CERTIFICATION PRACTICE STATEMENT UPDATE

Reference:	IZENPE-CPS UPDATE
Version no:	v 5.03
Date:	10th March 2015

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

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

General information

Document checklist

Title:	Certification Practice Statement Update
Version:	5.03
Approval date:	10/03/2015
Documentation used:	CPS 5.02
Author(s)	IZENPE Legal Office Izenpe technical department
Changes/Comments	5.03 is the updated version of 5.02

In accordance with section 9.11, the Izenpe S.A Certification Practice Statement allows modifications to be made to the Certification Practice Statement. This document presents the most current modifications. However, if you request, use or place trust in the certificates issued by Izenpe, S.A, you are responsible for reading the entire updated Certification Practice Statement.

ITEM 1_Adaptation

Amendment:

As a result of the audit performed by Izenpe in accordance with ETSI standards, and the inclusion of new services, the following amendments have been incorporated:

SECTION	AMENDMENT
Entire document	**All "recognized" have been replaced with "qualified"**
1. Introduction	**Original:** In addition, IZENPE follows the ETSI standards (European Telecommunications Standards Institute) and has obtained certification under the technical specifications (TS) of the 101 456 standard for issuing recognized certificates generated in a secure signature creation device (QCP Public + SSCD) and the 102 042 standard for issuing public key infrastructure certificates (PKI) following the extended validation certificate policy, EVCP, following guides approved by the CA/Browser Forum. **Changed to:** In addition, IZENPE follows the ETSI standards (European Telecommunications Standards Institute) and has obtained certification under the technical specifications (TS) of the 101 456 standard for issuing qualified certificates generated in a secure signature creation device (QCP Public + SSCD) and the 102 042 standard for issuing qualified and non-qualified certificates. For the secure server certificates that follow the Extended Validation Certificate Policy (EVCP) and for the secure server certificates that follow the Organizational Validation Certificates Policy (OVCP), the guides approved by the CA/Browser Forum will also be followed. **Original:** The technical specifications (TS) defined in these standards TS 101 456 and TS 102 042, establish the basic requirements for the operation and management practices of certification authorities issuing recognised and unrecognised certificates in accordance with European Parliament Directive 1999/93/EC incorporated into the Spanish legal system in Electronic Signature Act 59/2003.

	Changed to: The technical specifications (TS) defined in standards TS 101 456 and TS 102 042 establish the basic requirements for the operation and management practices for certification authorities that issue qualified and non-qualified certificates in accordance with European Parliament Directive 1999/93/EC incorporated into the Spanish legal system in Electronic Signature Act 59/2003, and later with EU Regulation 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS).
1.1 Presentation	Added: • "The Verification Service enables the User Entity to benefit from the use of certificates issued by IZENPE by verifying the status of certificates based on the CRL (Certificate Revocation List). • ZAIN is a trusted signature services platform which provides a series of online global, standardized security services (authentication, authorization, electronic signature and data protection). • IZENPE offers id@zki free of charge id@zki is a Java applet application integrated in a browser to provide electronic signature encryption. • The Izenpe digital signature service is a digital version of the traditional signature folder. It consists of a tray in which the person receives the to-be-signed documents. • The certified communication service ZIURRA acts as a Trusted Third Party ("digital notary"), giving proof that an email or SMS has been sent and that it has been received by the recipient. • The Publication Proof and Accreditation Service makes it possible to reliably verify the time the information included in a public contract is first made public. • EGOITZA is the certificate cloud hosting service which enables secure hosting of end user certificates. " **Removed:** • "IZENPE has a series of computer applications and technical specifications for the development of applications using an electronic signature, which it offers user entities through the issuing of a licence." **Added natural person, legal person and device to the table**

