Table of Contents

1 INTRODUCTION 3
2 DEFINITIONS 4
3 USES OF ELECTRONIC MEANS 6
   3.1 APPROPRIATE USES, 6
      – FOR AUTHENTICATION 6
      – FOR SIGNATURE, 6
   3.2 FORBIDDEN USES OF MEANS 7
      – AUTHENTICATION, the certificates should be used exclusively for the specific purpose for which they were intended, and may not be used for other functions and for other purposes. 7
      – SIGNATURE, the certificates should be used exclusively for the specific purpose for which they were intended, and may not be used for other functions and for other purposes, and only according to applicable law. 7
4 OBLIGATIONS 8
   4.1 IZENPE, 8
      4.1.1 GENERAL OBLIGATIONS 8
      4.1.2 AS ENTITY ISSUING ELECTRONIC IDENTIFICATION MEANS, 9
      4.1.3 AS ENTITY ISSUING ELECTRONIC SIGNATURE MEANS, 9
      4.3 CERTIFICATE SUBSCRIBER OBLIGATIONS 12
5 RESPONSIBILITIES 14
6 VERSION CONTROL 17
1 INTRODUCTION


As such, it issues resources for authentication and electronic signature.

- Authentication,
  In addition to identification means based on electronic certificates, Izenpe issues B@K and B@KQ, to authenticate a natural person with a reference number that matches the user’s National ID Document/Foreign Identification Number Card and a password.
  B@KQ also has a 16-position coordinate set.

- Signature,
  For signature purposes, Izenpe issues electronic certificates of different types and with different formats, according to specifications stipulated in the corresponding Specific Policy and the Certification Practises Statement.

Provider data.

<table>
<thead>
<tr>
<th>NAME OF PROVIDER</th>
<th>Ziurtapen eta Zerbitzu Empresa-Empresa de Certificación y Servicios, Izenpe, S.A.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Postal Address</td>
<td>c/ Beato Tomás de Zumárraga, nº 71, 1ª planta. 01008 Vitoria-Gasteiz (Spain)</td>
</tr>
<tr>
<td>WEBSITE</td>
<td><a href="http://www.izenpe.eus">www.izenpe.eus</a></td>
</tr>
<tr>
<td>EMAIL ADDRESS</td>
<td><a href="mailto:info@izenpe.com">info@izenpe.com</a></td>
</tr>
<tr>
<td>TELEPHONE</td>
<td>+34 902 542 542</td>
</tr>
</tbody>
</table>
2 DEFINITIONS

- **Electronic identification**, the process of using a person's identification data in electronic format to uniquely represent the natural or legal person, or a natural person representing a legal person.
- **Electronic identification means**, a material and/or immaterial unit that contains a person's identification data, used to authenticate with online services.
- **Authentication**, the electronic process that makes it possible to electronically identify a natural or legal person, or the origin and integrity of data in electronic format.
- **Electronic signature**, the data in electronic format annexed to other electronic data or logically associated with them, used by the signatory to sign.
- **Advanced electronic signature**, electronic signature that meets requirements stipulated by article 26 of the eIDAS Regulation.
- **Qualified electronic signature**, an advanced signature created with a qualified electronic signature creation device based on a qualified electronic signature certificate.
- **Electronic stamp certificate**, electronic statement that links validation data from a signature to a natural person and confirms, at minimum the name or pseudonym of that person.
- **Qualified electronic signature certificate**, an electronic signature certificate issued by a qualified trust service provider that meets the requirements established in Annex III of the eIDAS Regulation.
- **Trust services provider**, a natural or legal person who provides one or more trust services, either as a qualified provider or as a non-qualified provider of trust services.
- **Qualified trust service provider**, trust service provider that provides one of several qualified trust services and to whom the supervision authority has granted qualification;
- **Registration Entities**, entities that perform the tasks of identifying applicants, subscribers and owners of certificate keys, verifying the documentation accrediting the circumstances on the certificates, as well as validating and approving applications to issue, revoke and renew certificates.
- **Certificate Users.**
  - **Certificate applicant**, all certificates must be applied for by one person, on their own behalf or on behalf of an organisation.
  - **Signatory**, the person who holds a signature creation device and who acts on his or her own behalf or on behalf of an individual or legal entity.
  - **Certificate subscriber**, legal or natural person identified on the certificate.
  - **Key holder**, natural person who holds, or is responsible for custody of, the digital signature keys.

- **B@k**, this is an electronic identification means for natural persons for authentication and signature, made up of:

Ref.: IZENPE-Terms and Conditions _ v1.1
- A reference number that matches the user's National ID Number/Foreign ID Number Card.
- A password.
- A non-qualified certificate issued on an HSM.

