CERTIFICATION PRACTICE STATEMENT UPDATE

Reference:	IZENPE-DPC UPDATE
Version no.:	v 4.9
Date:	29 March 2011

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

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

Versions

Version	Date	Author(s)	Changes/Comments
4.9 is the updated version of CPS version 4.8	29/03/2011	IZENPE Legal Office	Changes in CPS version 4.8

General information

Document checklist

Title:	Certification Practice Statement Update
Reference code:	
Version:	4.9
Version date:	29/03/2011
Approval date	29/03/2011
Documentation used:	CPS 4.8

In accordance with point 8, 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: DOCUMENTATION RETENTION PERIOD

Amendment:

As a result of the Secure Server certificate with *Extended Validation* issued by IZENPE and following the audit conducted in compliance with *Webtrust for EV*, IZENPE retains the information and documentation related to *EV* type certificates and non recognized certificates for 7 years (see section 2.1.2 Obligations concerning the rendering of services).

ENTRY 2: SUNDRY CLARIFICATIONS

Amendment:

The following clarifications are made in order to better understand some of the sections of the CPS:

I. *Recognized certificate.*

- Recognized electronic signature certificates can also be used, if so defined in the corresponding type of certificate, to sign authentication messages, particularly SSL or TLS client challenges, S/MIME secure e-mail, encryption without key recovery and others.

  These certificate options are no longer equivalent to a handwritten signature (see section 1.3.4.1.1 *Recognized certificate,* letter b)).
- Only *Main Office* and *EV Main Office* recognized certificates are issued to reliably identify websites (see section 1.3.4.1.1 *Recognized certificate,* letter c)).

II. *Limitations on the usage of certificates.*

No certificate regulated by this Certification Practice Statement can be used to conduct transactions as a Registration Authority (see section 1.3.4.3. *Limitations on the usage of certificates,* paragraph 3*).*

III. Certificate application

The Certification Practice Statement is adapted to the *Specific documentation for each certificate*, establishing that *once the identity of the applicant has been verified before the Registration Authority, the applicant shall sign the Application of*

Issuance of Certificate, thereby accepting the Subscriber Contract and the Terms of Use (see section 1.4 *Certificate application*)

IV. Frequency of issuance of Certificate Revocation Lists

With regard to CRLs, if no revocations occur, the Certificate Revocation List is refreshed daily (see section 4.4.10, *CRL issuance frequency,* paragraph 2).

V. Key sizes and algorithms used

In addition to the CA root 2007, a second certificate with SHA-256 has been issued in the subordinate CAs (see section 6.1.5*, Key sizes and algorithms used).*

VI. Public key parameters generation

With regard to the keys generated using an HSM and the cryptographic keys generated on a cryptographic device: designed to comply with FIPS 140-1 Level 3 standards (for HSM and 2 for the latter) (see section 6.1.7).