1.3.1 Certification authorities	**Removed:** "Subordinate certification authorities **2003**. These CAs have been migrated to the new Izenpe CA root structure." **Removed tables of subordinate CAs from CA 2003** **Removed obsolete subCA SSL EV table**
1.3.3 End entity users of certificates	**Changed title "End entity users" to "End entity users of certificates"**
1.3.4 End entity users of timestamps	**Created point 1.3.4 "End entity users of timestamp services"**
1.3.5 Trusted third parties	**Original:** "For the purposes of this Certification Practice Statement, the natural and legal persons who receive certificates issued by IZENPE are relying parties and, as such, are governed by the stipulations contained in this Certification Practice Statement upon making the decision to effectively rely on the certificates." **Changed to:** "For the purposes of this Certification Practice Statement, the natural or legal persons who receive certificates and timestamps issued by IZENPE are third parties who trust in certificates and timestamps issued by IZENPE and, as such, are governed by the stipulations contained in this Certification Practice Statement when they decide to effectively trust the certificates or timestamps." **Original:** "Third parties are understood to rely on the certificates in accordance with the use they make thereof in their relationships with subscribers." **Changed to:** "Third parties are understood to trust the certificates and timestamps in accordance with the use they make thereof in their relationships with subscribers." **Original:** "Third parties shall exercise due diligence in using each type of certificate and shall keep to the principle of good faith and loyalty, abstaining from any

	fraudulent or neglectful conduct meant to repudiate messages issued within the level of trust attached to the category of certificate." **Changed to:** "Third parties shall exercise due diligence in using each type of certificate and timestamp and shall keep to the principle of good faith and loyalty, abstaining from any fraudulent or neglectful conduct meant to repudiate messages issued within the level of trust attached to the category of certificate or timestamp."
1.4.1 Appropriate certificate uses	**The following has been moved from the section entitled "Qualified certificate" to "Non-qualified certificate":** "The Electronic main office and Electronic main office EV certificates are issued to reliably identify websites. Electronic main office and stamp certificates are issued to public administrations for the identification of administrative headquarters and electronic stamping of documents, in accordance with *Law 11/2007 on electronic access of citizens to public services*." **Original in the section "Computer security certification":** "Secure server certificates (SSL and SSL EV) and certificates for entities responsible for computer devices are issued." **Changed to:** "Secure server certificates (SSL DV, SSL OV, SSL EV, Sede and Sede EV) and certificates for entities responsible for computer devices are issued."
1.6.1 Definitions	**Added:** "Timestamping Authority (TSA): authority that issues timestamp tokens"
2.2 Publication of Certificate Information	**Original:** "Information is available at the IZENPE web site http://www.izenpe.com 24 hours a day, 7 days a week." **Changed to:** "Information is available at www.izenpe.com 24 hours a day, 7 days a week." **Original:** "As for publication of Certificate Revocation Lists, certificate users and

	subscribers are ensured secure and fast access" **Changed to:** "As for publication of Certificate Revocation Lists, certificate users and subscribers are ensured secure, fast access free of charge."
2.2.1 Publication and notification policy	**Original:** "IZENPE shall notify users of changes in specifications or in the terms and conditions of services via the IZENPE website home page http://www.izenpe.com." **Changed to:** IZENPE shall notify users of changes in specifications or in the terms and conditions of services via the IZENPE website home page www.izenpe.com"
3.2.1 Methods to test private key ownership	**Original:** When a pair of keys is generated, • Where a key pair is generated by a Registration Authority, proof of possession of the private key is by virtue of the trusted procedure of delivery and acceptance of the cryptographic device and of the corresponding certificate and key pair stored within. • By the key owner, possession of the private key is demonstrated by the proper use of the certificate. **Changed to:** When a pair of keys is generated, • By a Registration Authority and the keys are stored on a cryptographic card, proof of possession of the private key is by virtue of the trusted procedure of delivery and acceptance of the cryptographic card and of the corresponding certificate and key pair stored within. • By a Registration Authority and the keys are stored in a HSM, the key owner, possession of the private key is demonstrated by virtue of the reliable custody of the HSM and the trusted procedure for exclusive access to keys by the subscriber. • By the key owner, possession of the private key is demonstrated by the proper use of the certificate.
3.3 Identification and authentication for requests to reissue keys	**Original:** "A new key pair is always generated after revocation and reissuance of a

