

## Konfiantza Globaleko Praktiken Adierazpena

© IZENPE 2025

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

[www.izenpe.eus](http://www.izenpe.eus)  
[izenpe@izenpe.eus](mailto:izenpe@izenpe.eus)



### Bertsioen historia

7.0 bertsioa baino lehenagoko aldaketak [www.izenpe.eus](http://www.izenpe.eus) webguneko "Ziurtapen-praktiken adierazpenari buruzko eguneratzeak eta jakinarazpenak" atalean kontsulta daitezke.



Bertsioa	Data	Egindako aldaketen laburpena
7,0	2021/07/14	Aldaketen taula gehitu da eguneratzeen dokumentua ordezkatzeko DPCren 4.9.12 atala eguneratu da, gako pribatua arriskuan dagoela frogatzeko erabilgarri dauden metodoak zehazteko
7,1	2022/01/13	Epigrafe hauek eguneratu dira: 6.2.1. Modulu kriptografikoen estandarrak. 9.3.3. Informazio konfidentziala babesteko erantzukizuna: araudiaren eguneraketa. 9.16.6: Beste xedapen batzuk
7,2	2022/09/01	Epigrafe hauek eguneratu dira: 1.1.1. 2007ko oinarrizko CA hierarkia (CN=izenpe.com): txip kriptografikoan indarrean dauden OIDetan sinadura-motaren balioa Kualifikatutik Aurreratura eguneratu da.
7,3	2022/10/21	Epigrafe hauek eguneratu dira: 1.1.1. 2007ko oinarrizko CA hierarkia (CN=izenpe.com): txip kriptografikoan indarrean dauden OIDetan politika-identifikatzailearen balioa QCP-n-ra eguneratu da, eta SSL EV ziurtagirien politika QEVCP-wra eguneratu da.
7,4	2023/09/13	1.4.1. Akatsak zuzentzea 1.6.2. Akatsak zuzentzea 2.3. Idazketa eguneratzea 6.1.2. FIPS eguneratzea 6.1.3. Banaketa-metodoak eguneratzea 7.1. Ziurtagirien profila eguneratzea
7,5	2023/11/08	4.9.8 puntua eguneratzea: CRLak sortu eta argitaratu arte igarotako denbora 9.16.6 puntua eguneratzea: jarraibideen gidaren lehentasunari buruz
8,0	2025/06/19	Ziurtapen Praktiken Adierazpena (DPC) 910/2014 (EB) Erregelamenduaren aldaketara egokitzea.
8,1	2025/10/06	1.2.2.4: integrazioa: 2025eko hierarkia 1,4: Sinadura sortzeko gailu seguruetan ziurtagiri kualifikatuaren OIDak <b>6.1.5</b> Gakoen luzera eguneratzea



## Aurkibidea

### Edukia

<b>1</b>	<b>Sarrera</b>	<b>16</b>
1.1	Aurkezpena	16
1.2	Dokumentuaren izena eta identifikazioa	17
1.2.1	Identifikazioa	17
1.2.2	Ziurtagiri-identifikatzaileak	18
1.3	Gako publikoaren azpiegiturako (PKI) parte-hartzaileak.	22
1.3.1	Ziurtapen-agintaritzak.	22
1.3.2	Erregistro-erakundeak.	27
1.3.3	Ziurtagirien harpidedunak.	27
1.3.4	Konfiantzazko hirugarrenak.	27
1.3.5	Beste partaide batzuk	28
1.4	Ziurtagiriaren erabilerak.	28
1.4.1	Ziurtagiriaren erabilera egokiak	28
1.4.2	Ziurtagiriaren erabilera debekatuak	38
1.5	Politiken kudeaketa.	38
1.5.1	Dokumentazioaren kudeaketarako arduraduna den erakundea.	38
1.5.2	Harremanetarako datuak.	38
1.5.3	DPCGaren egokitzapenaren arduradunak	38
1.5.4	DPCGren onarpen-prozedura	39
1.6	Definizioak eta akronimoak.	39
1.6.1	Definizioak.	39
1.6.2	Akronimoak	42



<b>2</b>	<b>Informazio-biltegien argitalpena eta arduradunak.</b>	<b>45</b>
2.1	Informazio-biltegia	45
2.2	Ziurtapen-informazioaren argitalpena.	45
2.2.1	Argitalpen- eta jakinarazpen-politika	45
2.2.2	Ziurtapen Globaleko Praktiken Adierazpenean argitaratu gabeko elementuak.	45
2.3	Argitalpen-maiztasuna.	45
2.4	Biltegirako sarbide-kontrola.	46
<b>3</b>	<b>Identifikazioa eta autentifikazioa.</b>	<b>47</b>
3.1	Izenak.	47
3.1.1	Izen-motak	47
3.1.2	Izenen esanahia.	47
3.1.3	Ezizenak.	47
3.1.4	Izen-formatuak interpretatzeko arauak.	47
3.1.5	Izenen bakartasuna	47
3.1.6	Marka erregistratuen izenei eta tratamenduari buruzko gatazkak ebaztea.	47
3.1.7	Jaulkitzailea (Issuer).	48
3.1.8	Gaia (Subject).	48
3.2	Identitatearen balidazioa.	48
3.2.1	Gako pribatuaren jabetza egiaztatze metodoak.	48
3.2.2	Erakundearen identitatearen autentifikazioa	48
3.2.3	Pertsona fisiko eskatzailearen identitatearen autentifikazioa..	49
3.2.4	Sinatzailearen balioztatu gabeko informazioa	49
3.2.5	Autoritatearen balidazioa.	49
3.2.6	Interoperaziorako irizpideak.	49



