ZIURTAPEN-PRAKTIKEN DEKLARAZIOAREN EGUNERATZEA

Erreferentzia: IZENPE-ACTUALIZACIÓN DPC

© IZENPE 2021

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 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.

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.

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	- Izenpek gako pribatuak biltegiratzearen aurreikuspena ezabatu da.
6.2.7	- Izenpek CAen gakoak sortzeko ETSI TS 102 042, 7.2.1 g) gomendioa eta Baseline Requirement Guidelines 17.7 gomendioa jarraitzen dituela jakinarazi da.

Dokumentuen kontrola

Izenburua:	Ziurtapen Praktiken Deklarazioa eguneratzea
Bertsioa:	5.04
Onartze-data:	2016/06/30
Erabilitako dokumentazioa:	ZPD 5.03
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

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 hartu 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 osatu 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_ 6.0 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	

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. – 4.9.3., 6.1.7., 9.10. 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. – 6.1.1. Gako-parea sortzea. Adierazten denez – 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 txertatu dira. – 9.13. Aplikatzekoa den araudia. Eguneratzea. – 9.14. Aplikatzekoa den araudia betetzea. Eguneratzea.
Argibideak	
Formatua eguneratzea	
Ezabatzeak	

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 erantsi da. – 5.3.2 Trebakuntza-baldintzak: RA operadoreen trebakuntza-baldintzak erantsi dira. – 9.4. Datu pertsonalen babesa: indarrean dagoen araudia egokitu da.
Argibideak	
Formatua eguneratzea	
Ezabatzeak	

Informazio orokorra_ 6.3 bertsioa, 6.2 bertsioaren eguneratze gisa

Dokumentuen kontrola

Izenburua:	Ziurtapen Praktiken Deklarazioa eguneratzea
Bertsioa:	6.3
Onartze-data:	2019/04/04
Erabilitako dokumentazioa:	ZPD 6.2
Egilea(k)	Izenpeko Aholkularitza Juridikoa. Izenpeko arlo teknikoa.
Aldaketak/Iruzkinak	6.3 bertsioa 6.2. bertsioaren eguneratzea da

ALDAKETAK

	EPIGRAFEA / ARGIBIDEAK
Aurreko bertsioarekiko eguneratzeak	– 1.1. atala: HSMko profilen ziurtapen-maila eguneratu da. Softwarean profesionalaren ziurtapen-mailan zegoen errorea zuzendu da – 1.1. atala: gailu-profila erantsi da – 1.3.1. atala: CAen zuhaitza eguneratu da.
Argibideak	
Formatua eguneratzea	
Ezabatzeak	

Dokumentuen kontrola

Izenburua:	Ziurtapen Praktiken Deklarazioa eguneratzea
Bertsioa:	6.4
Onartze-data:	2020/06/03
Erabilitako dokumentazioa:	ZPD 6.3
Egilea(k)	Segurtasun-arduraduna
Aldaketak/Iruzkinak	6.4 bertsioa 6.3. bertsioaren eguneratzea da

ALDAKETAK

EPIGRAFEA	ARGIBIDEAK
1. Sarrera	• ETSI arauen bertsio eguneratuak
1.1. Aurkezpena	• Konfiantza-zerbitzu kualifikatuen eta kualifikatu gabeen zerrenda erantsi da • Ziurtagiri-profil bakoitzean eIDAS sinadura motaren zutabea erantsi da • Mobileren, NQC goitizenaren eta IoT gailuaren profilak erantsi dira
1.3.1. Ziurtapen-agintaritzak.	• Oinarrizko CAren eta CA guztien profilak erantsi dira
1.4.2. Ziurtagiriaren erabilera debekatuak	• RA gisa tramiteak egiteko ziurtagiriak erabiltzeko debekua ezabatu da
1.5.2. Harremanetarako datuak	• Harremanetarako telefonoa eguneratu da
1.5.4. ZPDa onartzeko prozedura	• "Administrazio Kontseilua" "Segurtasun Batzordearekin" ordeztu eta eguneratu da, ZPDaren onarpenaren organo arduradun gisa
1.6.1. Definizioak	• Datuak Babesteko Erregelamendua erantsi da • ZZEaren definizioa TSParen definizioarekin ordeztu da
2.2. Ziurtapen-informazioaren argitalpena	• www.izenpe.eus web-gunean argitaratzeko zerbitzuari buruzko erreferentziak ezabatu dira • Izenperen SSLen URL testen erreferentzia erantsi da
2.2.1. Argitalpen- eta jakinarazte-politika	• ZPDan egindako aldaketak 30 egunez mantentzearen eta bertsio zaharrak kentzearen betebeharra ezabatu da
3.1.3. Izen-bakartasuna	• "Izenpek ez du ziurtagiri anonimorik jaulkitzen" testua ezabatu da
4.4.1. Ziurtagiria onartzeko prozesua	• "Harpidedunaren Kontratua" erreferentzia "Erabiltzeko terminoak eta baldintzak" erreferentziarekin ordeztu da

4.3.3. CAk beste entitate batzuei ziurtagiria jaulki izana jakinaraztea	• CTetan argitaratzeko Google-en politika eguneratu da
4.9.2. Nork eska dezake ziurtagiria ezeztatzea	• Ezeztatzea eska dezaketen profilak zehaztu dira, eta politika bakoitzari buruzko aipamena kendu da. Politika bakoitzean ZPDaren atal honen erreferentzia gehitu beharko da
4.9.3. Ezeztatzeko eskaeren tratamendua	• Ezeztatzea eskatzeko dauden kanalen zerrenda eguneratu da. Politika bakoitzean ZPDaren atal honen erreferentzia gehitu beharko da
4.9.10. Ezeztatzeak ohartarazteko eskura dauden beste modu batzuk	• Baliogabetzeen jakinarazpenetarako korporatiboen salbuespena ezabatu da.
5.1.2 RAetarako sarbide fisikoa	• Izenperen segurtasun-politika betetzeko betebeharra eguneratu da, Hornitzaileen Segurtasun Politika dela eta.
5.3.4. Trebakuntza eguneratzeko baldintzak eta maiztasuna	• “Trusted Roles”en urteko prestakuntzaren betekizuna erantsi da
5.3.7. Langileak kontratatzeko baldintzak	• Azpikontratatutako langileek Hornitzaileen Segurtasun Politika betetzeko betebeharra gehitu da
6.1.1. Gako-parea sortzea	• APP erantsi da gakoen edukitzaile gisa
6.1.5. Gakoen tamainak eta erabilitako algoritmoak	• SHA-256 eguneratu da, SHA-2rekin
6.2.8. Gako pribatua aktibatzeko metodoa	• Politika espezifikora birbideratzen da, kasuan kasuko aktibatze-mekanismoak ezagutzeko.
6.2.9. Gako pribatua desaktibatzeko metodoa	• Politika espezifikora birbideratzeko eta kasuan-kasuan desaktibatze-mekanismoak ezagutzeko zuzendu da
6.3.2. Ziurtagiriaren eragiketa-aldiak eta gako-parearen erabilera-aldiak	• EVez bestelako subCAen iraupena erantsi da
6.7. Sareko segurtasunaren kontrolak	• IPS sistemen existentzia erantsi da
7.3.3. OCSParen beste alderdi batzuk	• Izenperenak ez diren ziurtagirien kontsultei emandako OCSP erantzunari buruzko informazioa gehitu da
9.6.4. Erabiltzaileei eman beharreko informazioa: betebeharrak	• "Erabilera-baldintzei" buruzko aipamena ordeztu da "Erabiltzeko terminoak eta baldintzak eta Gako Publikoko Azpiegitura Dibulgatzeko Akordioa (PKI-PDS)" aipamenarekin • Izenperen argitalpen-zerbitzuarekiko erreferentziak ezabatu dira
9.6.7. Erregistro-entitatearen betebeharrak	• Eskuordetzeen kasuan, erregistro-entitate gisa funtzionatzen hasi aurretik, akordio bat sinatzeko betebeharra gehitu da

