ZIURTAPEN PRAKTIKEN DEKLARAZIOA

Erreferentzia:	IZENPE-ZPD
Bertsio zk.:	v 5.04
Data:	2016ko uztailaren 1a

© IZENPE 2016

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

Aurkibidea

Edukia

1 Sarrera 13

1.1 Aurkezpena 14

1.2 Identifikazioa 15

1.3 PKI gako publikoko azpiegituraren parte-hartzaileak 16

1.3.1 Ziurtapen-agintaritzek 16

1.3.2 Erregistro-entitateak 19

1.3.3 Ziurtagirien erabiltzaile diren azken entitateak 19

1.3.4 Konfiantzako hirugarren batzuk 20

1.4 Ziurtagiriaren erabilerak 21

1.4.1 Ziurtagiriaren erabilera egokiak 21

1.4.2 Ziurtagiriaren erabilera debekatuak 22

1.5 Politikak 23

1.5.1 Dokumentazioaren kudeaketaz arduratzen den entitatea 23

1.5.2 Harremanetarako datuak 23

1.5.3 Ziurtapen Praktiken Deklarazioaren egokitzapenaren arduradunak 23

1.5.4 Ziurtapen Praktiken Deklarazioa onartzeko prozedura 23

1.6 Definizioak eta akronimoak 23

1.6.1 Definizioak 23

1.6.2 Akronimoak 28

2 Argitalpena eta informazio-biltegiaren arduradunak 29

2.1 Informazio-biltegia 29

2.2 Ziurtapen-informazioaren argitalpena 29

2.2.1 Argitalpen- eta jakinarazte-politika 29

2.2.2 Ziurtapen Praktiken Deklarazioan argitaratzen ez diren elementuak 29

2.3 Argitalpen-maiztasuna 30

2.4 Biltegirako sarrera kontrolatzea 30

3 Izenak 31

3.1.1 Izen motak 31

3.1.2 Izenen formatuak interpretatzeko arauak 31

3.1.3 Izen-bakartasuna 31

3.1.4 Izenen eta marka erregistratuen tratamenduaren arloko gatazkak ebaztea 32

3.2 Identitatea balidatzea 32

3.2.1 Gako pribatuaren jabetza frogatzeko metodoak 32

3.2.2 Antolakundearen nortasuna kautotzea 32

3.2.3 Pertsona fisiko eskatzailearen nortasuna kautotzea 32

3.3 Gakoak berriro jaulkitzeko eskaeretarako identifikatzea eta kautotzea 33

3.4 Ezeztatzeko eskaeretarako identifikatzea eta kautotzea 33

4 Ziurtagirien bizi-zikloaren baldintza operatiboak 34

4.1 Ziurtagiria eskatzea 34

4.1.1 Eskaeraren egiaztapena 34

4.1.2 Inskribatzeko prozesua eta erantzukizunak. 34

4.2 Eskaerak prozesatzea 35

4.2.1 Identifikatzeko eta kautotzeko eginkizunak egitea 35

4.2.2 Eskaerak onartzea edo baztertzea 35

4.3 Ziurtagiria jaulkitzea 35

4.3.1 CAren jardunak ziurtagiriak jaulkitzean 36

4.3.2 Jaulkipena jakinaraztea harpidedunari 36

4.4 Ziurtagiria onartzea 36

4.4.1 Ziurtagiria onartzeko prozesua 36

4.4.2 CAk ziurtagiria argitaratzea 36

4.4.3 CAk beste entitate batzuei ziurtagiria jaulki izana jakinaraztea 36

4.5 Gako-parea eta ziurtagiriaren erabilera 36

4.5.1 Harpidedunaren gako pribatua eta ziurtagiriaren erabilera 36

4.5.2 Ziurtagirietan konfiantza duten hirugarren batzuek gako publikoa eta ziurtagiria erabiltzea 38

4.6 Ziurtagiria berritzea 39

4.6.1 Ziurtagiria berritzeko zirkunstantziak 39

4.6.2 Nork eska dezake ziurtagiria berritzea 39

4.6.3 Ziurtagiria berritzeko eskaeren tratamendua 39

4.6.4 Harpidedunari jakinaraztea 39

4.6.5 Ziurtagiri berritua onartzeko prozedura 39

4.6.6 Ziurtagiria argitaratzea 39

4.6.7 Beste entitate batzuei jakinaraztea 39

4.7 Ziurtagiria berritzea, haren gakoak berriro sortuta 39

4.7.1 Ziurtagiriaren gakoak berriro sortzeko zirkunstantziak 40

4.7.2 Nork eska dezake 40

4.7.3 Ziurtagiria berritzeko eskaeren tratamendua, gakoak berriro sortuta 40

4.7.4 Harpidedunari jakinaraztea 40

Ziurtapen berriko eskaeretarako erabiltzen den jakinarazpen-prozesu bera erabili beharko da. 40

4.7.5 Ziurtagiri berritua onartzeko prozedura 40

4.7.6 Ziurtagiria argitaratzea 40

4.7.7 Beste entitate batzuei jakinaraztea 40

4.8 Ziurtagiria aldatzea 40

4.9 Ezeztatzea 41

4.9.1 Ezeztatzeko zirkunstantziak 41

4.9.2 Nork eska dezake ziurtagiria ezeztatzea 42

4.9.3 Ezeztatzeko eskaeren tratamendua 42

4.9.4 Ezeztatzea prozesatzeko CAren epea 42

4.9.5 Konfiantzako hirugarren batzuek ezeztatzeak egiaztatzeko betebeharra 42

4.9.6 CRLak sortzeko maiztasuna 42

4.9.7 CRLak sortzen direnetik argitaratzen direnera arte emandako denbora 43

4.9.8 Ziurtagirien egoera online egiaztatzeko sistemaren erabilgarritasuna 43

4.9.9 On line ezeztatzea egiaztatzeko eskakizunak 43

4.9.10 Ezeztatzeak ohartarazteko eskura dauden beste modu batzuk 43

4.9.11 Arriskupean dagoen gakoaren eskakizun bereziak 44

4.10 Ziurtagirien egoera-zerbitzuak 44

4.10.1 Ezaugarri operatiboak 44

4.10.2 Zerbitzuaren erabilgarritasuna 44

4.11 Harpidetzari amaiera ematea 44

4.12 Gakoak zaintzea eta berreskuratzea 44

5 Segurtasun fisikoaren, prozeduren eta langileen kontrolak 45

5.1.1 Instalazioen kokalekua eta eraikuntza 45

5.1.2 Sarbide fisikoa 45

5.1.3 Elektrizitatea eta aire egokitua 45

5.1.4 Urarekiko erresistentzia 46

5.1.5 Suteen prebentzioa eta horien aurkako babesa 46

5.1.6 Euskarriak biltegiratzea 46

5.1.7 Hondakinen tratamendua 46

5.1.8 Instalazioetatik kanpoko babeskopia 46

5.2 Prozeduren kontrolak 46

5.2.1 Konfiantzazko funtzioak 46

5.2.2 Zeregin bakoitzerako pertsona kopurua 47
5.2.3 Eginkizun bakoitzean identifikatzea eta kautotzea 47
5.2.4 Eginkizunetan zereginak bereiztea 47
5.3 Langileen kontrolak 47
5.3.1 Historialei, kalifikazioei, esperientziari eta kautotzeei buruzko baldintzak 47
5.3.2 Historiala ikertzeko prozedurak 47
5.3.3 Trebakuntza-baldintzak 47
5.3.4 Trebakuntza eguneratzeko baldintzak eta maiztasuna 48
5.3.5 Lan-txandaketen segida eta maiztasuna 48
5.3.6 Baimendu gabeko konexioen zigorrak 48
5.3.7 Langileak kontratatzeko baldintzak 48
5.3.8 Langileei dokumentazioa ematea 48
5.4 Audit 48
5.4.1 Erregistratutako gertaera motak 48
5.4.2 Log fitxategien prozesamenduaren maiztasuna 49
5.4.3 Audit logaren atxikipen-aldia 49
5.4.4 Audit logaren babesa 49
5.4.5 Audit-logaren backup prozedura 49
5.4.6 Log-fitxategiak biltzea 49
5.4.7 Log-fitxategiak sortzea eragin duen ekintzaren jakinarazpena 49
5.4.8 Puntu ahulen azterketa 50
5.5 Erregistroak artxibatzea 50
5.5.1 Artxibatutako erregistroen mota 50
5.5.2 Fitxategiaren atxikipen-aldia 50
5.5.3 Artxiboaren babesa 50
5.5.4 Artxiboaren backup prozedurak 50

5.5.5 Erregistroen denbora zigilatzeko eskakizunak 50
5.5.6 Artxibatzeko sistema 50
5.5.7 Artxiboaren informazioa lortzeko eta egiaztatzeko prozedurak 50
5.6 Gakoak aldatzea 51
5.7 Larrialdietarako plana 51
5.7.1 Gertakariak kudeatzeko prozedurak 51
5.7.2 Datu eta software ustelen aurrean jarduteko plana 52
5.7.3 Gako pribatuaren konpromisoaren aurreko prozedura 52
5.7.4 Hondamendi baten ondoren, negozioaren jarraipena 53
5.8 CAren edo RAren amaiera 53
5.8.1 Ziurtapen-entitatea 53
5.8.2 Erregistro-entitatea. 53
6 Segurtasun teknikoaren kontrolak 54
6.1 Gako-parea sortu eta instalatzea 54
6.1.1 Gako-parea sortzea 54
6.1.2 Gako pribatua harpidedunari banatzea 54
6.1.3 Gako publikoa ziurtagiriaren jaulkitzaileari banatzea 54
6.1.4 Ziurtapen-entitatearen gako publikoa ziurtagirien erabiltzaileei banatzea 55
6.1.5 Gakoen tamainak eta erabilitako algoritmoak 55
6.1.6 Ziurtapen-sinaduretako algoritmoak 55
6.1.7 Gakoen erabilera baimenduak (KeyUsage field X.509v3) 56
6.2 Gako pribatua babestea 56
6.2.1 Modulu kriptografikoen estandarrak 56
6.2.2 Gako pribatua pertsona batek baino gehiagok kontrolatzea (m-tik n) 56
6.2.3 Gako pribatuaren zaintza 56
6.2.4 Gako pribatuaren babeskopia 57

6.2.5 Gako pribatua artxibatzea 57

6.2.6 Gako pribatuaren transferentzia, modulu kriptografikora edo modulu kriptografikotik 57

6.2.7 Gako pribatua modulu kriptografikoan biltegiratzea 57

6.2.8 Gako pribatua aktibatzeko metodoa 58

6.2.9 Gako pribatua desaktibatzeko metodoa 58

6.2.10 Gako pribatua deuseztatzeko metodoa 59

6.2.11 Modulu kriptografikoaren kalifikazioa 59

6.3 Gako-parea kudeatzearen beste alderdi batzuk 59

6.3.1 Gako publikoa artxibatzea 59

6.3.2 Ziurtagiriaren eragiketa-aldiak eta gako-parearen erabilera-aldiak 59

6.4 Aktibatzeko datuak 59

6.4.1 Aktibatzeko datuak sortzea eta instalatzea 59

6.4.2 Aktibatzeko datuak babestea 60

6.4.3 Aktibatzeko datuen beste alderdi batzuk 60

6.5 Segurtasun informatikoaren kontrolak 60

6.5.1 Segurtasun informatikorako berariazko eskakizun teknikoak 60

6.5.2 Segurtasun informatikoaren mailaren ebaluazioa 61

6.6 Bizitza-zikloaren kontrol teknikoak 61

6.6.1 Sistemen garapen-kontrolak 61

6.6.2 Segurtasunaren kudeaketa-kontrolak 62

6.6.3 Bizi-zikloaren segurtasun-kontrolak 62

6.7 Sareko segurtasunaren kontrolak 62

6.8 Denbora-iturria 62

7 Ziurtagirien profilak eta ezeztatutako ziurtagirien zerrendaren profilak 63

7.1 Ziurtagiriaren profila 63

7.1.1 Bertsio-zenbakia 63

7.1.2 Ziurtapenen luzapenak 63

7.1.3 Algoritmo-objektuen identifikatzailea 63

7.1.4 Izenen formatuak 63

7.1.5 Izenen murrizpenak 63

7.1.6 Ziurtagiriaren politikaren objektu-identifikatzailea 63

7.1.7 “Politika-murrizpenak” luzapenaren erabilera 64

7.1.8 Politika kalifikatzaileen sintaxia eta semantika 64

7.1.9 “certificate policy” luzapenerako tratamendu semantikoa 64

7.2 Ezeztatutako ziurtagirien zerrendaren profila 64

7.2.1 Bertsio-zenbakia 64

7.2.2 Zerrendako elementuen ezeztatutako ziurtagirien eta luzapenen zerrenda 65

7.3 OCSP profila 65

7.3.1 Bertsio-zenbakia 65

7.3.2 OCSParen luzapenak 65

8 Bete beharreko ikuskapenak 66

8.1 Ikuskapenaren maiztasuna 66

8.2 Ikuskatzailearen kualifikazioa 66

8.3 Ikuskatzailearen eta ikuskatutako enpresaren arteko harremana 66

8.4 Ikuskapenaren mende dauden elementuak 66

8.5 Urritasunen ondoriozko erabakiak hartzea 66

8.6 Emaitzen berri ematea 67

9 Beste lege eta jarduera gai batzuk 68

9.1 Tarifak 68

9.1.1 Ziurtagiriak jaulkitzeko edo berritzeko tarifak 68

9.1.2 Ziurtagirien egoerari buruzko informazioa eskuratzeko tarifa 68

9.1.3 Beste zenbait zerbitzutarako tarifak 68

9.1.4 Itzultze-politika 68

9.2 Finantza-erantzukizunak 68

9.3 Informazioaren konfidentzialtasuna 68

9.3.1 Informazio konfidentzialaren irismena 68

9.3.2 Irismenaren barruan ez dagoen informazioa 69

9.3.3 Informazio konfidentziala babesteko erantzukizuna 70

9.4 Datu pertsonalak babestea 70

9.4.1 Sarrera 70

9.4.2 Aplikazio-esparrua 70

9.4.3 Datu pertsonalak babesteko segurtasun-antolamendua. 71

9.4.4 Segurtasun-antolamenduaren eredua 71

9.4.5 Segurtasuna antolatzeko unitateen sailkapena 72

9.4.6 Datu pertsonalak dituzten fitxategien egitura 73

9.4.7 Segurtasuneko arauak eta prozedurak 73

Arauak 73

Prozedurak 74

9.5 Jabetza intelektualeko eskubideak 75

9.5.1 Ziurtagirien jabetza 75

9.5.2 Ziurtapen Praktikaren jabetza 75

9.5.3 Izenen gaineko informazioaren jabetza 75

9.5.4 Gakoen eta horiei dagokien materialaren jabetza 75

9.6 Betebeharrak eta bermeak 75

9.6.1 Zerbitzua egiteko betebeharrak 75

9.6.2 Jardun fidagarriko betebeharrak 76

9.6.3 Identifikazio-betebeharrak 77

9.6.4 Erabiltzaileei eman beharreko informazioa: betebeharrak 77

9.6.5 Egiaztapen-programak: betebeharrak 78

9.6.6 Ziurtapen-zerbitzuaren arautze juridikoa: betebeharrak 78

9.6.7 Erregistro-entitatearen betebeharrak 79

9.6.8 Ziurtagiri-eskatzailearen betebeharrak 79

9.6.9 Ziurtagiri-harpidedunaren betebeharrak 79

9.6.10 Ziurtagirien erabiltzaile egiaztatzailearen betebeharrak 80

9.6.11 Argitalpen Zerbitzuaren betebeharrak 81

9.7 Erantzukizunak 81

9.7.1 Ziurtapen-agintaritzaren erantzukizunak 81

9.7.2 Erregistro-agintaritzaren erantzukizunak 82

9.7.3 Harpidedunen betebeharrak 82

9.7.4 Ziurtagirietan konfiantza duten hirugarrenen erantzukizunak 83

9.8 Kalte-ordainak 83

9.9 Baliozkotze-aldia 83

9.9.1 Epea 83

9.9.2 Amaiera 84

9.9.3 Amaieraren ondorioak 84

9.10 Banako jakinarazpenak eta komunikazioa parte-hartzaileekin 84

9.11 Zuzenketak 84

9.11.1 Aldaketetarako prozedura 84

9.11.2 Jakinarazteko aldia eta mekanismoa 84

9.11.3 OIDa zer zirkunstantziatan aldatu behar den 85

9.12 Erreklamazioak eta auzien ebazpena 85

9.13 Aplikatzeko den araudia 85

9.14 Aplikatzekoa den araudia betetzea 85

9.15 Askotariko estipulazioak 86

1 Sarrera

Euskal administrazio publikoak informazioaren gizartea sustatu nahi izan du, eta helburua herritarren jarduera ekonomiko eta sozialetan informazioaren eta komunikazioaren teknologiak guztiz barneratzea da. Ildo horretan, herritarrei administrazioarekin harremanetan jartzeko aukera emango dieten tresnak bideratu nahi izan dira –betiere segurtasuna bermatuz–, informazioaren pribatutasuna, pertsonen intimitatea eta euren eskubideak babestea helburu.

Eusko Jaurlaritzak eta Foru Aldundiek elkar eraginkortasuna bermatuko duen ziurtapen eta sinadura elektronikorako sistema komuna elkarrekin garatzea erabaki zuten, beren sozietate informatikoen bitartez. Horrela, ematen diren ziurtagiriak administrazio batzuen zein besteen aplikazio eta prozeduretan baliagarriak izan daitezen lortu nahi zen.

Elkarlanerako borondate horren ondorioz, 2002ko ekainean "Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, IZENPE, SA" merkataritza-sozietatea eratu zuten goraxeago adierazitako sozietate informatikoek (aurrerantzean IZENPE deituko diogu).

Euskal administrazio publikoetako sozietate informatikoek ziurtapen elektronikoa garatzeko duten interesa kudeatzeko tresna edo antolakunde komuna da IZENPE, eta herritarren eta administrazioaren arteko harremana errazteko tresna ezin hobea dela erakutsi du.

1999/93/EE Zuzentaraua indargabetzen duen barne-merkatuko transakzio elektronikoetarako identifikazio elektronikoari eta konfiantza-zerbitzuei buruzko Europako Parlamentuaren eta Kontseiluaren uztailaren 23ko 910/2014 Araudiak Konfiantzako Zerbitzuen Egile Kualifikatu bihurtzeko aukera hartzen du aintzat (aurrerantzean eIDAS).

Ildo horretan, IZENPE euskal administrazioen mendeko Konfiantza Zerbitzuen Egile Kualifikatu gisa eratu da, eta haren helburu soziala da:

- Telekomunikazio-sareen bidezko gobernu elektronikoaren erabilera sustatzea eta gobernu elektronikoaren garapena indartzea, betiere transakzioen segurtasun, konfidentzialtasun, benetakotasun eta atzeraezintasuneko bermeekin.
- Segurtasun-zerbitzuak nahiz zerbitzu tekniko eta administratiboak ematea teknika eta bitarteko elektronikoak, informatikoak eta telematikoak erabiltzen diren komunikazioetan.

IZENPEk eskaintzen dituen identifikazio-mekanismoak araudi honetan zehazten diren irizpideen arabera definitu dira: 2015/1502 Gauzatze Araudia (EB), 2015eko irailaren 8ko Batzordearena, identifikazio elektronikoko baliabideen segurtasun-mailetarako zehaztapen eta prozedura teknikoak finkatzeari buruzkoa, betiere barne-merkatuko transakzio elektronikoetarako identifikazio elektronikoari eta konfiantza-zerbitzuei buruzko Europako Parlamentuaren eta Kontseiluaren 910/2014 Araudiaren (EB) 8. artikuluko 3. atalean xedatutakoaren arabera.

Era berean, zerbitzuak eraginkortasunez garatzeko eta ezartzeko helburuarekin, IZENPEk informazioaren segurtasuna kudeatzeko sistema ezarri du konfiantza-zerbitzuekin lotzen diren prozesuetarako, betiere ISO27001 estandarraren arabera.

IZENPEk ETSIren (Telekomunikazioetako Estandarren Europako Institutuaren) estandarren adierazpenak jarraitzen ditu, eta honako bi arau hauen zehaztapen teknikoen (TS) arabera lortu du ziurtapena: sinadura sortzeko gailu seguru batean (QCP Public + QSCD) sortutako ziurtagiri kualifikatuak jaulkitzeko 101 456 arauaren zehaztapen teknikoen arabera; gako publikoko ziurtagiriak jaulkitzeko 102 042 arauaren arabera; eta denbora-zigiluak jaulkitzeko 103 023 arauaren arabera. Balidazio hedatuko ziurtagirien politikari (EVCP) jarraitzen dioten zerbitzari seguruko ziurtagirietarako, erakundearen balidazio-politikari (OVCP) jarraitzen dioten zerbitzari seguruko ziurtagirietarako eta domeinuaren balidazio-politikari (DVCP) jarraitzen dioten zerbitzari seguruko ziurtagirietarako, CA/Browser Forum-ek onartutako gidei ere jarraituko zaie (www.cabforum.org web-gunean daude eskuragarri).

TS 101 456, TS 102 042 eta TS 102 023 arauen ezartzen diren TS zehaztapen teknikoek ziurtapenen kudeaketa eta praktikari buruzko oinarrizko baldintzak zehazten dituzte, eta baldintza horiek bete behar dituzte ziurtagiri kualifikatuak eta kualifikatu gabeak eta denbora-zigiluak jaulkitzen dituzten entitateek, baldin eta jaulkitzen dituzten ziurtagiriak Europako Parlamentuko eta Kontseiluko 1999/93/EE zuzentarauaren lege-esparruaren araberakoak –zuzentarau hori Espainiako erregimen juridikoan sinadura elektronikoari buruzko 1999/93 legearen bitartez sartu zen–; era berean, behar bezala eguneratu dira Europako beste arau batzuetan: ziurtagiriak jaulkitzeko EN 319 411-1 arauan, 910/2014 araudiaren arabera ziurtagiri kualifikatuak jaulkitzeko EN 319 411-2 arauan eta denbora zigiluak jaulkitzeko EN 319 421 arauan, betiere identifikazio elektronikoari eta barne-merkatuko transakzio elektronikoetarako konfiantzako zerbitzuei (eIDAS) buruzko 910/2104 araudiaren arabera.

1.1 Aurkezpena

IZENPEk honako zerbitzu kualifikatu hauek egiteko azpiegitura bat kudeatzen du:

a) Sinadura elektronikoak, zigilu elektronikoak edo denbora elektronikoko zigiluak sortzeko, egiaztatzeko eta baliozkotzeko.
b) Emate elektroniko ziurtatuko zerbitzuak egiteko.
c) Ziurtagiriak jaulkitzeko, ezeztatzeko eta baliozkotzeko.
d) Sinadurak, zigiluak edo ziurtagiri elektronikoak zaintzeko.

Ziurtapen Praktiken Deklarazio honen nahiz *Ziurtagiri bakoitzerako berariazko politika* dokumentuaren barruan, IZENPEk honako ziurtagiri hauek jaulkitzen ditu:

MOTA	ZIURTAGIRIA	EUSKARRIA	Ziurtatze-maila (eIDAS)
Pertsona fisikoa	Herritarra (kualifikatu gabea)	HSMa	Ez dago erabilgarri
	Herritarra (kualifikatua)	Txartela	Handia
		HSMa	Handia
	Korporatibo pribatua (kualifikatua)	Txartela	Handia
		HSMa	Handia
	Korporatibo pribatua (kualifikatu gabea)	Txartela	Kualifikatu gabea

	Erakunde publikoetako langilea (kualifikatua)	Txartela	Handia
		Nabigatzailea	Oinarrizkoa
		HSMa	Handia
	Korporatibo publikoa (kualifikatu gabea)	Txartela	Kualifikatu gabea
	Korporatibo publikoa (kualifikatua)	Txartela	Handia
		HSMa	Handia
		Nabigatzailea	Oinarrizkoa
	Ordezkaria (kualifikatua)	Txartela	Handia
		HSMa	Handia
Pertsona juridikoa	Zigilu juridikoa (kualifikatua)	Edukitzailea	Oinarrizkoa
	Zigilu administratiboa (kualifikatua)	Edukitzailea	Oinarrizkoa
		HSMa	Handia
Web-gunea	SSL DV	Softwarea	Kualifikatu gabea
	SSL OV		Kualifikatu gabea
	SSL EV		Kualifikatu gabea
	SSL Kualifikatua		Ez dago erabilgarri
	EV duen egoitza elektronikoa		Ez dago erabilgarri
Aplikazioa eta kode-sinadura	Aplikazioa	Edukitzailea	Kualifikatu gabea
	Kode-sinadura	Txartela	Kualifikatu gabea
		Fitxategia	Kualifikatu gabea

IZENPEk jaulkitako ziurtagiri mota bakoitzari dagozkion xehetasunak *Ziurtagiri bakoitzerako berariazko politika* dokumentuan arautzen dira. Dokumentu hori *Ziurtapen Praktiken Deklarazioa* dokumentu honekin batera dator.

1.2 Identifikazioa

IZENPEk Ziurtapen Praktiken Deklarazio honekin bat etorriz jaulkitako ziurtagiri mota bakoitza bereizita identifikatu ahal izateko, aipatutako ziurtagiri mota bakoitzari objektu-identifikatzaile (OID) bat esleitzen dio. Kontsultatu ahal izango dira www.izenpe.com web-gunean eskuragarri dagoen profilen dokumentuan. Gainera, ETSI EN 319 412-5 arauaren definizioaren arabera, identifikatzaile hauek hartu dira barnean:

- QcCompliance: ziurtagiri kualifikatua eIDAs-en arabera
- QcSSCD: sinadura sortzeko gailu kualifikatu batek jaulkitako ziurtagiria.
- QcRetentiodPeriod: dokumentazioaren atxikitze-aldia.
- QcPDS: erabiltzeko baldintzetarako ibilbidea.
- Qctype: sinadura mota adierazten du, betiere eIDAS-en arabera (zigilua, sinadura, web).

1.3 PKI gako publikoko azpiegituraren parte-hartzaileak

Ziurtapen-entitatearen administrazioan eta jardunean honako hauek hartzen dute parte:

- Ziurtapen-agintaritzek.
- Erregistro-entitateak.
- Ziurtagirien erabiltzaileak.

