CERTIFICATION PRACTICE STATEMENT UPDATE

Reference:	IZENPE-CPS UPDATE
Version no.:	v 5.0
Date:	21 March 2013.

© IZENPE 2013

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

General information

Document checklist

Title:	Certification Practice Statement Update
Version:	5.0
Approval date:	21/03/2013
Documentation used:	CPS 4.9
Author(s)	IZENPE Legal Office Izenpe technical department
Changes/Comments	5.0 is the updated version of CPS version 4.9

In accordance with point 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:

- Izenpe has updated the version of their Certificate Practice Statement based, until now, on the RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework to the RFC 3647.
  There are two types of changes:
    - Change in the structure to adapt it to legislation.
    - Minimal technical changes and increase them.
- Suspension is eliminated (only revocation will be possible) and an online and telephone revocation service is enabled that allows instant revocation in the event of telephone identification and 24 hour revocation for online identification.
- It indicates the policy to be applied in the case of CAs issuing recognised certificates: QCP Public+SSCD.
- This includes:
    - An obligation for all suppliers to comply with security rules.
    - Security Committee responsibilities and the supervisor's responsibility to review the CPS.
    - The description of how to use keys for the root CA and the subordinate CA.
    - A reference to the protocol for transport, storage and removal of HSMs.
    - The indication that Izenpe is always in control of the signature devices created to generate end user keys.
    - The indication that in the event of Izenpe closing, any third party authorisation would be understood to be no longer valid.
    - The algorithms used for the end users that will be recognised by industry and appropriate as recognised signatures, taking into account the certificate's validity.
    - Reference to the responsibility for holding end user keys.