +34 902 542 542.
  The following are required for identification:
  - Applicant National ID Number
  - Technical contact National ID Number
  - Applicant email
  - Complete site name (FQDN)
- Online, at the website www.izenpe.com
- Or by post, sending the certificate revocation application signed and validated before a notary.

Reasons for revocation

This may be viewed in the Certification Practises Statement www.izenpe.com

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: +34 902 542 542
  - Email: info@izenpe.com
  - Filling out the complaint and suggestion form, available at www.izenpe.com
  - 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.

- ☐ Annual audit planning is conducted according to ETSI criteria.

- ☐ Izenpe reports cases it deems as incidents (fraud, phishing, etc.) on 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.

3 CHANGE MANAGEMENT

Modifications to this document shall be approved by Izenpe's Security Committee.

Amendments 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.com.

4 CHANGE TRACKING

4.1 From version 0 to 1.0

Additional requirements

Requirements in section 2.2 added

Updated requirements

Requirements in sections 2.1 and 2.2 updated

Clarifications

Requirements in sections 2.2

Publisher

Table of contents added.

Footnote added

Requirements eliminated

Requirements in sections 2.1 and 2.2 eliminated

Year eliminated on cover page

4.2 From version 1.0 to 1.1

Updated requirements

Domain validation requirements updated, in section 2.2

Requirements eliminated

Graphs in sections 2.3 and 2.6 eliminated