3.3	Gakoak berriz ematea eskatzeko identifikazioa eta autentifikazioa.	49
3.3.1	Berritze arrunta.	49
3.3.2	Baliogabetze baten ondoko berritzea.	49
3.4	Baliogabetze-eskaeretarako identifikazioa eta autentifikazioa.	50
<b>4</b>	<b>Ziurtagirien bizi-zikloaren eskakizun operatiboak.</b>	<b>51</b>
4.1	Ziurtagiri-eskaera.	51
4.1.1	Eskaeraren egiaztapena.	51
4.1.2	Izena emateko prozesua eta erantzukizunak.	51
4.2	Eskaeren kudeaketa.	52
4.2.1	Identifikazio- eta autentifikazio-funtzioak betetzea.	52
4.2.2	Eskaerak prozesatzeko denbora.	52
4.3	Ziurtagiriaren jaulkipena.	52
4.3.1	CAren jarduerak jaulkipenean zehar	52
4.3.2	Ziurtagiriaren jaulkipena egingo da dagokion DPCP edo PDS dokumentuan jasotako baldintzen arabera.	52
4.3.3	Ziurtagiria egiaztatzea	52
4.4	Ziurtagiriaren onarpena	53
4.4.1	Ziurtagiriaren onarpen-prozesua	53
4.4.2	Ziurtagiria CAk argitaratzea.	53
4.4.3	CAk beste erakunde batzuei ziurtagiriaren jaulkipena jakinaraztea.	53
4.5	Gako-parea eta ziurtagiriaren erabilerak	53
4.5.1	Harpidedunaren gako pribatua eta ziurtagiriaren erabilera.	53
4.5.2	Gako publikoaren eta ziurtagiriaren erabilera – Hirugarrenen konfiantza	54
4.6	Ziurtagiriak berritzea	55
4.6.1	Ziurtagiria berritzeko inguruabarrak.	55



4.6.2	Nork eska dezake berritzea	55
4.6.3	Ziurtagiriaren berritze-eskaeren tratamendua.	55
4.6.4	Harpidedunari jakinaraztea.	56
4.6.5	Berritutako ziurtagiri baten onarpen-prozedura.	56
4.6.6	Ziurtagiria argitaratzea.	56
4.6.7	Beste erakunde batzuei jakinaraztea.	56
4.7	Ziurtagiriaren gakoak berritzea eta berreskuratzea.	56
4.7.1	Ziurtagiriaren gakoak berriz sortzeko inguruabarrak.	56
4.7.2	Nork eska dezake.	56
4.7.3	Gakoak berriro sortuz berritzeko eskaeren tratamendua.	56
4.7.4	Berritutako ziurtagiriaren onarpen-prozedura.	56
4.7.5	Ziurtagiria argitaratzea.	56
4.8	Ziurtagiria aldatzea	57
4.8.1	Ziurtagiriaren aldaketarako inguruabarrak.	57
4.8.2	Nork eska dezake ziurtagiriaren aldaketa	57
4.8.3	Ziurtagiriaren aldaketa-eskaeren tratamendua.	57
4.8.4	Ziurtagiriaren aldaketaren jakinarazpena.	57
4.8.5	Aldatutako ziurtagiriaren argitalpena.	57
4.8.6	Ziurtagiriaren aldaketa beste erakunde batzuei jakinaraztea.	57
4.9	Baliogabetua.	57
4.9.1	Baliogabetzeko egoerak	57
4.9.2	Nork eska dezake baliogabetzea	58
4.9.3	Baliogabetze-eskaeren tratamendua.	58
4.9.4	Baliogabetze-eskaeraren barkamen-epea.	59
4.9.5	CAk baliogabetzea prozesatzeko duen denbora-epea.	59