	• Hornitzaileen Segurtasun Politika betetzeko betebeharra erantsi da
9.7.1. Ziurtapen-agintaritzaren erantzukizunak	• Erantzukizun Zibilaren Aseguruaren zenbatekoa ezabatu da
9.11.1. Aldaketetarako prozedura	• Administrazio Kontseiluaren ordez Segurtasun Batzordea jarri da

Dokumentuen kontrola

Izenburua:	Ziurtapen Praktiken Deklarazioa eguneratzea
Bertsioa:	6.5
Onartze-data:	2020/07/10
Erabilitako dokumentazioa:	ZPD 6.4
Egilea(k)	Segurtasun-arduraduna
Aldaketak/Iruzkinak	6.5 bertsioa 6.4. bertsioaren eguneratzea da

ALDAKETAK

EPIGRAFEA	ARGIBIDEAK
1.5.2. Harremanetarako datuak	• Izenperen harremanetarako datuen taula erantsi da • Gorabeheren kasuan Izenperekin harremanetan jartzeko helbide elektronikoa erantsi da
1.5.3. Ziurtapen Praktiken Deklarazioaren egokitzapenaren arduradunak	• Izenperen harremanetarako datuen taula ezabatu da

Dokumentuen kontrola

Izenburua:	Ziurtapen Praktiken Deklarazioa eguneratzea
Bertsioa:	6.6
Onartze-data:	2020/09/01
Erabilitako dokumentazioa:	ZPD 6.5
Egilea(k)	Segurtasun-arduraduna
Aldaketak/Iruzkinak	6.6 bertsioa 6.5. bertsioaren eguneratzea da

ALDAKETAK

EPIGRAFEA	ARGIBIDEAK
Hainbat	Zenbait puntu erantsi dira RFC 3647 betetzeko
5.8.1. Ziurtapen-entitatea	Izenperen jarduerari uzteko baldintzak eguneratu dira
5.7.3. CAren gako pribatuaren konpromisoaren aurreko prozedura	CAen gakoen konpromisoetan egin beharreko urratsak zehaztu dira
I. eranskina	CA berrien profilak erantsi dira
9.4. Datu pertsonalak babestea	Sekzioa eguneratu da, RFC 3647 betetzeko

Informazio orokorra_ 6.7 bertsioa, 6.6 bertsioaren eguneratze gisa

Dokumentuen kontrola

Izenburua:	Ziurtapen Praktiken Deklarazioa eguneratzea
Bertsioa:	6.7
Onartze-data:	2020/11/26
Erabilitako dokumentazioa:	DPC 6.6
Egilea(k)	Segurtasun-arduraduna
Aldaketak/Iruzkinak	6.7 bertsioa 6.6. bertsioaren eguneratzea da

ALDAKETAK

EPIGRAFEA	ARGIBIDEAK
1.1 Helburua	2020ko oinarrizko CA berrien profilak gehitu dira

Informazio orokorra_ 6.8 bertsioa, 6.7 bertsioaren eguneratze gisa

Dokumentuen kontrola

Izenburua:	Ziurtapen Praktiken Deklarazioa eguneratzea
Bertsioa:	6.8
Onartze-data:	2021/02/12
Erabilitako dokumentazioa:	DPC 6.8
Egilea(k)	Segurtasun-arduraduna
Aldaketak/Iruzkinak	6.8 bertsioa 6.7. bertsioaren eguneratzea da

ALDAKETAK

EPIGRAFEA	ARGIBIDEAK
Gehigarri I	Barneko SSLen oinarrizko CA profila gehitu dira

Ainhoa Anitua Gil
Responsable de Marketing/ Marketing Arduraduna

Firmado digitalmente por ZIURTAPEN ETA ZERBITZU ENPRESA-EMPRESA DE CERTIFICACION Y SERVIC
Fecha: 2021.02.22 12:32:15 +01'00'