ZIURTAPEN PRAKTIKEN DEKLARAZIOAREN EGUNERATZEA

Erreferentzia: IZENPE-ACTUALIZACIÓN DPC

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

www.izenpe.com
info@izenpe.com
Tel.: 945 06 77 23

IZENPEren Ziurtapen Praktiken Deklarazioren 9.11. epigrafearen arabera, aldaketak egin daitezke Ziurtapen Praktiken Deklarazioan. Aldaketa horiek dokumentu honetan jaso badira ere, IZENPEk ematen dituen ziurtagiriak eskatzen edo erabiltzen badituzu, edo ziurtagiri horietaz fidatzen bazara, nahitaez ezagutu beharko duzu oso-osorik Ziurtapen Praktiken Deklarazio eguneratua.

Informazio orokorra_ 5.01 bertsioa, 5.0 bertsioaren eguneratze gisa

Dokumentuen kontrola

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

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 ordez, IZENPEren Segurtasun Batzordea jarri da.
6.1.1	- Edukitzaileak berak sortutako gakoen kasuan, gako horiek algoritmoko eta gakoen gutxieneko luzerako gomendioen 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 kriptografikoez kanpo biltegiratzen direnean, gako pribatuak behar bezala babestuko dira, hau da, fisikoki modulu kriptografikoen barruan izango luketen babes-maila berarekin. IZENPEk ziurtapen-agintaritzen gako pribatuak biltegiratzeko erabilitako HSM guztiek FIPS 140-2, 3. maila, ziurtapena dute.

Informazio orokorra_ 5.02 bertsioa, 5.02 bertsioaren eguneratze gisa

Dokumentuen kontrola

Izenburua:	Ziurtapen Praktiken Deklarazioa eguneratzea.
Bertsioa:	5.02
Onartze-data:	2014/09/16
Erabilitako dokumentazioa:	ZPD 5.01
Egilea(k)	IZENPEko Aholkularitza Juridikoa IZENPEko arlo teknikoa
Aldaketak/Iruzkinak	5.02 bertsioa 5.01. bertsioaren eguneratzea da

Zuzenketa:

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

EPIGRAFEA	ALDAKETA
5.5.2	- Argitu da ziurtagiriei buruzko informazioa eta komunikazioa 15 urtez gutxienez gordetzen dela ziurtagiri onartuen kasuan, eta 7 urtez gutxienez ziurtagiri onartu gabeen kasuan, betiere jaulkitzen diren datatik hartuta. -
6.1.5, 7.1.2 eta 7.1.3	- SHA1 algoritmoa SHA 2 algoritmoarekin ordeztu da. - Gakoen tamaina 1024 izatetik 2048 izatera pasa da.
6.2.3	- Ezabatu egin da IZENPEk gako pribatuak biltegiratzearen aurreikuspena.
6.2.7	- Jakinarazi da IZENPEk CAen gakoak sortzeko ETSI TS 102 042, 7.2.1 g) gomendioa eta Baseline Requirement Guidelines 17.7 gomendioa jarraitzen dituela.

Informazio orokorra_ 5.04 bertsioa, 5.03 bertsioaren eguneratze gisa

Dokumentuen kontrola

Izenburua:	Ziurtapen Praktiken Deklarazioa eguneratzea.
Bertsioa:	5.04
Onartze-data:	2016/06/30
Erabilitako dokumentazioa:	ZPD 5.04
Egilea(k)	IZENPEko Aholkularitza Juridikoa IZENPEko arlo teknikoa
Aldaketak/Iruzkinak	5.04 bertsioa 5.03. bertsioaren eguneratzea da