	certificate." **Changed to:** "In certificates in which Izenpe generates the keys, after revocation of the certificate and reissuance of a new certificate, the keys are always renewed."
4.1 Certificate request	**Original:** "Therefore, subject to the length limitations determined by the technical factors established in the content of the certificate, the given name and surname must be carefully taken from the identification documents" **Changed to:** "Therefore, subject to the length limitations determined by the technical factors established in the content of the certificate, the identification data are carefully taken from the identification documents"
4.2.2 Approve or deny applications	**Added:** "When this request is for a certificate that includes a domain name for the authentication of a server, Izenpe will examine the Certification Authority Authorization (CAA) register, in accordance with RFC 6844. If the CAAs are present but do not allow Izenpe to issue the certificates because the server is not registered, Izenpe will not issue the certificate but will allow applicants to make another request after Izenpe has resolved the incident."
4.2.3 Custody of the private key	**Added:** "In the case of "cloud certificates" the private keys for end user certificateswill be stored on secure cryptographic devices under standard FIPS 140-2, security level 3. "
4.3 Certificate issuance	**Added:** **"**No unlock codes (PIN or PUK) will be delivered in the case of certificates for which Izenpe does not generate the keys."
4.3.1 CA actions during issuance	**Original:** "Certificates can be issued either by means of a cryptographic device or a software mechanism." **Changed to:** Certificates can be issued either on a smartcard, HSM, or a software mechanism." **Original:**

	"Issuance procedure for certificates issued using a cryptographic device:" **Changed to:** "Issuance procedure for certificates issued on a smartcard:" **Added:** I. "Issuance procedure for certificates issued on HSM: • The Registration Authority authenticates the validity of the documentation submitted by the applicant. • Following authentication, the Registration Authority requests a certificate from IZENPE. • After verifying that the request has come from an authorized Registration Authority, IZENPE issues the certificate according to the established procedures and sends it to the Registration Authority. • After the Registration Authority has ascertained that the request comes from IZENPE, it then downloads the certificate to the signature creation device using a secure cryptographic device management process. • Should IZENPE decide not to issue the certificate (even when authentication procedures are correct), the applicant will be notified of the reasons for the decision." **Original:** "Together with the application form, the applicant generates a key pair in the server itself giving IZENPE the public key." **Changed to:** "Together with the application form, the applicant generates a key pair in the server itself giving IZENPE the technical request."
4.4.3 Notification of certificate issuance by the CA and other entities	**Original:** "IZENPE does not notify other entities about issuing your certificates" **Changed to:** "IZENPE does not notify other entities of issuing your certificates, except for EV certificates published on the Izenpe Certificate Transparency Log Server"
4.5.1 Private subscriber's key and use of the certificate	**Original:** **"**The subscriber," **Changed to:**

	“The subscriber who has custody of the keys,”
	
	Added:
	The subscriber whose keys are hosted on Izenpe
	• Will make proper use of the certificate and, in particular, comply with the usage limitations thereof.
	• Will diligently safeguard the private key to prevent unauthorized use in accordance with sections 6.1, 6.2 and 6.4 of the Certification Practice Statement.
	• Notify IZENPE and any other person the subscriber thinks might rely on the certificate without any reasonable delay if any of the following occur:
	  ○ Control over the subscriber's private key has been lost due to compromise of activation data or for any other reason.
	  ○ 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.
	• Will cease using the private key at the end of the certificate validity period.
	• Will transfer specific obligations to key owners.
	• Will refrain from monitoring, interfering with, or reverse engineering the technical implementation of certification services without prior written approval from the Certification Authority.
	• Refrain from intentionally compromising 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.
	• Subscribers of qualified certificates who generate digital signatures using the private key corresponding to the public key listed in the certificate must acknowledge in the appropriate legal instrument that such electronic signatures are equivalent to handwritten signatures, provided that a cryptographic device is used, pursuant to the provisions of article 3.4 of the LFE.