1.3.1 Ziurtapen-agintaritzek

IZENPEk honako ziurtapen-agintaritza hauek ditu:

- Oinarrizko ziurtapen-agintaritza
- Mendeko ziurtapen-agintaritzak

OINARRIZKO ZIURTAPEN AGINTARITZA

Mendeko ziurtapen-agintaritzei ziurtagiriak jaulkitzen dizkien ziurtapen-agintaritza da.

Subject	CN = Izenpe.com O = IZENPE S.A. C = ES
Validity dates	from 13/12/2007 until 13/12/2037
Thumbprint	2f 78 3d 25 52 18 a7 4a 65 39 71 b5 2c a2 9c 45 15 6f e9 19
Subject alternative name	Nombre RFC822=info@izenpe.com Dirección del directorio: STREET=Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz O=IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8

MENDEKO ZIURTAPEN AGINTARITZAK

Azken entitateei ziurtagiri elektronikoak jaulkitzen dizkieten ziurtapen-agintaritzak dira.

- CA, Herritar / Entitate kualifikatuak
- CA, Herritar / Entitate kualifikatu gabeak
- CA, Herri Administrazio kualifikatu gabeak
- CA, Herri Administrazio kualifikatuak
- CA, Eusko Jaurlaritzako langileak
- CA, SSL EV

CA, Herritar / Entitate kualifikatuak

Subject	CN = Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (4) OU = NZZ Ziurtagiri publikoa - Certificado publico SCI O = IZENPE S.A. C = ES
SubjectAlternativeName	Dirección URL=http://www.izenpe.com Nombre RFC822=info@izenpe.com Dirección del directorio: STREET=Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz O=IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
Validity dates	From miércoles, 20 de octubre de 2010 9:16:02 until domingo, 13 de diciembre de 2037 0:00:00
thumbprint	08 d8 d6 2a 1a 15 36 c5 3a 0f 9a 18 35 bf 82 c9 f0 96 83 23

CA, Herritar / Entitate kualifikatu gabeak

Subject	CN = Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (3) OU = NZZ Ziurtagiri publikoa - Certificado publico SCI O = IZENPE S.A. C = ES
SubjectAlternativeName	Dirección URL=http://www.izenpe.com Nombre RFC822=info@izenpe.com Dirección del directorio: STREET=Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz O=IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
Validity dates	From miércoles, 20 de octubre de 2010 9:18:07 until domingo, 13 de diciembre de 2037 0:00:00
thumbprint	87 56 60 a3 5c b1 03 d7 e0 bb 00 44 24 f1 6d bf bf 21 e0 b4

CA, Herri Administrazio kualifikatuak

Subject	CN = EAEko HAetako langileen CA - CA personal de AAPP vascas (2) OU = AZZ Ziurtagiri publikoa - Certificado publico SCA O = IZENPE S.A.

	C = ES
SubjectAlternativeName	Dirección URL=http://www.izenpe.com Nombre RFC822=info@izenpe.com Dirección del directorio: STREET=Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz O=IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
Validity dates	From miércoles, 20 de octubre de 2010 9:22:40 until domingo, 13 de diciembre de 2037 0:00:00
thumbprint	93 a1 44 6b 61 99 4b 5b 0e 99 d0 5b 14 cd bb 32 2e 6c 17 64

CA, Herri Administrazio kualifikatu gabeak

Subject	CN = EAEko Herri Administrazioen CA - CA AAPP Vascas (2) OU = AZZ Ziurtagiri publikoa - Certificado publico SCA O = IZENPE S.A. C = ES
SubjectAlternativeName	Dirección URL=http://www.izenpe.com Nombre RFC822=info@izenpe.com Dirección del directorio: STREET=Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz O=IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
Validity dates	From miércoles, 20 de octubre de 2010 9:23:33 until domingo, 13 de diciembre de 2037 0:00:00
thumbprint	f7 9c da 11 e7 91 74 19 a0 41 8d b8 4b a7 43 c5 31 3a d7 f0

CA, Eusko Jaurlaritzako langileak

Subject	CN = Eusko Jaurlaritzako langileen CA - CA personal Gobierno Vasco OU = Ziurtagiri publikoa - Certificado publico O = IZENPE S.A. C = ES
SubjectAlternativeName	Dirección URL=http://www.izenpe.com Nombre RFC822=info@izenpe.com Dirección del directorio:

	STREET=Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz O=IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
Validity dates	From jueves, 11 de febrero de 2010 11:45:37 until martes, 11 de febrero de 2020 11:45:37
thumbprint	25 e9 d1 6d f8 d6 4a 60 73 40 8c be 24 8e 52 9c 23 9e 32 92

CA, SSL EV

Subject	CN = CA de Certificados SSL EV OU = BZ Ziurtagiri publikoa - Certificado publico EV O = IZENPE S.A. C = ES
SubjectAlternativeName	Dirección URL=http://www.izenpe.com Nombre RFC822=info@izenpe.com Dirección del directorio: STREET=Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz O=IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
Validity dates	From miércoles, 20 de octubre de 2010 9:28:56 until martes, 20 de octubre de 2020 9:28:56
thumbprint	6c 48 4d 0f 4d b2 95 ec 67 eb b3 e0 5e 3d c2 14 49 2a 9a b8

1.3.2 Erregistro-entitateak

Ziurtapen Praktiken Deklarazio hau IZENPEk ziurtagiriak jaulki eta kudeatzeko prozeduretan baliatzen dituen erregistro-entitateei aplikatuko zaie.

Erregistro Entitateak ziurtagirien gakoen eskatzaileak, harpidedunak eta edukitzaileak identifikatuko dituzten entitateak dira; horrez gain, ziurtagirietan jasotzen diren inguruabarrak egiaztatzen dituen dokumentazioa ziurtatzen dute, eta ziurtagiriak jaulkitzeko, ezeztatzeko eta berritzeko eskaerak baliozkotzen eta onartzen dituzte.

Erregistro-entitateak izango dira, IZENPE bera edota IZENPErekin dagokion lege-tresna sinatzen duen entitate erabiltzailea.

1.3.3 Ziurtagirien erabiltzaile diren azken entitateak

Ziurtagirien erabiltzaile diren azken entitateak ziurtagiri digitalak jaulki, kudeatu eta erabiltzeko zerbitzuak jasotzen dituzten pertsona eta erakundeak dira.

Honako entitate hauek izango dira ziurtapen-sistemaren azken entitate erabiltzaileak:

- Ziurtagirien eskatzaileak
- Ziurtagiriaren sinatzailea
- Ziurtagirien harpidedunak
- Gakoen edukitzaileak

Ziurtagiri bakoitzerako xehetasunak *Ziurtagiri bakoitzerako berariazko dokumentazioan* zehazten dira.

Ziurtagirien eskatzaileak, ziurtagiri oro pertsona batek eskatu behar du, bere izenean edo erakunderen baten izenean.

Sinatzailea, sinadura sortzeko gailua duen pertsona, eta nor bere izenean edota ordezkatzen duen pertsona fisiko edo juridikoaren izenean jarduten du.

Ziurtagirien harpidedunak, ziurtagirian identifikatutako pertsona fisikoak edo juridikoak dira harpidedunak.

Gakoen edukitzaileak, sinadura digitaleko gakoak dituzten edo horien gaineko ardura duten pertsona fisikoak dira.

1.3.4 Konfiantzako hirugarren batzuk

Ziurtapen Praktiken Deklarazio honen barruan, IZENPEk jaulkitako ziurtagiriak eta denbora-zigiluak jasotzen dituzten pertsona fisiko edo juridikoak ziurtagirietan eta denbora-zigiluetan konfiantza duten hirugarren batzuk dira; beraz, ziurtagiri eta denbora-zigilu horietan konfiantza izatea erabakitzen dutenean, ziurtapen-praktiken deklarazio honetan jasotakoa aplikatuko zaie.

Hirugarrenek ziurtagirietan eta denbora-zigiluetan jartzen duten konfiantza, bestalde, harpidedunekiko harremanetan ziurtagiri horietaz egiten duten erabilera objektiboaren araberakoa izaten dela jotzen da.

Aipatutako erabilera egiten denean, honako hau egiaztatu behar da bereziki: hirugarrenak mezuei erantsitako ziurtagiri edo sinadura digitaletan konfiantzarik ez duela adierazten duen deklaraziorik ez dagoela, hirugarrenak ziurtagiri eta sinadura digitaletan konfiantza izan zuela finkatzeko, betiere ziurtagiriak baliozkoak badira, sinadurak ziurtagiriak indarrean zeudela sortuak badira eta ziurtagiri jakin batean konfiantza izateko gainerako baldintzak betetzen badira.

Hirugarrenek arduraz erabili behar dituzte ziurtagiri mota guztiak eta fede onez eta leialtasunez jardun behar dute. Halaber, ez dute izan behar ziurtagiriaren edo denbora-zigiluaren kategoriari dagokion konfiantza-esparruaren barruan bidalitako mezuei uko egitea helburu duten iruzur- edo zabarkeria-jarrerarik.

1.4 Ziurtagiriaren erabilerak

Jarraian IZENPEk jaulkitako ziurtagiriekin zer baimentzen den eta zer debekatzen den zehaztuko da.

1.4.1 Ziurtagiriaren erabilera egokiak

Ziurtagiri kualifikatua

Ziurtagiri kualifikatuen erabilerari dagokionez:

Sinadura elektronikoko ziurtagiri kualifikatuek harpidedunaren identitatea eta gako pribatuaren edukitzailearen identitatea bermatzen dituzte. Sinadura sortzeko gailu seguruekin erabiltzen direnean, ezin hobeak dira onartutako sinadura elektronikoari euskarria emateko, hau da, ziurtagiri kualifikatuan oinarritzen den eta gailu seguruaren bidez sortu den sinadura elektroniko aurreratuari euskarria emateko. Hori dela eta, eIDAS araudiarekin bat etorriz, lege-ondorioetarako eskuz idatzitako sinaduraren baliokidetzat jotzen da, beste eskakizunik bete behar izan gabe.

Sinadura elektronikoko ziurtagiri kualifikatuak, dagokion ziurtagiri motan hala definitzen bada, kautotze-mezuak sinatzeko ere erabil daitezke, bereziki SSL edo TLS bezeroen testiguak, S/MIME posta elektroniko segurua, gako-berreskurapen gabeko zifratzeak eta beste zenbait. Sinadura digital horrek sinadura-ziurtagiriaren harpidedunaren identitatea bermatzen du.

Horrez gain, ziurtagiri horiek sinadura elektroniko aurreraturako eta kautotzeko hainbat modutarako ere balio dute, sinadura-gako pribatua modu fidagarrian babesten duten aplikazio informatikoekin batera erabiliz gero.

Zigilu elektronikoko ziurtagiriak pertsona juridiko batekin lotzen ditu zigilu bat baliozkotzeko datuak, eta pertsona horren izena berresten du. Zigilu elektronikoak sortzeko aukera ematen dute, eta, hartara, dokumentu elektroniko jakin bat pertsona juridiko batek jaulki duela frogatzen dute eta dokumentuaren jatorriari eta integritateari buruzko ziurtasuna gehitzen dute.
IZENPEk jaulkitzen dituen zigilu elektronikoko ziurtagiriek eIDAS araudiaren III. eranskinaren betekizunak betetzen dituzte ziurtagiri kualifikatutzat jotzeko.

Web-gunea kautotzeko ziurtagiriek web-gune jakin bat kautotzeko aukera ematen dute, eta ziurtagiria jaulki zaion pertsona juridikoarekin edo fisikoarekin lotzen dute web-gunea. IZENPEk jaulkitako web-ziurtagiriek eIDAS araudiaren IV. eranskinaren betekizunak betetzen dituzte ziurtagiri kualifikatutzat jotzeko

Egoitza eta ziurtagiri elektronikoko ziurtagiriak egoitza elektronikoa eta dokumentuen zigilatze elektronikoa identifikatzeko jaulkitzen dira, betiere *Zerbitzu Publikoetarako Hiritarren Sarrera Elektronikoari buruzko ekainaren 22ko 11/2007 Legean* aurreikusitakoaren arabera.

IZENPEren ziurtagiri kualifikatuek ETSI EN 319 411-2 arau teknikoari jarraitzen diote.

Ziurtagiri kualifikatu gabea

Ziurtagiri kualifikatu gabeek ez dute fedez bermatzen harpidedunaren identitatea eta, hala badagokio, gako pribatuaren edukitzailearen identitatea; IZENPEk bai bermatzen duela ETSI EN 319 411-1 arauaren betekizunen arabera jaulkitzen dela. Edonola ere, sinatzeko erabiliz gero, sinadura sortzeko gailu behar bezain seguru batekin batera erabili beharko da. Horrelakoetan, ez da sinatzaileak eskuz idatzitako sinaduraren baliokide izaten.

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

Gailu informatikoko ziurtagiria

Gailu informatikoen eragiketaz arduratzen diren entitateei zerbitzari seguruko ziurtagiriak (SSL DV, SSL OV, SSL EV, Egoitza, Egoitza EV eta SSL kualifikatua) eta aplikazio-ziurtagiriak jaulkitzen zaizkie.

Mota horretako ziurtagiriek CA/Browser Forum-en onartutako eta ETSIren EN 319 411-1 arau teknikoaren arabera ikuskatutako arauei jarraitzen diete, balidatze hedatuko politikarako zein oinarrizkorako.

Kode-sinaduraren ziurtagiria.

Titular diren entitateei ematen zaie, software horren osagairen baten egiazkotasuna eta osotasuna bermatzeko.

Ziurtagirien erabilera-esparrua

Erabilera-esparruari dagokionez bi kasu bereizten dira:

- IZENPEk jaulkitako eta herritarrei, oro har, zuzendutako ziurtagiriak harpidedunek erabiliko dituzte, edo, hala badagokio, gakoen edukitzaileek, Nortasun Ziurtapen Digitaleko ziurtagiriak entitate publiko erabiltzaileekiko harremanetan, baita ziurtagiri horren erabilera onartu duten erakunde publiko eta pribatuekiko harremanetan ere.

  Ziurtagiri bakoitzaren erabilpen-esparruari dagozkion xehetasunak *Ziurtagiri bakoitzerako berariazko dokumentazioan* kontsulta daitezke.

- IZENPEk jaulkitako eta entitate erabiltzaileek eskatutako ziurtagiriak, bestalde, horiek pertsona fisiko edo juridiko diren aldetik dituzten ezaugarrien esparruan erabiliko dira, betiere eIDAS arauaren zehaztapenen arabera. Dena den, gakoen edukitzaileek beste erabilera batzuetarako erabili ahal izango dituzte ziurtagiri horiek, baina beti aurreko atalean adierazten diren erabilera-mugak errespetatzen badira.

  Ziurtagiri bakoitzaren erabilpen-esparruari dagozkion xehetasunak *Ziurtagiri bakoitzerako berariazko dokumentazioan* kontsulta daitezke.

1.4.2 Ziurtagiriaren erabilera debekatuak

Berezkoa duten zereginerako eta ezarritako helbururako erabili behar dira ziurtagiriak, eta ez beste inongo zeregin eta eginkizunetarako.

Era berean, ziurtagiriak aplikatzekoa den legearen arabera soilik erabili beharko dira.

Ziurtapen Praktiken Deklarazio honen erregulazioaren mende dauden ziurtagiriak ezin izango dira erabili entitate-erregistro gisa izapideak egiteko.

Ziurtagiriak ez dira diseinatu egoera arriskutsuetan kontrol-ekipo gisara edo hutsegiteen aurkako jardueretan erabiltzeko (instalazio nuklearren funtzionamenduan, nabigazio-sistemetan, airetiko komunikazioetan, armamentuaren kontrol-sistemetan...). Jarduera horietan, akats batek heriotza, zauriak edo ingurumen-kalte larriak eragin ditzake.

1.5 Politikak

1.5.1 Dokumentazioaren kudeaketaz arduratzen den entitatea

IZENPE (Mediterraneoaren hiribidea 14, Gasteiz eta IFZ: 01337260) da ziurtapen-praktiken deklarazio hau aplikagarri duten ziurtagiri publikoak ematen dituen ziurtapen-entitatea.

1.5.2 Harremanetarako datuak

Zerbitzu-egilearen izena	Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, SA
Posta-helbidea:	Tomas Zumarraga Dohatsuaren kalea, 71-1. 01008 Vitoria-Gasteiz
Posta elektronikoko helbidea:	info@Izenpe.com
Telefonoa	902 542 542

1.5.3 Ziurtapen Praktiken Deklarazioaren egokitzapenaren arduradunak

IZENPEren administrazio-kontseilua arduratzen da Ziurtapen Praktiken Deklarazio hau onartzeaz, baita hari egin beharreko aldaketak onartzeaz ere.

1.5.4 Ziurtapen Praktiken Deklarazioa onartzeko prozedura

Dokumentu honetan egindako azken aldaketak IZENPEren Administrazio Kontseiluak onartuko ditu, ezarritako baldintzak betetzen direla egiaztatu eta gero.

1.6 Definizioak eta akronimoak

1.6.1 Definizioak

- **Datuak Babesteko Espainiako Agentzia (APD):** zuzenbide publikoko ente bat da, berezko izaera juridikoa du eta ahalmen publiko eta pribatu osoa. Askatasun osoz burutzen ditu bere funtzioak, Administrazio Publikoen mende egon gabe. Helburu nagusia datuak babesteari buruzko legedia betetzen dela zaintzea eta legediaren aplikazioa kontrolatzea da.

- **Ziurtapen Agintaritza (CA):** Ziurtapen Agintaritza behar diren ziurtagiriak jaulkitzen dituen entitatea da, Erregistro Agintaritzak hala eskatu ondoren, modu automatizatuan eta Tokiko Erregistro Autoritatearen baieztapena jaso ondoren.
- **Erregistro Agintaritza (RA):** erregistro-agintaritza arduratzen da ziurtagirien gakoen eskatzaileak, harpidedunak eta edukitzaileak identifikatzeaz, baita ziurtagirietan jasotzen diren inguruabarrak egiaztatzen dituen dokumentazioa egiaztatzeaz eta ziurtagiriak jaulkitzeko, ezeztatzeko eta berritzeko eskaerak baliozkotzeaz eta onartzeaz. Erabiltzaileak Erregistro Agintaritzara joan behar du ziurtagiri bat eskatzeko, Erregistro Agintaritzarekin lotuta dagoen Ziurtapen Agintaritzaren bermearekin.
- **Denbora Zigilatzeko Agintaritza (TSA):** denbora-zigiluak jaulkitzen dituen agintaritza.
- **Ziurtagiria:** Ziurtapen Zerbitzuen Egileak elektronikoki sinatutako dokumentu elektronikoa da, sinadura egiaztatzeko datuak sinatzailearekin lotzen ditu eta haren identitatea baieztatzen du.
- **Oinarrizko ziurtagiria:** harpidedun gisa IZENPEren hierarkiako Ziurtapen Agintaritza bat duen ziurtagiria. Agintaritza horren sinadura egiaztatzeko datuak Ziurtapen Zerbitzuen Egile gisa daude sinatuta, agintaritzarenak diren sinadura sortzeko datuekin. IZENPEko entitate jaulkitzaileek hierarkia bat osatzen dute, horrela, oinarrizko entitate bat dago, komuna edozein ziurtagiritarako, eta mendeko entitate bat baino gehiago, ziurtagiri mota desberdinetarako.
- **Ziurtagiri kualifikatua:** Ziurtapen Zerbitzuen Egile batek emandako ziurtagiri elektronikoak dira. Ziurtapen Zerbitzuen Egile horrek eIDAS arauan ezarritako baldintzak betetzen ditu, identitateari eta eskatzaileen inguruko bestelakoei dagokienez, eta ematen dituzten ziurtapen-zerbitzuen bermeei dagokienez.
- **Ziurtagiri kualifikatu gabeak:** ziurtagiri arruntak dira, ziurtagiri kualifikatuen lege-aintzatespenik gabekoak.
- **Gakoa:** zifratze- eta deszifratze-eragiketak kontrolatzeko erabilitako sinbolo-sekuentzia.
- **Konfidentzialtasuna:** konfidentzialtasuna dokumentu elektroniko bat pertsona-zerrenda jakin bati izan ezik gainerako erabiltzaile guztiei eskuraezin egiteko gaitasuna da. Horrela, komunikazioak beste batzuek entzun ezin izateko moduan egitea eta dokumentuak adierazitako hartzaileak soilik irakurri ahal izateko moduan igortzea lortu dezakegu.
- **Kriptografia:** kriptografia matematikaren adar bat da, eta aztertzen duena da nola eraldatu informazio irakurgarria zuzenean ezin irakurtzeko moduan, hau da, irakurtzeko deszifratu behar izateko moduan.
- **Sinadura sortzeko datuak (Gako Pribatua):** gako pribatua zenbaki bakar eta sekretua da eta pertsona bakar bati dagokio, horrela, pertsona bere gako pribatuaren bitartez identifika daiteke. Gakoa asimetrikoa da gako publikoarekiko. Gako batek beste gako batek sinatu edo zifratu duena egiaztatu eta deszifratu dezake.
- **Sinadura Egiaztatzeko Datuak (Gako Publikoa):** gako publikoa pertsona bakar bati dagokion zenbaki bakarra da baina, gako pribatua ez bezala, edonork jakin dezake.

Prozedura matematikoen bitartez gako pribatuarekin lotu eta sinadura digitalak zifratzeko eta egiaztatzeko balio du.

- **Ziurtapen Praktiken Deklarazioa (ZPD):** IZENPEk edonorentzat eskuragarri duen deklarazioa, erraz lortu daitekeena, elektronikoki eta dohainik. segurtasun-dokumentuaren balioa du eta bertan zehazten dira –eIDAS arauaren esparruan– zein diren Ziurtapen Zerbitzuen Egileen betebeharrak, sinadura sortzeko nahiz egiaztatzeko datuak kudeatzeari dagokionez eta ziurtagiri elektronikoak kudeatzeari dagokionez, hala nola, zein diren aplikagarri diren baldintzak ziurtagiria eskatzean, jaulkitzean, erabiltzean nahiz iraungitzean, zein diren segurtasun-neurri teknikoak eta antolakuntzari dagozkionak, zein diren ziurtagirien indarraldiari buruzko profilak eta informazio-mekanismoak. Bertan zehazten da, halaber, koordinazio-prozedurak izan behar direla dagozkien erregistro-publikoekin, ziurtagirietan aipatzen den ahalmenaren indarraldiari buruzko informazioa –erregistro horietan aginduz jaso beharko dira– berehala elkarri trukatzeko.
- **Ziurtagirien direktorioa:** ITU-Tren X.500 estandarraren araberako informazio-biltegia. Horrela, IZENPEk ziurtagirien direktorio eguneratua mantentzen du eta direktorio horrek egindako ziurtagiriak emango ditu aditzera.
- **Sinadura sortzeko gailu kualifikatua:** sinadura elektronikoak sortzeko gailua, eIDAS arauaren II. eranskinean zerrendatzen diren betekizunak betetzen dituena.
- **Sinadura elektronikoa:** sinatzaileak sinatzeko erabiltzen dituen formatu elektronikoko datuak, beste datu elektroniko batzuei erantsiak edo horiekin modu logikoan lotuak.
- **Sinadura elektroniko aurreratua:** eIDAS arauaren 26. artikuluan aintzat hartzen diren betekizunak betetzen dituen sinadura elektronikoa.
- **Sinadura elektroniko kualifikatua:** sinadura elektroniko aurreratua, sinadura elektronikoak sortzeko gailu kualifikatu bidez sortzen dena eta sinadura elektronikoko ziurtagiri kualifikatu batean oinarritzen dena.
- **Sinatzailea:** sinadura sortzeko gailua duen pertsona, eta nor bere izenean edota ordezkatzen duen pertsona fisiko edo juridikoaren izenean jarduten du.
- **Hash edo hatz-marka:** mezu bati hash funtzioa aplikatu ostean lortzen den emaitza, tamaina zehatzekoa, eta hasierako datuetara modu unibokoan lotuta dagoena.
- **HSM (segurtasun-modulu kriptografikoa):** gako kriptografikoak sortu eta babesten dituen segurtasunerako gailua.
- **Gako Publikoen Azpiegitura (PKI, Public Key Infrastructure):** PKIak ziurtapen-sistema zein entitatek osatuko duten zehazten du, entitate horiek zein betekizun betetzen duten, zein arau eta protokolori jarraitu behar zaion sistema barnean lan egiteko, informazio digitala nola kodetzen den eta nola transmititzen den, eta zein izango den azpiegiturak kudeatzen dituen objektu eta dokumentuetako informazioa. Horrek guztiak Gako Publikoko teknologia izango du oinarri (bi gako).
- **Abenduaren 13ko 15/1999 Lege Organikoa, datu pertsonalak babesteari buruzkoa:** Lege Organiko honen helburua da datu pertsonalak baliatzerakoan pertsona fisikoen askatasun publikoak eta oinarrizko eskubideak bermatu eta babestea, batez ere, pertsona horien ohorea eta intimitate pertsonal eta familiakoa.

- **Ezeztatutako Ziurtagirien Zerrenda (CRLak):** IZENPEk jaulkitzen dituen ziurtagiri ezeztatuek osatzen duten zerrenda da, eta berehalako ezeztatze bat gertatzen den bezain laster geratzen da jasota zerrendan. Bada beste web-zerbitzu iraunkor bat ere, IZENPEk ezeztatutako ziurtagirien eguneratze inkremental telematikoa kontsultatzeko aukera eskaintzen duena. Ezeztatutako Ziurtagirien Zerrendak argitaratzeari dagokionez, sarbide azkarra eta segurua bermatzen zaie erabiltzaileei eta ziurtagirien harpidedunei.
- **Ziurtagiriaren serie-zenbakia:** balio osoa eta bakarra da, eta modu unibokoan dago edozein Ziurtapen Zerbitzuen Egilek jaulkitako ziurtagiri bati lotuta.
- **OCSP (Online Certificate Status Protocol):** ziurtagiri elektroniko baten egoera frogatzen duen protokolo informatikoa da.
- **OID (Object Identifier):** aldagai oso ez negatiboek –puntu batez banatuta– osatzen duten sekuentzia. Erregistratutako objektuei egokitu dakieke, eta bakarrak dira gainerako OID guztien artean.
- **PIN (Personal Identification Number):** mekanismo honen beraren babespean dagoen baliabide batera sartu behar duen subjektuak bakarrik ezagutu behar duen karaktere-sekuentzia.
- **Ziurtapen-politika:** Ziurtapen Praktiken Deklarazioari erantsitako dokumentua da, eta bertan jasotzen da zein den ziurtagirien aplikazio-eremua, karaktere teknikoak, ziurtapen-zerbitzuak ematerakoan jarraitutako prozeduretarako arauak, baita ziurtagirien erabilpen-baldintzak ere.
- **Gakoen edukitzailea:** kautotzeko gakoak eta sinadura digitala dituzten eta horiek zaintzeaz arduratzen diren pertsona fisikoak izango dira.
- **Ziurtapen Zerbitzuen Egilea (ZZE):** ziurtagiri elektronikoak jaulkitzen dituen edota sinadura elektronikoarekin lotutako bestelako zerbitzuak ematen dituen pertsona fisiko edo juridikoa da.
- **Konfiantzako zerbitzuen egile kualifikatua (TSP):** konfiantzako zerbitzuen egilea, eIDAS arauaren araberako konfiantzako zerbitzu bat edo batzuk egiten dituena eta ikuskapen-organismoaren eskutik kualifikazioa lortu duena.
- **Egiaztapen Aurreratuko Zerbitzua:** zerbitzu honek aukera ematen dio zerbitzuaren Entitate Erabiltzaileari IZENPEk jaulkitako ziurtagiriak erabiltzeko. Horretarako, ziurtagirien egoera begiratzen du, OCSP (Online Certificate Status Protocol) protokoloaren bidez.
- **Argitalpen Zerbitzua:** ziurtapen-sistemarekin lotutako dokumentazioa argitaratzen duen zerbitzua da, eta ziurtagirien erabiltzaile guztientzat egon behar du erabilgarri.
- **Denbora Zigiluen Zerbitzua:** Denbora Zigiluen Zerbitzuak entitate erabiltzaileari aukera ematen dio bermatzeko denbora-tarte jakin batean informazio jakin bat bazegoela.
- **Zerbitzari segurua:** web-zerbitzari bat da eta, bertan, komunikazioa zifratuta doa batetik bestera, modu seguruan. Eragiketa hori egin ahal izateko, zerbitzariak ziurtagiri bat izan beharko du.
- **Ziurtagiriaren eskatzailea:** nork bere buruaren izenean, edota erakunde batenean, ziurtagiri bat jaulkitzea eskatzen duen pertsona da.

- **SSL (Secure Socket Layer):** protokolo honek bide ematen du zifratutako informazioa Interneteko nabigatzaile baten eta zerbitzari baten artean transmititzeko.
- **Ziurtagiriaren harpideduna:** Ziurtapen Zerbitzuen Egileak ziurtatutako gako publikoaren bitartez identitate pertsonala elektronikoki sinatutako datuei lotua duen pertsona.
- **Txartel kriptografikoa:** Sinadura Sortzeko Gailu Seguru gisa hartzen den txartela da, eta harpidedunak, besteak beste sinatzeko eta kautotzeko erabiltzen diren gako pribatuak biltzeko, sinadura elektronikoak sortzeko eta datu-mezuak deszifratzeko erabil dezake.
- **Hirugarrengoengan konfiantza duten hirugarren batzuk:** IZENPEk jaulkitako ziurtagiriak jasotzen dituzten pertsona fisikoak edo juridikoak dira. Ziurtagirietan konfiantza duten hirugarren batzuk dira eta, hirugarrenak diren heinean, Ziurtapen Praktiken Deklarazioan ezarritakoa zaie aplikagarri, baldin eta ondorioetarako ziurtagiri horietan benetan konfiantza badute.
- **Ziurtagirien erabiltzaileak:** ziurtagirien erabiltzaile diren azken entitateak ziurtagiri digitalak jaulki, kudeatu eta erabiltzeko zerbitzuak jasotzen dituzten pertsona eta erakundeak dira.
- **Zigilu baten sortzailea:** zigilu elektroniko bat sortzen duen pertsona juridikoa.
- **Zigilu elektronikoa:** formatu elektronikoko datuak, formatu elektronikoko beste datu batzuei eransten zaizkienak edo horiekin modu logikoan lotzen direnak, azken horien jatorria eta integritatea bermatzeko.
- **Zigilu elektroniko aurreratua:** eIDAS arauaren 36. artikuluan aintzat hartzen diren betekizunak betetzen dituen zigilu elektronikoa.
- **Zigilu elektroniko kualifikatua:** zigilu elektroniko aurreratua, zigilu elektronikoak sortzeko gailu kualifikatu bidez sortzen dena eta zigilu elektronikoko ziurtagiri kualifikatu batean oinarritzen dena.
- **Zigilu elektronikoa sortzeko datuak:** zigilu elektronikoko egileak zigilu elektronikoa sortzeko erabiltzen dituen datu bakarrak.
- **Zigilu elektronikoko ziurtagiria:** deklarazio elektronikoa, zigilu bat baliozkotzeko datuak pertsona juridiko batekin lotzen dituena, eta pertsona horren izena berresten duena.
- **Zigilu elektronikoko ziurtagiri kualifikatua:** konfiantzako zerbitzuen egile kualifikatu batek jaulkitako zigilu elektronikoetako ziurtagiria, eIDAS arauaren eranskinean ezarritako betekizunak betetzen dituena.
- **Zigilu elektronikoa sortzeko gailua:** zigilu elektronikoa sortzeko erabiltzen den tresna edo programa informatiko konfiguratua.
- **Zigilu elektronikoa sortzeko gailu kualifikatua:** eIDAS arauaren II. eranskinean zerrendatzen diren betekizunak mutatis mutandis betetzen dituen zigilu elektronikoak sortzeko gailua.

- **Denbora-zigilu elektronikoa:** formatu elektronikoko datuak, formatu elektronikoko beste datu batzuk une jakin batekin lotzen dituztenak eta azken datu horiek une horretan bazeudela frogatzen dutenak.
- **Denbora-zigilu kualifikatu elektronikoa:** eIDAS arauaren 42. artikuluan ezartzen diren betekizunak betetzen dituen denbora-zigilu elektronikoa.

1.6.2 Akronimoak

ARL: Ziurtapen Agintaritzak Ezeztatzeko Zerrenda.

CA: Ziurtapen Agintaritza.

CN: Common Name (izen arrunta).

CRL: Certificate Revocation List (ezeztatutako ziurtagirien zerrenda).

DN: Distinguished Name (izen bereizgarria).

ZPD: Ziurtapen Praktiken Deklarazioa

QSCD: Sinadura sortzeko gailu kualifikatua

ETSI: European Telecommunications Standards Institute

GN: ziurtagiri baten edukitzailearen izen berezia

HSM: Hardware Security Module (segurtasun-modulu kriptografikoa).

SEL: Sinadura elektronikoari buruzko abenduaren 19ko 59/2003 Legea.

LRA: tokiko erregistro-agintaritza.

OCSP: Online Certificate Status Protocol (Ezeztatutako Ziurtagirien Argitalpen Zerbitzua, data eta ordu batetik aurrera).

OID: Object Identifier (objektu-identifikatzaile bakarra).

PIN: Personal Identification Number (identifikazio pertsonaleko zenbakia).

PKCS: Public Key Cryptography Standards (RSA Laborategiek garatutako PKI estandarrak).

PKI: Public Key Infrastructure (gako publikoen azpiegitura)

ZZE: Ziurtapen Zerbitzuen Egilea

RA: Erregistro-agintaritza.

SSL: Secure Socket Layer

TSA: Denbora Zigilatzeko Agintaritzaren zerbitzaria

eIDAS: 1999/93/EE Zuzentaraua indargabetzen duen Europako Parlamentuaren eta Kontseiluaren identifikazio elektronikoari eta barne-merkatuko transakzio elektronikoetarako konfiantzako zerbitzuei buruzko uztailaren 23ko 910/2014 Araudia

2 Argitalpena eta informazio-biltegiaren arduradunak

2.1 Informazio-biltegia

IZENPEk informazio publikoko biltegia du http://www.Izenpe.com helbidean, eta asteko zazpi egunetan eta eguneko 24 orduetan dago eskuragarri.

2.2 Ziurtapen-informazioaren argitalpena

IZENPEren Argitalpen Zerbitzuaren bitartez ziurtapen digitalari buruzko informazioa eta zerbitzu osagarriei buruzko informazioa argitaratzen da.

IZENPEk

- On line informazioaren eskuragarritasuna bermatzen du.
  Dena den, dokumentu horren bertsio osoa, paperezko euskarrian, eman ahal da ikuskapenak, inspekzioak edo ziurtapen-zerbitzuen beste egile batzuekin ziurtapen gurutzatuak egin behar direnean, edo gakoen edukitzaileak edo hirugarren batek hala eskatzen dutenean.
- Jaulkitako ziurtagirien erregistroa azkar eta modu seguruan kontsultatzeko aukera eskaintzen du. Ziurtagirietan konfiantza duten hirugarrenek ere kontsulta dezakete erregistroa.
- Ziurtagirien sistema eguneratua mantentzen du eta sistema horrek egindako ziurtagiriak, horiek indarrean dauden edo beren indarraldia eten edo iraungi den emango du aditzera.
- Ezeztatutako Ziurtagirien Zerrendak (CRLak) jaulkitzen ditu eta, erabiltzailearentzako eskuragarri egonez gero, ziurtagiriak denbora errealean egiaztatzeko zerbitzuak eskaintzen ditu, Online Certificate Status Protocol-aren bidez (OCSP).
- Ezeztatutako Ziurtagirien Zerrendak argitaratzeari dagokionez, sarbide azkarra, segurua eta doakoa bermatzen zaie erabiltzaileei eta ziurtagirien harpidedunei.

2.2.1 Argitalpen- eta jakinarazte-politika

Zerbitzuaren zehaztapenetan edo baldintzetan egindako aldaketak IZENPEren web-orri nagusiaren (www.izenpe.com) bidez jakinaraziko dizkie IZENPEk erabiltzaileei.

30 egunez egingo da aldaketen aipamena, eta bertan jasoaraziko da aldatu den dokumentua, eguneratze-dokumentua eta bertsio berria.

30 egunera, egindako aldaketen aipamena kenduko da , baita bertsio zaharra dokumentaziotik ere. Azken hori IZENPEk gordeko du gutxienez 15 urtez, eta kontsultatu ahal izango dira interesatuen justifikazio arrazoituaren ondoren.

2.2.2 Ziurtapen Praktiken Deklarazioan argitaratzen ez diren elementuak

Ziurtapen Praktiken Deklarazio honetako “9.3.2 Irismenaren barruan ez dagoen informazioa” atalean lehendik dauden osagaiei, azpiosagaiei eta elementuei, baina horien

konfidentzialtasuna gordetzeko publikoarentzat erabilgarri ez daudenei, egiten zaie erreferentzia.

2.3 Argitalpen-maiztasuna

Ziurtapen Praktiken Deklarazioa onartzen den unean ematen da argitara. Ziurtapen Praktiken Deklarazioan egin beharreko aldaketak dokumentu honek dioenaren arabera egin behar dira.

Ziurtagirien egoerari buruzko informazioa dokumentu honetako “4.9.6 Geroago” eta “4.9.9 On line ezeztatzea egiaztatzeko eskakizuna” atalek diotenaren arabera argitaratu behar da.

2.4 Biltegirako sarrera kontrolatzea

IZENPEk bere biltegian argitaratutako informazioa irakurtzen uzten du, baina kontrolak ezartzen ditu baimenik gabeko jendeak Zerbitzu horretan erregistrorik sar ez dezan, lehendik zeudenak alda edo ezaba ez ditzan, eta horko informazioaren osotasuna eta egiazkotasuna babesteko.

IZENPEk sistema fidagarriak erabiltzen ditu informazio-biltegira sartzeko. Horrela:

- Baimendutako jendeak bakarrik erants dezake informazioa edo egin ditzake aldaketak.
- Informazioaren egiazkotasuna egiaztatzea badago.
- Ziurtagiriak kontsultarako daude eskuragarri.
- Segurtasun-baldintzei eragiten dien aldaketa oro antzeman egiten da.

3 Izenak

3.1.1 Izen motak

Azken entitateko ziurtagiri guztiek izen bereizgarri bat daukate Subject Name eremuan.

Ziurtagiriaren subject eremuko izen bereizgarria osatzen duten ezaugarriak ziurtagiriaren profilaren atalean bildutakoak dira.

Common Name eremuaren balio kautotua harpidedunaren eta, hala badagokio, gakoen edukitzailearen izena da.

Batzuetan*, subjectAltName* eremua erabiltzen da subjektua identifikatzeko izena (Subject Name eremukoa ez bezalakoa) edukitzeko.

Igorlea

Eremu honetan egoten da IZENPEren identifikazioa, hori baita ziurtagiria izenpetu eta jaulki duen ziurtapen-entitatea.

Eremu horrek ezin du zuriz egon, eta nahitaez eduki beharko du hainbat ezaugarri dituen izen bereizgarria (DN) –izen bat edo etiketa bat eta hori dagokion balioa–.

Mendeko CAen issuer eremua bat dator ziurtagiri horiek jaulki dituen CAren subject eremuarekin.

Gaia

Harpidedunaren edo IZENPEk jaulkitako ziurtagiriaren titularraren identifikazioa egoten da eremu honetan (horren Issuer eremuan identifikatutako CA).

Eremuak ez du hutsik egon behar; nahitaez eduki behar du izen bereizgarri bat (DN). Hainbat ezaugarri ditu izen bereizgarriak: izena edo etiketa, eta horri dagokion balioa.

Ziurtagiri bakoitzerako berariazko dokumentazioan ezartzen da ziurtagiri bakoitzaren profil zehatza.

3.1.2 Izenen formatuak interpretatzeko arauak

Ziurtagiri batean subject-ak eta jaulkitzailearen izenak pertsona (fisikoa edo juridikoa) edo gailua identifikatzen du, eta esanahia izan beharko du, RAk izen edo goitizen horien eta dagozkien entitateen arteko loturaren ebidentzia baitu. Izenak ezin izango dira engainagarriak izan. Horrek ez ditu baztertzen “**¡Error! No se encuentra el origen de la referencia.** Izen-akartasuna” atalean definitzen diren goitizen-ziurtagiriak.

3.1.3 Izen-bakartasuna

Harpidedunen eta, hala badagokio, gakoen edukitzaileen izenak bakarrak dira ziurtagiri mota bakoitzerako. Common name-ak (CN) izenean espazioetako eta bakartasuneko eskakizunak bete beharko ditu. IZENPEk ez du ziurtagiri anonimorik jaulkitzen. IZENPEk goitizen-ziurtagiriak jaulki ditzake, baina ezin izango dira CA ziurtagiriak edo mendeko CA ziurtagiriak izan. Ziurtagiri mota bakoitzaren profilaren xehetasunak kontsulta daitezke www.izenpe.com web-gunean.

3.1.4 Izenen eta marka erregistratuen tratamenduaren arloko gatazkak ebaztea

Etorkizuneko harpidedunak hirugarrenen eskubideak urratzeko moduko izenik ez dute jarri behar ziurtagiri-eskatzaileek ziurtagiriak jaulkitzeko eskaeretan.

IZENPEk ez du erabakitzen ziurtagiri-eskatzaileak baduen eskubiderik ziurtagiri-eskaeran ageri den izenaren gainean. Halaber, ez du artekari- edo arbitro-lanik egiten, eta ez du beste inola ebazten pertsona-, erakunde- edo domeinu-izenen jabetzaren gaineko auzirik.

IZENPEk eskubidea dauka ziurtagiri-eskubiderik ez onartzeko izenei buruzko auziak direla eta.

3.2 Identitatea balidatzea

3.2.1 Gako pribatuaren jabetza frogatzeko metodoak

Gako-parea

- Erregistro-entitate batek sortua bada eta gakoak txartel kriptografiko batean kokatuta daudenean, honela frogatzen da gako pribatuaren jabetza: gailu kriptografikoa entregatzeko eta onartzeko prozedura fidagarriaren indarrez, horri dagokion ziurtagiriaren bitartez, eta barruan duen gako-pareari esker.
- Erregistro-entitate batek sortua bada eta gakoak HSM batean kokatuta daudenean, honela frogatzen da gako pribatuaren jabetza: HSMan zaintzeko prozedura fidagarriaren indarrez, eta gakoak harpidedunak soilik eskuratzeko prozedura fidagarriaren bitartez.
- Ziurtagiriaren gakoen edukitzaileak sortua bada, honela frogatzen da gako pribatuaren jabetza: ziurtagiria behar bezala erabiliz.
- Nabigatzailearen gakoen edukitzaileak sortua bada, honela frogatzen da gako pribatuaren jabetza: gako-parea sortzeko eta ziurtagiria jaulkitzeko prozedura fidagarriaren bidez.
- Gailu mugikorraren gakoen edukitzaileak sortua bada, honela frogatzen da gako pribatuaren jabetza: gako-parea sortzeko eta ziurtagiria jaulkitzeko prozedura fidagarriaren bidez.

3.2.2 Antolakundearen nortasuna kautotzea

IZENPE araudi honen zehaztapenetan oinarritzen da: 2015/1502 Gauzatze Araudia (EB), 2015eko irailaren 8ko Batzordearena, identifikazio elektronikoko baliabideen segurtasun-mailetarako zehaztapen eta prozedura teknikoak finkatzeari buruzkoa, betiere barne-merkatuko transakzio elektronikoetarako identifikazio elektronikoari eta konfiantza-zerbitzuei buruzko Europako Parlamentuaren eta Kontseiluaren 910/2014 Araudiaren (EB) 8. artikuluko 3. atalean xedatutakoaren arabera. Kontsultatu dagokion politika.

3.2.3 Pertsona fisiko eskatzailearen nortasuna kautotzea

IZENPE araudi honen zehaztapenetan oinarritzen da: 2015/1502 Gauzatze Araudia (EB), 2015eko irailaren 8ko Batzordearena, identifikazio elektronikoko baliabideen segurtasun-mailetarako zehaztapen eta prozedura teknikoak finkatzeari buruzkoa, betiere barne-merkatuko transakzio elektronikoetarako identifikazio elektronikoari eta konfiantza-zerbitzuei buruzko Europako Parlamentuaren eta Kontseiluaren 910/2014 Araudiaren (EB) 8. artikuluko 3. atalean xedatutakoaren arabera. Kontsultatu dagokion politika.

3.3 Gakoak berriro jaulkitzeko eskaeretarako identifikatzea eta kautotzea

Berriro jaulkitzeko eskaera baten identifikazio- eta kautotze-baldintzak dagokien politikan garatuko dira.

3.4 Ezeztatzeko eskaeretarako identifikatzea eta kautotzea

Ezeztatzeko eskaera baten kautotze-baldintzak dagokien politikan garatuko dira.

4 Ziurtagirien bizi-zikloaren baldintza operatiboak

Ziurtapen Praktiken Deklarazio honek ziurtagirietarako komunak diren baldintza operatiboak arautzen ditu. IZENPEk kanpoko CA batekin cross certification egiten badu, CA horri eskatuko dio honako Ziurtapen Praktiken Deklarazio honetan definitzen diren eskakizun guztiak betetzea, baita lotuta dauden ziurtapen-politikak ere.

Ziurtagiri mota bakoitzerako berariazko erregulazioa dagokion politikan kontsultatu beharko da.

4.1 Ziurtagiria eskatzea

Ziurtagiria edo dagokion dokumentazioa jaulkitzean eta/edo banatzean izandako akats teknikoen ondoriozko ezeztatzeak eragindako jaulkitzeen kasuan, ez da beharrezkoa izango *ziurtagiria jaulkitzeko beste eskaera bat* egitea.

Zuzen jasoko dira, ziurtagiriaren edukian ezarritako muga teknikoen barruan, ziurtagiri mota bakoitzari dagozkion datu identifikatzaileak. Kontsultatu *Ziurtagiri bakoitzerako berariazko politika* dokumentua.

4.1.1 Eskaeraren egiaztapena

Ziurtagiria jaulki aurretik, IZENPEk eskaera jasoarazitako datuak egiaztatuko ditu, dagokion ziurtapen-politikaren arabera.

4.1.2 Inskribatzeko prozesua eta erantzukizunak.

IZENPEren erregistro-entitateek edo IZENPErekin dagokion lege-tresna izenpetzen duten entitate erabiltzaileek egingo dituzte ziurtagirian jasoarazi den informazioa identifikatzeko eta egiaztatzeko zereginak, eta ziurtagiri horiek jaulkitzeko, ezeztatzeko eta berritzeko eskaerak balidatuko eta onartuko dituzte. Azken horiek honako betebehar hauek hartu beharko dituzte bere gain:

- Eskatzailearen, harpidedunaren eta gakoen edukitzailearen nortasuna eta beste zenbait datu pertsonal egiaztatzea –ziurtagirien xedeetarako garrantzizkoak direnak edo ziurtagirietan daudenak–, prozedura hauen arabera.
- Kudeatzen dituen ziurtagirien jaulkipenari, berritzeari, ezeztatzeari edo berraktibatzeari buruzko dokumentazio eta informazio guztia gordetzea.
- IZENPEri garaiz jakinaraztea ziurtagiriak azkar eta modu fidagarrian ezeztatzeko eskaeren berri.
- IZENPEri artxiboak erabiltzen uztea, baita jardueretarako erabiltzen diren prozeduren eta horretarako behar den informazioaren mantentze-lanen ikuskapena egiten ere.
- IZENPEri jakinaraztea ziurtagiriak jaulki, berritu edo berraktibatzeko eskaeren berri, baita hark jaulkitzen dituen ziurtagiriei buruzko beste zeinahi alderdiren berri ere.

- Garaiz begiratzea ziurtagirien iraunaldian eragina izan dezaketen ezeztatzeko zergatiak.
- Ziurtagiriak jaulki, berritu eta ezeztatzeko IZENPEk ezarritako prozedurak eta gai horretaz indarrean dagoen legeriak agindutakoa betetzea.
- Ziurtagiri motak eskatzen badu, bere gain hartu ahal izango du sinadura elektronikoa sortzeko eta egiaztatzeko prozedura teknikoak harpidedunaren eta/edo gakoen edukitzailearen esku jartzeko eginkizuna.

4.2 Eskaerak prozesatzea

4.2.1 Identifikatzeko eta kautotzeko eginkizunak egitea

IZENPEren erantzukizuna da harpideduna behar bezala identifikatzea. Prozesu hori ziurtagiria jaulki aurretik egin beharko da.

Dena den, ziurtagiri mota bakoitzerako xehetasunak *Ziurtagiri bakoitzerako berariazko politika* dokumentuan begiratu behar dira.

4.2.2 Eskaerak onartzea edo baztertzea

Ziurtagiria eskatu ondoren, RAk eskatzaileak emandako informazioa egiaztatu beharko du, harpidedunaren identitatearen balidazioa barne.

Informazioa zuzena ez bada, RAk eskaerari ezezkoa emango dio eta eskatzailearekin harremanetan jarriko da arrazoia jakinarazteko. Zuzena bada, berriz, ziurtagiria jaulkitzeari ekingo zaio.

Eskaera hori zerbitzari bat kautotzeko domeinu-izen bat barnean hartzen duen ziurtagiri baterako denean, IZENPEk baimendutako CAen erregistroa (CAA erregistroa) aztertuko du, RFC 6844 arabera. CAA erregistro horiek badaude eta, erregistratuta ez dagoelako, IZENPEri ez badiote ziurtagiri horiek jaulkitzeko aukera ematen, IZENPEk ez du ziurtagiri hori jaulkiko, baina eskatzaileek eskaera egin ahal izango dute berriro, behin IZENPEk balizko gorabehera hori konpondu ahal izan duenean.

Dena den, ziurtagiri mota bakoitzerako xehetasunak *Ziurtagiri bakoitzerako berariazko politika* dokumentuan begiratu behar dira.

4.3 Ziurtagiria jaulkitzea

Ziurtagiria egiteak berarekin dakar eskaeraren azken onarpena, eta osoa. IZENPEk ziurtagiria jaulkiko du eta dagokion ziurtapen-politikan finkatutako baldintzen arabera emango du. Horrez gain, IZENPEk edukitzaileari desblokeatzeko kodeak emango dizkio, betiere gakoak IZENPEk sortu baditu.

Ziurtagiria jaulkitzeko eskaeratik hilabeteko epea pasa eta eskatzaileak ziurtagiria jaso ez badu, IZENPErekin jarri beharko da harremanetan.

4.3.1 CAren jardunak ziurtagiriak jaulkitzean

Ziurtagiri bakoitza jaulkitzeko zehaztasunak *Ziurtagiri bakoitzerako berariazko politika* dokumentuan begiratu behar dira.

4.3.2 Jaulkipena jakinaraztea harpidedunari

IZENPEk ziurtagiriaren jaulkipenaren berri emango dio harpidedunari.

4.4 Ziurtagiria onartzea

Ziurtagiria onartzeak berekin dakar harpideduna bat etortzea IZENPEren eta harpidedunaren eskubideak eta betekizunak zehazten dituen xehetasunekin eta baldintzekin, baita IZENPEren ziurtapen digitaleko zerbitzuen gidaritza teknikoa eta operatiboa egiten duen Ziurtapen Praktiken Deklarazio hau ezagutzea ere.

Harpidedunak edo gakoen edukitzaileak 15 eguneko epea du (ziurtagiria ematen zaionetik kontatzen hasita) ziurtagiriak behar bezala funtzionatzen duela egiaztatzeko eta, hala behar izanez gero, IZENPEri itzultzeko.

Arrazoi teknikoengatik gaizki funtzionatzen duelako (besteak beste, ziurtagiriaren euskarriak gaizki funtzionatzen duelako, programak bateraezinak direlako, ziurtagiriko oker teknikoagatik, etab.) edo ziurtagiriko datuak oker daudelako itzultzen bada, IZENPEk ezeztatu egingo du ziurtagiria, eta beste bat jaulkiko du.

4.4.1 Ziurtagiria onartzeko prozesua

Ziurtagiriaren eskaera-dokumentuaren sinadurarekin batera, erabiltzeko baldintzak eta harpidedunaren kontratua ere onartzen dira, biak nahitaez bete beharrekoak.

4.4.2 CAk ziurtagiria argitaratzea

Harpidedunak ziurtagiria onartu eta sortu ostean, IZENPEren barneko ziurtagiri-biltegietan emango da argitara ziurtagiri hori. Harpidedun bakoitza bere ziurtagirira sartu ahal izango da IZENPEren web-aplikazio batetik.

4.4.3 CAk beste entitate batzuei ziurtagiria jaulki izana jakinaraztea

Zerbitzari seguruko ziurtagiriak (SSL) argitara emango dira IZENPEren Certificate Transparency Log Server (CT) zerbitzuan, Symantec-en, Digicert-en eta Google-en. Gainerako ziurtagiriak ez zaizkie beste entitate batzuei jakinaraziko.

4.5 Gako-parea eta ziurtagiriaren erabilera

4.5.1 Harpidedunaren gako pribatua eta ziurtagiriaren erabilera

Bere gakoak zaintzen dituen harpidedunak,

- Ziurtagirien euskarriak ongi erabili eta gordeko direla bermatuko du.
- Ziurtagiria egokiro erabiliko du, eta, zehazki, ziurtagirien erabilera-mugak aintzat hartuko ditu.
- Arretaz zainduko du gako pribatua, baimendu gabeko erabilerak saihestearren, Ziurtapen Praktiken Deklarazioko 6.1, 6.2 eta 6.4 sailek agintzen dutenaren arabera.
- IZENPEri eta, harpidedunaren ustez, ziurtagirian konfiantza duen edonori hau jakinaraziko dio, justifikatzerik ez dagoen atzerapenik gabe:
    - Gako pribatua galdu, norbaitek ostu edo arriskuan jarri izana.
    - Gako pribatuaren kontrola galdu izana, aktibatze-datuak (gailu kriptografikoaren PIN kodea, adibidez) arriskuan jartzeagatik edo beste edozein arrazoirengatik.
    - Ziurtagiriaren edukian dauden okerrak edo izandako aldaketak (harpidedunak dakizkienak edo jakin litzakeenak). Aldaketak ziurtagiria ezeztatzea badakar, horretarako eskaera egin behar du harpidedunak.
- Gako pribatua erabiltzeari utziko dio ziurtagiriaren balio-epea amaitu ondoren.
- Gakoen edukitzaileei jakinaraziko die zein betebehar dagozkien.
- Ez du ziurtagiri-zerbitzuen ezartze teknikoa kontrolatuko eta manipulatuko, ezta atzeranzko ingeniaritzako ekintzarik egingo ere, aurrez Ziurtapen Entitatearen idatzizko baimenik eduki gabe.
- Ez du ziurtagiri-zerbitzuen segurtasuna arriskuan nahita jarriko.
- Ez ditu ziurtagirietako gako publikoei dagozkien gako pribatuak erabiliko inongo ziurtagiri izenpetzeko, ziurtapen-entitatea balitz bezala.
- Ziurtagirian zerrendatutako gako publikoari dagokion gako pribatua erabiliz sinadura digitalak sortzen dituen ziurtagiri kualifikatuen harpidedunak aitortu egin behar du, dagokion bitarteko juridikoaz, sinadura elektroniko horiek eskuz idatzitako sinaduren baliokide direla, gailu kriptografikoa erabiltzen denean, betiere Sinadura Elektronikoari buruzko Legearen 3.4. artikuluak agintzen duenaren arabera.

Bere gakoak IZENPEn gordetzen dituen harpidedunak,

- Ziurtagiria egokiro erabiliko du, eta, zehazki, ziurtagirien erabilera-mugak aintzat hartuko ditu.
- Arretaz zainduko du aktibatzeko gakoa, baimendu gabeko erabilerak saihestearren, Ziurtapen Praktiken Deklarazioko 6.1, 6.2 eta 6.4 sailek agintzen dutenaren arabera.
- IZENPEri eta, harpidedunaren ustez, ziurtagirian konfiantza duen edonori hau jakinaraziko dio, justifikatzerik ez dagoen atzerapenik gabe:
    - Gako pribatuaren kontrola galdu izana, aktibatze-datuak arriskuan jartzeagatik edo beste edozein arrazoirengatik.

- Ziurtagiriaren edukian dauden okerrak edo izandako aldaketak (harpidedunak dakizkienak edo jakin litzakeenak). Aldaketak ziurtagiria ezeztatzea badakar, horretarako eskaera egin behar du harpidedunak.

- Gako pribatua erabiltzeari utziko dio ziurtagiriaren balio-epea amaitu ondoren.
- Ziurtapen Praktiken Deklarazio honetan adierazten diren betebeharrak onartuko ditu.
- Ez du ziurtagiri-zerbitzuen ezartze teknikoa kontrolatuko eta manipulatuko, ezta atzeranzko ingeniaritzako ekintzarik egingo ere, aurrez Ziurtapen Entitatearen idatzizko baimenik eduki gabe.
- Ez du ziurtagiri-zerbitzuen segurtasuna arriskuan nahita jarriko.
- Ziurtagirian zerrendatutako gako publikoari dagokion gako pribatua erabiliz sinadura digitalak sortzen dituen ziurtagiri kualifikatuen harpidedunak aitortu egin behar du, dagokion bitarteko juridikoaz, sinadura elektroniko horiek eskuz idatzitako sinaduren baliokide direla, sinadura sortzeko gailu kualifikatu bat erabiltzen denean, betiere eIDAS arauak agintzen duenaren arabera.

4.5.2 Ziurtagirietan konfiantza duten hirugarren batzuek gako publikoa eta ziurtagiria erabiltzea

Ziurtagirien erabiltzaile egiaztatzaileak honako betebehar hauek ditu:

- Eman nahi zaion erabilerarako ziurtagiria egokia den ala ez jakiteko, informazioa iturri independenteetatik jasotzea.
- Ziurtagiriak erabiltzeko baldintzak ezagutzea, Ziurtapen Praktiken Deklarazioan aurreikusitakoaren arabera.
- Emandako ziurtagirien baliozkotasuna edo ezeztapena egiaztatzea. Horretarako, ziurtagirien egoerari buruzko informazioa erabiliko da.
- Ziurtagirien hierarkiako ziurtagiri guztiak egiaztatzea, sinadura digitalean edo hierarkiako ziurtagiriren batean konfiantza jarri baino lehen.
- Kontuan izatea ziurtagiria erabiltzeko dauden mugak, nonahi daudelarik ere: ziurtagirian bertan nahiz egiaztatzailearen kontratuan.
- Kontuan izatea kontratuan edo beste nonbait finkatutako badaezpadako neurri guztiak, edozein delarik ere haren izaera juridikoa.
- Jakinaraztea ziurtagiriari buruzko gertaera edo egoera irregular guztiak, ziurtagiria ezeztatzeko arrazoia izan daitekeenak.
- Ziurtagiri-zerbitzuen ezartze teknikoa ez kontrolatzea, manipulatzea edo atzeranzko ingeniaritzako ekintzarik ez egitea, aurrez IZENPEren idatzizko baimenik gabe.
- Ziurtagiri-zerbitzuen segurtasuna arriskuan nahita ez jartzea.
- Sinadura elektroniko horiek eskuz egindako sinaduren baliokideak direla onartzea, eIDAS arauaren arabera.

4.6 Ziurtagiria berritzea

Ziurtagiria berritzea harpidedunari beste ziurtagiri bat jaulkitzean datza, betiere harpidedunaren (edo beste parte-hartzaile batzuen) informazioa, gako publikoa edo ziurtagirian agertzen den beste edozein informazio aldatu behar izan gabe. Ziurtagiri motaren araberako balio-aldia izango du. Jaulkitzearen kostuak www.izenpe.com web-gunean adierazten dira. Gakoei eutsi ahal izango zaie berariazko ziurtapen-politikan adierazten diren kasuetan.

4.6.1 Ziurtagiria berritzeko zirkunstantziak

IZENPEk zentzuzko ahaleginak egingo ditu harpidedunei jakinarazteko ziurtagiria laster iraungiko dela. Ziurtagiria iraungi aurreko 60 egunen barruan egin ohi da jakinarazpena.

4.6.2 Nork eska dezake ziurtagiria berritzea

Edozein harpidedunek eskatu ahal izango du haren ziurtagiria berritzea, baldin eta berariazko ziurtapen-politikan deskribatutako zirkunstantziak betetzen badira. IZENPEk ez du inoiz automatikoki berritzen ziurtagiri bat.

4.6.3 Ziurtagiria berritzeko eskaeren tratamendua

Harpideduna IZENPErekin harremanetan jar daiteke bere ziurtagiria berritzea eskatzeko. IZENPEk eskaera nola formalizatu azalduko dio. Dagokion ziurtapen-politikaren jarraibideak aplikatuko dira.

4.6.4 Harpidedunari jakinaraztea

Ziurtapen berriko eskaeretarako erabiltzen den jakinarazpen-prozesu bera erabili beharko da.

4.6.5 Ziurtagiri berritua onartzeko prozedura

Ziurtapen berriko eskaeretarako erabiltzen den prozesu bera erabili beharko da.

4.6.6 Ziurtagiria argitaratzea

Ziurtagiria berritu ostean, ziurtagiri berria beharrezkotzat jotzen diren ziurtagiri-biltegietan eman ahal izango da argitara.

4.6.7 Beste entitate batzuei jakinaraztea

4.4.3. puntuan jasotakoaren arabera.

4.7 Ziurtagiria berritzea, haren gakoak berriro sortuta

“Re-key” prozesua da beste ziurtagiri bat sortzea beste gako publiko batekin (eta beste serie-zenbaki batekin), baina ziurtagiri zaharraren subject-aren edukiari eutsita. Ziurtagiri berriak balio-informazio berria eta gako-pare berria izango du, baina subject bera mantenduko du.

Ziurtagiria berritzean berrituko dira gakoak, berariazko ziurtapen-politikaren arabera.

4.7.1 Ziurtagiriaren gakoak berriro sortzeko zirkunstantziak

Ziurtagiria berritzeko prozesuaren barruan sortuko dira berriro ziurtagiriaren gakoak, ZPDaren 3.2 atalean aditzera ematen den moduan. Era berean, ziurtagiriaren gakoak arriskuan daudenean ere sortu ahal izango dira berriro gakoak.

4.7.2 Nork eska dezake

IZENPEk CAen ziurtagirien gakoak sor ditzake, beste CA bat edo beste subCA bat sortzeko zeremonia-dokumentuaren arabera. IZENPEk, halaber, TSA eta VA zerbitzuaren ziurtagirien gakoak berriro sor ditzake, barne-prozeduraren arabera.

Edozein harpidedunek eskatu ahal izango du haren ziurtagiria berritzea, baldin eta berariazko ziurtapen-politikan deskribatutako zirkunstantziak betetzen badira.

4.7.3 Ziurtagiria berritzeko eskaeren tratamendua, gakoak berriro sortuta

Harpideduna IZENPErekin harremanetan jar daiteke bere ziurtagiria berritzea eskatzeko. IZENPEk eskaera nola formalizatu azalduko dio. Dagokion ziurtapen-politikaren jarraibideak aplikatuko dira.

4.7.4 Harpidedunari jakinaraztea

Ziurtapen berriko eskaeretarako erabiltzen den jakinarazpen-prozesu bera erabili beharko da.

4.7.5 Ziurtagiri berritua onartzeko prozedura

Ziurtapen berriko eskaeretarako erabiltzen den prozesu bera erabili beharko da.

4.7.6 Ziurtagiria argitaratzea

Ziurtagiria berritu ostean, ziurtagiri berria beharrezkotat jotzen diren ziurtagiri-biltegietan eman ahal izango da argitara.

4.7.7 Beste entitate batzuei jakinaraztea

4.4.3. puntuan jasotakoaren arabera.

4.8 Ziurtagiria aldatzea

Ziurtagiriko daturen bat aldatu behar izanez gero, IZENPEk ziurtagiria ezeztatuko du eta beste bat jaulkitzeari ekingo dio.

4.9 Ezeztatzea

4.9.1 Ezeztatzeko zirkunstantziak

Honako egoera hauetan ezeztatuko ditu ziurtagiriak IZENPEk:

- Ziurtagiriak ezeztatzea sinatzaileak, edo hori ordezkatzen duen pertsona fisikoak edo juridikoak eskatuta edota hirugarren baimendu batek edo pertsona juridikoko ziurtagiri elektronikoa eskatu duen pertsona fisiko batek eskatuta.
- Sinatzailearen edo ziurtapen-zerbitzuen egilearen sinadura sortzeko datuak urratzen direnean edo arriskuan jartzen direnean, edo sinatzaileak edo hirugarren batek datu horiek bidegabe erabiltzen dituenean.
- Ebazpen judizial edo administratiboren batek hala agintzen duenean.
- Sinatzailearen nortasun juridikoa iraungitzea edo hiltzea, ordezkatuaren nortasun juridikoa iraungitzea edo hiltzea, sinatzailearengan edo ordezkatuarengan gerora ezintasun iraunkorra edo partziala agertzea, ordezkaritzari amaiera ematea, ordezkatutako pertsona juridikoa desegitea, edo pertsona juridiko batek egindako ziurtagirietan islatzen diren sinadura sortzeko datuak zaindu eta erabiltzeko baldintzak aldatzea.
- IZENPEk jarduera eteten badu, baldin eta, sinatzailearen aurretiko onarpena dela medio, hark jaulkitako ziurtagiri elektronikoen kudeaketa ez bazaizkio transferitzen beste ziurtapen-zerbitzuen egileren bati.
- Ziurtagiria lortzeko emandako datuak aldatzea edo ziurtagiria emateko egiaztatutako zirkunstantziak aldatzea.
- Ziurtagiria galtzen bada edo lapurtzen badute, edo erabiltzeko ez dela geratzen bada ziurtagiriaren euskarria hondatu delako edo Ziurtapen Politikak aurreikusten ez duen beste euskarri batera aldatu delako.
- Aldeetakoren batek dagozkion betebeharrak betetzen ez dituenean.
- Ziurtagiria jaulkitzean akatsen bat gertatu bada, ezarritako prozedurari ez egokitzeagatik edo jaulkitze-prozesuan arazo teknikoak sortzeagatik.
- Sinadura sortzeko datuen hitzarmenetik kanpoko gorabeherak direla medio, IZENPEk jaulkitako ziurtagirien fidagarritasuna eta sistemen segurtasuna arriskuan jartzen bada.
- Ziurtagiria edo harekin lotzen den dokumentazioa jaulkitzean eta/edo banatzean akats teknikorik gertatzen bada.
- Ziurtagiria eskatu zen egunetik hiru hilabete iragan direnean eskatzaileak jaso duen arte.
- IZENPEk ziurtagiria jaulkitzeko eskaera bat jasotzen duenean, eta politika bereko eta bakartasun-irizpide bereko beste ziurtagiri bat dagoenean, ezeztatu egingo da indarrean dagoen ziurtagiria, baina eskatzaileak ezeztatzeko eskaera egin ondoren.

4.9.2 Nork eska dezake ziurtagiria ezeztatzea

Kontsultatu *Ziurtagiri bakoitzerako berariazko politika* dokumentua.

4.9.3 Ezeztatzeko eskaeren tratamendua

Ezeztatzea eskatzen duenak IZENPEren aurrean bideratuko du *ziurtagiria ezeztatzeko eskaera*. Ezeztapena eskatzailea, harpideduna edo gakoen edukitzailea ez den beste pertsona batek eskatuko balu –ezeztatu aurretik edo ezeztatzen den unean bertan–, IZENPEk gakoen edukitzaileari eta ziurtagiriaren harpidedunari jakinaraziko die ziurtagiria baliorik gabe geratuko dela, baita horren zergatia ere.

Eskatzaileak honako bide hauetatik ezeztatu ahal izango du ziurtagiria:

- Bertaratuta, IZENPEren aurrean.
- Telefono bidez, 902 542 542 telefonora deituta.
- Online, www.izenpe.com web-orrian edo posta elektroniko bidez, ziurtagiri onartu batekin elektronikoki sinatutako eskaera baliatuta.
- Edo posta bidez, ziurtagiria ezeztatzeko eskaera sinatuta eta notario aurrean legitimatu ostean bidalita.

Ziurtagiri motari dagokion berariazko politika kontsultatu, identifikaziorako zer beharko den jakiteko.

Ezeztatzeko eskaera kautotua eta ezeztapena justifikatzen duen informazioa erregistratu eta artxibatu egingo dira.

4.9.4 Ezeztatzea prozesatzeko CAren epea

"**¡Error! No se encuentra el origen de la referencia.** Ezeztatzeko eskaeren tratamendua" talean aditzera emandakoa egin ostean, eta RAk (edo IZENPEk "**¡Error! No se encuentra el origen de la referencia.** Ezeztatzeko zirkunstantziak" atalean adierazitako kasuetan) behar bezala tramitatutako ezeztatzearen ondoren, berehala ezeztatuko da ziurtagiria.

4.9.5 Konfiantzako hirugarren batzuek ezeztatzeak egiaztatzeko betebeharra

Ziurtagirien egoera egiaztatzea derrigorrezkoa da ziurtagirien erabilera bakoitzerako, bai ezeztatzeen zerrenda (CRL) kontsultatuta, bai OCSP zerbitzuan kontsultatuta.

IZENPEk informazioa ematen die egiaztatzaileei, dagokion CRLa eta/edo OCSPa non eta nola aurkitu jakin dezaten.

4.9.6 CRLak sortzeko maiztasuna

Ezeztatutako Ziurtagirien Zerrenda (CRL, hemendik aurrera) berehala jaulkitzen du IZENPEk, ezeztapen bat egiten den une berean.

CRLan adierazten da beste CRL bat jaulkitzeko programatuta dagoen unea, aurreko CRLan adierazitako epea amaitu baino lehen ere CRL bat jaulkitzea badagoen arren. Ziurtagiririk berritzen ez bada, ziurtagiriak ezeztatzeko zerrenda egunero birsortuko da.

Azken entitatearen ziurtagirien CRLa 24 orduero gutxienez jaulkitzen da, edo ezeztatze bat gertatzen denean, eta 10 egunez da baliagarria.

CAen ziurtagirien (ARLen) CRLa 12 hilero jaulkitzen da edo ezeztatze bat gertatzen denean.

Ezeztatzen diren ziurtagiria CRLtik kenduko dira. Une horretatik aurrera, 15 urtez gorde behar da ezeztapena IZENPEren barne-erregistroan.

4.9.7 CRLak sortzen direnetik argitaratzen direnera arte emandako denbora

CRLa sortzen denetik 30 segundokoa da gehieneko latentzia-denbora.

4.9.8 Ziurtagirien egoera online egiaztatzeko sistemaren erabilgarritasuna

"IZENPEk egiaztatze-zerbitzua eskaintzen die –denbora errealean– entitate erabiltzaileei OCSP (Online Certificate Status Protocol) protokoloaren bitartez; horrenbestez, erabilera-aplikazioek egiaztatzen dute ziurtagiriaren egoera."

Zerbitzua eguneko 24 orduetan erabili daiteke, asteko 7 egunetan.

4.9.9 On line ezeztatzea egiaztatzeko eskakizunak

CRLen zerbitzua, librea, erabiltzeak eskatuko du,

- Jaulkitako azken CRLa beti egiaztatzea –hori ziurtagirian bertan jasotzen den URL helbidean, “CRL Distribution Point” luzapenean, deskargatu ahal izango da–.
- Erabiltzaileak, horrez gain, hierarkiaren ziurtapen-kate bidezko CRLak ere egiaztatzea.
- Erabiltzaileak ziurtatzea balidatu nahi den ziurtagiria jaulki duen agintaritzak sinatzen duela ezeztatzeko zerrenda.

Ezeztatzen diren ziurtagiriak CRLtik kenduko dira.

OCSP zerbitzua, librea, erabiltzeak eskatuko du,

- Ziurtagirian bertan agertzen den URL helbidea egiaztatzea, “Authority Info Access” luzapenean.
- Erabiltzaileak ziurtatzea balidatu nahi den ziurtagiria jaulki duen CAk sinatu duela erantzuna.

4.9.10 Ezeztatzeak ohartarazteko eskura dauden beste modu batzuk

Ziurtagiri korporatiboen kasuan izan ezik, zeinetan mezuak zuzenduagoak diren, IZENPEk informaziorako mezu elektronikoa bidaltzen dio ziurtagiriaren harpidedunari ziurtagiri kualifikatu bat ezeztatzearen berri emateko.

4.9.11 Arriskupean dagoen gakoaren eskakizun bereziak

Ziurtagiriaren gako pribatua arriskupean badago, gakoen harpidedunak edo edukitzaileak IZENPEri eman behar dio horren berri, horrek ziurtagiria ezeztatzeko eskaera egin dezan eta ziurtagiriaren erabilera eten dadin.

IZENPEren CAren gako pribatua arriskupean badago, dokumentu honen 5.7.3 atalak dioena egin behar da.

4.10 Ziurtagirien egoera-zerbitzuak

4.10.1 Ezaugarri operatiboak

IZENPEk ezeztatutako ziurtagirien zerrendak (CRL) argitaratzeko doako zerbitzua eskaintzen du, horietara sartzeko mugarik gabe. Horrez gain, OCSP (Online Certificate Status Protocol) protokoloaren bidez ziurtagiriak balidatzeko zerbitzuak eskaintzen ditu.

4.10.2 Zerbitzuaren erabilgarritasuna

IZENPEk ziurtagiriak ezeztatzeko 24x7 zerbitzua eskaintzen die entitate erabiltzaileei (24 ordukoa asteko 7 egunetan).

4.11 Harpidetzari amaiera ematea

Ziurtagiria ez da baliozkoa izango indarraldia amaitu denean edo ezeztatu denean.

Berariazko politikan adierazten da ziurtagiri bakoitzaren iraungitzea.

4.12 Gakoak zaintzea eta berreskuratzea

IZENPEk ez du zerbitzu hori eskaintzen.

5 Segurtasun fisikoaren, prozeduren eta langileen kontrolak

IZENPEk segurtasun fisikoko kontrolak dauzka zerbitzuak egiten dituen leku guztietan.

5.1.1 Instalazioen kokalekua eta eraikuntza

Informazioa prozesatzen den tokiek honako baldintza fisiko hauek betetzen dituzte:

- Informazioa prozesatzeko instalazioak dituen eraikina fisikoki sendoa da, kanpoko hormak eraikuntza sendokoak dira, eta segurtasun-kamerek etengabe zaintzen dute. Sartzeko baimena duten pertsonek bakarrik izango dute sarbidea.
- Ate eta leiho guztiak itxita eta babestuta daude, baimenik ez duen inor sartu ez dadin.

5.1.2 Sarbide fisikoa

Datuak Prozesatzeko Zentroa

IZENPEren instalazioek sarbide fisikorako kontrol-sistema osatu bat dute. Hauek dira sistema horren ezaugarriak:

- Segurtasun-perimetro bat, lur errealetik sabai errealeraino, baimenik gabeko inor sar ez dadin.
- Instalazioetarako sarbide fisikoko kontrola,
    - Horretarako baimena duten langileak soilik sar daitezke.
    - Aldiro ikuskatzen eta eguneratzen dira eremu segurura sartzeko baimenak.
    - Langile guztiek eraman behar dute identifikazio-elementuren bat, erraz ikusten dela, eta ez daramanari langileek eurek eskatzea bultzatzen du enpresak.
    - Gainbegiratu egiten dira IZENPEren jarduerarekin zerikusirik ez duten eta haren instalazioetan lanean aritzen diren langileak.

Sarbideen log fitxategi bat dago, leku seguruan gordeta.

IZENPEra sartzeko ateek sarbide-mekanismoak dauzkate.

IZENPEk ziurtapen-zerbitzua egiteko erabiltzen dituen elementuak monitorizatzen dituen telebista-zirkuitu itxi bat.

Erregistro-agintaritzak (RAk)

RAek IZENPEren segurtasun-politikan definitutako beharrezko segurtasun-irizpideak betetzen dituzte.

5.1.3 Elektrizitatea eta aire egokitua

Datuak Prozesatzeko Zentroak energia- eta aireztapen-sistema egokiak ditu, lantoki fidagarri bat izan dadila bermatzeko.

Era berean, IZENPEren instalazioek etengabeko elikadura-funtzionalitatea dute (SAI eta multzo elektrogenoa), energiarik gabe geratu edo aire egokituaren sistema hondatuz gero ekipoa behar bezainbat denboraz martxan edukitzen duena, sistemak modu ordenatuan itxi daitezen.

5.1.4 Urarekiko erresistentzia

IZENPEk beharrezko neurriak hartu ditu urak eragindako kalteetatik eratorritako arriskuak gutxitzeko.

5.1.5 Suteen prebentzioa eta horien aurkako babesa

IZENPEren Datuak Prozesatzeko Zentroak oztopo fisikoak ditu, lur errealetik sabai errealerainokoak, baita suteak automatikoki detektatzeko sistemak ere, honako helburu hauekin:

- Sutea hasi dela jakinaraztea IZENPEko zaintze-zerbitzuari eta langileei.
- Aireztatze-sistema deskonektatzea, suteen aurkako ateak ixtea, elektrizitate-hornidura etetea eta itzaltze-sistema automatikoa abiaraztea.

5.1.6 Euskarriak biltegiratzea

Babeskopien euskarriak modu seguruan biltzen dira.

5.1.7 Hondakinen tratamendua

Informazio-euskarriak deuseztatzeko prozedurak arautuko dituen politika ezarri da.

Informazio konfidentziala duten euskarriak deuseztatu egiten dira, deuseztatu eta gero berreskuraezina izateko moduan.

5.1.8 Instalazioetatik kanpoko babeskopia

IZENPEk babeskopiak istripuetatik babestuta biltegiratzen ditu, eta kokaleku nagusian gerta daitekeen edozein hondamenditan kaltetuak ez gertatzeko moduko distantzia batean.

5.2 Prozeduren kontrolak

5.2.1 Konfiantzazko funtzioak

“Konfiantzazko eginkizunak” dira behar bezala egin ezean istripuagatik edo asmo txarrez segurtasun-arazoak sor ditzaketen funtzioak dituztenak.

“Konfiantzazko eginkizun” bati dagozkion funtzioak behar bezala gauzatzen direnaren probabilitatea handitzeko asmoz, bi alderdi hartu behar dira kontuan:

- Lehenbizikoa erroreak saihesteko eta jarrera desegokiak debekatzeko teknologia diseinatzea eta konfiguratzea da.
- Bigarrena funtzioak hainbat lagunen artean banatzea da asmo txarreko jarduera gauzatzeko hainbat lagunekin adostea beharrezkoa izateko.

IZENPEk antolakundean garatu diren rolen definizio osoa du. Horietarako guztietarako eginkizunak eta erantzukizunak definituta daude.

5.2.2 Zeregin bakoitzerako pertsona kopurua

Sistemaren segurtasuna indartzeko, eginkizun bakoitzerako pertsona desberdinak esleitzen dira salbuespen batekin: operadorearen eginkizuna administratzaileak egin dezake.

Gainera, eginkizun baterako lagun bat baino gehiago eslei daiteke.

5.2.3 Eginkizun bakoitzean identifikatzea eta kautotzea

Konfiantzazko eginkizunek behar bezain segurua den bitarteko batez kautotzea eskatzen dute, eta beti erabiltzaile pertsonalekin.

IZENPEk bakoitzaren eginkizunak zehazten dituen berariazko dokumentazioa du.

5.2.4 Eginkizunetan zereginak bereiztea

IZENPEk CIMC (Certificate Issuing and Management Component) segurtasun-politikari jarraitzen dio, eta haren segurtasun-ereduan dago definituta.

5.3 Langileen kontrolak

5.3.1 Historialei, kalifikazioei, esperientziari eta kautotzeei buruzko baldintzak

Egin behar dituen zerbitzuetan esperientzia eta kalifikazioak dituen langileak enplegatzen ditu IZENPEk.

Konfiantzazko eginkizunak dituzten langileek ez dute IZENPEko eragiketen inpartzialtasunari kalte egin diezaioketen interesik.

5.3.2 Historiala ikertzeko prozedurak

IZENPEk Giza Baliabideetako prozeduren barruan bidezko ikerketak egiten ditu edozein pertsona kontratatu aurretik. Lege-mugen ondorioz, ez da barnean hartzen aurrekari penalak egiaztatzeko aukera.

5.3.3 Trebakuntza-baldintzak

IZENPEren langileek eskatutako trebakuntza jasoko dute, funtzioak betetzean beren trebetasuna ziurtatzeko. Urtean behin, gutxienez, egingo dira prestakuntza-jardunak, honako puntu hauekin gutxienez:

- Ziurtapen Praktiken Deklarazioaren kopia bat emango zaie.
- Segurtasunaren gaineko kontzientziazioa.
- Softwarearen eta hardwarearen funtzionamendua eginkizun jakin bakoitzerako.
- Segurtasun-prozedurak eginkizun jakin bakoitzerako.
- Funtzionamendu eta administrazioko prozedurak eginkizun jakin bakoitzerako.

- Hondamenak konpontzeko prozedurak.
- Gertakariak kudeatzeko prozedura.

5.3.4 Trebakuntza eguneratzeko baldintzak eta maiztasuna

IZENPEren PKI eragiketan aldaketa garrantzitsu bat egiten den bakoitzean, trebakuntza-plana egingo da, eta plana gauzatzea dokumentatuko da. Edonola ere, urteko prestakuntzak beti hartzen du barnean edukia berrikustea.

5.3.5 Lan-txandaketen segida eta maiztasuna

Lanpostuaren beharren arabera txandakatzen dira langileak lanpostuan, edota langileak berak eskatuta.

5.3.6 Baimendu gabeko konexioen zigorrak

Informazioaren segurtasuneko gertakariak

IZENPEk segurtasun-larrialdiak kudeatzeko plana du.

Zigor Prozesua

Zigor-prozesua definitzen duen barne-erregimen diziplinarioa dago.

5.3.7 Langileak kontratatzeko baldintzak

IZENPEk bere zerbitzuen jardunarekin lotuta azpikontratatzen dituen langile guztiek IZENPEren beraren langileek bete beharreko eskakizun berak bete beharko dituzte.

5.3.8 Langileei dokumentazioa ematea

Konfiantzazko eginkizunekin lotutako langile guztiek honako hauek jasotzen dituzte:

- Ziurtapen Praktiken Deklarazioaren kopia bat.
- Eginkizun bakoitzaren betebeharrak eta prozedurak zehazten diren dokumentazioa.
- Sistemaren osagaietako bakoitzaren jardunari buruzko eskuliburuak.

5.4 Audit

IZENPEren eta erregistro-entitateen softwareak sortutako gertaera aipagarriak berregiteko, log fitxategiak erabiliko dira, baita haiek eragin zituen erabiltzailea edo gertaera ere. Halaber, artekaritza-tresnatzat ere erabili ahal izango dira gerta litezkeen auzietan, une jakin batean sinadura baten baliozkotasuna egiaztatuz.

5.4.1 Erregistratutako gertaera motak

Honako log hauek biltegiratzen dira:

- Ziurtagiri-eskaera berriak
- Baztertutako ziurtagiri-eskaerak
- Kontuetarako sarbideen urraketak
- Ziurtagirien sinadura

- Ziurtagiriak ezeztatzea
- Kontuen logon-a
- CRLen sinadura
- CAetako aldaketak
- Ziurtagirien iraungipena

Zerrenda hau ez da inklusiboa, eta ziurtagirien kudeaketarekin edo administrazio-funtzioekin zuzenean lotzen diren ekitaldietara mugatuta dago. Zehazki, ez dira barnean hartzen beste leku batzuetan erregistratuta dauden gertaera teknikoak.

Gertaera bakoitzaren data eta ordua grabatzeko, denbora-datu fidagarria erabiltzen da.

5.4.2 Log fitxategien prozesamenduaren maiztasuna

Log-ak etengabe prozesatzen dira eta hilean behin ikuskatzen ditu segurtasun-arduradunak. Ikuskapen-txostenak alderdi hauek hartzen ditu barnean:

- Baimendu gabe sartzeko egindako saioen zerrenda
- CA bakoitzean izan diren huts-egiteak
- Fidagarriak ez diren IP lerrunetan jaulkitako SSL ziurtagiriak

5.4.3 Audit logaren atxikipen-aldia

Linean eduki behar da log fitxategian sortutako informazioa, artxibatzeko garaia iritsi arte. Artxibatu ondoren, 7 urtez gorde behar dira log fitxategiak.

5.4.4 Audit logaren babesa

Log-eko informaziorako sarbidea ematen zaie haien eginkizunak egiteko sarbidea behar duten langile guztiei. Auditore eginkizuna betetzen duena sartu ahal izango da. Egunkaria datu-basean biltegiratuta dago eta sarbidea hainbat mailatan babestuta dago.

Eragotzita dago log-erregistroak baimenik gabe ezabatzea eta erregistro horiek aldatzea. Log-datuen galera saihesteko larrialdiko neurriak ere badaude.

5.4.5 Audit-logaren backup prozedura

Logak datu-basean kokatzen dira, eta, hartara, datu-basearen eguneroko backup-ean barnean hartzen dira.

5.4.6 Log-fitxategiak biltzea

CAren, RAren eta LRAren log-fitxategiak IZENPEren barne-sistemetan gordetzen dira.

5.4.7 Log-fitxategiak sortzea eragin duen ekintzaren jakinarazpena

Ez dago aurreikusita log-fitxategietako jardueraren berri gertaeraren eragileari jakinaraztea.

5.4.8 Puntu ahulen azterketa

Hiru hilean behin egiten da IZENPEren barne-sistemen kanpoko zein barneko urrakortasunen azterketa. Gainera, urtero egiten da sartze-testa.

5.5 Erregistroak artxibatzea

5.5.1 Artxibatutako erregistroen mota

Honako datu mota edo fitxategi mota hauek artxibatzen dira, besteak beste:

- Erregistro-prozedurarekin eta ziurtagiriak eskatzearekin zerikusia duten datuak;
- Aurreko ataleko ikuskapen-erregistroak;
- Gakoen historikoa.

5.5.2 Fitxategiaren atxikipen-aldia

Ziurtagiri kualifikatuei buruzko informazio eta dokumentazio guztia 15 urtez gordeko da (jaulkitzen diren datatik zenbatzen hasita) eta gainerako ziurtagiriei dagokiena 7 urtez (ziurtagiria amaitzen den datatik hasita).

5.5.3 Artxiboaren babesa

Artxiboa kudeatzeko prozedurak adierazten du zer babes-neurri hartuko diren paperezko erregistroak zein formatu elektronikoko erregistroak manipulatu ez daitezen eta haien edukia suntsitu ez dadin.

5.5.4 Artxiboaren backup prozedurak

Segurtasun-kopien eta kontingentzia-planen arloko politika finkatu da, eta gertakari baten aurrean jarduteko irizpideak eta estrategiak definitzen ditu politika horrek. Gertakarien aurrean jarduteko estrategia osoaren diseinua, beraz, aktiboen inbentarioan eta arriskuen azterketan oinarritzen da.

5.5.5 Erregistroen denbora zigilatzeko eskakizunak

IZENPEk erabiltzen dituen informazio-sistemek bermatu egiten dute haiek egiten diren denbora-uneak erregistratzea. Sistemetako denbora-uneak data- eta ordu-sistema seguru batek sortzen ditu. Sistema guztiek iturri horrekin sinkronizatzen dute beren denbora-unea.

5.5.6 Artxibatzeko sistema

IZENPEren instalazioetan dago artxibatzeko sistema, baita zerbitzuak egiten dituen entitateetan ere.

5.5.7 Artxiboaren informazioa lortzeko eta egiaztatzeko prozedurak

Horretarako baimena duten langileek bakarrik eskura dezakete informazio hori. Sarrera fisikoen eta logikoen aurkako babesak ditu informazioak, honako Ziurtapen Praktiken Deklarazio honen 5. eta 6. atalak agintzen dutenari jarraituz.

5.6 Gakoak aldatzea

CA baten gako pribatua arriskupean ez egoteko, gakoa aldatu egin beharko da erabilitako algoritmoen segurtasun-mailaren arabera. Behin aldatu ondoren, gako berria sinadura-eginkizunetarako soilik erabili beharko da. Gako zaharrak, baliozkoa izaten jarraitzen badu ere, eskuragarri egon beharko du sinadura zaharrak egiaztatzeko, betiere harekin sinatu diren ziurtagiri guztiak iraungitzen diren arte. Gako pribatu zaharra gako horrekin sinatutako ziurtagiriak dituzten CRLak sinatzeko soilik mantendu beharko da, eta gako berriaren babes-maila berarekin babestuko da. CA gako berria sortzeko prozedura definitzen da CA berria sortzeko eta CA zaharra migratzeko zeremonia-dokumentuan. 6.1.5. atalak definitzen du erabilitako algoritmoen eta gakoaren tamaina.

5.7 Larrialdietarako plana

5.7.1 Gertakariak kudeatzeko prozedurak

Larrialdietarako Planak zehazten du zer egin behar den, zer baliabide eta zenbat langile erabili behar diren, baldin eta k ematen dituen ziurtapen-zerbitzuak eta baliabideak ezin erabili uzten dituen edo hondatzen dituen gertakariren bat gertatzen bada (nahita eragindakoa edo halabeharrezkoa).

Larrialdietarako Planaren helburu nagusiak hauek dira:

- Berreskuratze-lanen eraginkortasuna areagotzea, hiru fase hauek erabiliz:
  - Jakinarazteko/ebaluatzeko/aktibatzeko fasea, kalteak ebaluatzeko eta plana aktibatzeko.
  - Berreskuratzeko fasea, behin-behingoz eta partzialki zerbitzuak berriro martxan jartzeko, harik eta jatorrizko sisteman izandako kalteak konpondu arte.
  - Konpontzeko fasea, sistema eta prozesuak bere ohiko martxara itzularazteko.
- Ohiko martxaren etenaldi luzeetan ordezko DPZ batean ziurtapen-zerbitzuak partzialki egiteko behar diren jarduerak, baliabideak eta prozedurak identifikatzea.
- Erantzukizunak esleitzea IZENPEk jarritako langileei eta gida bat prestatzea etenaldi luzeetan ohiko martxa berreskuratzeko.
- Planifikatu den larrialdirako estrategian esku hartzen duten eragile guztien koordinazioa bermatzea (entitateko sailak, kanpoko harremanak eta saltzaileak).

Ziurtapen-zerbitzuak egiteko beharrezko diren eginkizun, eragiketa eta baliabide guztiei aplikatu behar zaie IZENPEren Larrialdietarako Plana. Ziurtapen-zerbitzuetan diharduten IZENPEko langileei aplikatu behar zaie aipatu plana.

Larrialdietarako Planak talde jakin batzuen esku-hartzea aurreikusten du IZENPEren jardueren berreskuratze-lanetan.

Larrialdietarako Planak zehazten du kalteen ebaluazioa eta ekintza-plana nola egin behar diren.

Algoritmoa, erabilitako gako-tamainaren konbinazioa edota segurtasun teknikoa kaltetuko duen edozein ezbehar tekniko sortzen bada, aipatu Larrialdietarako Plana aplikatuko da.

Jasotako inpaktuaren azterketa egingo da. Azterketa horretan segurtasun-arazoaren larritasuna, arazoaren esparrua eta gertatutakoa konpontzeko estrategia aztertuko dira. Egondako inpaktuaren azterketa-txostenean, gutxienez, honako puntu hauek zehaztuko dira:

- Kontingentziaren deskribapen zehatza, denbora-esparrua etab.
- Larritasuna, esparrua.
- Proposatutako irtenbidea edo irtenbideak.
- Hautatutako irtenbidea zabaltzeko plana. Plan horretan, gutxienez, honako puntu hauek hartuko dira kontuan:
    - Erabiltzaileei jakinaraztea, eraginkorrena dela uste den bidea erabilita. Ziurtagirietako eskatzaileei nahiz harpidedunei eta egiaztatzaileei (fidagarriak diren hirugarrenak).
    - Sortutako kontingentziaren berri web-orrian ematea.
    - Kaltetutako ziurtagiriak ezeztatuko dira.
    - Berritze-estrategia.

5.7.2 Datu eta software ustelen aurrean jarduteko plana

IZENPEren kontingentzia-planak egoera horien aurrean jarduteko estrategia jasotzen du.

5.7.3 Gako pribatuaren konpromisoaren aurreko prozedura

Oinarrizko CAk ezeztatu egingo du CA jaulkitzaile jakin baten ziurtagiria CA horren gako pribatua arriskupean badago.

Oinarrizko CAk CA jaulkitzailearen ziurtagiria ezeztatu beharra gertatuz gero, berehala jakinarazi behar die honako hauei:

- CA jaulkitzaileari.
- CA hori erregistratzeko baimena duten RA guztiei.
- CA horrek jaulkitako ziurtagirien sinatzaile titular guztiei.

Oinarrizko CAk ARLn ere (Ziurtapen Agintaritzak Ezeztatzeko Zerrenda) ere argitaratuko du ezeztatutako ziurtagiria.

Ezeztapena eragin zuten arazoak konpondu ondoren, Oinarrizko CAk hau egin behar du:

- Beste ziurtagiri bat sortu CA jaulkitzailerako.
- CAk jaulkitako ziurtagiri berri eta CRL guztiak gako berriarekin sinatzen direla ziurtatzea.

CA jaulkitzaileak kaltetutako azken entitate guztiei jaulki ahal dizkie ziurtagiriak.

Arriskupean dagoen gakoa oinarrizko CArena bada, kendu egingo da ziurtagiria aplikazio guztietatik eta beste bat banatuko da.

5.7.4 Hondamendi baten ondoren, negozioaren jarraipena

CAren jarduera eten egingo da harik eta hondamendia gainditzeko prozedura osatu eta zentro nagusian edo ordezkoan behar bezala funtzionatzen hasten den arte.

IZENPEren Larrialdietarako eta Negozioaren Jarraipenerako Plana aktibatuko da.

5.8 CAren edo RAren amaiera

5.8.1 Ziurtapen-entitatea

IZENPEk CAren Amaiera Plana du, eta bertan horretarako gauzatuko den prozedura zehazten da.

Jarduera etetea erabakiz gero, harpidedunari jakinarazi behar dio IZENPEk ziurtapen-zerbitzuak egiteari uztekotan dela, jarduera eten baino bi hilabete lehenago, gutxienez. Harpidedunak jakinarazpena jasoko duela bermatzen duen bideren bat erabili behar du IZENPEk hura bidaltzeko.

Era berean, TSPei, nabigatzaileen fabrikatzaileei eta IZENPErekin kontratu bidezko loturaren duten entitate guztiei emango zaie haien ziurtagirien erabileraren berri.

IZENPEren Zuzendaritza Nagusiak du jakinarazpen horren erantzukizuna, eta hark erabakiko du horretarako mekanismorik egokiena zein den.

IZENPEk jarduera beste ziurtapen-zerbitzuen egileren bati transferitzea erabakiz gero, ziurtagirien harpidedunari eta Industria, Energia eta Turismo Ministerioari emango die transferentzia-akordioen berri. Horretarako, IZENPEk transferentzia-baldintzak zehazten dituen agiria bidaliko dio harpidedunari, baita harpidedunaren eta ziurtagiriak transferitzen zaizkion ZZEren arteko harremanak erregulatuko dituzten erabilera-arauak ere. Jakinarazpenak jasoko dela bermatzen duen bideren bat erabili behar da hura bidaltzeko, jarduera eten baino bi hilabete lehenago, gutxienez.

Harpidedunak espresuki onartu behar du ziurtagirien transferentzia, eta onartu egin behar ditu ZZE berriaren baldintzak, transferentziaren hartzailearenak ere. Bi hilabete igaro eta ez badago transferentzia-hitzarmenik, edo harpidedunak ez badu hura espresuki onartzen, ezeztatu egingo dira ziurtagiriak.

Jakinarazpena 2 hilabete lehenago bidaltzeko epea amaitu eta beste ZZEren batzuekin akordiorik lortu ezean, automatikoki ezeztatuko dira ziurtagiri guztiak.

IZENPErekin zerbitzugintzako kontratua duten beste hirugarren batzuen edozein baimen (identifikatzeko, jaulkitzeko, gordetzeko, eta abar) amaitutzat emango da.

5.8.2 Erregistro-entitatea.

Erregistro-entitateak, bereganatzen dituen eginkizunak bertan behera uzten dituenean, IZENPEri transferituko dizkio dauzkan erregistroak, informazioa artxibatuta edukitzeko obligazioa duen bitartean; bestela, baliogabetu eta deuseztatu egingo da.

6 Segurtasun teknikoaren kontrolak

6.1 Gako-parea sortu eta instalatzea

6.1.1 Gako-parea sortzea

Oinarrizko CAren eta mendeko CAren gako kriptografikoak hardware-modulu kriptografiko (HSM) batean sortu beharko dira, betiere betetzen duena FIPS 140-2 arauaren 3. maila (edo goragokoa) eta Common Criteria EAL 4+ araua, dagokion babes-profilean.

RAen gako kriptografikoak modulu kriptografiko (HSM) batek sortu beharko ditu, betiere FIPS 140-2 arauaren 2. maila (edo goragokoa) betetzen duena.

VAren gako kriptografikoak hardware-modulu kriptografiko (HSM) batek sortu beharko ditu, betiere FIPS 140-2 arauaren 3. maila (edo goragokoa) betetzen duena.

TSAren gako kriptografikoak hardware-modulu kriptografiko (HSM) batek sortu beharko ditu, betiere FIPS 140-2 arauaren 3. maila (edo goragokoa) betetzen duena.

ETSI TS 119 312 arauan definitzen diren gako luzera minimoaren eta algoritmoaren gomendioak kontuan izanik sortu beharko dira azken erabiltzaileen gako kriptografikoak. IZENPEk gakoak sortzen dituen kasuetan, gakoak honako gailu hauetan sortu ahal izango dira:

- Txartel/token kriptografikoan
- HSMan

Gakoak sortzen dituena azken erabiltzailea den kasuetan, gakoak honako gailu hauetan sortu ahal izango dira:

- Erabiltzailearen nabigatzailearen ziurtagirien edukitzailea
- Web-zerbitzariko gakoen edukitzailea
- IZENPEren edukitzaile segurua
- IZENPEren telefono mugikorrerako aplikazioaren edukitzailea

6.1.2 Gako pribatua harpidedunari banatzea

Gako pribatua hainbat modutan emango da, ziurtagiri motaren eta gailu motaren arabera. Kontsultatu dagokion ziurtapen-politika.

6.1.3 Gako publikoa ziurtagiriaren jaulkitzaileari banatzea

Hona hemen gako publikoa IZENPE osatzen duten edo harekin lankidetzan jarduten duten entitateetatik dagokion ziurtagiri-jaulkitzaileari emateko metodoa:

- IZENPEk sortutako gakoak (txartela, tokena, HSMa): gailu kriptografikoan bertan edo edukitzaile seguruan biltzen direnak.
- Nabigatzailean sortutako gakoak: nabigatzailearen ziurtagirien edukitzailean biltzen direnak.
- Telefono mugikorrean sortzen diren gakoak: IZENPEren aplikazioaren edukitzailean biltzen direnak.
- Zerbitzari Seguruko Ziurtagiriko gakoak (SSL): IZENPEk posta elektroniko bidez eta X.509 formatuan bidaliko dio harpidedunari ziurtagiria, edo erabiltzailearen esku jarriko da SSL kudeaketa-aplikazioan.

- Harpidedunak gako publikoen gako pribatua edukitzaile seguruan sortu duenean: IZENPEk posta elektroniko bidez bidaliko du X.509 formatuan.

6.1.4 Ziurtapen-entitatearen gako publikoa ziurtagirien erabiltzaileei banatzea

IZENPEren CAen gako publikoak hainbat bidetatik banatzen dira, besteak beste, IZENPEren web-orriaren bitartez. Gainera, Ziurtapen Praktiken Deklarazio honetako 1.3.1.1. eta 1.3.1.2. ataletan, oinarrizko CAen eta CA jaulkitzaileen arrastoak daude.

6.1.5 Gakoen tamainak eta erabilitako algoritmoak

Kasu guztietan erabilitako algoritmoa RSA da, SHA-256 duena.

Gakoen tamaina kasuen araberakoa izango da:

- Gutxienez 2048 bit pertsona fisikoen, juridikoen eta gailuen gakoetarako, OCSP zerbitzarietarako, TSA zerbitzarietarako eta ziurtagiri teknikoetarako.
- 4096 bit gutxienez, 2007 ondoren jaulki diren CAetarako

6.1.6 Ziurtapen-sinaduretako algoritmoak

IZENPEk ziurtagiriak sinatzeko erabiltzen duen algoritmo-identifikatzailea (AlgorithmIdentifier) SHA-256 da (hash algoritmoa), RSArekin batera (sinadura-algoritmoa). Algoritmo-identifikatzaile hori ""Identifier for SHA-2 checksum with RSA encryption for use with Public Key Cryptosystem One defined by RSA Inc."" da. Erabilitako padding-eskema emsa-pkcs1-v2.1 da (RFC 3447, 9.2 sekzioaren arabera)”.

Azken erabiltzaileen ziurtagiriak SHA-256 duen RSArekin daude sinatuta. Ziurtagiriarekin sinatzeko, SHA-256 duen RSA edo altuagoa erabiltzeko gomendatzen die azken erabiltzaileei IZENPEk.

IZENPEk industriak onartzen duen eta sinadura onartuko xederako egokia den algoritmo kualifikatu bat erabiltzen du. Horretarako, ziurtagiriaren indarraldia hartuko da aintzat, eta CAB/Forum-ek eta ETSIren estandarrek adierazitako gomendioei jarraituko zaie.

Algoritmoa, erabilitako gako-tamainaren konbinazioa edota segurtasun teknikoa kaltetuko duen edozein ezbehar tekniko sortzen bada, aipatu Larrialdietarako Plana aplikatuko da. Jasotako inpaktuaren azterketa egingo da. Azterketa horretan segurtasun-arazoaren larritasuna, arazoaren esparrua eta gertatutakoa konpontzeko estrategia aztertuko dira. Egondako inpaktuaren azterketa-txostenean, gutxienez, honako puntu hauek zehaztuko dira:

- Kontingentziaren deskribapen zehatza, denbora-esparrua etab.
- Larritasuna, esparrua.
- Proposatutako irtenbidea edo irtenbideak.
- Hautatutako irtenbidea zabaltzeko plana. Plan horretan, gutxienez, honako puntu hauek hartuko dira kontuan:
    - Erabiltzaileei jakinaraztea, eraginkorrena dela uste den bidea erabilita. Ziurtagirietako eskatzaileei nahiz harpidedunei eta egiaztatzaileei (fidagarriak diren hirugarrenak).

- Sortutako kontingentziaren berri web-orrian ematea.
- Kaltetutako ziurtagiriak ezeztatuko dira.
- Berritze-estrategia.

6.1.7 Gakoen erabilera baimenduak (KeyUsage field X.509v3)

Key Usage eta Extended Key Usage luzapena barnean hartzen dute ziurtagiri guztiek, gakoen erabilera gaituak adierazita.

Oinarrizko CA gakoak erabiltzen dira mendeko CAen ziurtagiria, ARLak eta TSAren ziurtagiria sinatzeko. Mendeko CAen edo CA jaulkitzaileen gakoak soilik erabiltzen dira azken erabiltzaileko ziurtagiriak eta CRLak sinatzeko.

Azken ziurtagirietarako onartzen diren gako-erabilerak definituta daude www.izenpe.com web-gunean eskura dagoen ziurtagiri-profiletako dokumentuan.

6.2 Gako pribatua babestea

6.2.1 Modulu kriptografikoen estandarrak

Segurtasun kriptografikoaren modulua (HSM) gako kriptografikoak sortzen eta babesten dituen segurtasun-gailua da. HSMek FIPS 140-2 irizpidearen 3. maila, gutxienez, bete beharko dute, edo Common Criteria EAL 4+ irizpidea, dagokion babes-profilerako.

IZENPEk HSM bat garraiatzean eta biltegiratzean manipulatu ez dela egiaztatzeko protokoloak mantentzen ditu.

Sinadura elektroniko kualifikaturako ziurtagiriak dituzten gailu kriptografikoei dagokienez, sinadura sortzeko gailu kualifikatu gisa onartuak (QSCD), CC EAL4+ segurtasun-maila betetzen dute; baina ITSEC E3 edo FIPS 140-2 2. maila, gutxienez, ziurtagiri baliokideak ere onartzeko modukoak dira.

Erabili diren harpidedun-gailuetarako erreferentziazko Europako araua da Batzordearen 2016ko apirilaren 25eko 2016/650 Gauzatze Erabakia (EB).

IZENPEk, nolanahi ere, IZENPEk gakoak sortzeko erabiltzen dituen harpidedun-gailuak prestatzearen, biltegiratzearen eta banatzearen gaineko kontrola mantentzen du.

6.2.2 Gako pribatua pertsona batek baino gehiagok kontrolatzea (m-tik n)

CAetako gako pribatuak erabiltzeko, bi lagunen onarpena behar da gutxienez.

6.2.3 Gako pribatuaren zaintza

Oinarrizko CAren gako pribatua FIPS 140-2, 3. maila, arauarekin eta/edo CC EAL4+ arauarekin ziurtatutako hardware-gailu kriptografiko batekin zainduta dago, eta, hala, bermatuta dago gako pribatua inoiz ez dagoela gailu kriptografikoaz kanpo. Gako pribatua aktibatzeko eta erabiltzeko, behar-beharrezkoa da lehentxeago aditzera emandako pertsona askotako kontrola.

Mendeko CAen gako pribatuak FIPS 140-2, 3. maila, arauarekin ziurtatutako gailu kriptografiko seguruetan daude zainduta.

"Ziurtagiria hodeian" zerbitzuaren kasuan, ziurtagirien azken erabiltzaileko gako pribatuak gailu kriptografiko seguruetan gordeta daude –FIPS 140-2 3. maila arauarekin ziurtatuta daude gailu horiek–.

Harpidedunak gako pribatua zaintzen duen kasuetan, hura arduratuko da bere kontrolpean soilik mantentzeaz.

6.2.4 Gako pribatuaren babeskopia

Bada CAren (oinarrizkoa edo mendekoa) modulu kriptografikoetako gakoak berreskuratzeko prozedura bat, eta larrialdietan aplika daiteke.

Bada IZENPEk gakoak zaintzen dizkien harpidedunen modulu kriptografikoetako gakoak berreskuratzeko prozedura bat, eta larrialdietan aplika daiteke.

Bi kasuetan, 6.2.2. atalean adierazitako kontrol berberak egingo dira.

6.2.5 Gako pribatua artxibatzea

IZENPEk ez du ziurtagiriak sinatzeko gako pribatua artxibatuko, haren baliagarritasuneko aldia amaitu ostean.

CAren sistemaren osagaiek haien artean komunikatzeko, sinatzeko eta informazioa zifratzeko erabiltzen dituzten barne-ziurtagirien gako pribatuak artxibatuko dira, azken ziurtagiria jaulki ondoren.

Zaintzen diren harpidedunen gako pribatuak harpidedunek beraiek artxiba ditzakete, sinadura sortzeko gailuaren bidez edo beste metodo batzuen bidez; izatez, beharrezkoak izan daitezke gako publikoarekin zifratutako informazio historikoa deszifratzeko, betiere zaintzako gailuak eragiketa ahalbidetzen badu.

IZENPEk kudeatzen dituen harpidedunen gako pribatuak ez dira artxibatzen ziurtagiria iraungi edo ezeztatu ondoren.

6.2.6 Gako pribatuaren transferentzia, modulu kriptografikora edo modulu kriptografikotik

HSM batean sortzen dira oinarrizko CAren gako pribatua, mendeko CAak, VA eta TSA –6.2.1. puntuan zehaztutakoaren arabera–, eta ezin dira esportatu. Larrialdietarako neurri gisa, gako pribatuak berreskura daitezke, 6.2.4. atalaren arabera.

Azken erabiltzaileko ziurtagiriak jaulkitzeko erabiltzen diren gailu hauetan gakoak modulu kriptografikoan sortzen dira, eta ezin da gako pribatua esportatu:

- ✓ Txartel/token kriptografikoa
- ✓ HSMa

Gakoak sortzen dituena harpideduna bera denean, harpideduna bera izango da gakoen zaintzaren arduraduna.

6.2.7 Gako pribatua modulu kriptografikoan biltegiratzea

Oinarrizko CAren eta mendeko CAen gakoen zeremonia-dokumentu bat dago, eta bertan deskribatzen dira gako pribatua sortzeko prozesuak eta hardware kriptografikoaren erabilera.

IZENPEk, CAen gakoak sortzeko, ETSI EN 319 411-1 gomendioa eta Baseline Requirement Guidelines 17.7 gomendioa jarraitzen ditu.

IZENPEk, “hodeian” biltegiratutako azken erabiltzailearen ziurtagirien gakoak sortzeko, Europako Batzordearen gomendioak (eIDAS) eta 2016ko apirilaren 25eko Batzordearen 2016/650 Gauzatze Erabakia (EB) jarraitzen ditu.

IZENPEk, txartel kriptografikoko harpidedunen gakoak sortzeko, Europako Batzordearen gomendioa (eIDAS) eta EN 319 411-1 gomendioa jarraitzen ditu.

Gako pribatuak modulu kriptografikoez kanpo biltegiratzen diren kasuan, gako pribatuak behar bezala babestuko dira, hau da, fisikoki modulu kriptografikoen barruan izango luketen babes-maila berarekin.

6.2.8 Gako pribatua aktibatzeko metodoa

M-tik n gailu kriptografiko (txartel) aldi batera erabiltzea eskatzen duen prozesu baten bidez aktibatzen dira oinarrizko CAren eta mendeko CAen gakoak.

Harpidedunaren gako pribaturako sarrera gakoa sortu den gailuaren mende dago:

- ✓ Txartel/token kriptografikoa: PIN baten bidez egiten da. Gailuak bertara sartzearen aurkako babes-sistema bat du, blokeatu egiten da sarrera-kode okerra hirutan baino gehiagotan sartzen denean. Harpidedunak gailua desblokeatzeko kode bat du. Hiru aldiz oker sartzen bada, gailua behin betiko blokeatuko da, eta erabilezin geratuko da.
- ✓ “Hodeian" kokatutako ziurtagiria: kautotzeko bigarren gailu bat gaituko da, ziurtagiri motaren arabera aldatu ahal izango dena. Ikusi berariazko ziurtapen-politika.
- ✓ Edukitzaile segurua: pasahitz bidez sartuko da.
- ✓ Telefono mugikorreko aplikazioa: PIN bidez sartuko da.
- ✓ Nabigatzailea: pasahitz bidez sartuko da.

6.2.9 Gako pribatua desaktibatzeko metodoa

Oinarrizko CAren gakoak, mendeko CAk, VA eta TSA desaktibatu egingo dira saioa denbora batez jarduerarik gabe badago.

Harpidedunaren gako pribaturako sarrera gakoa sortu den gailuaren mende dago:

- ✓ Txartel/token kriptografikoa: gailu kriptografikoa irakurgailutik ateratzean, aribideko edozein eragiketa bukatzen da, eta PIN bidez egiten da. Lehenespenez, PINaren “katxeoa” aktibatuta ez dagoenez gero, automatikoki desaktibatuko da gakoa erabilera bakoitzarekin.
- ✓ “Hodeian" kokatutako ziurtagiria: ziurtagiri motaren arabera. Ikusi berariazko ziurtapen-politika.
- ✓ Edukitzaile segurua: harpidedunaren erantzukizuna da gako pribaturako sarbidea desaktibatzea eta, hartara, edukitzailea konfiguratzea.
- ✓ Telefono mugikorreko aplikazioa: erabilera bakoitzarekin automatikoki desaktibatuko da gakoa.
- ✓ Nabigatzailea: pasahitz bidez sartuko da. Harpidedunaren erantzukizuna da gako pribaturako sarbidea desaktibatzea eta edukitzailea konfiguratzea.

6.2.10 Gako pribatua deuseztatzeko metodoa

CAren gakoak suntsitzeko prozedura bat dago.

CAen gako probatuak dituen HSMa kentzen bada, suntsitu egingo dira horiek.

“Hodeian” dauden ziurtagirien gako pribatuen kasuan, IZENPErekiko erlazioa amaitzen denean edo iraungitzen direnean ezabatuko dira gakoak.

Prozedura hori ez zaie aplikatzen txartel kriptografikoan jaulkitako erabiltzailea kautotzeko gakoari edo sinadura-gakoari, gakoa berritzeko gailu kriptografiko bera berriro erabiltzen denean izan ezik. Horretan, aurreko gakoa suntsituko da eta euskarri berean beste gako batzuk sortuko dira.

6.2.11 Modulu kriptografikoaren kalifikazioa

Dokumentu honen 6.2.1 atalean aditzera ematen denaren arabera.

6.3 Gako-parea kudeatzearen beste alderdi batzuk

6.3.1 Gako publikoa artxibatzea

CAk sortutako ziurtagiriak, eta beraz, gako publikoak, CAk gordeko ditu indarrean dagoen legediak arautzen duen denboraldian.

6.3.2 Ziurtagiriaren eragiketa-aldiak eta gako-parearen erabilera-aldiak

IZENPEk jaulkitako ziurtagirien erabilera-aldiak dira:

- ✓ Oinarrizko CAren ziurtagiria 30 urtez da baliozkoa.
- ✓ Mendeko CAen ziurtagiriak (EVak izan ezik) oinarrizko CA iraungi arte dira baliozkoak.
- ✓ EVak jaulkitzen dituen CAren ziurtagiria 10 urtez da baliozkoa.
- ✓ Oinarrizko zein mendeko CAen ziurtagirien gako-aldaketa eskari bidez egingo da, eta industriak zehaztutako estandarren arabera.
- ✓ Azken erabiltzaileko ziurtagiriek kasuen araberako iraupena izango dute, kontsultatu berariazko politika. Pertsona fisikoaren eta juridikoaren ziurtagiri guztietan, ziurtagiria berritzeak gakoak sortzea ekarriko du.

6.4 Aktibatzeko datuak

6.4.1 Aktibatzeko datuak sortzea eta instalatzea

Oinarrizko CAren eta mendeko CAen gakoak aktibatzeko datuak oinarrizko CA eta mendeko CAk sortzeko zeremonian sortuko dira.

Harpidedunaren gako pribatua aktibatzeko datuen sorrera eta instalazioa, bestalde, hura sortuta dagoen gailuaren mende daude:

- ✓ Txartel/token kriptografikoa: PIN bat sortuko da ziurtagiria jaulkitzeko prozesuan, eta orri berezi batean inprimatuko da –zuzenean ikusteko aukera ematen ez duen babes-sistema du orri horrek–. IZENPEk ez du PINa ezagutzen.

- ✓ “Hodeian" kokatutako ziurtagiria: kautotzeko bigarren gailu bat gaituko da, ziurtagiri motaren arabera aldatu ahal izango dena. Ikusi berariazko ziurtapen-politika. IZENPEk ez du aktibatzeko datua ezagutuko.
- ✓ Edukitzaile segurua: harpidedunak sortzen eta mantentzen du aktibazio-datua.
- ✓ Telefono mugikorreko aplikazioa: OTP bat sortzen da eta harpidedunari ematen zaio, eta OTP horretatik sortzen du harpidedunak aktibazio-datua.
- ✓ Nabigatzailea: OTP bat sortzen da eta harpidedunari ematen zaio, eta OTP horretatik sortzen du harpidedunak aktibazio-datua.

6.4.2 Aktibatzeko datuak babestea

Oinarrizko CAren gakoak aktibatzeko datuak hainbat txartel fisikotan banatuta daude, eta gutxienez bi pertsona beharko dira edozein eragiketa egiteko. Txartelen gakoak IZENPEren kutxa gotorrean zainduta daude.

Mendeko CAen gakoak aktibatzeko datuak hainbat txartel fisikotan banatuta daude, eta gutxienez bi pertsona beharko dira edozein eragiketa egiteko. Txartelen gakoak hainbat kutxa gotorretan zainduta daude.

TSAren eta VAren gakoak mendeko CAen gakoen HSM berean sortzen eta kudeatzen dira. Arau berak aplikatzen dituzte.

Harpidedunek sekretuan mantendu behar dituzte aktibazio-datuak.

6.4.3 Aktibatzeko datuen beste alderdi batzuk

Ikusi ziurtagiri mota bakoitzerako berariazko politika.

6.5 Segurtasun informatikoaren kontrolak

6.5.1 Segurtasun informatikorako berariazko eskakizun teknikoak

Badira hainbat kontrol IZENPEren ziurtagiri-zerbitzua egiteko sistemaren elementuen kokalekuetan (CAk, IZENPEren datu-baseak, IZENPEren Internet zerbitzuak, CA eragiketa eta sarearen kudeaketa):

- Eragiketa-kontrolak.
  - Eragiketa-prozedura guztiak behar bezala dokumentatuta daude beren eragiketa-eskuliburuetan.

    Larrialdietarako Plan bat dago.
  - Birusen eta kode kaltegarrien aurka babes-tresnak ezarrita daude.
  - Ekipamendua etengabe mantentzen da, ekipamendua une oro erabilgarri eta osorik dagoela ziurtatzearren.
  - Informazio-euskarriak, baliabide nahasgarriak eta ekipamendu zaharkituak ziurtasunez babesteko, ezabatzeko eta deuseztatzeko prozedura dago.
- Datu-trukeak. Datu-truke hauek zifratuta doaz dagokien konfidentzialtasuna ziurtatzeko.
  - RAen eta erregistroko datu-baseen arteko erregistro-datuen trukea.

– Aurreerregistroko datuen trukea.

– RAen eta CAen arteko komunikazioa.

- Ezeztapenen argitalpen-zerbitzuak behar bezalako funtzionalitateak ditu 24x7 funtzionatzea bermatzeko.
- Sarbide-kontrolak.

  – Erabiltzaile bakarreko IDak erabiliko dira; hartara, egiten dituzten ekintzekin lotuko dira erabiltzaileak eta ekintzen erantzukizuna eskatuko zaie.

  – "Pribilegioak ahalik eta gutxien ematea" printzipioa erabiliko da eskubideak esleitzeko.

  – Lanpostuz aldatzen duten edo erakundea uzten duten erabiltzaileen sarbide-eskubideak berehala ezabatuko dira.

  – Erabiltzaileei esleitutako sarbide-maila hiru hilean behin berrikusiko da.

  – Pribilegio bereziak "kasuak kasu" emango dira eta ezabatu egingo dira hura esleitzea eragin zuen kausa amaitzean.

  – Pasahitzen kalitateari dagozkion arteztarauak daude.

IZENPEk segurtasun-politika eta berariazko prozedurak ditu hainbat mailatan segurtasuna bermatzeko.

6.5.2 Segurtasun informatikoaren mailaren ebaluazioa

Ziurtapen-zerbitzuak egiteko erabilitako produktuek ISO/IEC 15408 estandarrean oinarritzen den nazioarteko ziurtagiria dute.

6.6 Bizitza-zikloaren kontrol teknikoak

6.6.1 Sistemen garapen-kontrolak

Softwarea produkzio-sistemetan ezartzea kontrolatzen da.

Sistema horietan sor daitezkeen arazoak saihesteko, kontrol hauek egiten dira:

- IZENPEren politikak aplikazioen eta sistemen garapen segururako arauak hartzen ditu barnean.
- Aldaketak kontrolatzeko prozedura formala existitzen da. Beharrezkoetara mugatzen dira, eta kontrol zorrotzaren mende daude.
- Sistema eragileak aldatzen direnean, Negozioaren Jarraitasun Planak kritikotzat jotzen dituen negozio-aplikazioak berraztertzen dira.
- Sistema seguruko ingeniaritza-printzipioak ezartzen dira.
- Garapen-ingurunea behar bezala babestuta dago.
- Garapen kanporatua ikuskatzen eta kontrolatzen du IZENPEk.
- Garapenean segurtasun funtzionaleko probak egiten dira.

- Onarpen-probetako programak ezartzen dira informazio-sistema berrietarako, eguneratzeetarako eta bertsioetarako.
- Proba-datuak hautatzen dira, eta babestuta eta kontrolatuta daude.

6.6.2 Segurtasunaren kudeaketa-kontrolak

IZENPEk etengabe monitorizatzen du, betiere sistemek eta komunikazioek IZENPEren Segurtasun Politikaren arabera dihardutela ziurtatzeko. Prozesu guztiak logeatzen eta auditatzen dira, indarrean dauden legeriaren eta araudiaren arabera.

6.6.3 Bizi-zikloaren segurtasun-kontrolak

Probak egiteko datu kopuru handia behar da, produkzio-datuetatik ahalik eta hurbilenekoak. Informazio pertsonala duten produkzioko datu-baseak erabiltzea saihesten da.

6.7 Sareko segurtasunaren kontrolak

Sareko segurtasuna maila askotariko zonifikazioaren kontzeptuan oinarritzen da, firewall erredundante ugari erabilita. Sare ez-seguruen bitartez transferitzen den informazio konfidentziala modu zifratuan transferitzen da, SSL/TLS protokoloak erabilita.

6.8 Denbora-iturria

IZENPEk Armadaren Errege Behategirako konexio baten bidez lortzen du bere sistemen denbora, NTP protokoloari jarraituta, betiere Eusko Jaurlaritzarekin ezarritako konexioaren bitartez. NTP protokoloaren deskribapena IETF RFC 5905 estandarrean aurki daiteke.

Barne-zerbitzu horretan oinarrituta, denbora zigilatzeko zerbitzua (TSA) eskaintzen du IZENPEk, eta zerbitzu hori erabili ahal izango da dokumentu arbitrarioetan denbora-zigiluak sortzeko, betiere IETF RFC 3161 estandarraren arabera eta ETSI EN 319 421 estandarraren arabera. Informazio gehiago IZENPEren Denbora Zigilatzeko Praktiken Deklarazioan.

7 Ziurtagirien profilak eta ezeztatutako ziurtagirien zerrendaren profilak

7.1 Ziurtagiriaren profila

IZENPEk jaulkitako ziurtagiriek honako arau hauei jarraitzen diete:

- Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 5280) 2002ko apirilekoa.
- Internet X.509 Public Key Infrastructure Authority Information Access Certificate Revocation List (CRL) Extension (RFC 4325), 2005eko abendukoa.
- Update to DirectoryString Processing in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 4630), 2006ko abuztukoa.
- ITU-T Recommnendation X.509 (2005): Information Tecnology – Open Systems Interconnection – The Directory: Autentication Framework.
- ETSI TS 101 867 Qualified Certificate Profile.
- RFC 3739: Internet X.509 Public Key Infraestructure – Qualified Certificate Profile.

7.1.1 Bertsio-zenbakia

Ziurtapen Praktiken Deklarazio honen arabera jaulkitako ziurtagiriek X509 estandarraren 3. bertsioa erabiltzen dute (populate version field with integer "2").

7.1.2 Ziurtapenen luzapenak

www.izenpe.com web-gunean eskuragarri dagoen profilen dokumentuan adierazitakoak.

7.1.3 Algoritmo-objektuen identifikatzailea

IZENPEk ziurtagiria sinatzeko erabiltzen duen algoritmo-identifikatzailea (AlgorithmIdentifier) SHA-256/RSA da; "Identifier for SHA-2 checksum with RSA encryption for use with Public Key Cryptosystem One defined by RSA Inc."-en identifikatzailearekin bat dator.

7.1.4 Izenen formatuak

www.izenpe.com web-gunean eskuragarri dagoen profilen dokumentuan adierazten dira formatuak. Dokumentu honen 1.3.1 puntuan daude CAen profilak.

7.1.5 Izenen murrizpenak

Ez da "name constraints" luzapena barnean hartzen IZENPEren mendeko agintaritzako ziurtagirietan; horrenbestez, ez da horrelako murrizketa motarik.

7.1.6 Ziurtagiriaren politikaren objektu-identifikatzailea

Ziurtapen Praktiken Deklarazio honetako 1.2. atalean zehaztutakoaren arabera.

7.1.7 “Politika-murrizpenak” luzapenaren erabilera

Ez da politika-murrizpenik erabiltzen.

7.1.8 Politika kalifikatzaileen sintaxia eta semantika

Certificate Policies luzapenak politika-kalifikatzaile hauek ditu:

- **CPS Pointer:** IZENPEren Ziurtapen Praktiken Deklaraziorako erakuslea du, http://www.Izenpe.com/cps."
- **User notice:** hirugarren batek ziurtagiria egiaztatzen duenean, aplikazio bat eskatuta edo erabiltzaile batek eskatuta, pantailan bistaratzen den testu-oharra.
- **Policy Identifier:** ziurtagiriaren OIDa adierazten du

User Notice ziurtagiri guztietarako komuna (SSL ziurtagiriak izan ezik):

USER NOTICE	Kontsulta www.izenpe.com-en baldintzak eta kondizioak ziurtagirian fidatu edo erabili aurretik - Consulte en www.izenpe.com los términos y condiciones antes de utilizar o confiar en el certificado

7.1.9 “certificate policy” luzapenerako tratamendu semantikoa

Certificate Policy luzapenari esker, IZENPEk ziurtagiriarekin zer politika lotzen duen eta politika horiek non aurki daitezkeen identifika daiteke.

7.2 Ezeztatutako ziurtagirien zerrendaren profila

IZENPEk jaulkitako ziurtagiriek honako arau hauei jarraitzen diete:

Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 5280) 2002ko apirilekoa.

Internet X.509 Public Key Infrastructure Authority Information Access Certificate Revocation List (CRL) Extension (RFC 4325), 2005eko abendukoa.

Update to DirectoryString Processing in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 4630), 2006ko abuztukoa.

7.2.1 Bertsio-zenbakia

2. bertsioa (populate version field with integer "1").

7.2.2 Zerrendako elementuen ezeztatutako ziurtagirien eta luzapenen zerrenda

Erabili diren luzapenak honako hauek dira:

Eremua	Nahitaezk.	Kritikoa
X.509v2 Extensions		
1. Authority Key Identifier	Bai	Ez
2. CRL Number	Bai	Ez
3. Issuing Distribution Point	Bai	Ez
4. Reason Code	Ez	Ez
5. Invalidity Date	Bai	Ez

7.3 OCSP profila

IZENPEk jaulkitako ziurtagiriek honako arau hauei jarraitzen diete:

Internet X.509 Public Key Infrastructure Online Certificate Status Protocol-OCSP (RFC 6960) June 2013

7.3.1 Bertsio-zenbakia

3. bertsioa.

7.3.2 OCSParen luzapenak

Eremua	Nahitaezk.	Kritikoa
1. Issuer Alternative Name	Ez	Ez
2. Subject Key Identifier	Ez	Ez
3. CRL Distribution Point	Ez	Ez
4. Key Usage	Bai	Bai
5. Enhanced Key usage	Bai	Bai

8 Bete beharreko ikuskapenak

Segurtasun-baldintzak betetzen diren egiaztatzea –segurtasun-ikuskapena edo segurtasun-azterketa ere deitzen zaio– honetarako egiten da: IZENPEren ziurtapen-zerbitzuko sistemaren segurtasun-plana betetzen dela bermatzeko eta hari egokitzeko. Ikuskapen Plan batean dago zehaztuta jarduera hori.

Egiaztapenak in situ egiten dira, IZENPEko langileek prozedurak eta berariazko babes-neurriak aintzat hartzen dituzten jakiteko.

8.1 Ikuskapenaren maiztasuna

Aldiro begiratzen da ziurtapen-sistema bat datorren segurtasun-baldintzekin. Aurreikusitako beste jarduera batzuekin batera planifikatzen eta gauzatzen da zeregin hori.

8.2 Ikuskatzailearen kualifikazioa

Ikuskatzaileak badu gaitasuna eta eskarmentua –aski frogatuak biak– ekoizpen-sistema seguruen ikuskaritzak egiten, egiaztapen digitaleko sistemena bereziki. EN 319 403 arauaren arabera egiaztatuta egon beharko du.

8.3 Ikuskatzailearen eta ikuskatutako enpresaren arteko harremana

Erakundearen barruko edo kanpoko ikuskatzaileak erabiltzen dira; nolanahi ere, ikuskatu behar den ekoizpen-zerbitzuarekin funtzionamendu-loturarik ez dutenak behar dute izan.

8.4 Ikuskapenaren mende dauden elementuak

Hauek dira ikuskatu beharreko elementuak:

- PKI prozesuak.
- Informazio-sistemak.
- Datuak prozesatzeko zentroaren babes-sistema.
- Dokumentuak.

IZENPEren Ikuskapen Planean dago zehaztuta elementu horietako bakoitzaren ikuskapena nola egin behar den.

8.5 Urritasunen ondoriozko erabakiak hartzea

IZENPEk etengabeko hobekuntzako eredua ezartzen du, eta betetze-ikuskapen baten emaitzak eredu horren arabera tratatzen dira. Larritasunaren eta premiazkotasunaren arabera, ohar, hobekuntza eta desadostasun guztiak jarraipen-sistema batean sartzen dira, eta gertakari edo arazo gisa tratatzen dira. Laguntza-tresna baten bidez, IZENPEk ziurtatzen du arazo guztiak epearen barruan tratatuko direla.

8.6 Emaitzen berri ematea

Segurtasun Batzordeari eman behar zaizkio ikuskapen-txostenak, hark azter ditzan.

Ikuskapena dela-eta ziurtagiriren bat ezeztatu behar izanez gero, IZENPEren Argitalpen Zerbitzuan argitaratu behar da txostena, ezeztapenaren egiaztagiri gisara.

9 Beste lege eta jarduera gai batzuk

9.1 Tarifak

IZENPEk dagozkion ordain ekonomikoak jasoko ditu, Administrazio Kontseiluak onartutako tarifen arabera.

9.1.1 Ziurtagiriak jaulkitzeko edo berritzeko tarifak

Erabiltzaileek ziurtagiriak jaulkitzearen edo berritzearen ordain gisa ordaindu beharreko tarifak 10.1. atalean jaso dira.

9.1.2 Ziurtagirien egoerari buruzko informazioa eskuratzeko tarifa

IZENPEk ziurtagirien egoerari buruzko doako informazio-zerbitzuak eskaintzen ditu CRLen edo OCSParen bidez.

9.1.3 Beste zenbait zerbitzutarako tarifak

Beste zerbitzu batzuetarako tarifak IZENPEren eta eskainitako zerbitzu horien bezeroen artean finkatuko dira.

9.1.4 Itzultze-politika

IZENPEk ez du itzultze-politikarik.

9.2 Finantza-erantzukizunak

IZENPEk, erregistro-entitateek eta entitate erabiltzaileek behar adina baliabide daukate dagozkien eragiketak eta jarduerak gauzatzeko.

IZENPEk erantzukizun zibileko asegurua du, ziurtagiriak sortzeko unean izan daitezkeen eta zehazki egiten den jarduerara zabal daitezkeen hutsuneak eta/edo hutsegiteak berdintzeko. IZENPEk eta erregistro-entitateek esku hartzen badute, harpidedunekin eta ziurtagirien erabiltzaileekin duten harremana ez da mandatuzkoa, ezta mandatu-hartzailearen eta mandatu-emailearen artekoa ere. Harpidedunek eta ziurtagirien erabiltzaileek ez dute IZENPE eta erregistro-entitateak inongo prestazio ematera behartzeko eskubiderik, ez kontratu bidez, ez antzeko beste inongo bitartekoz baliatuz.

