



ZIURTAPEN PRAKTIKEN DEKLARAZIOAREN EGUNERATZEA

Erreferentzia: IZENPE-ACTUALIZACIÓN DPC
Bertsio zkia.: v 5.01
Data 2013ko uztailaren 19a

© IZENPE 2013

Dokumentu hau IZENPErena da. Osotasunean soilik erreproduzi daiteke.

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

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



Informazio orokorra

Dokumentuen kontrola

Izenburua:	Ziurtapen Praktiken Deklarazioa
Bertsioa:	5.01
Onartze-data:	2013/07/19
Erabilitako dokumentazioa:	ZPD 5.0
Egilea(k)	IZENPEko Aholkularitza Juridikoa IZENPEko arlo teknikoa
Aldaketak/Iruzkina	5.01 bertsioa 5.0. bertsioaren eguneratzea da



IZENPE, Saren Ziurtapen Praktiken Deklarazioren 9.11. epigrafearen arabera, aldatetak egin daitezke Ziurtapen Praktiken Deklarazioan. 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_Egokitzapena

Zuzenketa:

ETSI arauen araberako TUV IT ikuskaritzaren ondorioz, honako aldaketa hauek sartu dira:

EPIGRAFEA	ALDAKETA
5.8.1	- IZENPErekin zerbitzugintzako kontratua duten beste hirugarren batzuen edozein baimen (identifikatzeko, jaulkitzeko, gordetzeko, eta abar) amaitutzat emango da.
9.6.1	- Segurtasuneko araudia eta estandarrak betetzea (datu pertsonalak babesteari buruzko Lege Organikoa, ISO, ETSI eta IZENPEren segurtasun-politika). - Gordetzeko zerbitzuaren hornitzaileei segurtasuneko araudia eta estandarrak (datu pertsonalak babesteari buruzko Lege Organikoa, ISO, ETSI eta IZENPEren segurtasun-politika) bete ditzaten eskatzea.
9.6.7	- Segurtasuneko araudia eta estandarrak betetzea (datu pertsonalak babesteari buruzko Lege Organikoa, ISO, ETSI eta IZENPEren segurtasun-politika).
9.11.2	- IZENPEren ordeztasun, IZENPEren Segurtasun Batzordea jarri da.
6.1.1	- Edukitzaileak berak sortutako gakoaren kasuan, gako horiek algoritmoko eta gakoaren gutxienezko luzerako gomendioaren arabera sortu beharko dira, ETSI TS 102 176an definitutako moduan.
6.1.6	- Erabilitako padding-eskema emsa-pkcs1-v2.1 da (RFC 3447, 9.2 sekzioaren arabera).
6.2.7	- Gako pribatuak modulu kriptografikoen kanpo biltegiatzen diren kasuan, gako pribatuak behar bezala babestuko dira, hau da, fisikoki modulu kriptografikoen barruan izango luketen babes-maila berarekin. IZENPEk ziurtagintza-agintaritzen gako pribatuak biltegiatzeko erabilitako HSMs guztiek FIPS 140-2, 3. maila, ziurtagintza dute.