4.9.3 Processing revocation requests	**Removed:** “The following are required for identification: ○ Telephone Identification Password (given on the password sheet) ○ DNI / NIE ○ TIN of the entity for certificates for legal persons” **Added:** "Consult the Specific Documentation on the particular type of certificate for identification requirements."
4.9.4 CA deadline to process the revocation	**Original:** “Once what is set forth in section 4.9.3 has been completed, and the revocation duly processed by the RA, the revocation will be made immediately effective in accordance with current legislation.” **Changed to:** “Once what is set forth in section 4.9.3 has been completed, and the revocation duly processed by the RA, the revocation will be made effective in accordance with current legislation.”
4.9.10 Other revocation notifications available	**Original:** “IZENPE does not have any other ways of notifying users to check the status of their certificates.” **Changed to:** "Izenpe sends an email to notify the certificate subscriber when a qualified certificate has been revoked.
6.1.1 Key pair generation	**Original:** • “User certificates issued on a cryptographic hardware device: keys are generated by the cryptographic device” **Changed to:** • User certificates issued on a cryptographic card or HSM: keys are generated by the cryptographic device
6.1.2 Private key delivery to subscriber	**Original:** • “Certificates issued on a cryptographic hardware device: private keys for authentication and advanced electronic signature are delivered on a cryptographic device” **Changed to:**

	• "Certificates issued on a cryptographic card: private keys for authentication and signature are delivered on a cryptographic device" **Added:** • Certificates issued on HSM: private keys for authentication and signature are hosted on a cryptographic device.
6.1.5 Key sizes and algorithms used	**Original:** • Not less than 2048 bits for keys for natural persons, OCSP Server and TSA Server and technical certificates. **Changed to:** • Not less than 2048 bits for keys for natural or legal persons or for device keys, OCSP Server and TSA Server and technical certificates.
6.1.6 Certificate signature algorithms	**Original:** "The algorithm identifier (AlgorithmIdentifier) used by IZENPE to sign the certificates is SHA-1 (hash algorithm) with RSA (signature algorithm) which corresponds to "Identifier for SHA-1 checksum with RSA encryption for use with Public Key Cryptosystem One defined by RSA Inc." The SHA-256 algorithm began to be used in 2007 and will transition gradually in line with the technology environment. The padding scheme used is emsa-pkcs1-v2.1 (according to RFC 3447 section 9.2). End user certificates are signed with RSA with SHA-1. Izenpe recommends that end users employ RSA with SHA-1 or higher (SHA-224 or SHA-256) when signing a certificate." **Changed to:** "The algorithm identifier (AlgorithmIdentifier) used by IZENPE to sign the certificates is SHA-2 (hash algorithm) with RSA (signature algorithm) which corresponds to "Identifier for SHA-2 checksum with RSA encryption for use with Public Key Cryptosystem One defined by RSA Inc." The padding scheme used is emsa-pkcs1-v2.1 (according to RFC 3447 section 9.2). End user certificates are signed with RSA with SHA-2. Izenpe recommends that end users employ RSA with SHA-2 or higher when signing a certificate."
6.2.1 Standards for cryptographic modules	**Original:** "Cryptographic devices with advanced electronic signature certificates, suitable as secure signature creation devices (DSCF)..." **Changed to:** Cryptographic devices with qualified electronic signature certificates, suitable as secure signature creation devices (DSCF)..."

