CERTIFICATION PRACTICE STATEMENT UPDATES

Reference: IZENPE-CPS UPDATE.

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

www.izenpe.com
info@izenpe.com
Tel.: 945 06 77 23

Izenpe's Certification Practises Statement, as per section 9.11, states that the Certification Practises Statement may be modified. Although these modifications are shown in this document, if you apply for, use or trust the certificates issued by Izenpe, you must be aware of the entire updated Certification Practises Statement.

General information_ version 5.061as update of version 5.0

Document control

Title:	Certification Practises Update.
Version:	5.01
Approval date:	19/07/2013
Documentation used:	CPS 5.0
Author(s)	Izenpe Legal Consulting Izenpe Technical Area
Changes/Comments	Version 5.01 is the updated version of 5.0

Amendment:

As a result of TUV IT audit per ETSI standards, the following modifications are included:

SECTION	MODIFICATION
5.8.1	- Any authorisation with a thirty party with whom Izenpe holds a service provision contract (identification, issue, hosting, etc.) shall be deemed as terminated.
9.6.1	- Complying with security standards and regulations (Spanish Data Protection Act, ISO, ETSI and Izenpe Security Policy). - It will demand that hosting suppliers meet the security standards and rules (Data Protection Act, ISO, ETSI and Izenpe Security Policy).
9.6.7	- Compliance with security standards and regulations (Spanish Data Protection Act, ISO, ETSI and Izenpe Security Policy).
9.11.2	- Izenpe is replaced by the IZENPE Security Committee
6.1.1	- In the case of keys generated by the actual holder, they should be generated following the algorithm and minimum key length recommendations defined in ETSI TS 102 176."
6.1.6	- The padding scheme used is emsa-pkcs1-v2.1 (according to RFC 3447 section 9.2)."
6.2.7	- In cases where private keys are stored outside the cryptographic modules, they will be protected so as to ensure the same level of protection as if they were physically inside the cryptographic modules. All HSMs used by Izenpe to store private keys for Certification Authorities have level 3 FIPS 140-2 certification.

Document control

Title:	Certification Practises Update.
Version:	5.02
Approval date:	16/09/2014
Documentation used:	CPS 5.01
Author(s)	Izenpe Legal Consulting Izenpe Technical Area
Changes/Comments	Version 5.02 is the updated version of 5.01

Amendment:

As a result of TUV IT audit per ETSI standards, the following modifications are included:

SECTION	MODIFICATION
5.5.2	- It is clarified that the information and documentation regarding certificates is kept, as of the date of issue, for 15 years for recognised certificates, and 7 for non-recognised certificates.
6.1.5, 7.1.2 and 7.1.3	- Algorithm SHA1 is replaced by SHA2. - The size of the keys goes from 1024 to 2048.
6.2.3	- Izenpe's precaution of hosting private keys is eliminated.
6.2.7	- It is hereby informed that in generating CA keys, Izenpe follows the recommendations of ETSI TS 102 042, 7.2.1 g), and Baseline Requirement Guidelines 17.7.

General information _ version 5.04 as update of version 5.03

Document control

Title:	Certification Practises Update.
Version:	5.04
Approval date:	30/06/2016
Documentation used:	CPS 5.04
Author(s)	Izenpe Legal Consulting Izenpe Technical Area
Changes/Comments	Version 5.04 is the updated version of 5.03

EXCHANGES

Additional requirements	➢ New representative profiles, stamp, qualified SSL and non-qualified citizen ➢ The assurance level for all profiles (existing and new) was identified ➢ New certificate extensions required by EN standards were indicated
Updated requirements	➢ ETSI EN standard requirements and references were updated, per the eIDAS regulation
Clarifications	➢ Points were updated to adapt them to applicable ETSI and CABForum standards
Publisher	
Requirements eliminated	➢ All requirements for the time stamp service (TSA) were eliminated. ➢ All references to SHA-1 were eliminated

General information _ version 5.05 as update of version 5.04

Document control

Title:	Certification Practises Update.
Version:	5.05
Approval date:	26/10/2016
Documentation used:	CPS 5.04
Author(s)	Izenpe Legal Consulting Izenpe Technical Area
Changes/Comments	Version 5.05 is the updated version of 5.04

CHANGES

Additional requirements	➢ Section 1.1. *Presentation*: includes the representative certificate type in container format.
Updated requirements	➢ Section 4.4.3.*Notification of certificate issuance by the CA and other entities*: CT is eliminated from Izenpe. ➢ Section 5.8.1. *Termination of CA or RA*: this includes providing for "individuals appointed by the Board of Administrators who shall decide upon the most appropriate mechanisms" with all managers to notify cessation of a certificate issue service (5.8.1). ➢ Section 4.9.9. Online revocation verification requirements: the text "*Revoked certificates that expire shall be removed from the CRL* is expanded with the text *"Revoked certificates that expire shall be removed from the CRL. However, information will still be offered on the certification's status through online verification, regardless of its expiry."*
Clarifications	
Publisher	
Requirements eliminated	

General information_ version 5.06 as update of version 5.05.

Document control

Title:	Certification Practises Update.
Version:	5.06
Approval date:	10/11/2016
Documentation used:	CPS 5.05
Author(s)	Izenpe Legal Consulting Izenpe Technical Area
Changes/Comments	Version 5.06 is the updated version of 5.05

CHANGES

Additional requirements	➢
Updated requirements	➢
Clarifications	
Publisher	
Requirements eliminated	➢ All references to HSM and certificate in the cloud eliminated

General information _ version 5.07 as update of version 5.06

Document control

Title:	Certification Practises Update.
Version:	6.0
Approval date:	1/06/2017
Documentation used:	CPS 5.06
Author(s)	Izenpe Legal Consulting Izenpe Technical Area
Changes/Comments	Version 6.0 is the updated version of 5.06

CHANGES

	SECTION / CLARIFICATION
Updates to the previous version	– Introduction. Izenpe shall bear ETSI EN 301549 recommendations in mind. – 1.1. Presentation . References to the identification resources issued by Izenpe are updated, as required by the eIDAS regulation. – 4.9.3Izenpe's website address is updated, now www.izenpe.eus. – 5.8.1. In the event that activity is terminated, it is specified that Izenpe shall inform this termination to the competent body at least 2 months beforehand.
Clarifications	
Format updates.	
Eliminations.	

General information _ version 6.1 as update of version 6.0

Document control

Title:	Certification Practises Update.
Version:	6.1
Approval date:	16/03/2018
Documentation used:	CPS 6.0
Author(s)	Izenpe Legal Consulting Izenpe Technical Area
Changes/Comments	Version 6.1 is the updated version of 6.00

CHANGES

	SECTION / CLARIFICATION
Updates to the previous version	– 1.1. Presentation . References to the identification resources issued by Izenpe are updated, as required by the eIDAS regulation. – 4.9.3., 6.1.7., 9.10 Izenpe's website address is updated, now www.izenpe.eus . – 5.8.1. In the event that activity is terminated, it is specified that Izenpe shall inform this termination to the competent body at least 2 months beforehand. – 6.1.1. Key pair generation. It is established that – All cryptographic keys must be generated following definitions in ETSI TS 119 312. – The public example is a prime number equal to or greater than 3. – 6.5.1. Specific computer security technical requirements It is established that all operator accounts with capacity to issue certificates have double factor-based access control. – 7.2. Profile of the certificate revocation list As described in RFC 6962, a pre-certificate shall not be considered a certificate with the characteristics defined in RFC 5280. – 7.3. OCSP Profile

	– Compliance of OCSP responses pursuant to standard RFC 6960. – 7.3.3.Other aspects regarding the OCSP are added. – 9.13. Applicable regulations. Update. – 9.14. Meeting applicable regulations. Update.
Clarifications	
Format updates.	
Eliminations.	

General information_ version 6.2 as update of version 6.1

Document control

Title:	Certification Practises Update.
Version:	6.2
Approval date:	04/12/2018
Documentation used:	CPS 6.1
Author(s)	Izenpe Legal Consulting Izenpe Technical Area
Changes/Comments	Version 6.2 is the updated version of 6.1

CHANGES

	SECTION / CLARIFICATION
Updates to the previous version	– 9.6.8. Obligations of certificate applicant: the requirement to pay the amount for the certificate is added. – 5.3.2 Training requirements: RA operator training requirements are added. – 9.4. Personal data protection: adapted to regulations in force.
Clarifications	
Format updates.	
Eliminations.	

General information _ version 6.3 as update of version 6.2

Document control

Title:	Certification Practises Update.
Version:	6.3
Approval date:	04/04/2019
Documentation used:	CPS 6.2
Author(s)	Izenpe Legal Consulting Izenpe Technical Area
Changes/Comments	Version 6.3 is the updated version of 6.2

CHANGES

	SECTION / CLARIFICATION
Updates to the previous version	– Section 1.1: assurance level of HSM profiles has been updated. Error corrected in professional assurance level in software. – Section 1.1: device profile added – Section 1.3.1: CA tree updated
Clarifications	
Format updates.	
Eliminations.	