This is for online consultation and processing in different services of the user entities.

- **B@kQ**, this is an electronic identification means for natural persons for authentication and signature, made up of:
  - A reference number that matches the user's National ID Number/Foreign ID Number Card.
  - A password.
  - A set of coordinates with 16 possible positions.
  - And a qualified certificate issued on an HSM.

B@kQ is for online consultation and processing in different services of the user entities.
3 USES OF ELECTRONIC MEANS

3.1 APPROPRIATE USES,

- **FOR AUTHENTICATION**
  These electronic means are for authentication, and should be used for the subscriber’s, or if applicable, the key holder’s electronic authentication, with public administrations that accept them.

- **FOR SIGNATURE,**
  
  **Qualified certificates for natural or legal person**
  Qualified signature and seal certificates may be used, if defined as such by the corresponding certificate, to sign authentication messages, particularly for client SSL or TLS challenges, secure S/MIME email, encrypted without password recovery, or others. This digital signature guarantees the identity of the signature certificate subscriber.

  Moreover, said certificates may support different kinds of authentication and the advanced electronic signature, used in conjunction with IT applications that protect the signature’s private key in a highly reliable fashion.

  Website and electronic stamp certificates should only be used with public administrations for the electronic stamp for documents.

  **Non-qualified certificates for natural or legal person**
  Non-qualified certificates do not reliably guarantee the identity of the subscriber and, if applicable, of the private key holder;

  If used to sign, it must be used along with a device that generates a reasonably secure signature, not equal to the signatory’s handwritten signature.

  Non-qualified signature certificates may also be used, if defined as such by the corresponding certificate, to sign authentication messages, particularly for client SSL or TLS challenges, secure S/MIME email, encrypted without password recovery, or others.

  **Computer security certification**
  Secure server certificates and certificates for entities responsible for computer devices are issued.

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

  Website certificates should only be used with public administrations to identify the website.

  **Code signature certificate.**
These certificates are issued to owner entities to guarantee the authentication and integrity of a software component.

3.2 FORBIDDEN USES OF MEANS

- **AUTHENTICATION**, the certificates should be used exclusively for the specific purpose for which they were intended, and may not be used for other functions and for other purposes.

- **SIGNATURE**, the certificates should be used exclusively for the specific purpose for which they were intended, and may not be used for other functions and for other purposes, and only according to applicable law.

No certificate issued by Izenpe may be used to carry out procedures as a Registration Authority.

The certificates are not designed, intended, or authorised for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation, communication, or control systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage.
4 OBLIGATIONS

4.1 IZENPE

4.1.1 GENERAL OBLIGATIONS

Security,

− Use trustworthy systems and products which are protected against modification and ensure the technical and, where applicable, cryptographic security of the processes supported by them in accordance with the Security Policy.

− Taking measures against the falsification of means, and guaranteeing confidentiality in the generation process and delivery to the signatory through a secure procedure.

− Use trustworthy systems to store certificates in a verifiable form so that only authorised persons can make entries and changes, information can be checked for authenticity, certificates are publicly available for retrieval in only those cases for which the certificate-holder’s consent has been obtained, and any technical changes compromising these security requirements are apparent.

− Perform regular security checks to verify conformity with the established security requirements.

− The correct management of its security through implementation of an Information Security Management System in accordance with the requirements established in ISO/IEC 27001, which includes but is not limited to the following measures:
  • Perform a comprehensive security incident management procedure to ensure detection, resolution and optimisation.
  • Maintain contacts and appropriate relationships with special interest groups in the area of security, including specialists, security forums and professional associations devoted to information systems security.
  • Properly plan the maintenance and evolution of systems in order to guarantee good performance at all times and provide service that complies with the expectations of users and clients.

− It will demand that hosting suppliers meet the security standards and rules (General Register of Data Protection, ISO, ETSI, CABForum and Izenpe Security Policy).

Staff,

− Employ personnel who possess the knowledge, experience, and qualifications necessary to provide the services offered and the appropriate security and management procedures in the area of electronic signature.

− It will meet the security standards and rules (General Register of Data Protection, ISO, ETSI and Izenpe Security Policy).
Procedure,

– Before issuing and delivering the means of identification and/or signature, Izenpe informs the subscriber of the terms and conditions for use, of its price - when established - its limitations to use and the binding legal instruments referenced, if applicable, by the Certification Practises Statement.

– Izenpe has a plan for finalisation of cessation of activity, stipulating the conditions under which this shall take place.

– IZENPE will inform the key holder about the expiry of their certificate prior to or at the same time as the electronic certificate expires, specifying the reasons and date and time that the certificate will no longer be effective.

– All of this public information regarding certificates is included in Izenpe's Publication Service, defined in the Certification Practises Statement.

4.1.2 AS ENTITY ISSUING ELECTRONIC IDENTIFICATION MEANS,

– Shall identify the user with the assurance levels defined in the eIDAS.

– Shall guarantee that the identification data is complementary.

– Shall ensure that the user holds the elements to identify him/her.

– Shall comply with technical and staff requirements stipulated by applicable legislation.

– Before issuing and delivering the means of identification, Izenpe shall inform the subscriber of the terms and conditions for use, of its price - when established - its limitations to use and the binding legal instruments.

– IZENPE provides public mechanisms to verify the validity of certificates through systems described in the Certification Practice Statement.

– Izenpe shall offer self-authentication mechanisms to verify the validity of the identification mechanisms.

4.1.3 AS ENTITY ISSUING ELECTRONIC SIGNATURE MEANS,

– Obligation of providing service.

Izenpe provides its certification services according to the Certification Practises Statement, which provides details on its roles, operational procedures and security measures, and specifically, undertakes to comply with all obligations applicable, except for those specifically carried out by the Registration Entity, as long as it is not acting as said Entity.

The Certification Authority undertakes the following obligations:

- It will not copy the signature creation data of the person to whom it has administered services.
- It will maintain a system which indicates whether a certificate is issued, revoked, suspended or expired.
- It will use a secure method to retain a record of all of the information and documentation connected with qualified certificates and valid certification practice statements for at least 15 years from the time of issuance, so that the signatures can be verified; information relative to other types of certificates shall be retained for 7 years.

- It will make sure that the signatory is in possession of the signature creation data corresponding to the verification data contained in the certificate.

- It will guarantee that the signature verification and creation data is complementary, as long as both of them are generated by the certification services provider, and that the identity contained on the certificate unambiguously matches the public key contained therein.

- Rapidity and security in providing the service. In particular, it provides a fast, secure and free service aimed at checking certificate validity and ensures secure and immediate notification of the termination of effectiveness of the certificates in agreement with this Certification Practice Statement. The service is available 24 hours X 7 days a week.

- Compliance with the technical and personnel requirements as established by current legislation on electronic signature:
  - Demonstrate the reliability necessary for providing certification services.
    - Guarantee that the date and time when the certificate was issued or when it expired can be precisely determined. **Obligations regarding legal regulation over the certification service.**
      - Izenpe undertakes all obligations directly incorporated into the certificate, or incorporated by reference. Incorporation by reference is made by including an object identifier or other form of link to a certificate.

- The legal instrument that binds IZENPE and the applicant, subscriber or key holder and the relying party is in writing and in readily understandable language.

- Provisions to comply with the Certification Practises Statement.

- Indication of the applicable Certification Practice Statement and indication, where applicable, as to whether the certificates are issued to the public and the need to utilise a secure signature creation device or message decryption.

- Clauses concerning the issuance, revocation, renewal and, where applicable, recovery of private keys.

- Declaration stating that the information contained in the certificate is correct unless otherwise notified by the subscriber.

- Consent for storing the information used for the subscriber log file, for supplying a cryptographic device and for the disclosure of such information to third parties should IZENPE terminate its services without revocation of valid certificates.

- Limits on certificate use.
• Information on how to validate a certificate, including the requirement of checking certificate status, and the conditions in which parties can reasonably rely on a certificate.

• Applicable responsibility limitations, including uses for which Izenpe accepts or denies responsibility.

• Retention period for certificate application information.

• Retention period for audit log.

• Applicable dispute resolution procedures.

• Applicable law and competent jurisdiction.

• Whether IZENPE has been declared in conformity with the certification policies of other public entities and, if so, with what system.

• How Izenpe's asset liability is guaranteed.

4.2 REGISTRATION AUTHORITY

The Registration Authority undertakes the following obligations:

− To validate the identity and other personal details of the applicant, subscriber and key owner, if applicable, on the identification means, or information relevant for the purpose of the them in accordance with these procedures.

− To keep all of the information and documentation concerning them, and manage their issuance, renewal, revocation or reactivation.

− To notify IZENPE of revocation applications with due diligence and in a fast and reliable manner.

− To allow IZENPE access to its procedures archives and audit logs in order to perform its functions and maintain the necessary information.

− To inform IZENPE of all issuance, renewal, revocation applications and any other aspects related to the means issued by IZENPE.

