



CERTIFICATION PRACTICE STATEMENT UPDATE

Reference: IZENPE-CPS UPDATE
Version no: v4.6
Date: 16 of november, 2009

© IZENPE 2009

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



Versions

Version	Date	Author(s)	Changes/Comments
4.6 updates CPS version 4.5	xx/xx/2009	IZENPE Legal Office	Modifications derived from CPS version 4.5



General information

Document checklist

Title:	Certification Practice Statement Update
Reference code:	
Version:	4.6
Version date:	xx/xx/2009
Approval date	xx/xx/2009
Documentation used:	CPS 4.5



In accordance with point 8, the Izenpe S.A Certification Practice Statement allows modifications to be made to the Certification Practice Statement. Despite the fact that these modifications appear in this document, if you request, use or place trust in the certificate issued by Izenpe, S.A, you must be aware of the whole updated Certification Practice Statement.

Update entry 1

New subordinate CAs

Amendment: CPS Version 4.4



ENTRY 1: NEW TYPES OF CERTIFICATES

Amendment:

IZENPE, in accordance with Act 11/2007, of 22 June, on Electronic Access of Citizens to Public Services, issues two new types of certificates (see section 1.1):

- Electronic main office certificate
- Electronic main office certificate EV (extended validation)



ENTRY 2: NEW CAUSE FOR REVOCATION

Amendment:

A new cause for revocation has been added (see section 4.4.1).

m). If IZENPE receives an application for issuance of certificate, and a valid certificate of the same class and uniqueness already exists, the valid certificate will be revoked upon revocation request from the applicant.



ENTRY 3: PROTECTION OF PERSONAL INFORMATION

Amendment:

Section 9 on Personal Data Protection is updated.



ENTRY 4: WEBTRUST FOR CERTIFICATION AUTHORITIES – EXTENDED VALIDATION AUDIT CRITERIA

Amendment

In compliance (version 1.1), the following clarifications have been incorporated,

- I. With regard to the special requirements regarding key compromise,

If the private key associated with the certificate is compromised the subscriber/key owner shall notify the Registration Authority to request certificate revocation and cease using the certificate (see section 4.4.17)

- II. With regard to the method of destroying the private key,

In addition to putting on record the existence of the procedure for the destruction of CA keys,

The following is specified:

This procedure is not applied to user signature or authentication keys, since they are not created by the CA, except in the case of key changeover using the same cryptographic device. In such cases the previous key will be destroyed and new keys will be generated on the same media (see section 6.2.8)