4.9.6	Konfiantzazko hirugarrenek baliogabetzeak egiaztatzeko betebeharra.	59
4.9.7	CRLen sorreraren maiztasuna.	59
4.9.8	CRLen sorkuntza eta argitalpenaren arteko denbora-tartea.	59
4.9.9	Online baliogabetze-berrespenaren eskakizunak.	60
4.9.10	Baliogabetze-ohartarazpenen bestelako bideak.	60
4.9.11	Gakoa arriskuan: eskakizun bereziak.	60
4.9.12	Ziurtagiria eteteko inguruabarrak	61
4.9.13	Nork eska dezake etetea	61
4.9.14	Etete-eskaera egiteko prozedura.	61
4.9.15	Etete-epearen mugak.	61
4.10	Ziurtagirien egoerari buruzko zerbitzuak.	61
4.10.1	Funtzionamendu-ezaugarriak	61
4.10.2	Zerbitzuaren eskuragarritasuna	61
4.10.3	Aukerako ezaugarriak.	61
4.11	Harpidetza amaitzea.	61
4.12	Gakoen zaintza eta berreskurapena	62
4.12.1	Gakoak zaintzeko eta berreskuratzeko jardunbideak eta politikak.	62
4.12.2	Saio-gakoa babesteko eta berreskuratzeko jardunbideak eta politikak.	62
<b>5</b>	<b>Segurtasun fisikoko kontrolak, prozedurazkoak eta langileekin lotutakoak.</b>	<b>63</b>
5.1	Segurtasun fisikoko kontrolak.	63
5.1.1	Instalazioen kokapena eta eraikuntza.	63
5.1.2	Sarbide fisikoa	63
5.1.3	Elektrizitatea eta aire girotua.	63
5.1.4	Ureztatze-arriskuaren aurkako babesa	64



5.1.5	Suteen prebentzioa eta babeseta.	64
5.1.6	Euskarrien biltegitratzea.	64
5.1.7	Hondakinen tratamendua.	64
5.1.8	Instalazioetatik kanpoko babeskopien biltegitratzea.	64
5.2	Prozeduren kontrolak.	64
5.2.1	Konfiantzazko rolak	64
5.2.2	Pertsona-kopurua zeregin bakoitzeko.	64
5.2.3	Rol bakoitzerako identifikazioa eta autentifikazioa	65
5.2.4	Rol desberdinetako zereginen bereizketa.	65
5.3	Langileen kontrolak.	65
5.3.1	Historiala, kualifikazioa, esperientzia eta autentifikazioari buruzko eskakizunak.	65
5.3.2	Historialaren ikerketa-prozedurak.	65
5.3.3	Prestakuntza-baldintzak	65
5.3.4	Prestakuntza-eguneratzeen eskakizunak eta maiztasuna.	65
5.3.5	Lanpostuen txandakatze-sekuentzia eta maiztasuna.	66
5.3.6	Baimendu gabeko jardueren aurkako zigorrak.	66
5.3.7	Langileen kontratazioaren eskakizunak.	66
5.3.8	Langileei dokumentazioa ematea.	66
5.4	Auditoria.	66
5.4.1	Erregistratzen diren gertaeren motak.	66
5.4.2	Logen prozesamendu-maiztasuna.	67
5.4.3	Audit logaren atxikipen-epea.	67
5.4.4	Audit logaren babeseta.	67
5.4.5	Audit logaren babeskopia egiteko prozedura.	67



5.4.6	Logen bilketa.	67
5.4.7	Zaurgarritasunen analisisia.	67
5.5	Erregistroak artxibatzea.	67
5.5.1	Artxibatutako erregistro-motak.	67
5.5.2	Artxiboaren atxikipen-epea.	68
5.5.3	Artxiboaren babesak	68
5.5.4	Artxiboaren babeskopia egiteko prozedurak.	68
5.5.5	Erregistroen denbora-zigilurako eskakizunak.	68
5.5.6	Artxibo-sistema.	68
5.5.7	Artxibo-informazioa eskuratzeko eta egiaztatze prozedurak.	68
5.6	CAren gakoak aldatzea.	68
5.7	Gertaeren kudeaketa eta kontingentzia-plana.	69
5.7.1	Salaketak kudeatzeko prozedura.	69
5.7.2	Datu edo software hondatuaren aurrean jarduteko plana.	70
5.7.3	CAren gako pribatuaren konpromisoaren aurreko prozedura	70
5.7.4	Hondamendi baten ondorengo negozioaren jarraipena.	70
5.8	CA edo RAren amaiera.	70
5.8.1	Ziurtapen Erakundea.	70
5.8.2	Erregistro Erakundea.	71
<b>6</b>	<b>Segurtasun teknikoko kontrolak</b>	<b>72</b>
6.1	Gako-pareen sorrera eta instalazioa.	72
6.1.1	Gako-parearen sorrera.	72
6.1.2	Gako pribatuaren banaketa sinatzaileari.	72
6.1.3	Gako publikoa ziurtagiriaren jaulkitzaileari banatzea.	72



6.1.4	Ziurtagiriaren jaulkitzailearen gako publikoaren banaketa ziurtagiri-erabiltzaileei.	72
6.1.5	Gakoen tamainak.	73
6.1.6	Gako publikoaren sorkuntza-parametroak eta kalitatearen egiaztapena.	73
6.1.7	Gakoen erabilera onartuak (X.509 v3 KeyUsage field).	74
6.2	Gako pribatuaren babesa.	74
6.2.1	Modulu kriptografikoen estandarrak.	74
6.2.2	Gako pribatuaren gaineko kontrol partekatua (n/m)..	74
6.2.3	Gako pribatuaren zaintza.	74
6.2.4	Gako pribatuaren babeskopia.	75
6.2.5	Gako pribatua artxibatzea	75
6.2.6	Gako pribatuaren transferentzia modulu kriptografikora edo hortik kanpora.	75
6.2.7	Gako pribatuaren biltegitratzea modulu kriptografikoan.	75
6.2.8	Gako pribatuaren aktibazio-metodoa	75
6.2.9	Gako pribatuaren desaktibazio-metodoa	76
6.2.10	Gako pribatuaren suntsiketa-metodoa	76
6.2.11	Modulu kriptografikoaren kalifikazioa.	76
6.3	Gako-parearen kudeaketari buruzko beste alderdi batzuk.	76
6.3.1	Gako publikoa artxibatzea.	76
6.3.2	Ziurtagiriaren jardunaldia eta gako-parearen erabilera-epea.	76
6.4	Aktibazio-datuak	77
6.4.1	Aktibazio-datuen sorrera eta instalazioa.	77
6.4.2	Aktibazio-datuen babesa.	77
6.4.3	Aktibazio-datuen beste alderdi batzuk	77
6.5	Segurtasun-informatikoko kontrolak	77



6.5.1	Segurtasun informatikoaren eskakizun tekniko espezifikoak	77
6.5.2	Informatika-segurtasunaren mailaren ebaluazioa.	78
6.6	Bizitzaren zikloko kontrol teknikoak	78
6.6.1	Sistemak garatzeko kontrolak.	78
6.6.2	Segurtasuna kudeatzeko kontrolak	79
6.6.3	Bizitza-zikloaren segurtasun-kontrolak	79
6.7	Sareko segurtasun-kontrolak	79
6.8	Denbora-iturria.	79
<b>7</b>	<b>Ziurtagirien profilak eta baliogabetutako ziurtagirien zerrendak.</b>	<b>80</b>
7.1	Ziurtagiri-profila	80
7.1.1	Bertsioaren zenbakia	80
7.1.2	Ziurtagiriaren luzapenak.	80
7.1.3	Algoritmoen objektu-identifikatzaileak.	80
7.1.4	Izenen formatuak.	81
7.1.5	Izen-murrizketak.	81
7.1.6	Ziurtagiri-politikaren objektu-identifikatzailea (OID)	81
7.1.7	Politika-murrizketen luzapenaren erabilera.	81
7.1.8	Politika-kualifikatzaileen sintaxia eta semantika.	81
7.1.9	“Certificate policy” hedapenaren tratamendu semantikoa.	81
7.2	Ziurtagiri baliogabetuen zerrendaren profila.	81
7.2.1	Bertsioaren zenbakia	82
7.2.2	Ziurtagiri baliogabetuen zerrenda eta bertako elementuen hedapenak.	82
7.3	OCSP profila.	82
7.3.1	Bertsioaren zenbakia	82
7.3.2	OCSP luzapenak.	82



7.3.3	OCSPren beste alderdi batzuk.	83
<b>8</b>	<b>Betetze-auditoriak</b>	<b>84</b>
8.1	Auditoriaren maiztasuna.	84
8.2	Auditorearen kualifikazioa.	84
8.3	Auditorearen eta auditatutako erakundearen arteko harremana.	84
8.4	Auditoriaren objektu diren elementuak.	84
8.5	Erabakiak hartzea, akatsen ondorioz.	84
<b>9</b>	<b>Beste gai legal eta jarduerarekin lotutakoak.</b>	<b>85</b>
9.1	Tarifak	85
9.1.1	Ziurtagirien jaulkipen- edo berritze-tarifak.	85
9.1.2	Ziurtagirietarako sarbidearen tarifak.	85
9.1.3	Ziurtagirien egoerari buruzko informazioa eskuratzeko tarifak.	85
9.1.4	Beste zerbitzu batzuen tarifak.	85
9.1.5	Itzulketarako politika.	85
9.2	Finantza-erantzukizuna	85
9.2.1	Erantzukizun zibileko aseguruak.	85
9.2.2	Beste aktibo batzuk	85
9.2.3	Amaierako entitateentzako aseguruak eta bermeak.	86
9.2.4	Informazio konfidentzialaren esparrua	86
9.2.5	Irismenean ez dagoen informazioa.	86
9.2.6	Informazio konfidentziala babesteko erantzukizuna.	87
9.3	Datu pertsonalen babesa.	87
9.3.1	Pribatutasun-plana	87
9.3.2	Pribatu gisa hartzen den informazioa.	87
9.3.3	Pribatutzat jotzen ez den informazioa	87



9.3.4	Informazio pribatua babesteko erantzukizuna.	87
9.3.5	Informazio pribatuaren erabilerari buruzko abisua eta baimena.	89
9.3.6	Zabalkundea, prozesu judizial edo administratiboaren arabera.	89
9.3.7	Informazioa hedatzeko beste inguruabar batzuk	89
9.4	Jabetza intelektualeko eskubideak	89
9.4.1	Ziurtagirien jabetza.	89
9.4.2	DPCGren jabetza.	89
9.4.3	Izenekin lotutako informazioaren jabetza	89
9.4.4	Gakoak eta haiekin lotutako materialaren jabetza.	89
9.5	Betebeharrak eta bermeak.	89
9.5.1	CAren betebeharrak	89
9.5.2	Erregistro-erakundearen betebeharrak.	92
9.5.3	Jabeen betebeharrak.	93
9.5.4	Konfiantza duten aldeen betebeharrak.	94
9.5.5	Beste partaideen betebeharrak.	94
9.6	Bermeetatik uko egitea.	95
9.7	Arduraren mugak	95
9.7.1	Ziurtapen Agintaritzaren ardura	95
9.7.2	Erregistro-erakundearen erantzukizunak	95
9.7.3	Harpidedunen erantzukizunak	96
9.7.4	Ziurtagirietan konfiantza duten hirugarrenen erantzukizunak	97
9.8	Kalte-ordainak.	97
9.9	Balio-aldia.	97
9.9.1	Indarrean jartzea	97
9.9.2	Amaiera	97



9.9.3	Amaieraren ondorioak.	97
9.10	Jakinarazpen indibidualak eta partaideekiko komunikazioa.	97
9.11	Dokumentu honen aldaketak.	97
9.11.1	Aldaketetarako prozedura.	97
9.11.2	Jakinarazpenaren epea eta mekanismoa.	98
9.11.3	OID bat aldatzea beharrezkoa den egoerak.	98
9.12	Kexak eta gatazken konponbidea.	98
9.13	Aplikagarri den araudia.	99
9.14	Araudi aplikagarria betetzea.	99
9.15	Askotariko arauak.	99
9.15.1	Akordio osoa	99
9.15.2	Esleipena.	100
9.15.3	Banakortasuna	100
9.15.4	Betetzea	100
9.15.5	Ezinbestea	100
9.15.6	Beste xedapen batzuk	100



## 1 Sarrera

---

1. Informazioaren Gizartearen sustatzaile diren heinean, eta herritarren jarduera ekonomiko eta sozialetan informazioaren eta komunikazioaren teknologien (IKT) integrazio osoa bermatzeko asmoz, euskal administrazio publikoek beharrezko tresnak ezarri dituzte herritarrak administrazio, erakunde eta enpresa ezberdinekin harremanetan jartzeko. Horretarako, betiere segurtasun-berme handienekin, informazioaren pribatutasuna, pertsonen intimitatea eta euren eskubideen babesa bermatzea dute helburu.
2. Oinarri horiekin, Eusko Jurlaritzak eta foru-aldundiek, beren informatika-elkarteen bidez eta lankidetzaz-esparru batean, ziurtapeneko eta sinadura elektronikoko sistema propio eta bateratu bat garatzea erabaki zuten. Sistema horrek elkarreragingarritasuna bermatuko du, eta, horrela, emandako ziurtagiriak baliozkoak izango dira administrazio ezberdinetako aplikazio eta prozeduretan.
3. Elkarlanean aritzeko gogo horren lehenengo erakusgarri gisa, 2022ko ekainean, "Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, IZENPE, SA" (aurrerantzean, IZENPE) merkataritza-sozietatea sortu zen. Lankidetzaz honen helburua da konfiantzazko zerbitzuak garatzea, herritarren eta administrazioaren arteko harremanak sinplifikatzeko bide egoki gisa.

### 1.1 Aurkezpena

4. eIDAS Erregelamenduak<sup>1</sup> Konfiantzazko Zerbitzuen Emaile Kualifikatu gisa jarduteko aukera aurreikusten du.
5. Izenpe Konfiantzazko Zerbitzuen Emaile Kualifikatu gisa eratu da, euskal administrazioen mendeko erakunde moduan, eta hau da haren xede soziala:
  - Telekomunikazio-sareen bidezko gobernu elektronikoaren erabilera sustatzea eta haren garapena indartzea, betiere beharrezko segurtasun-, konfidentzialtasun-, benetakotasun- eta ukaezintasun-bermeekin transakzioetan.
  - Era berean, segurtasun- eta administrazio-zerbitzuak eta zerbitzu teknikoak eskaintzea, komunikazioetan baliabide elektroniko, informatiko eta telematikoen bidez.
6. Izenpek eskaintzen dituen identifikazio-mekanismoak definituta daude Europako Batzordearen 2015eko irailaren 8ko 2015/1502 (EB) Exekuzio Erregelamenduaren arabera, "identifikazio elektronikoaren bitartekoen segurtasun-mailen gutxieneko zehaztapen eta prozedura teknikoak ezartzen dituen" erregelamendua, eIDAS Erregelamenduaren 8. artikuluko 3. apartatuan xedatutakoarekin bat etorritik.