General information _ version 6.4 as update of version 6.3

Document control

Title:	Certification Practises Update.
Version:	6.4
Approval date:	03/06/2020
Documentation used:	CPS 6.3
Author(s)	Security Manager
Changes/Comments	Version 6.4 is the updated version of 6.3

CHANGES

SECTION	CLARIFICATION
1. Introduction	• ETSI standard versions updated
1.1 Introduction	• Qualified and non-qualified trust service list added • eIDAS signature type column added for each certificate profile • Mobile, NQC pseudonym and IoT device profiles added
1.3.1 Certification Authorities	• Root CA and all CA profiles added
1.4.2 Prohibited certificate uses	• Prohibition to use certificates to conducted procedures as RA eliminated
1.5.2 Contact data	• Contact telephone updated
1.5.4 CPS approval procedure	• "Board of Administration" updated as "Security Committee" as body responsible for CPS approval
1.6.1 Definitions	• Data Protection Regulation added • SCP definition replaced by TSP's
2.2 Publishing certificate information	• References to publication service on www.izenpe.eus eliminated • The reference to Izenpe's SSL test URLs has been added
2.2.1 Publication and notification policy	• Obligation to keep changes made in the CPS for 30 days eliminated, along with the obligation to remove old versions
3.1.3 Uniqueness of names	• The text "Izenpe does not issue anonymous certificates" is eliminated
4.4.1 Certificate acceptance process	• The reference to the "subscriber contract" is replaced with "Terms and Conditions for Use"

4.4.3 Notification of certificate issuance by the CA and other entities	• The publication policy in Google CTs is updated
4.9.2 Who can reply for revocation	• Details are provided on profiles that can apply for revocation, and the reference to each policy is removed. Each policy must reference this section of the CPS
4.9.3 Processing revocation requests	• The list of available channels to apply for revocation is updated. Each policy must reference this section of the CPS
4.9.10 Other revocation notifications available	• The exception of corporate for revocation notifications is eliminated
5.1.2 Physical access to RAs	• The obligation to comply with Izenpe's Security Policy is updated with the Provider Security Policy
5.3.4 Retraining frequency and requirements	• The annual training requirement is added in "Trusted Roles"
5.3.7 Personnel hiring requirements	• The obligation for subcontracted personnel to comply with the Provider Security Policy is added
6.1.1 Key pair generation	• The APP is added as the key container
6.1.5 Key size and algorithms used	• SHA-256 is updated with SHA-2
6.2.8 Method of activating private key	• Redirected to the specific policy to know activation mechanisms in each case
6.2.9 Method of deactivating private key	• Corrected to redirect to the specific policy to know deactivation mechanisms in each case
6.3.2 Certificate operation periods and key pair use periods	• The duration of different subCAs is added to the EVs'
6 Network security controls	• The existence of IPS systems is added
7.3.3 Other OCSP aspects	• Information on the OCSP response to consultations on certificates that are not Izenpe's is added
9.6.4 User information obligations	• References to "Conditions for Use" are replaced with "Terms and Conditions for Use and Agreement to Share the Public Key Infrastructure (PKI-PDS)" • References to Izenpe's publication service are eliminated
9.6.7 Registration Authority obligations	• The obligation to sign an agreement before beginning to operate as a Registration Authority, if delegated, is added • The obligation to comply with the Provider Security Policy is added
9.7.1 Certification Authority	• The Civil Liability Insurance amount is eliminated

responsibilities	
9.11.1 Procedure for changes	• The Board of Administrators is replaced by the Security Committee

General information _ version 6.5 as update of version 6.4

Document control

Title:	Certification Practice Update.
Version:	6.5
Approval date:	10/07/2020
Documentation used:	CPS 6.4
Author(s)	Security Manager
Changes/Comments	Version 6.5 is the updated version of 6.4

CAMBIOS

EPÍGRAFE	ACLARACION
1.5.2 Contact information	• Added the table of contact details for Izenpe • Added the contact email for security incidences
1.5.3 In charge of adapting the Certificate Practice Statement	• Removed the table of contact details for Izenpe

ZIURTAPEN ETA ZERBITZU ENPRESA-EMPRESA DE CERTIFICACION Y SERVIC

Firmado digitalmente por ZIURTAPEN ETA ZERBITZU ENPRESA-EMPRESA DE CERTIFICACION Y SERVIC
Fecha: 2020.07.16 12:52:15 +02'00'