# ZIURTAPEN PRAKTIKEN DEKLARAZIOAREN EGUNERATZEA

Erreferentzia: IZENPE-ACTUALIZACIÓN DPC
Bertsio zkia.: v 4.9
Data: 2011ko martxoaren 29a



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

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

# Bertsioen kontrola

| Bertsioa | Data | Egilea(k) | Aldaketak/Iruzkinak |
|---|---|---|---|
| 4.9 bertsioa ZPDaren 4.8 bertsioaren eguneratzea da | 2011/03/29 | IZENPEren Aholkularitza Juridikoa | ZPDaren 4.8 bertsioan eragin diren aldaketak |

# Informazio orokorra

## Dokumentuen kontrola

| | |
|---|---|
| **Izenburua:** | Ziurtapen Praktiken Deklarazioa eguneratzea. |
| **Erreferentzia-kodea:** | |
| **Bertsioa:** | 4.9 |
| **Argitalpen-data:** | 2011/03/29 |
| **Onespen-data:** | 2011/03/29 |
| **Erabilitako dokumentazioa:** | ZPD 4.8 |

IZENPE, SAren Ziurtapen Praktiken Deklarazioak, 8. epigrafearen arabera, Ziurtapen Praktiken Deklarazioan aldaketak egiteko aukera ematen du. Aldaketa horiek dokumentu honetan jaso badira ere, IZENPE, SAk ematen dituen ziurtagiriak eskatzen edo erabiltzen badituzu, edo ziurtagiri horietaz fidatzen bazara, nahitaez ezagutu beharko duzu oso-osorik Ziurtapen Praktiken Deklarazio eguneratua.

# 1. SARRERA: DOKUMENTAZIOA KONTSERBATZEKO EPEAK

**Zuzenketa:**

IZENPEk *balidazio hedatua* duten ziurtapenak jaulkitzearen ondorioz, eta *Webtrust for EV* araua betetzeko egindako ikuskapenaren ondoren, argitu behar da IZENPEk 7 urtez gordetzen duela informazio eta dokumentazio guztia, *EV* motako ziurtagiriei dagokiena ez ezik, onartu gabeko ziurtagiriei dagokiena ere bai (ikus *2.1.2 Zerbitzua egiteko betebeharra* epigrafea).

## 2. SARRERA: HAINBAT ARGIBIDE

**Zuzenketa:**

ZPDren epigrafe batzuk ulergarriagoak izateko, honako argibide hauek eman dira:

I. *Ziurtagiri onartua.*

- Sinadura elektronikoko onartutako ziurtagiriak kautotze-mezuak sinatzeko ere erabil daitezke –dagokion ziurtagiri motan hala definitzen bada–, bereziki SSL edo TLS bezeroen testiguak, S/MIME posta elektroniko segurua, gako-berreskurapen gabeko zifratzeak eta beste zenbait.

  Ezabatu egiten da eskuz idatzitako sinaduraren baliokide gisa jotzearen aipamena (ikus *1.3.4.1.1 Ziurtagiri onartua* epigrafearen b) atala).
- Argitu egiten da *Egoitza* motako eta *Balidazio hedatuko egoitza* motako ziurtagiri onartuak soilik jaulkitzen direla webguneak modu fidagarrian identifikatzeko (ikus *1.3.4.1.1 Ziurtagiri onartua* epigrafearen c) atala).

II. *Ziurtagiriak erabiltzeko mugak.*

Argitu egiten da Ziurtapen Praktiken Deklarazio honen erregulazioaren mende dagoen ziurtagirietako bat bera ere ezin dela erabili erregistro-entitate gisa izapideak egiteko (ikus *1.3.4.3. Ziurtagiriak erabiltzeko mugak* epigrafeko hirugarren paragrafoa*).*

III. Ziurtagiria eskatzea

Ziurtapen Praktiken Deklarazioa egokitu egin zaio ziurtagiri bakoitzerako berariazko dokumentazioan zehaztutakoari, eta honakoa ezarriko du: *Eskatzailearen nortasuna*

*Erregistro Entitatearen aurrean egiaztatu ondoren, eskatzaileak ziurtagiria jaulkitzeko eskaera sinatu beharko du, eta hala harpidedunaren kontratua eta erabilera-baldintzak onartuko ditu* (ikus *1.4. Ziurtagiriaren eskaera* epigrafea).

IV. Ezeztatutako ziurtagirien zerrendak jaulkitzeko maiztasuna

Ezeztatutako Ziurtagirien Zerrendei (CRLei) dagokienez, ezeztatzeak gertatzen ez badira, ezeztatutako ziurtagirien zerrenda egunero berrituko da (Ikus *4.4.10. Ezeztatutako ziurtagirien zerrendak jaulkitzeko maiztasuna* epigrafea, bigarren paragrafoa).

V. Gakoen tamainak eta erabilitako algoritmoak

Oinarrizko CA 2007n ez ezik, mendeko CAetan ere jaulki da SHA-256 duen bigarren ziurtagiri bat (ikus *6.1.5. Gakoen tamainak eta erabilitako algoritmoak* epigrafea).

VI. Gako publikoko parametroak sortzea

HSM euskarrian sortutako gakoei dagokienez zein gailu kriptografikoak sortutako gako kriptografikoei dagokienez, FIPS 140-2 gomendioak jarraituko dira, 3. mailakoak lehenengoetarako eta 2. mailakoak bigarrenetarako (ikus 6.1.7. epigrafea).