---

<sup>1</sup> Europako Parlamentuaren eta Kontseiluaren 2014ko uztailaren 23ko 910/2014 (EB) Erregelamendua identifikazio elektronikoari eta barne-merkatuko transakzio elektronikoetarako konfiantzazko zerbitzuei buruzkoa da, eta 1999/93/EE Zuzentaraua indargabetzen du [2024/1183 (EB) Erregelamenduak aldatu zuen, 2024ko apirilaren 11ko Europako Parlamentuarenak eta Europako Kontseiluarenak, baita 910/2014 (EB) Erregelamendua ere, nortasun digitalaren Europako esparrua ezartzeari dagokionez].



7. Era berean, zerbitzuak modu eraginkorrean garatu eta ezartzeko helburuarekin, Izenpek informazioaren segurtasunerako kudeaketa-sistema bat ezarri du konfiantzazko zerbitzuekin lotutako prozesuetarako, ISO 27001 estandarren arabera.
8. Konfiantzazko zerbitzuak emateko, Izenpek ETSI (Europako Telekomunikazioen Estandarren Institutua) erakundeak ezarritako estandarrei jarraitzen die. Segurtasun-zerbitzuko ziurtagiriak (SSL) eskaintzeko, gainera, CA/Browser Forum-ek onartutako gidalerroak aplikatzen dira, zeinak eskuragarri baitaude [www.cabforum.org](http://www.cabforum.org) webgunean.
9. Arau hauetan definitzen diren zehaztapen teknikoek (ETSI TS) oinarrizko baldintzak ezartzen dituzte, hau da, ziurtagiri kualifikatuak eta kualifikatu gabekak eta denbora-zigiluak ematen dituzten konfiantzazko zerbitzuen emaleen kudeaketari eta praktikei dagozkienak, eIDAS Erregelamenduaren lege-esparruaren barruan. Araudi hori “Konfiantzazko zerbitzu elektronikoen zenbait alderdi arautzen dituen azaroaren 11ko 6/2020 Legearen” arabide juridikoan dago sartuta. Zehaztapen horiek behar bezala eguneratu dira Europako arau berri batzuetan: EN 319 411-1, ziurtagiriak emateko; EN 319 411-2, eIDAS Erregelamenduaren arabera kualifikatutako ziurtagiriak emateko; eta EN 319 421, denbora-zigiluak emateko, eIDAS Erregelamenduan jasotzen den moduan.
10. ETSI EN 319 401 araua betez, zeinak konfiantzazko zerbitzuak eta azken erabiltzaileentzako produktuak eskuragarriak izatea eskatzen baitu, Izenpek lanean dihardu herritar guztiak — bereziki desgaitasunen bat dutenek eta adinekoek— Izenperekin harremanetan jartzean informazioa eta zerbitzu elektronikoak baldintza berdinetan eskuratu ahal izan ditzaten, beren egoera pertsonala, baliabideak edo ezagutzak alde batera utzita. Helburu horiek lortzeko, ETSI EN 301 549 arauan jasotako gomendioak kontuan hartuko dira.
11. Izenpek bideoaren bidezko urrutiko identifikazioa txertatzen du ziurtagiriak egiteko, arau hauen arabera: “ETD/465/2021 Agindua, maiatzaren 6koa, Ziurtagiri elektronikoko kualifikatuak emateko bideoaren bidezko urruneko identifikazio-metodoak arautzen dituena, eta ETD/743/2022 Agindua, uztailaren 26koa, maiatzaren 6ko ETD/465/2021 Agindua aldatzen duena”.
12. Edonola ere, Izenperen webgunearen, produktuen edo zerbitzuen irisgarritasunari buruzko edozein kontsulta helaraz daiteke [info@izenpe.com](mailto:info@izenpe.com) helbide elektronikoen bidez edo [www.izenpe.eus](http://www.izenpe.eus) webgunean eskuragarri dagoen inprimakiaren bidez.
13. Zerbitzu kualifikatuetatik harago, Izenpek beste konfiantzazko zerbitzu ez-kualifikatu batzuk ere baditu, honako hauek nabarmentzekoak direlarik:
  - Sinadura elektronikoko ziurtagiri elektronikoko ez-kualifikatuak ematea.
  - Webguneen autentifikaziorako ziurtagiri elektronikoko ez-kualifikatuak ematea.
  - Kualifikatu gabeko sinadurak baliozkotzea.

## 1.2 Dokumentuaren izena eta identifikazioa

### 1.2.1 Identifikazioa

14. Dokumentu honen izenburua “Izenperen Konfiantzazko Praktiken Adierazpen Globala” da, eta barne-mailan DPCG akronimoaren bidez aipatuko da. Dokumentu hau RFC 3647-ren egiturari jarraikiz dago antolatuta.