ALDAKETAK

Eskakizun osagarriak	➢ Ordezkariaren, zigiluaren, SSL kualifikatuaren eta herritar kualifikatu gabearen profil berriak txertatu dira. ➢ Profil guztien (daudenen eta berrien) ziurtapen-maila identifikatu da. ➢ EN arauek eskatutako ziurtagirien luzapen berriak adierazi dira.
Eskakizun eguneratuak	➢ eIDAS araudiari dagozkion ETSIren EN arauen erreferentziak eta eskakizunak eguneratu dira
Argibideak	➢ Puntuak eguneratu dira, aplikatzekoak diren ETSIren eta CABForumen arauetara egokitzeko
Editoriala	
Ezabatutako eskakizunak	➢ Denbora zigilatzeko zerbitzurako (TSA) betekizun guztiak ezabatu dira ➢ SHA-1aren erreferentzia ezabatu da

Informazio orokorra_ 5.05 bertsioa, 5.04 bertsioaren eguneratze gisa

Dokumentuen kontrola

Izenburua:	Ziurtapen Praktiken Deklarazioa eguneratzea.
Bertsioa:	5.05
Onartze-data:	2016/10/26
Erabilitako dokumentazioa:	ZPD 5.04
Egilea(k)	IZENPEko Aholkularitza Juridikoa IZENPEko arlo teknikoa
Aldaketak/Iruzkinak	5.05 bertsioa 5.04. bertsioaren eguneratzea da

ALDAKETAK

Eskakizun osagarriak	➢ 1.1. *Aurkezpena* epigrafea: ordezkariaren ziurtagiri mota barnean hartzen da, edukitzaile-euskarrian.
Eskakizun eguneratuak	➢ 4.3.3. *CAk beste entitate batzuei ziurtagiria jaulki izana jakinaraztea* epigrafea: IZENPEren CTa kendu da. ➢ 5.8.1. *CAren edo RAren amaiera* epigrafea: "edo Administrazio Kontseiluak izendatutako pertsona/ak; horrek erabakiko du mekanismorik egokiena" aurreikuspena barnean hartu da, betiere ziurtagiriak jaulkitzeko zerbitzua uzten denean hori jakinarazteko ardura dutenen artean (5.8.1.). ➢ 4.9.9. On line ezeztatzea egiaztatzeko eskakizunak epigrafea: "*Ezeztatzen diren ziurtagiriak, CRLtik kenduko dira*" esaldia osatuko da, "*Ezeztatzen diren ziurtagiriak CRLtik kenduko dira, baina ziurtagiriaren egoerari buruzko informazioa eskaintzen jarraituko da on lineko egiaztatzearen bitartez, iraungita egonik ere*".
Argibideak	
Editoriala	
Ezabatutako eskakizunak	

Informazio orokorra_ 5.06 bertsioa, 5.05 bertsioaren eguneratze gisa

Dokumentuen kontrola

Izenburua:	Ziurtapen Praktiken Deklarazioa eguneratzea.
Bertsioa:	5.06
Onartze-data:	2016/11/10
Erabilitako dokumentazioa:	ZPD 5.05
Egilea(k)	IZENPEko Aholkularitza Juridikoa IZENPEko arlo teknikoa
Aldaketak/Iruzkinak	5.06 bertsioa 5.05. bertsioaren eguneratzea da

ALDAKETAK

Eskakizun osagarriak	➢
Eskakizun eguneratuak	➢
Argibideak	
Editoriala	
Ezabatutako eskakizunak	➢ HSMaren eta hodeiko ziurtagiriaren erreferentzia guztiak ezabatu dira

Informazio orokorra_ 5.07 bertsioa, 5.06 bertsioaren eguneratze gisa

Dokumentuen kontrola

Izenburua:	Ziurtapen Praktiken Deklarazioa eguneratzea.
Bertsioa:	6.0
Onartze-data:	2017/06/01
Erabilitako dokumentazioa:	ZPD 5.06
Egilea(k)	IZENPEko Aholkularitza Juridikoa IZENPEko arlo teknikoa
Aldaketak/Iruzkinak	6.0 bertsioa 5.06. bertsioaren eguneratzea da