− To validate, with due diligence, the circumstances for revocation that might affect the means' validity.

− To comply with the procedures established by IZENPE and with the current legislation in this area, in its management operations connected with the issuance, renewal and revocation of the means.

− If necessary, it may undertake the role of making the signature creation (private key) and electronic signature verification (public key) technical procedures available to the key holder.
4.3 CERTIFICATE SUBSCRIBER OBLIGATIONS

- Provide IZENPE with complete and appropriate information in accordance with the requirements described in the Certification Practice Statement, particularly with regard to the registration procedure.
- Guarantee that the information that should be included therein, is truthful, complete and up-to-date.
- Understand and accept the terms and conditions of use of the certificate, and any changes that may be made to the terms and conditions.
- Give prior consent to the issuance and delivery of a certificate.
- Guarantee proper use and conservation of certificate supports.
- Appropriately use the certificate, and specifically, comply with limitations to certificate use.
- Be diligent in custody of credentials, in order to prevent unauthorised uses, as established in the Certification Practices Statement.
- Notify Izenpe and any other individual that the subscriber believes may trust the certificate, without unjustifiable delays, of:
  - The loss, theft of potential compromise of its credentials.
  - Inaccuracy or changes to the certificate content, as notified to or suspected by the subscriber, calling for the revocation of the certificate when such changes constitute a cause for revocation.
- To stop using the identification means after the validity period has expired.
- Transfer specific obligations to key holders.
- Not monitor, manipulate or perform reverse engineering on technical implementation of certification services, without prior written authorisation from the Certification Entity.
- Not intentionally compromise the security of certification services.
- Will refrain from using the private keys corresponding to the public keys included in the certificates for the purpose of signing a certificate as if performing the function of a Certification Authority.

Certificate subscriber agrees conditions in CPS published at www.izenpe.com/dpc, and the corresponding certificate policy, also available in www.izenpe.eus

4.4 OBLIGATIONS OF CERTIFICATE VERIFIERS

Certificate verifiers agree to the following obligations:

- Independently assess the appropriateness of the use of a certificate and determine that it will, in fact, be used for an appropriate purpose.
- Know the conditions of use for certificates, as stipulated in the Certification Practises Statement.
- Verify the validity or revocation of the certificates issued, using information on certificate status.
- Verify all certificates in the certificate hierarchy before relying on a digital signature or on any of the certificates in the hierarchy.
- Bear in mind any usage limitations on certificates, whether contained in the certificate itself or in the verifier contract.
- Bear in mind any precautions included in a contract or other instrument, regardless of legal nature.
- Notify IZENPE of any inaccuracy or defect in a certificate which may be considered cause for revocation.
- Not monitor, manipulate or perform reverse engineering on technical implementation of certification services, without prior written authorisation from Izenpe.
- Not intentionally compromise the security of certification services.
- The qualified certificate user must recognise, in the due legal instrument, that such electronic signatures are electronic signatures equivalent to handwritten signatures, as per eIDAS.
5 RESPONSIBILITIES

5.3 CERTIFICATION AUTHORITY RESPONSIBILITIES
IZENPE shall be held liable for,

- Harm and damage caused to any individual or entity, due to a lack of or delay in inclusion in the consulting service for the validity of certificates or expiry of certificate validity.
- Harm and damage caused to any individual, due to a lack of or delay in inclusion in the verification service for the validity of the identification mechanism.
- Additionally, IZENPE shall assume full liability for the actions of persons to which it has delegated authority to perform the functions necessary for rendering certification services. Thus, IZENPE maintains insurance coverage liability of 3,500,000 euros for damages incurred as a result of the use of the certificates.

IZENPE shall be held responsible for negligence or lack of due diligence in certification services provided, as well as when it fails to comply with obligations stipulated in legislation on electronic signatures, except for in the following cases:

- It shall not be held responsible for harm caused by information contained in the Certificates, as long as the content therein substantially complies with the Certification Practises Statement.
- Certificate expiration, provided that it substantially complies with the publication obligations set forth in this Certification Practice Statement.
- For undue use, or for use after revoking the identification means.
- In no event shall IZENPE be held liable for any direct, indirect, special, incidental, or consequential damages, or for any loss of profits, loss of data, or punitive damages arising from, or in connection with, the use, delivery, license, performance or non-performance of certificates, digital signatures or any other transactions or services offered or contemplated by this Certification Practice Statement arising from misuse.
- For damages to subscribers or bona fide third parties due to inaccuracies in the information contained in the certificate when such information has been certified by an official, notarised or otherwise authorised document, except in the case of documents supplied by the Registration Authority.

