# CERTIFICATION PRACTICE STATEMENT UPDATE

| | |
|---|---|
| Reference: | IZENPE-CPS UPDATE |
| Version no.: | v 5.01 |
| Date: | 19 July 2013 |

© IZENPE 2013

This document is the property of IZENPE and may be reproduced only 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:** | 5.01 |
| **Approval date:** | 19/07/2013 |
| **Documentation used:** | CPS 5.0 |
| **Author(s)** | IZENPE Legal Office |
| | IZENPE Legal Office |
| **Changes/Comments** | 5.01 is the updated version of 5.0 |

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 certificate issued by Izenpe, S.A, you are responsible for reading the entire updated Certification Practice Statement.

## ENTRY 1_Adaptation

**Amendment:**

As a result of the TUV IT audit in accordance with ETSI standards, the following amendments have been included:

| HEADING | AMENDMENT |
|---|---|
| 5.8.1 | - Any authorisation with a thirty party with whom Izenpe holds a service provision contract (identification, issue, hosting, etc.) will be taken as finalised. |
| 9.6.1 | - It will meet the security standards and rules (Data Protection Act, ISO, ETSI and Izenpe Security Policy).<br>- It will demand that hosting suppliers meet the security standards and rules (Data Protection Act, ISO, ETSI and Izenpe Security Policy). |
| 9.6.7 | - To meet the security standards and rules (Data Protection Act, ISO, ETSI and Izenpe Security Policy). |
| 9.11.2 | - Izenpe is replaced by 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 |