ALDAKETAK

	EPIGRAFEA / ARGIBIDEAK
Aurreko bertsioarekiko eguneratzeak	– Sarrera. – IZENPEk ETSI EN 301 549 gomendioak izango ditu kontuan. 1.1. Aurkezpena. IZENPEk jaulkitako identifikazio-bitartekoen erreferentziak eguneratu dira, eIDAS araudiak eskatzen duenari jarraituta. – 4.9.3. IZENPEren web-helbidea eguneratu da, orain www.izenpe.eus da. – 5.8.1. Jarduerari uzten bazaio, zehaztu da IZENPEk jarduera uztearen berri emango diola organo eskudunari eta gutxienez 2 hilabete aurretik egin beharko duela. –
Argibideak	
Formatua eguneratzea	
Ezabatzeak	

Informazio orokorra_ 6.1 bertsioa, 6.0 bertsioaren eguneratze gisa

Dokumentuen kontrola

Izenburua:	Ziurtapen Praktiken Deklarazioa eguneratzea.
Bertsioa:	6.1
Onartze-data:	2018/03/16
Erabilitako dokumentazioa:	ZPD 6.0
Egilea(k)	IZENPEko Aholkularitza Juridikoa IZENPEko arlo teknikoa
Aldaketak/Iruzkinak	6.1 bertsioa 6.00. bertsioaren eguneratzea da

ALDAKETAK

	EPIGRAFEA / ARGIBIDEAK
Aurreko bertsioarekiko eguneratzeak	– 1.1. Aurkezpena. – IZENPEk jaulkitako identifikazio-bitartekoen erreferentziak eguneratu dira, eIDAS araudiak eskatzen duenari jarraituta. – 5.8.1. Jarduerari uzten bazaio, zehaztu da IZENPEk jarduera uztearen berri emango diola organo eskudunari eta gutxienez 2 hilabete aurretik egin beharko duela. – 6.1.1. Gako-parea sortzea. Adierazten da – Gako kriptografiko guztiak sortzean, ETSI TS 119 312 gomendioan definitutakoari jarraituko zaio. – Esponente publikoaren balioa zenbaki lehen bat da, 3 edo handiagoa. – 6.5.1. Segurtasun informatikorako berariazko eskakizun teknikoak Adierazi da ziurtagiriak jaulkitzeko ahalmena duten operadore-kontu guztiek faktore bikoitzean oinarritutako sarbide-kontrola dutela. – 7.2. Ezeztatutako ziurtagirien zerrendaren profila RFC 6962 arauan deskribatzen denaren arabera, aurreziurtagiri bat ez da inola ere hartuko RFC 5280 arauan definitutako ezaugarriak dituen ziurtagiritzat. – 7.3. OCSP profila – OCSP erantzunen adostasuna, RFC 6960 arauaren arabera. – 7.3.3. OCSPari dagozkion beste alderdi batzuk txertatzen dira.

	– 9.13. Aplikatzeko den araudia. Eguneratzea. – 9.14. Aplikatzekoa den araudia betetzea. Eguneratzea.
Argibideak	
Formatua eguneratzea	
Ezabatzeak	

Informazio orokorra_ 6.2 bertsioa, 6.1 bertsioaren eguneratze gisa

Dokumentuen kontrola

Izenburua:	Ziurtapen Praktiken Deklarazioa eguneratzea.
Bertsioa:	6.2
Onartze-data:	2018/12/04
Erabilitako dokumentazioa:	ZPD 6.1
Egilea(k)	IZENPEko Aholkularitza Juridikoa. IZENPEko arlo teknikoa.
Aldaketak/Iruzkinak	6.2 bertsioa 6.1. bertsioaren eguneratzea da

ALDAKETAK

	EPIGRAFEA / ARGIBIDEAK
Aurreko bertsioarekiko eguneratzeak	– 9.6.8. Ziurtagiri-eskatzailearen betebeharrak: ziurtagiriaren zenbatekoa ordaintzeko eskakizuna eransten da. – 5.3.2 Trebakuntza-baldintzak: RA operadoreen trebakuntza-baldintzak eransten dira. – 9.4. Datu pertsonalen babesa: indarrean dagoen araudia egokitzen da.
Argibideak	
Formatua eguneratzea	
Ezabatzeak	