CERTIFICATE POLICY

SECURE SERVER (SSL)

February 2018

Version 1.3

© IZENPE

This document is owned by IZENPE, and can only be reproduced entirely.

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 certificate 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 Practice 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), 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 which 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	**Office EV**
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 or 2 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 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.

– *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 (Office EV)** ,*

  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 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
Electronic Office	1.3.6.1.4.1.14777.1.1.3	2.23.140.1.2.2
Electronic Office EV	1.3.6.1.4.1.14777.6.1.2	2.23.140.1.1

Certificate serial numbers will have at least 64 bits of output from a CSPRNG.

1.3 Community and scope of use

The following are considered **users,**

- Certificate applicant, legal person applying for the certificate. Once the certificate is issued, the applicant is referred to as the Subscriber.
- Certificate subscriber, legal person identified in 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 Practice Statement, in the PKI Disclosure Statement (PDS).

2 OPERATIONAL REQUIREMENTS

2.1 List of required documentation

SSL DV, SSL OV, SSL EV Office, Office EV	Request form duly completed and signed (electronic or handwritten)
SSL OV, SSL EV Sede, Sede EV	Accreditation of the information about the entity: – Official Name – Validity period – Postal address – Country
SSL EV Sede EV	Acceditation of: – Name, position and legal capacity of: of the person who authorizes the request, of the certificate applicant and of the request signer. – Tax identification number – Phone number – In case of private entities: document
Sede, SedeEV	Reference to the official publication of the site in the bulletin

2.2 Application Procedure

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

  By signing the Issue Application, the applicant accepts the Conditions of the PKI Disclosure Statement (PDS).

- 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) Email to the Registrant's contact (registrant, tech or admin), obtained through a whois consultation, including a random value Izenpe will require an answer including the same random value b) Change agreed upon on website: publication on the path domain/.well-known/pki-validation of a file with a challenge sent by Izenpe. ➢ Previous to the issuance of any SSL certificate, Izenpe checks the DNS for the existence of a CAA

	record for each dNSName in the subjectAltName extension, according to the RFC 6844 requirements. In case the certificate is issued, it will be done before the TTL of the CAA registry, and in any case in no more than 8 hours. Izenpe always processes "issue" and "issuewild" tags, and may not dispatch reports of issuance requests to the contact(s) listed in the "iodef" tag. The CAA records that identify domains for which Izenpe is authorized to issue are "izenpe.com" and "izenpe.eus". ➢ In case the country is included, it will be validated in: ➢ Data Protection Agencies. ➢ Eudel for municipalities in the Basque Country. ➢ Corresponding Public Registry ➢ 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**	➢ Verification of applicant entity's validity and applicant's capacity to request the certificate: • 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 corresponding registry or simple informative note Through the Izenpe online application for SSL certificates application, the entity can create the users associated with the employees that allow the issuance of certificates for such entity. The validity of the entity and applicant's capacity will not be required in the case of valid qualified corporate certificate, entity or stamp issued by Izenpe to the applicant, as long as the certificate was issued in the past 825 days (13 months in case of EVs). ➢ Email verification that the applicant is aware of the certificate's processing. ➢ Verification of post address in: ➢ Data Protection Agencies. ➢ Eudel for municipalities in the Basque Country. ➢ Official Registry In case 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. ➢ Verification of list of denials in Izenpe's internal databases. ➢ Verification of high-risk applications in MacAfee TrustedSource.
	➢ Verification of the entity's tax identification number:

SSL EV **EV Office**	• Public entity: Data Protection Agencies, Official Bulletin o corresponding official registry • Private entity: Data Protection Agencies, original certification of corresponding registry or simple informative note • Business: Data Protection Agencies o corresponding official registry • Non-commercial entity: validation that the entity is an International qualified Organization ➢ Verification of operational existence Private entities must accredit that they perform bank operations with a regulated financial institution. ➢ 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 the name, position and capacity of the person authorizing the Request, of the Applicant of the certificate and of the signer of the Request. ➢ Dual signature of documentation verification by, ➢ Legal Assessment ➢ Technical Department

NOTES

- Izenpe will always be in charge of carrying out the verification of 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 dual just 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 825 days for the rest.
- Izenpe does NOT issues certificates to IP addresses
- Izenpe considers the following trusted sources:

    - Data Protection Agencies
    - Eudel for municipalities in the Basque Country
    - Official Registry
    - Official bulletins
    - Certification issued by the Secretary/Attorney
    - ICANN
    - Whois of each ccTLD

- In case it's not in this list, Izenpe will consider the following criteria to consider a trusted source:

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

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 amount 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 Certificate revocation

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, and it'll be effective within the following 24 hours.
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.

Additionally, in case of subordinate CA certificates, these will be revoked within a maximum period of 7 days if one or more of the following occurs:

The Issuing CA SHALL revoke a Subordinate CA Certificate within seven (7) days if one or more of the following occurs:

1. The Subordinate CA requests revocation in writing
2. The Subordinate CA notifies the Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization
3. The Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of BRs
4. Izenpe obtains evidence that the Certificate was misused
5. Izenpe is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with this document or the applicable Certificate Policy or Certification Practice Statement
6. Izenpe determines that any of the information appearing in the Certificate is inaccurate or misleading
7. Izenpe ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate
8. Izenpe's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository
9. Revocation is required by the Izenpe's Certificate Policy and/or Certification Practice Statement
10. The technical content or format of the Certificate presents an unacceptable risk to Application Software
11. Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given 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: +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. Izenpe will open an investigation within a maximum period of 24 hours from receipt, and the actions to be taken will be decided taking into account the criteria of section 4.9.5 of the BRs.
- ☐ Annual audit planning is conducted according to ETSI criteria. Izenpe also performs the internal audits defined in section 8.7 of the BRs
- ☐ 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.
- ☐ Audits are based on ETSI EN 319 411-1

3 CHANGE MANAGEMENT

Modifications to this document shall be approved by Izenpe's Security Committee. Such Committe reviews annually the CPS or in case there is any change. That review includes the Certificate Policy.

Amendments to 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.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

4.3 From version 1.1 to 1.2

Updated requirements

Updated CAA validation requirements in 2.2 section.

Clarifications

Requirements in sections 2.2

4.4 From version 1.2 to 1.3

	EPÍGRAFE / ACLARACION
Actualizaciones respecto a la versión anterior	– 1. Introduction In the scope of the Google Certificate Transparency project, the SSL EV and EV Site certificates issued will be published in the CT service of the Log Servers suppliers with which Izenpe has an agreement. – 1.1. Description of certificates ▪ Update of the regulations regarding the regulation of the seal certificate. ▪ Update of the validity of the certificates, which may be 1 or 2 years – 1.2 Identification ▪ CA / B FORUM OIDs included ▪ Serial numbers of the certificates will have at least 64 bits of entropy – Sections 1.3 and following Adaptation of terminology of EV certificates to private entities certificates – 14. General provisions ▪ Obligations of identification. It is indicated that in all cases Izenpe verifies ownership or control over the domain. ▪ Obligations of the subscriber of the certificate. Those determined in the Public Key Disclosure Agreement (PDS) are included. – Sections 1, 2 and 3 Inclusion of clarifications on compliance with BR.
Clarifications	
Actualizaciones de formato.	
Eliminaciones.	