15. Izenpeko Segurtasun Batzordeak aldizka berrikusten ditu erakundearen aurrean dauden arriskuak, eta behar diren tratamendu-planak onartzen ditu, DPCG honetan eta dibulgazio-testuetan (PDS) zehaztutako zerbitzuen segurtasuna bermatzeko.
16. Ziurtagiri-mota bakoitzaren erabilera-baldintzak, mugak, erantzukizunak, propietateak eta beste edozein informazio espezifiko PDS dokumentuetan jasoko dira —betiere DPCG honen mende daudenak— eta, halakorik badago, DPC berezietan.
17. Prozedura hauek nagusiki ETSI (European Telecommunications Standards Institute) erakundearen arauetan oinarritzen dira.
18. Izenpek DPCG honetan ezarritakoaren arabera jaulkitzen duen ziurtagiri mota bakoitza modu indibidualean identifikatzeko, objektu-identifikatzaile (OID) bat esleitzen zaio ziurtagiri-mota bakoitzari. [www.izenpe.eus](http://www.izenpe.eus) webgunean eskuragarri dagoen profil-dokumentuan kontsulta daitezke. Gainera, ETSI EN 319 412-5 arauaren definizioaren arabera, honako identifikatzaile hauek sartzen dira:
  - QcCompliance: eIDAS Erregelamenduaren arabera ziurtagiri kualifikatua.
  - QcSSCD: sinadura sortzeko gailu kualifikatuan jaulkitako ziurtagiria.
  - QcRetentionPeriod: dokumentazioaren atxikipen-epea.
  - QcPDS: dibulgazio-testuetarako (PDS) bidea.
  - QcType: eIDAS Erregelamenduaren arabera sinadura-motaren adierazlea (zigilua, sinadura, weba).

### 1.2.2 Ziurtagiri-identifikatzaileak

19. Izenpek azpiegitura bat du funtzionamenduan, honako zerbitzu kualifikatu hauek eskaintzeko:
  - Sinadura elektronikoko ziurtagiri elektronikoko kualifikatuak ematea.
  - Zigilu elektronikoko ziurtagiri elektronikoko kualifikatuak ematea.
  - Webguneen autentifikaziorako ziurtagiri elektronikoko kualifikatuak ematea.
  - Denbora-zigilu elektronikoko kualifikatuak emateko zerbitzua.

20. DPCG honen eta PDSen esparruan, Izenpek honako ziurtagiri-mota hauek ematen ditu:

#### 1.2.2.1 Oinarrizko 2007 CAren hierarkia: (CN=izenpe.com)

##### 1.2.2.1.1 eIDAS ziurtagiri kualifikatua.

Deskribapena	Politika	OID
Herritarren ziurtagiriak		
Herritarra (txipa)	QCP-n	1.3.6.1.4.1.14777.2.18.1
BaKQ (HSM)	QCP-n	1.3.6.1.4.1.14777.2.18.3



Erakundearen ordezkariaren ziurtagiriak		
Ordezkarria (softwarea)	QCP-n	1.3.6.1.4.1.14777.2.12
Ordezkarria (txipa)	QCP-n	1.3.6.1.4.1.14777.2.16
Ordezkarria (txipa) - sinadura kualifikatua	QCP	1.3.6.1.4.1.14777.2.12.5
SPJ erakundearen ordezkariaren ziurtagiriak		
SPJ erakundearen ordezkaria (HSM)	QCP-n	1.3.6.1.4.1.14777.2.15
SPJ erakundearen ordezkaria (txipa)	QCP-n	1.3.6.1.4.1.14777.2.13
SPJ erakundearen ordezkaria (txipa)-sinadura kualifikatua	QCP	1.3.6.1.4.1.14777.2.13.5
SPJ erakundearen ordezkaria (software)	QCP-n	1.3.6.1.4.1.14777.2.17
Enplegatu publikoaren ziurtagiriak (PEP)		
Enplegatu publikoa (txipa)	QCP-n	1.3.6.1.4.1.14777.4.14.1
Enplegatu publikoa (softwarea)	QCP-n	1.3.6.1.4.1.14777.4.14.2
Enplegatu publikoa (HSM)	QCP-n	1.3.6.1.4.1.14777.4.14.3
Ezizena duen enplegatu publikoaren langile-ziurtagiriak (PEP)		
Ezizena duen erakunde publikoko langileak (txipa) – SINADURA	QCP-n	1.3.6.1.4.1.14777.4.13.1.1
Ezizena duten entitate publikoko langileak (software)	QCP-n	1.3.6.1.4.1.14777.4.13.2
Profesionalaren ziurtagiriak		
Korporatibo kualifikatua (txipa)	QCP-n	1.3.6.1.4.1.14777.2.19.1
Korporatibo kualifikatua (software)	QCP-n	1.3.6.1.4.1.14777.2.19.2
Korporatibo kualifikatua (HSM)	QCP-n	1.3.6.1.4.1.14777.2.19.3
Erakundearen zigilu elektronikoko ziurtagiriak		
Erakundearen zigilua (edukiontzia)	QCP-l	1.3.6.1.4.1.14777.2.11
Erakundearen zigilua (HSM)	QCP-l	1.3.6.1.4.1.14777.2.20
Administrazioen zigilu elektronikoko ziurtagiriak		
Administrazioaren zigilua (software)	QCP-l	1.3.6.1.4.1.14777.4.11.2
Administrazioaren zigilua (HSM)	QCP-l	1.3.6.1.4.1.14777.4.11.3
Webeko autentifikazio-ziurtagiriak		
SSL kualifikatua	QEVCP-w	1.3.6.1.4.1.14777.50.3.2
SSL kualifikatua	QEVCP-w	1.3.6.1.4.1.14777.6.1.3