6.2.3 Custody of the private key	**Original:** “It will be the subscriber's responsibility to keep the private key under their exclusive control” **Changed to:** “In cases where subscribers keep the private key, it will be their responsibility to keep it under their exclusive control”
6.2.5 Private key archiving	**Removed:** “The CA will never archive the private keys for the subscribers' recognized certificates.”
6.2.6 Transfer of the private key to or from the cryptographic module	**Original:** “Only in the case of contingency is the procedure described in 6.2.4 used to enter private keys into cryptographic modules.” **Changed to:** “Only in the case of contingency will the procedure described in 6.2.4 be used to recover private keys in the cryptographic modules.”
6.2.7 Storage of the private key in the cryptographic module	**Added:** “For generating the keys for end user certificated stored "in the cloud", Izenpe follows the recommendations of the European Commission (eIDAS) and the European Technical Specification CEN/TS 419241.”
6.2.8 Method of activating private key	**Added:** "Access of the subscriber's private key in the case of certificates stored "in the cloud" will have a second authentication factor, which may vary depending on the type of certificate.
6.2.9 Method of deactivating private key	**Original:** “Removal of the cryptographic device from the reader will deactivate any action in operation.” **Changed to:** “Removal of the cryptographic card from the reader will deactivate any action in operation.”
6.2.10 Method of destroying private key	**Added:** "Private keys of certificates stored "in the cloud" will be eliminated once

	the relationship with Izenpe has ended or the certificates have expired. " **Original:** "This procedure is not applied to user signature or authentication keys, since they are not created by the CA, except in the case of key changeover using the same cryptographic device. In such cases the previous key will be destroyed and new keys will be generated on the same media." **Changed to:** "This procedure is not applied to user signature or authentication keys issued on a cryptographic card, except in the case of key changeover using the same cryptographic device. In such cases the previous key will be destroyed and new keys will be generated on the same media."
6.4.1 Activation data generation and installation	**Added:** • Certificates issued "in the cloud": the use of the private key associated with each certificate requires a second authentication factor.
6.8	**Original:** "The description of the NTP protocol can be found in the IETF PKIX, RFC 1305 standard." **Changed to:** "The description of the NTP protocol can be found in the IETF RFC 5905 standard".
7.3	**Original:** Internet X.509 Public Key Infrastructure Online Certificate Status Protocol-OCSP (RFC 2560) June 1999 **Changed to:** Internet X.509 Public Key Infrastructure Online Certificate Status Protocol-OCSP (RFC 6960) June 2013
8 Timestamping Authority (TSA) Practices Statement)	**Created point 8 "Timestamping Authority (TSA) Practices Statement"**
10.4.6 Structure of files containing personal data	**Original:** • Human Resources: medium security level • Curriculum Vitae: medium security level **Changed to:** • Human Resources: basic security level

	• Curriculum Vitae: basic security level
10.6.1 Obligations concerning the rendering of services	**Original:** “It will not store or copy the signature creation data of the person to whom it has administered services” **Changed to:** “It will not copy the signature creation data of the person to whom it has administered services”
10.6.2 Obligations concerning trusted operations	**Original:** "ensures secure and immediate notification of the expiration or suspension of certificates" **Changed to:** "ensures secure and immediate notification of the termination of effectiveness of the certificates" **Original:** “Ensure that the date and time when a certificate is issued, terminated or expired can be determined precisely” **Changed to:** “Ensure that the date and time when a certificate is issued or expired can be determined precisely”
10.6.7 Registration Authority obligations	**Removed:** • “To request that IZENPE suspend a certificate for the amount of time needed to verify the documentation that gave rise to revocation of the certificate.” **Original:** • 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, revocation and reactivation of certificates. **Changed to:** • 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, revocation and reactivation of certificates.
10.6.10 Obligations of certificate verifiers	**Original:** • Verify the validity, suspension or revocation of the certificates issued,

	using information on certificate status. **Changed to:** • Verify the validity or revocation of the certificates issued, using information on certificate status.
10.6.11 Obligations of the Timestamping Authority	**Created point 10.6.11 "Obligations of the Timestamping Authority"**
10.6.12 Timestamp subscriber obligations	**Created point 10.6.12 "Timestamp subscriber obligations"**
10.6.13 Obligations of third party timestamp verifiers	**Created point 10.6.13 "Obligations of third party timestamp verifiers"**
10.7.2 Responsibility of the Timestamping Authority	**Created point 10.7.2 "Responsibility of the Timestamping Authority"**
10.13	**Added:** • EU Regulation 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS).