

UPDATE OF THE CERTIFICATION PRACTISE STATEMENT

Reference: IZENPE-CPS UPDATE.

© IZENPE 2018

This document is the property of IZENPE. It may only be reproduced in its entirety.

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

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



Izenpe's Certification Practises Statement, as per section 9.11, 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 5.01 as 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.



General information __version 5.02 as update of version 5.02

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

CHANGES

Additional requirements	<ul style="list-style-type: none">➤ 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	<ul style="list-style-type: none">➤ ETSI EN standard requirements and references were updated, per the eIDAS regulation
Clarifications	<ul style="list-style-type: none">➤ Points were updated to adapt them to applicable ETSI and CABForum standards
Publisher	
Requirements eliminated	<ul style="list-style-type: none">➤ 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	<ul style="list-style-type: none">➤ Section 1.1. <i>Presentation</i>: includes the representative certificate type in container format.
Updated requirements	<ul style="list-style-type: none">➤ Section 4.4.3. <i>Notification of certificate issuance by the CA and other entities</i>: CT is eliminated from Izenpe.➤ Section 5.8.1. <i>Termination of CA or RA</i>: 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; however, information shall still be offered on the status of the certificate through online verification, regardless of whether or not it has expired" <i>has been added to "Revoked certificates that expire shall be removed from the CRL."</i>
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	<ul style="list-style-type: none">– 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.– 4.9.3. 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.
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	<ul style="list-style-type: none">– 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<ul style="list-style-type: none">– 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



	<ul style="list-style-type: none">– Compliance of OCSF responses pursuant to standard RFC 6960.– 7.3.3. Other aspects regarding the OCSF are added.– 9.13. Applicable regulations. Updating.– 9.14. Meeting applicable regulations. Updating.
Clarifications	
Format updates.	
Eliminations.	