9.3 Informazioaren konfidentzialtasuna

9.3.1 Informazio konfidentzialaren irismena

Zerbitzuak egiteko, IZENPEk eta erregistro-entitateek hainbat informazio bildu eta biltegiratu beharra daukate, zenbait datu pertsonal ere tarteko direla. Interesatuei eurei eskatzen zaie informazio hori, haien onarpen esplizituaz. Interesatuaren onarpenik gabe ere jaso daiteke informazioa, datuak babesteko legeriak horretarako baimena ematen duen kasuetan.

IZENPEk eta erregistro-entitateek ziurtagiriak jaulkitzeko, horiek mantentzeko eta sinadura elektronikoari dagozkion beste zerbitzu batzuk egiteko behar dituzten datuak bakarrik biltzen dituzte, eta ezin dira bestelako xedeetarako erabili sinatzailearen baimen zehatzik gabe.

IZENPEk zaindu egiten du datu-emaileen intimitatea, datu pertsonalak babesteko indarrean dagoen legeriak agintzen duen legez.

IZENPEk eta erregistro-entitateek ez dute datu pertsonalik plazaratzen eta inori uzten, Ziurtapen Praktiken Deklarazio honetako dagozkien atalek eta IZENPEren eta erregistro-entitateen jarduera-amaiera kasurako dagokion atalak aurreikusitako egoeretan izan ezik.

IZENPEk eta erregistro-entitateek konfidentzialtzat gordetzen dituzte honako informazio hauek:

- Ziurtagiri-eskaerak –onartuak zein onartu gabeak–, baita ziurtagiriak jaulkitzeko eta mantentzeko eskuratutako gainerako informazio guztia ere, dagokion atalean zehaztutako informazioa izan ezik.
- IZENPEk sortutako edo biltegiratutako gako pribatuak.
- Transakzioen erregistroak, erregistro osoak eta transakzioen ikuskapen-erregistroak ere barne direla.
- IZENPEk edo erregistro-entitateek eta horien ikuskatzaileek sortutako eta/edo mantendutako barne- eta kanpo-ikuskapenen erregistroak.
- Negozioen jarraitutasun-planak eta larrialdietarako planak.
- Segurtasun-politika eta -planak.
- Eragiketen eta gainerako eragiketa-planen dokumentazioa, hala nola artxibatzea, kontrolatzea eta antzeko beste zenbait.

9.3.2 Irismenaren barruan ez dagoen informazioa

Honako informazio hau ez-konfidentzialtzat jotzen da, eta halakotzat onartzen dute interesatuek eurek ere IZENPErekin daukaten tresna juridiko loteslean:

- Jaulkitako ziurtagiriak, edo jaulkitze-bidean direnak.
- Pertsona fisikoa den harpidedun batek IZENPEk jaulkitako ziurtagiri batekin duen lotura.
- Ziurtagiriaren harpidedunaren izen-abizenak ziurtagiriaren harpideduna eta sinatzailea pertsona fisikoa bada, edo gakoen edukitzailearenak ziurtagiriaren harpideduna pertsona juridikoa edo administrazio-organoa bada, baita titularraren beste edozein zirkunstantzia edo datu pertsonal ere, ziurtagiriaren xedeetarako garrantzizkoa bada.
- Hala agertzen bada, ziurtagiriaren harpidedunaren helbide elektronikoa –ziurtagiriaren harpideduna eta sinatzailea pertsona fisikoa bada–, gakoen edukitzailearen helbide elektronikoa –ziurtagiriaren harpideduna pertsona juridikoa edo administrazio-organoa bada–, edo harpidedunak esleitutako helbide elektronikoa –gailuetarako ziurtagiriak badira–.

- Ziurtagiriak finkatzen dituen muga eta erabilera ekonomikoak.
- Ziurtagiriaren balio-epea, baita ziurtagiriaren jaulkitze- eta iraungitze-datak ere.
- Ziurtagiriaren serie-zenbakia.
- Ziurtagiriaren egoera guztiak, baita horietako bakoitzaren hasiera-data ere. Zehazki: sortzeko eta/edo entregatzeko zain, balidatua, ezeztatua, etena edo iraungia, baita egoera-aldaketa eragin zuen zergatia ere.
- Ezeztatutako Ziurtagirien Zerrendak (CRLak), baita ezeztatze-egoerei dagozkien gainerako informazioak ere.
- IZENPEren Argitalpen Zerbitzuan dagoen informazioa.
- Ziurtapen Praktiken Deklarazioko informazio konfidentzialen atalean ageri ez den gainerako informazio guztia.

9.3.3 Informazio konfidentziala babesteko erantzukizuna

Legeak horretarako aurreikusten dituen kasuetan bakarrik argitaratuko dute informazio konfidentziala IZENPEk edo erregistro-entitateek.

Ziurtagiriko datuen fidagarritasuna bermatzen duten erregistroak, zehazki, prozedura judizial batean ziurtapena egiaztatzeko eskatzen badituzte argitaratuko dira, baita ziurtagiriaren harpidedunaren baimenik gabe ere.

Ziurtagiriak argitaratzean sinadura elektronikoari buruzko abenduaren 19ko 59/2003 Legearen 18.c) artikuluak agintzen duenari jarraituko zaio.

9.4 Datu pertsonalak babestea

9.4.1 Sarrera

IZENPEk, ziurtapen-zerbitzuen emaile den heinean, datu pertsonalen fitxategiak babestu egiten ditu, datu pertsonalak babesteari buruzko abenduaren 13ko 15/1999 Legean aurreikusitakoari jarraikiz, baita datu pertsonalak babesteari buruzko 15/1999 Lege Organikoa garatzeko Araudia onartzen duen 1720/2007 Errege Dekretuan aurreikusten denari, eta gainerako garapeneko araudiari jarraikiz ere.

Sinadura elektronikoari buruzko Legean ezarritakoa kontuan izanik, Ziurtapen Praktiken Deklarazio hau segurtasun-dokumentutzat hartzen da, betiere datu pertsonalak babesteari buruzko legedian aurreikusten den helburuetarako. Gisa horretako dokumentu batek bete behar dituen baldintzak betetzen ditu.

9.4.2 Aplikazio-esparrua

Datu pertsonalak dituzten fitxategiak babesteko segurtasun-dokumentuan, IZENPEk bere fitxategietan dauden datu pertsonalen babesa bermatzeko beharrezko segurtasun-neurriak ezartzen ditu, betiere datu pertsonalak tratatzen dituzten instalazioetan, euskarri-plataformetan eta informazio-sistemetan oinarrituta –automatizatuetan, automatizatu gabeetan zein mistoetan–.

Horrela, segurtasun-dokumentuan honako alderdiak jorratuko dira:

- Datu pertsonalak babesteko segurtasun-antolamendua.
- Datu pertsonalak dituzten fitxategien egitura eta segurtasun-mailak.
- Segurtasuneko arauak eta prozedurak.

Bestalde, datu pertsonalak tratamendu, sarrera, aldaketa edo galera baimendu gabeen aurrean eraginkortasunez babestuko badira, informazio hori eskuratzeko erabil daitezkeen bide guztiak kontrolatuko dira.

Horrela, hauek dira datu pertsonalak dituzten IZENPEren fitxategietara sartu ahal izateko zuzeneko edo zeharkako bide izan daitezkeen baliabideak –ondorio horretarako araudiak kontrolatu behar dituenak–:

- Fitxategiak kokatuta dauden eta horien euskarriak edo dokumentuak biltegiratzen diren tratamendu-zentroak edo -instalazioak eta lokalak.
- Fitxategiak kokatuta dauden eta fitxategi automatizatuekin lan egiten den sistema eragilearen eta komunikazio-sistemaren ingurunea eta zerbitzariak.
- Baimendu gabeko dokumentazio eta informazioko fitxategiak.
- Datuetara sartzeko ezarritako sistemak (automatizatuak, eskuzkoak edo mistoak).

9.4.3 Datu pertsonalak babesteko segurtasun-antolamendua.

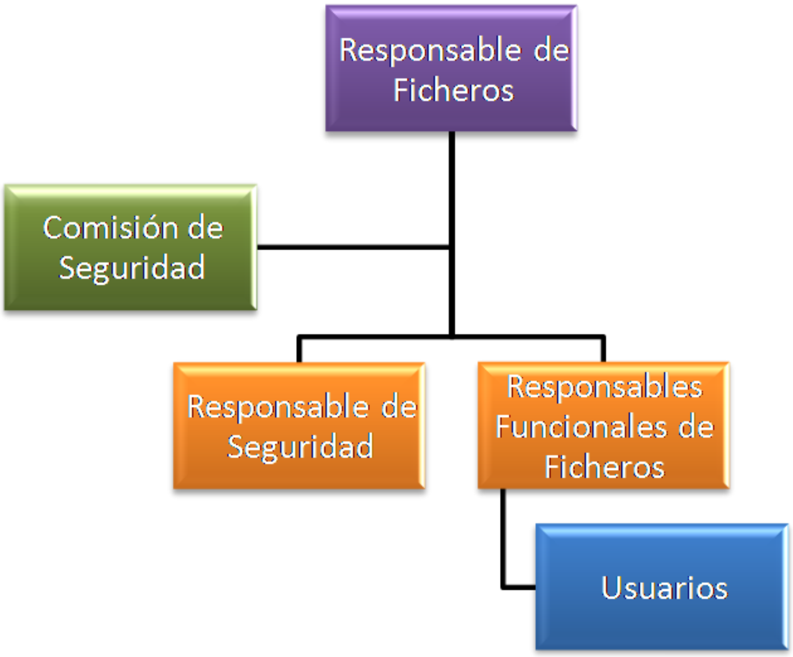
Atal honetan deskribatzen da IZENPEk datu pertsonalen segurtasuna bermatzeko ezarritako segurtasun-antolamendua.

Segurtasun-antolamenduaren eredua aurkezten da. Tartean dauden unitateak ez ezik, horien arteko mendetasun hierarkikoa eta funtzionala ere identifikatzen eta aurkezten da.

IZENPEren segurtasun-dokumentuan, segurtasun-antolamenduko unitateetako bakoitzak garatu beharreko funtzioak zehazten dira.

9.4.4 Segurtasun-antolamenduaren eredua

Organigrama honetan jasotzen da IZENPEren datu pertsonalen segurtasuna kudeatzeko eta kontrolatzeko segurtasun-egituraren irudikapen grafiko sinplifikatua. Segurtasunaren antolamenduan inplikatutako unitateak irudikatzen dira, baita horien arteko lotura hierarkikoak edo funtzionalak ere (zehazki, fitxategien arduraduna, segurtasun-batzordea, segurtasuneko arduraduna, IZENPEren fitxategien arduradun funtzionalak eta erabiltzaileak).



Fitxategien arduraduna / Segurtasun-batzordea / Segurtasun-arduraduna / Fitxategien arduradun funtzionalak / Erabiltzaileak

9.4.5 Segurtasuna antolatzeko unitateen sailkapena

Aurretik deskribatutakoaren arabera, segurtasunaren antolamendurako segurtasun-dokumentuan zerrendatutako unitateak eta langileak honako kategoria hauetan sailkatzen dira:

- Fitxategiaren arduraduna, fitxategiaren xedeari, edukiari eta erabilerari buruzko erabakiak hartzen dituen pertsona fisikoa edo juridikoa.

  Fitxategiaren segurtasunaz arduratzen da, eta beharrezko segurtasun-neurriak hartzen eta ezartzen ditu, dokumentu hau bete behar duten langileek dagozkien funtzioen garapenean eragina duten arauak ezagut ditzaten.

  Dokumentua eguneratuta mantentzen du, eta datuen segurtasunaren arloan indarrean dauden xedapenetara egokitu beharko du beti dokumentu honen edukia.

- Segurtasun-arduraduna, fitxategiko arduradunak izendatzen duen pertsona honek fitxategiko datuei aplika dakizkiekeen segurtasun-neurriak koordinatzeko eta kontrolatzeko funtzioak bete behar ditu.

  Fitxategiko arduradunarekin elkarlanean, segurtasun-dokumentuaren hedapena bultzatzen du, eta berau betetzen dela zaintzeko lanetan ere laguntzen du.

- Segurtasun-batzordea, informazioaren segurtasunari eta datuen babesari dagozkion erabakiak hartzean, antolakundeko unitateen kontsulta eta laguntzarako organo gorena da. Bere eskumenak baliatzean, Batzordeak eskuordetze bidez jarduten du, IZENPEren ordezkaritza gorena den Zuzendaritza-Gerentziaren babes osoarekin –datu pertsonalak dituzten fitxategien arduraduna den aldetik– eta fitxategi horiek atxikitzen diren zuzendaritza-organoen babes osoarekin –horien ardura duten barne-organo diren aldetik–.

- Fitxategien arduradun funtzionala, zerbitzuen ikuspuntu funtzionaletik Informazio Sistemen alderdi operatiboetan erabakiak hartzeaz arduratzen den pertsonari dagokion irudia da. Irudi horiek fitxategien arduradun den IZENPEren ordezkaritzan jardungo dute. Tartean den zerbitzuaren kudeaketaren arduradunak, hau da, arloetako bakoitzeko arduradunak izango dira funtzio hori beteko duten IZENPEren pertsonak.
- Fitxategiaren erabiltzailea, bere funtzioak betetzean datu pertsonalak tratatzen dituen edo datu horiek eskura dituen pertsona da. Erabiltzaile horiek, datu pertsonalen alorrean, Segurtasun Dokumentuan biltzen diren arauak eta prozedurak errespetatu beharko dituzte, baita indarrean dagoen eta aplikatzekoa den legeriaren ondoriozkoak ere.

9.4.6 Datu pertsonalak dituzten fitxategien egitura

Ziurtapen Praktiken Deklarazio honen ondorioetarako, IZENPE da Datuak Babesteko Espainiako Agentziak datu pertsonalak dituzten honako fitxategi hauen (aurrerantzean FITXATEGIEN) arduraduna:

- Erabiltzaileak: oinarrizko segurtasun-maila.
- Administrazio-kudeaketa: oinarrizko segurtasun-maila.
- Giza baliabideak: oinarrizko segurtasun-maila.
- Curriculum Vitaea: oinarrizko segurtasun-maila.
- Dokumentazioaren sarrera eta irteerako erregistro-fitxategia: oinarrizko segurtasun-maila.
- Transakzioak: oinarrizko segurtasun-maila.
- Hirugarren batzuekiko harremanak: oinarrizko segurtasun-maila.

Fitxategiek datu pertsonalak dituztenez gero, 1720/2007 Errege Dekretuaren 81. artikuluan ezartzen denez, dagozkien segurtasun-neurri guztiak izango zaizkie aplikatzekoak.

Fitxategien egituraren deskribapena Antolamenduaren Segurtasun Dokumentuan zehazten da.

9.4.7 Segurtasuneko arauak eta prozedurak

Datu pertsonalen segurtasuna bermatuko duten neurri, arau eta prozedura zehatzak daude.

Horretarako, segurtasun-dokumentuak arreta berezia eskaintzen dio sistema eragilearen inguruneari, baita segurtasun-dokumentuaren babespeko fitxategiaz baliatzen diren ordenagailuak kokatzen diren lokalei eta lanpostuei ere.

Arauak

IZENPEk, bere funtzioen jardunean, tratatzen dituen datu pertsonalen babesa bermatzeko beharrezko arauak ditu, eta, horrela, mota horretako datuei aplikatzekoa zaien legeria betetzen du.

Arau horiek IZENPEren zerbitzu, dependentzia eta informazio-sistema guztiei aplikatzen zaizkie; edozein formatutan (paperean, informatikoan, bideoan, ...) biltzen diren datu pertsonal guztiei aplikatzen zaie, elementu horiek erabiltzen dituen pertsona edozein izanik ere (barnekoa zein kanpokoa).

Zehazki, honako hauek dira ezarritako arauak:

- Segurtasun-arduradunari fitxategien komunikazioari buruzko araudia.
- Erabiltzaileen administrazioari buruzko araudia.
- Maila handiko fitxategien sarrera-erregistroari buruzko araudia.
- Datu pertsonalak dituzten euskarriak eta/edo dokumentuak sartzea eta irtetea baimentzeari buruzko araudia.
- Datu pertsonalak dituzten eskarien eta dokumentuen erregistroari buruzko araudia.
- Euskarriak eta/edo dokumentuak identifikatzeari eta inbentariatzeari buruzko araudia.
- Datu pertsonalak dituzten euskarriak eta/edo dokumentuak berrerabiltzeari eta suntsitzeari buruzko araudia.
- Aldi baterako fitxategien tratamenduari buruzko araudia.
- Segurtasun-dokumentuan xedatutakoa egiaztatzeko kontrolari buruzko araudia.
- Aldian behin ikuskapenak egiteari buruzko araudia.
- Probetan benetako datu pertsonalak erabiltzeari buruzko araudia.
- IZENPEren lokaletara eta dependentzietara eta datu pertsonaletara fisikoki sartzeko kontrolari buruzko araudia.
- Datu pertsonalak dituzten fitxategiak sortzeari, aldatzeari eta ezabatzeari buruzko araudia.
- Fitxategiak garatzeko eta ezartzeko segurtasun-neurriei buruzko araudia.
- Babes-kopiak egiteari buruzko araudia.
- Datu pertsonalak babesteari buruzko araudia.
- Automatizatu gabeko euskarriak eta/edo dokumentuak kudeatzeari eta zaintzeari buruzko araudia.
- Automatizatu gabeko fitxategiak artxibatzeari buruzko araudia.
- Automatizatu gabeko fitxategietan biltegiratzeko gailuei buruzko araudia.
- Automatizatu gabeko fitxategietako dokumentuak kopiatzeari eta erreproduzitzeari buruzko araudia.
- Automatizatu gabeko dokumentazioa eskuratzeari buruzko araudia.
- Komunikazioetako segurtasun-neurriei buruzko araudia.

Prozedurak

Bestalde, IZENPEk datu pertsonalen babesa bermatzeko beharrezko prozedurak ditu.

Prozedura horiek IZENPEren zerbitzu, dependentzia eta informazio-sistema guztiei aplika dakizkieke; edozein formatutan (paperean, informatikoan, bideoan, ...) biltzen diren datu pertsonal guztiei aplikatzen zaie, elementu horiek erabiltzen dituen pertsona edozein izanik ere (barnekoa zein kanpokoa).

Zehazki, honako hauek dira ezarritako prozedurak:

- Erabiltzaileak administratzeko prozedura.
- Gertakariak jakinarazteko eta kudeatzeko prozedura
- Babeskopiak egiteko prozedura.
- Datuak berreskuratzeko prozedura.
- Datu pertsonaletara sartzeko eskubideaz baliatzeko prozedura.
- Datu pertsonalak zuzentzeko eta ezabatzeko eskubideaz baliatzeko prozedura.

- Datu pertsonaletarako oposizio-eskubideaz baliatzeko prozedura.

9.5 Jabetza intelektualeko eskubideak

9.5.1 Ziurtagirien jabetza

IZENPE da jaulkitzen dituen ziurtagirien gaineko jabetza intelektualeko eskubideak dituen erakunde bakarra.

Ez dira eskubide horietan sartzen ziurtapen digitaleko sistemaren aplikaziotik eratorritako eta hirugarren baten jabetzapeko jabetza intelektualeko eskubideak.

Arau berberak aplikatu behar zaizkio ziurtagiriak ezeztatzeko informazio-sistemari.

9.5.2 Ziurtapen Praktikaren jabetza

IZENPE da honako Ziurtapen Praktiken Deklarazio honen jabea.

9.5.3 Izenen gaineko informazioaren jabetza

Harpidedunak eta, hala badagokio, gakoen edukitzaileak, gorde egiten ditu ziurtagiriko markaren, produktuaren edo deitura komertzialaren gaineko eskubide guztiak (baldin eta eskubiderik badauka).

Harpideduna eta, hala badagokio, gakoen edukitzailea da ziurtagiriaren izen bereizgarriaren jabea. Ziurtapen Praktiken Deklarazioko 3. atalean zehaztutako informazioek osatzen dute aipatutako izena.

9.5.4 Gakoen eta horiei dagokien materialaren jabetza

Ziurtagirien harpidedunak dira gako-pareen jabeak.

9.6 Betebeharrak eta bermeak

IZENPEk, ziurtagiriak ziurtapen-praktiken deklarazio honen arabera jaulkitzen dituen ziurtapen-entitatea den aldetik, bere gain hartzen ditu betebehar hauek.

9.6.1 Zerbitzua egiteko betebeharrak

Izenpe, SAk Ziurtapen Praktiken Deklarazio honen arabera ematen ditu ziurtapen-zerbitzuak, horrek zehazten baititu bere zereginak, jarduteko prozedurak eta segurtasun-neurriak. Bereziki, dagozkion betebehar guztiak betetzeko ardura bere gain hartzen du, erregistro-entitateak praktika hauetan berariaz egiten dituenak izan ezik, baldin eta erregistro-entitate gisa jarduten ez badu. Ziurtapen-entitatearen betebeharrak honako hauek dira:

- Zerbitzuak egin zaizkion pertsonaren sinadura sortzeko datuak ez kopiatzea.
- Egindako ziurtagiriak adieraziko dituen eta ziurtagiri horiek indarrean dauden edo indarraldia eten edo iraungi den adieraziko duen sistema mantentzea.
- Ziurtagiri kualifikatuei eta unean une indarrean dauden ziurtapen-praktiketako deklarazioei buruzko informazio eta dokumentazio guztia edozein baliabide seguru

bidez erregistratzea, gutxienez 15 urtez egiten diren unetik bertatik kontatzen hasita. Hortaz, egiten diren sinadurak eta gainerako ziurtagiriei dagozkienak 7 urtez egiaztatu ahal izango dira.

- Sinatzaileak sinadura sortzeko datuak dituela ziurtatzea –ziurtagirian jasoarazten diren egiaztatzeari dagozkion datuak–.
- Sinadura sortzeko eta egiaztatzeko datuen osagarritasuna bermatzea, betiere biak ziurtapen-zerbitzuen egileak sortu baditu.
- 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, CABForum eta IZENPEren segurtasun-politika) bete ditzaten eskatzea.

9.6.2 Jardun fidagarriko betebeharrak

IZENPEk honako hau bermatzen du:

- Ziurtagirian agertzen den identitatea ziurtagirian agertzen den gako publikoari dagokiola, era unibokoan.
- Zerbitzua bizkor eta modu seguruan eskaintzea. Bereziki, ziurtagirien baliozkotasuna kontsultatzeko zerbitzu bizkorra eta segurua erabiltzeko aukera ematen du, eta ziurtagirien eraginkortasuna modu seguruan eta berehala iraungi edo bertan behera utziko bada, horren berri emango duela bermatzen du, Ziurtapen Praktiken Deklarazio honek aurreikusten duenarekin bat etorriz. Zerbitzua eguneko 24 orduetan erabili daiteke, asteko 7 egunetan.
- Sinadura elektronikoen arloan indarrean dagoen legeriak finkatzen dituen eskakizun teknikoak eta langileei buruzkoak betetzea:

    1. Ziurtatze-zerbitzuak egiteko beharrezko fidagarritasuna frogatzea.

    2. Ziurtagiri bat jaulki edo bere indarraldia amaitu den eguna eta ordua zehaztasunez adierazi ahal izan dadin bermatzea.

    3. Eskaintzen diren ziurtatze-zerbitzuak egiteko behar adinako kualifikazioa, ezagutzak eta esperientzia duten langileak erabiltzea, baita sinadura elektronikoaren esparruko segurtasuneko eta kudeaketako prozedura egokiak ere.

    4. Erabiltzen diren sistemak eta produktuak fidagarriak izatea, aldaketa ororen aurka babestuta daudenak eta jasaten dituzten ziurtatze-prozesuen segurtasun teknikoa eta –hala badagokio– kriptografikoa bermatzen dutenak, betiere Segurtasun Politikari jarraituz.

    5. Ziurtagirien faltsifikazioaren aurkako neurriak hartzea eta konfidentzialtasuna bermatzea sinadura (gako pribatua) sortzeko datuen eratze-prozesuan, 6. atalak dioenaren arabera. Gainera, sinatzaileari prozedura seguru baten bidez ematea.

    6. Sistema fidagarriak erabiltzea ziurtagiri kualifikatuak biltegiratzeko. Sistema horiek ziurtagiriak kautotzeko aukera eman behar dute, eta baimendurik gabeko pertsonek datuak aldatu ahal izatea saihestu beharko dute. Sinatzaileak aditzera eman dituen pertsonak eta kasu jakin batzuetan, soilik, sartu ahal izango dira datu horietara, eta hala bermatu behar du sistema

horrek. Gainera, segurtasun-baldintzetan eragina izan dezakeen edozein aldaketa antzeman beharko dute sistema horiek.

- Segurtasunaren kudeaketa egokia, Informazioaren Segurtasuna Kudeatzeko Sistema ezartzeari esker, betiere ISO/IEC 27001 arauak ezarritako printzipioen arabera. Honako neurri hauek, besteak beste, hartu dira aintzat:
    1. Segurtasuna aldian behin egiaztatzea, ezarritako estandarrekiko adostasuna ziurtatzearren.
    2. Segurtasun-gertakarien kudeaketa osoa gauzatzea, gertakari horiek hauteman, ebatzi eta optimizatu direla bermatzearren.
    3. Segurtasunaren arloan interes berezia duten taldeekin harreman egokiak izatea, hala nola adituekin, segurtasun-foroekin, eta informazioaren segurtasunaren arloko elkargo profesionalekin.
    4. Sistemen mantentze-lana eta bilakaera behar bezala planifikatzea, erabiltzaileen eta bezeroen iguripenak berme osoz beteko dituen zerbitzua eta etekin egokia ziurtatzearren.

9.6.3 Identifikazio-betebeharrak

Ziurtagiri kualifikatuen kasuan, IZENPEk ziurtagiriaren harpideduna identifikatzen du, betiere Batzordearen 2015eko irailaren 8ko 2015/1502 Gauzatze Araudian (EB) eta Ziurtapen Praktiken Deklarazio honetan definitutako ziurtatze-mailen arabera.

9.6.4 Erabiltzaileei eman beharreko informazioa: betebeharrak

- Harpidedunari ziurtagiria jaulki eta eman aurretik, honen berri jakinarazten dio hari IZENPEk: ziurtagiria erabiltzeko bete behar diren baldintzen, prezioaren –finkatuta badago–, erabilera-mugen eta Ziurtapen Praktiken Deklarazio honen 2.1.1.6. atalean dauden tresna juridiko lotesleen berri.