For harm and damage caused to the subscriber or third parties in good faith due to failure to comply with duties inherent to the role of subscriber or third parties who trust in the certificates.

5.4 REGISTRATION AUTHORITY RESPONSIBILITIES
Any organisation other than IZENPE that acts in the role of Registration Authority shall be liable to IZENPE for damages incurred in the performance of the duties it assumes, in the terms established in the corresponding legal agreement.
5.5 RESPONSIBILITIES OF THE IDENTIFICATION MEANS HOLDER

- For falsehood or factual error committed during the registration process.
- For the use of the identification means in electronic communications with unauthorised persons.
- The failure to protect the secrecy associated with the identification means or to otherwise take reasonable precautions to prevent the loss, disclosure, modification or unauthorised use of the private keys.

5.6 SUBSCRIBER RESPONSIBILITIES

The Subscriber shall be held liable for all of the authenticated electronic transactions using a digital signature generated with the Subscriber's private key when the certificate has been validated through the verification services provided by IZENPE.

If no notification of loss or theft of the certificate is received, as laid down in this Certificate Practice Statement, any liability resulting from the unauthorised use and/or misuse of the certificates shall, in all cases, be the responsibility of the Subscriber.

By accepting the certificates the Subscriber undertakes to protect and, where applicable, indemnify IZENPE, the Registration Authorities and the User Entities for any act or omission that may result in damages, loss, debts, legal fees or any other type of expense, including payment for professional services, incurred by IZENPE, the Registration Authorities and the User Entities, caused by the use or publication of certificates, and which result from:

- the failure to comply with the terms and conditions laid down in the legal instrument that binds it to the Certification Authority,
- The use of digital certificates in electronic communications with unauthorised persons.
- Falsehood or factual error made by the Subscriber.
- failure by the Subscriber to disclose a material fact in the certificates, if the misrepresentation or omission was made negligently or with intent to deceive IZENPE, the Public Entity Users or parties relying on the Subscriber's certificate.
- the failure to protect the private key or to otherwise take reasonable precautions to prevent the loss, disclosure, modification or unauthorized use of the private keys.

In this regard, Izenpe shall not be held responsible for harm and damage caused to the subscriber or third parties in good faith due to failure to comply with the following duties inherent to the role of subscriber:

- Provide IZENPE or the Registration Authority with full, complete and precise information on their certificate applications and the any other information needed for the issuance or revocation thereof, when inaccuracies in the information have not been detected by the service provider.
- Promptly notify IZENPE or the Registration Authority of any changes in the information submitted for the certificate.
- Diligently safeguard signature creation data to keep it strictly confidential and protect it from unauthorised access or disclosure.
Apply for the revocation of a certificate if the Subscriber becomes aware of or suspects the compromise of signature creation data.

Refrain from using the signature creation data when the validity period has expired or when the service provider notifies the Subscriber that such data is no longer valid.

Observe the limitations listed in the certificate with regard to possible uses and employ the certificate in conformance with the terms and conditions set forth and communicated to the signer of the certificate services.

5.7 RESPONSIBILITIES OF THIRD PARTIES TRUSTING IN CERTIFICATES

A relying party who vests trust in a certificate that has not been verified assumes all of the risks associated thereto and under no circumstances shall hold IZENPE, the Registration Authorities, User Entities or Subscribers liable for any circumstance resulting from their trust in such certificates and signatures.

In this regard, Izenpe shall not be held liable for harm and damage caused to the subscriber or third parties in good faith if the recipient of the signed documents fails to comply with one of the following diligence tasks:

- Verify and bear in mind restrictions on the certificate in regards to possible uses and the broken-down amount of transactions that may be performed therewith.

- Make sure the certificate is valid.
## 6 VERSION CONTROL

### 6.3 Change control _for Version 1.0_

| Updated requirements |  |
| Clarifications |  |
| Publisher |  |
| Requirements eliminated | ➢ Conditions for use.  
➢ Subscriber contract. |

### 6.4 Change control _for version 1.0 to 1.1_

| Updates to the previous version | ➢ Update to document name.  
➢ Section 2, a specific section with definitions is included.  
➢ Section 3, the difference between using identification means as attention and as signature is explained.  
➢ Section 4, a new classification of party obligations is included.  
➢ Section 5, the certification authority’s Responsibilities are updated. |
| Clarifications |  |
| Format updates. |  |
| Eliminations. | ➢ Section 2. Section 2 is eliminated, on the types of certificates and the formats in which they are issued. |