  “Ziurtagiria erabiltzeko baldintzak” izeneko testuaren bidez egiten da hori. Posta elektronikoz nahiz komunikabide iraunkorren baten bidez transmititu behar da testua, ongi ulertzeko moduan idatzita betiere.

- IZENPEk gakoen edukitzaileari haren ziurtagiriaren indarraldia iraungitzearen berri eman beharko dio, ziurtagiri elektronikoaren indarraldia amaitu edo eten aurretik edo aldi berean, eta ziurtagiria indarrik gabe geratzearen arrazoiak zehaztuko dizkio, baita data eta ordua ere.
- Bi hilabete lehenago jakinaraziko die IZENPEk sinatzaileei ziurtapen-zerbitzuak egiteari utzi egingo diola, eta, hala badagokio, ziurtagirien kudeaketa eskualdatzen zaion emailearen ezaugarrien berri emango die. Dokumentu honek aurreikusitakoaren arabera egin behar dira sinatzaileekiko komunikazioak.
- IZENPEk badu jarduera eteteko amaiera-plan bat eta, bertan, etete hori zein baldintzatan egingo litzatekeen zehazten da.
- Ziurtagiriei buruzko informazio publiko guztia IZENPEren Argitalpen Zerbitzuan jaso da, Ziurtapen Praktiken Deklarazio honen 2.6. atalean.

9.6.5 Egiaztapen-programak: betebeharrak

IZENPEk edonork erabiltzeko ziurtagirien baliozkotasuna egiaztatzeko bitarteko publikoak eskaintzen ditu Ziurtapen Praktiken Deklarazio honetan deskribatzen diren sistemen bidez.

9.6.6 Ziurtapen-zerbitzuaren arautze juridikoa: betebeharrak

IZENPEk bere gain hartzen ditu ziurtagirian ageri diren betebehar guztiak, baita beste batzuen erreferentzia gisara hartutakoak ere. Erreferentzia bidez jasotzeko, objektu-identifikatzailea edo dokumentuari lotzeko beste bideren bat erantsi behar zaio ziurtagiriari.

Idatzizko hizkuntza ulergarria da IZENPE eta eskatzailea, harpideduna edo gakoen edukitzailea lotesten dituen tresna juridikoa, baita ziurtagirian konfiantza duen hirugarrena ere. Honako eduki hauek izan behar ditu, gutxienik, aipatu tresnak:

- Ziurtapen Praktiken Deklarazio honetako 2.1.4., 2.1.5., 2.1.6., 2.2., 2.3. eta 2.4. atalek diotena betetzeko aginduak.
- Zein Ziurtapen Praktiken Deklarazio den aplikagarri adierazi behar du, eta, hala badagokio, zehaztu egin behar du ziurtagiriak salgai daudela eta sinadura sortzeko nahiz mezuak deszifratzeko gailu segurua erabili behar dela.
- Gako pribatuak jaulki, ezeztatu eta, hala badagokio, berreskuratzeko bete beharreko klausulak.
- Ziurtagirian dagoen informazioa zuzena dela adierazi behar du, harpidedunak kontrakoa jakinarazten ez badu behintzat.
- Sinadura sortzeko gailu segurua hornitzeko erabilitako informazioa biltegiratzeko baimena, betiere harpideduna erregistratzeko, gailu kriptografikoa hornitzeko eta informazio hori beste batzuei uzteko, baldin eta IZENPEren eragiketak ziurtagiri baliozkoak ezeztatu gabe amaitzen badira.
- Ziurtagiria erabiltzeko mugak, 1.3.2. atalekoak barne.
- Ziurtagiriak nola balidatu jakiteko informazioa, ziurtagiriaren egoera egiaztatzea barne dela, baita ziurtagirian dezenteko konfiantza izateko baldintzei buruzkoa ere.
- Aplikagarri diren erantzukizun-mugak, barne direla IZENPEk bere erantzukizuna onartzen edo baztertzen duen erabilerak.
- Ziurtagiri-eskaerei buruzko informazioa zenbat denboraz eduki behar den artxibatuta.
- Ikuskaritza-erregistroak zenbat denboraz eduki behar diren artxibatuta.
- Auziak konpontzeko aplikagarri diren prozedurak.
- Aplikagarri den legea eta eskumena duen jurisdikzioa.
- IZENPE entitate publikoren baten edo batzuen ziurtapen-politikekiko bateragarri aitortu duten, eta, hala badagokio, zein sistemaren arabera.
- IZENPEren ondare-erantzukizuna bermatzeko era.

9.6.7 Erregistro-entitatearen betebeharrak

Honako betebehar hauek hartzen ditu bere gain erregistro-entitateak:

- Eskatzailearen, harpidedunaren eta gakoen edukitzailearen nortasuna eta beste zenbait datu pertsonal egiaztatzea –ziurtagirien xedeetarako garrantzizkoak direnak edo ziurtagirietan daudenak–, prozedura hauen arabera.
- Kudeatzen dituen ziurtagirien jaulkipenari, berritzeari, ezeztatzeari edo berraktibatzeari buruzko dokumentazio eta informazio guztia gordetzea.
- IZENPEri garaiz jakinaraztea ziurtagiriak azkar eta modu fidagarrian ezeztatzeko eskaeren berri.
- IZENPEri artxiboak erabiltzen uztea, baita jardueretarako erabiltzen diren prozeduren eta horretarako behar den informazioaren mantentze-lanen ikuskapena egiten ere.
- IZENPEri jakinaraztea ziurtagiriak jaulki, berritu edo berraktibatzeko eskaeren berri, baita hark jaulkitzen dituen ziurtagiriei buruzko beste zeinahi alderdiren berri ere.
- Garaiz begiratzea ziurtagirien iraunaldian eragina izan dezaketen ezeztatzeko zergatiak.
- Ziurtagiriak jaulki, berritu, ezeztatu eta berraktibatzeko IZENPEk ezarritako prozedurak eta gai horretaz indarrean dagoen legeriak agindutakoa betetzea.
- Segurtasuneko araudia eta estandarrak betetzea (datu pertsonalak babesteari buruzko Lege Organikoa, ISO, ETSI eta IZENPEren segurtasun-politika).

Hala dagokionean, bere gain hartu ahal du eginkizun hau ere: gakoen edukitzailearen esku jartzea sinadura (gako pribatua) sortzeko eta sinadura elektronikoa (gako publikoa) egiaztatzeko prozedura teknikoak.

9.6.8 Ziurtagiri-eskatzailearen betebeharrak

Honako betebehar hauek ditu ziurtagiri-eskatzaileak:

- Ziurtagiri-eskaerak egiteko eman duen informazioaren egiazkotasuna, osotasuna eta gaurkotasuna bermatzea, baita haietan jarri beharreko informazioarena ere.
- Berariazko dokumentazioan finkatutako eskaera-prozedura betetzea.

9.6.9 Ziurtagiri-harpidedunaren betebeharrak

- Informazio osoa eta egokia ematea IZENPEri, Ziurtapen Praktiken Deklarazioko eskakizunen arabera, erregistro-prozedurari dagokionez batez ere.
- Ziurtagirietan jarri beharreko informazioaren egiazkotasuna, osotasuna eta gaurkotasuna bermatzea.
- Ziurtagiriak erabiltzeko baldintzak jakitea eta onartzea, baita haiei egiten zaizkien aldaketak ere.
- Ziurtagiriren bat jaulki eta eman aurretik, horretarako onarpena ematea.

- Ziurtagirien euskarriak ongi erabili eta gordeko direla bermatzea.
- Ziurtagiria egokiro erabiltzea, eta, zehazki, ziurtagirien erabilera-mugak aintzat hartzea.
- Arretaz zaintzea gako pribatua, baimendu gabeko erabilerak saihestearren, Ziurtapen Praktiken Deklarazioko 6.1, 6.2 eta 6.4 sailek agintzen dutenaren arabera.
- IZENPEri eta harpidedunaren ustez ziurtagirian konfiantza duen edonori honako hau jakinaraztea, justifikatzerik ez dagoen atzerapenik gabe:
    1. Gako pribatua galdu, norbaitek ostu edo arriskuan jarri izana.
    2. Gako pribatuaren kontrola galdu izana, aktibatze-datuak (gailu kriptografikoaren PIN kodea, adibidez) arriskuan jartzeagatik edo beste edozein arrazoirengatik.
    3. Ziurtagiriaren edukian dauden okerrak edo izandako aldaketak (harpidedunak dakizkienak edo jakin litzakeenak). Aldaketak ziurtagiria ezeztatzea badakar, horretarako eskaera egin behar du harpidedunak.

Gako pribatua erabiltzeari uztea ziurtagiriaren balio-epea amaitu ondoren.

Gakoen edukitzaileei jakinaraztea zein betebehar dagozkien.

Ziurtagiri-zerbitzuen ezartze teknikoa ez kontrolatzea, manipulatzea edo atzeranzko ingeniaritzako ekintzarik ez egitea, aurrez Ziurtapen Entitatearen idatzizko baimenik eduki gabe.

Ziurtagiri-zerbitzuen segurtasuna arriskuan nahita ez jartzea.

Ziurtagirietako gako publikoei dagozkien gako pribatuak ez erabiltzea inongo ziurtagiri izenpetzeko, ziurtapen-entitatea balitz bezala.

Ziurtagiriari dagokion gako pribatua erabiliz sinadura digitalak sortzen dituen ziurtagiri kualifikatuen harpidedunak aitortu egin behar du, dagokion bitarteko juridikoaz, sinadura elektroniko horiek eskuz idatzitako sinaduren baliokide direla, gailu kriptografikoa erabiltzen denean, betiere eIDAS arauan agintzen duenaren arabera.

9.6.10 Ziurtagirien erabiltzaile egiaztatzailearen betebeharrak

Ziurtagirien erabiltzaile egiaztatzaileak honako betebehar hauek ditu:

- Eman nahi zaion erabilerarako ziurtagiria egokia den ala ez jakiteko, informazioa iturri independenteetatik jasotzea.
- Ziurtagiriak erabiltzeko baldintzak zein diren jakitea, Ziurtapen Praktiken Deklarazioak eta egiaztatzailearen eta IZENPEren arteko ziurtapen-zerbitzuak egiteko kontratuak aurreikusten dutenaren arabera.
- Emandako ziurtagirien baliozkotasuna edo ezeztapena egiaztatzea. Horretarako, ziurtagirien egoerari buruzko informazioa erabiliko da.
- Ziurtagirien hierarkiako ziurtagiri guztiak egiaztatzea, sinadura digitalean edo hierarkiako ziurtagiriren batean konfiantza jarri baino lehen.

- Kontuan izatea ziurtagiria erabiltzeko dauden mugak, nonahi daudelarik ere: ziurtagirian bertan nahiz egiaztatzailearen kontratuan.
- Kontuan izatea kontratuan edo beste nonbait finkatutako badaezpadako neurri guztiak, edozein delarik ere haren izaera juridikoa.
- Jakinaraztea ziurtagiriari buruzko gertaera edo egoera irregular guztiak, ziurtagiria ezeztatzeko arrazoia izan daitekeenak.
- Ziurtagiri-zerbitzuen ezartze teknikoa ez kontrolatzea, manipulatzea edo atzeranzko ingeniaritzako ekintzarik ez egitea, aurrez IZENPEren idatzizko baimenik gabe.
- Ziurtagiri-zerbitzuen segurtasuna arriskuan nahita ez jartzea.

Ziurtagiri kualifikatuen erabiltzailea behartuta dago aitortzera –dagokion tresna juridikoan– sinadura elektroniko horiek eskuz idatzitako sinaduren baliokideak direla, eIDAS arauaren arabera.

9.6.11 Argitalpen Zerbitzuaren betebeharrak

Ez da aplikagarria, Argitalpen Zerbitzua ez baita entitate independentea.

9.7 Erantzukizunak

9.7.1 Ziurtapen-agintaritzaren erantzukizunak

IZENPEk arduragabekeriarengatik edo behar adinako ardurarik izan ez delako erantzungo du, Ziurtapen Praktiken Deklarazio honetan deskribatutako zerbitzuetan, baita sinadura elektronikoari buruzko legerian ezartzen diren betebeharrak betetzen ez direnean. Honako kasu hauetan izan ezik:

- IZENPE ez da ziurtagirietako informazioek eragindako kalteen erantzule izango, betiere, haien edukiak Ziurtapen Praktiken Deklarazioa betetzen badu.
- IZENPE ez da ziurtagirien eraginkortasuna agortzearen erantzule izango, betiere, Ziurtapen Praktiken Deklarazioan aurreikusitako argitalpen-betebeharrak betetzen baditu.
- IZENPE ez da sor daitezkeen kalte zuzen edo zeharkako, berezi, intzidentziazko eta emergenteen erantzule izango, ezta eskuratu gabeko irabazien, datu-galeren eta zigor-kalteen erantzule ere –aurreikusteko modukoak izan edo ez–, baldin eta horiek ziurtagirien, sinadura digitalen edo Ziurtapen Praktiken Deklarazioan eskaintzen edo aurreikusten den bestelako edozein transakzio edo zerbitzuren erabilera, entrega, baimen, funtzionamendu edo funtzionamendu ezarekin lotuta badaude eta behar ez bezalako erabilerak eragin baditu.
- IZENPE ez da ziurtagirian ageri diren datuen zehaztapen-ezagatik harpidedunari edo fede oneko hirugarren pertsonei eragindako kalte eta galeren erantzule izango, baldin eta datu horiek dokumentu publiko baten bidez (notaritzakoa, judiziala edo administratiboa) ziurtatu badira, Erregistro Entitateak eman duen dokumentu bidez denean izan ezik.

- IZENPE ez da ziurtagiriez fidatzen diren harpidedunek edo hirugarren pertsonek dituzten betebeharrak ez betetzeagatik harpidedunari edo fede oneko hirugarren pertsonei eragindako kalteen erantzule izango.

IZENPE erantzule izango da, dena den, ziurtagirien indarraldiari buruzko edota ziurtagirien indarraldia iraungitzeari buruzko kontsulta-zerbitzuan ez sartzeak edo berandu sartzeak kalterik edo hondamenik eragiten badio inori bere lanean, betiere Sinadura Elektronikoari buruzko Legearen 22. artikuluak agintzen duenez.

Era berean, ziurtapen-zerbitzuak egiteko beharrezko funtzioak hirugarren batzuen esku uzten dituenean, bere gain hartuko du pertsona horien jardunaren ondorioz hirugarren pertsonen aurrean sor daitekeen edozein erantzukizun. Ildo horretan, 3.500.000 euroko zenbatekoa duen erantzukizun zibileko asegurua eratu da, ziurtagirien erabilerak eragin ditzakeen kalteen eta galeren erantzukizun-arriskuari aurre egiteko.

9.7.2 Erregistro-agintaritzaren erantzukizunak

IZENPE ez den eta erregistro-entitate gisara aritzen den erakunde oro bere gain hartutako eginkizunek eragiten dituzten kalteen erantzule izango da IZENPEren aurrean, dagokion lege-tresnak finkatzen duenaren arabera.

Identifikazio-funtzioak ziurtagirien harpidedun diren Administrazio Publikoek egiten dituztenean, Administrazio Publikoen ondare-erantzukizuna izango da aplikagarria, Administrazio Publikoen Erregimen Juridikoko Legeak eta Administrazio Prozedura Erkideak agintzen dutenez.

9.7.3 Harpidedunen betebeharrak

Bere gako pribatuarekin sortutako sinadura digital baten bidez kautotutako komunikazio elektroniko guztien erantzule izango da harpideduna, baldin eta IZENPEren egiaztapen-zerbitzuek ziurtagiria baliozkoa dela egiaztatzen badute.

Ziurtagiria galdu egin dela edo lapurtu egin dutela jakinarazten ez den bitartean –Ziurtapen Praktiken Deklarazio honetan agintzen duen legez–, harpidedunari dagokio ziurtagiriak baimenik gabe eta/edo era desegokian erabiltzearen erantzukizuna.

Ziurtagiriak onartzearekin batera, erantzukizun hau hartzen du bere gain harpidedunak: kalte guztietatik salbu uztekoa eta, hala badagokio, kalte-ordainak ordaintzekoa IZENPEri, erregistro-entitateei, eta entitate erabiltzaileei kalteak, galerak, zorrak, gastu prozesalak edo zeinahi bestelakoak eragiten dituzten ekintzengatik edo ez-egiteengatik, barne direla IZENPEri, erregistro-entitateei, edo entitate erabiltzaileei ziurtagiriak erabiltzeagatik edo argitaratzeagatik dagozkien ordainsariak. Honako arrazoi hauek eragin dezakete aipatu erantzukizuna:

- Ziurtapen-entitatearekin lotzen duen tresna juridikoaren aginduak ez betetzeak.
- Baimendu gabeko jendearekiko komunikazio elektronikoetan ziurtagiri digitalak erabiltzeak.
- Harpidedunak datuak faltsutzeak edo akats faktikoak egiteak.
- Zabarkeriagatik edo IZENPE entitate publiko erabiltzaileak edo harpidedunaren ziurtagirian konfiantza eduki dezaketen hirugarrenak engainatzeko asmoz ziurtagirietan funtsezko datuak ez jartzeak.

- Gako pribatuak gordetzeko eta horiek ez galtzeko, inork ez jakiteko, ez aldatzeko edo baimenik gabe ez erabiltzeko agindua ez betetzeak.

IZENPE ez da ziurtagiriez fidatzen diren harpidedunei edo fede oneko hirugarren pertsonei harpidedunari dagozkion honako betekizun hauek ez betetzeak eragindako kalteen erantzule izango:

- IZENPEri edo erregistro-entitateari informazio egiazkoa, osoa eta zehatza ematea ziurtagirian jarri beharreko edo hura jaulki edo ezeztatzeko behar diren datuei buruz, baldin eta zerbitzu-egileak ezin izan badu datuen zehaztasun-eza antzeman.
- Ahalik eta azkarren jakinaraztea IZENPEri edo erregistro-entitateari ziurtagirian dauden zirkunstantzien aldaketa ororen berri.
- Arretaz gordetzea sinadura sortzeko datuak, horien konfidentzialtasuna bermatzeko eta horietara inor ez sartzeko edo inork ez datuak ezagutarazteko.
- Ziurtagiria ezeztatzeko eskatzea zalantzarik egonez gero sinadura sortzeko datuen konfidentzialtasunaz.
- Sinadura sortzeko datuak ez erabiltzea ziurtagiriaren balio-epea agortu edo zerbitzu-egileak baliogabetzearen berri eman ondoren.
- Ziurtagirian jasotzen diren erabilpen-mugak aintzat hartzea, eta ziurtapen-zerbitzuen sinatzaileari jakinarazitako eta finkatutako baldintzen arabera erabiltzea.

9.7.4 Ziurtagirietan konfiantza duten hirugarrenen erantzukizunak

Ziurtagiri baliogabeaz edo egiaztatu gabeko sinadura digitalaz fidatzen den hirugarrenak bere gain hartzen ditu horri loturiko arrisku guztiak eta ez dauka inongo erantzukizunik eskatzerik IZENPEri, erregistro-entitateei, entitate erabiltzaileei edo harpidedunei ziurtagiri eta sinadura horietaz fidatzeak eragindako gorabeherengatik.

IZENPEk ez du erantzukizunik izango harpidedunari edo fede oneko hirugarrenei eragindako kalteengatik, baldin eta sinatutako dokumentuen hartzaileak ez badu betetzen honako arreta-betekizun hauetakoren bat:

- Egiaztatzea eta kontuan hartzea ziurtagiria erabiltzeko eta harekin egin daitezkeen transakzioen banakako zenbatekoari buruzko murriztapenak.
- Ziurtagiriaren baliozkotasuna egiaztatzea.

9.8 Kalte-ordainak

IZENPEk kalte-gabetasun klausulak ezartzen ditu harpidedunarekin edo egiaztatzailearekin lotzen duten tresna juridikoetan, haiek beren betebeharrak edo aplikagarri den legeria urratzen dituzten kasuetarako.

9.9 Baliozkotze-aldia

9.9.1 Epea

ZPD argitaratzen den unean sartzen da indarrean.

9.9.2 Amaiera

Gaur egungo ZPDa dokumentuaren beste bertsio bat argitaratzen den unean indargabetuko da.

Bertsio berriak oso-osorik ordeztuko du aurreko dokumentua.

9.9.3 Amaieraren ondorioak

Aurreko ZPD baten mende jaulki diren eta indarrean dauden ziurtagirietarako, bertsio berria nagusituko zaio aurreko bertsioari, honen aurkakoa ez den guztian.

9.10 Banako jakinarazpenak eta komunikazioa parte-hartzaileekin

IZENPEk, harpidedunarekiko tresna juridiko loteslean, jakinarazpenetarako bitartekoak eta epeak ezarriko ditu.

Oro har, IZENPEren web-orria, www.izenpe.com, erabiliko da edozein jakinarazpen eta komunikazio egiteko.

9.11 Zuzenketak

9.11.1 Aldaketetarako prozedura

Dokumentu honetan egiten diren aldaketak IZENPEren Administrazio Kontseiluak onartuko ditu. Aldaketa horiek Ziurtapen Praktiken Deklarazioaren dokumentuan jasoko dira. IZENPEk bermatzen ditu dokumentu horren mantentze-lanak.

Ziurtapen Praktiken Deklarazioaren bertsio eguneratuak eta egindako aldaketak gordailuan kontsulta daitezke, helbide honetan: www.izenpe.com.

IZENPE Ziurtapen Praktiken Deklarazioa alda dezake, berak bakarrik, baldin eta prozedura honi jarraitzen badio:

- Aldaketa teknikoki, legalki eta komertzialki justifikatuko da eta IZENPEren zuzendaritzak abala eman beharko du.
- Zehaztapenen bertsio berriaren alde tekniko eta legal guztiak hartuko dira kontuan.
- Aldaketa-kontrola ezarriko da, ondoriozko zehaztapenek bete nahi ziren baldintzak eta aldaketa eragin zutenak betetzen dituztela bermatzeko.
- Zehaztapenak aldatzeak erabiltzailearengan dituen eraginak ezarriko dira, eta aldaketa horiek hari jakinarazteko beharra aztertuko da.

9.11.2 Jakinarazteko aldia eta mekanismoa

IZENPEren Segurtasun Batzordeak urtero berraztertuko du ZPDa, eta bertan aldaketa bat egin behar den guztietan. Berrazterketa hori batera egingo dute dokumentua lantzeaz eta mantentzeaz arduratzen diren eta zeregin horretan parte hartzen duten arloek.

IZENPEk aldaketak egin ahal izango ditu dokumentu horretan, aurrez erabiltzaileei horien berri eman beharrik gabe, esate baterako:

- Akats tipografikoak zuzentzea dokumentuan
- Harremanetako informazioa aldatzea.

Beste aldaketa batzuk berriz erabiltzaileei jakinarazi beharko zaizkie, esate baterako:

- Aldaketak zehaztapenetan edo zerbitzu-baldintzetan.
- URLak aldatzea

9.11.3 OIDa zer zirkunstantziatan aldatu behar den

Dokumentu honetan deskribatutako prozeduretakoren bat aldatzen den zirkunstantzietan aldatu beharko da OIDa.

9.12 Erreklamazioak eta auzien ebazpena

IZENPEk kontsumoko artekaritza-sistemaren kontrolpean dihardu, aplikagarri zaion legeriak aurreikusten duenaren arabera. Hala, eskatzaileen edo harpidedunen kexuak edo erreklamazioak artatu eta ebatziko ditu, eta hartzen duen erabakia loteslea eta betearazlea izango da alde bientzat, herritarren ziurtagiriei dagokienez betiere.

Xede horretarako, eskatzaileak edo harpidedunak sistema hori onartzen duela joko da dagokion Kontsumoko Artekaritza Batzordean artekaritza-eskaera formalizatzen duen une beretik.

Kontsumoko artekaritza-sistematik at dauden herritarraren ziurtagirien esparruan eskatzaileengandik edo harpidedunengandik sor daitekeen beste edozein auzi dagokion jurisdikzioaren esku geratuko da.

9.13 Aplikatzeko den araudia

Ziurtapen Praktiken Deklarazio hau gauzatzeari, egiteari, interpretatzeari eta baliozkotasunari dagozkien alor guztietan aplikatu behar da sinadura elektronikoari buruzko Espainiako legeria.

Honako hau da dokumentu honi eta ondoriozko eragiketei aplika dakiekeen araudia:

- Sinadura elektronikoari buruzko abenduaren 19ko 59/2003 Legea.
- Administrazio Publikoen Administrazio Prozedura Erkideari buruzko 39/2015 Legea.
- Sektore Publikoaren Erregimen Juridikoari buruzko 40/2015 Legea.
- Datuak babesteari buruzko 15/1999 Lege Organikoa.
- Identifikazio elektronikoari eta barne-merkatuko transakzio elektronikoetarako konfiantzako zerbitzuei buruzko 910/2104 Europako araudia (eIDAS).

9.14 Aplikatzekoa den araudia betetzea

Jurisdikzio eskuduna une bakoitzean legeria prozesal espainiarrak agintzen duena izango da.

Edonola ere, IZENPEk jakinarazi du 10.13. atalean adierazten diren araudiak betetzen dituela.

9.15 Askotariko estipulazioak

Berez da baliozkoa Ziurtapen Praktiken Deklarazio honetako klausula bakoitza eta ez ditu gainerakoak baliogabetzen. Baliorik gabeko edo osatu gabeko klausula baliokidea den beste batekin ordeztuko da.

IZENPEren eskubideei eta betebeharrei zuzenean eragiten dien eta gainerako aldeei eragiten ez dien Ziurtapen Praktiken Deklarazio honetako agindu bakar bat ere ez da zuzendu, ukatu, gehitu, aldatu edo ezabatu behar, IZENPEren idatzizko eta kautotutako dokumentu bidez ez bada. Aldaketa hori ez da, inondik ere, berritze iraungitzailea, aldatzaile hutsa baizik, eta ez die eragiten gainerako aldeen bestelako eskubideei eta betebeharrei.

IZENPEri zuzentzen zaizkion komunikazio idatziak helbide honetara bidali beharko dira:

IZENPE, SA
Tomas Zumarraga Dohatsuaren kalea, 71-1.
01008 Vitoria-Gasteiz