#### 1.2.2.1.2 Ziurtagiri ez-kualifikatuak.



Deskribapena	Politika	OID
<b>Herritarraren ziurtagiri ez-kualifikatuak</b>		
BaK	NCP	1.3.6.1.4.1.14777.5.2.5
Izenpe Mobile (APP)	NCP	1.3.6.1.4.1.14777.5.2.5.4
Autonomoa (softwarea)	NCP	1.3.6.1.4.1.14777.5.2.7.2
<b>Profesionalaren ziurtagiri ez-kualifikatuak</b>		
Ezizena duen enplegatu publikoa (txipa) Autentifikaziorako	NCP+	1.3.6.1.4.1.14777.4.13.1.2
Ezizena duen enplegatu publikoa (txipa) Zifratzerako	N/A	1.3.6.1.4.1.14777.4.13.1.3
Korporatibo ez-kualifikatua (txipa) Korporatibo publiko ez-aitortua (txipa)	NCP+	1.3.6.1.4.1.14777.1.1.1
Korporatibo pribatu ez-aitortua (txipa)	NCP+	1.3.6.1.4.1.14777.5.2.2
<b>Web-autentifikaziorako ziurtagiri ez-kualifikatuak</b>		
SSL DV	DVCP	1.3.6.1.4.1.14777.1.2.4
SSL OV	OVCP	1.3.6.1.4.1.14777.1.2.1
<b>Aplikazioaren ziurtagiri ez-kualifikatuak</b>		
Aplikazioa (softwarea)	NCP	1.3.6.1.4.1.14777.1.2.2
<b>IOT gailuen ziurtagiri ez-kualifikatuak</b>		
Gailua (softwarea)	NCP	1.3.6.1.4.1.14777.1.3.2

## 1.2.2.2 Oinarrizko 2020 CAren hierarkia

### 1.2.2.2.1 SSL ziurtagiriak.

Deskribapena	Politika	OID
<b>Webeko autentifikazio-ziurtagiriak</b>		
SSL DV	DVCP	1.3.6.1.4.1.14777.14.1.2

### 1.2.2.2.2 Denbora-zigilatzearen ziurtagiriak.

Deskribapena	Politika	OID
<b>Denbora-zigilatzearen ziurtagiriak</b>		
TSA		1.3.6.1.4.1.14777.10.1



### 1.2.2.3 Oinarrizko 2024 CAren hierarkia

#### 1.2.2.3.1 Ziurtagiri kualifikatua Eidas.

Deskribapena	Politika	OID
Webeko autentifikazio-ziurtagiriak		
SSL kualifikatua	QEVCW	1.3.6.1.4.1.14777.50.3.2

#### 1.2.2.3.2 Ziurtagiri ez-kualifikatuak

Deskribapena	Politika	OID
Web-autentifikaziorako ziurtagiri ez-kualifikatuak		
SSL DV	DVCP	1.3.6.1.4.1.14777.50.1.2
SSL OV	OVCP	1.3.6.1.4.1.14777.50.2.2

### 1.2.2.4 Oinarrizko 2025 CAren hierarkia

Deskribapena	Politika	OID
Herritarren ziurtagiriak		
Herritarra (txipa)	QCP-n	1.3.6.1.4.1.14777.51.1.1
BaKQ (HSM)	QCP-n	1.3.6.1.4.1.14777.51.1.3
Erakundearen ordezkariaren ziurtagiriak		
Ordezkarria (softwarea)	QCP-n	1.3.6.1.4.1.14777.51.3.2
Ordezkarria (txipa)	QCP-n	1.3.6.1.4.1.14777.51.3.1
Ordezkarria (txipa) - sinadura kualifikatua	QCP	1.3.6.1.4.1.14777.51.3.5
SPJ erakundearen ordezkariaren ziurtagiriak		
SPJ erakundearen ordezkaria (txipa)	QCP-n	1.3.6.1.4.1.14777.51.4.1
SPJ erakundearen ordezkaria (txipa)-	QCP	1.3.6.1.4.1.14777.51.4.5
SPJ erakundearen ordezkaria (software)	QCP-n	1.3.6.1.4.1.14777.51.4.2
Enplegatu publikoaren ziurtagiriak (PEP)		
Enplegatu publikoa (txipa)	QCP-n	1.3.6.1.4.1.14777.52.1.1
Enplegatu publikoa (softwarea)	QCP-n	1.3.6.1.4.1.14777.52.1.2
Enplegatu publikoa (HSM)	QCP-n	1.3.6.1.4.1.14777.52.1.3
Ezizena duen enplegatu publikoaren langile-ziurtagiriak (PEP)		
Ezizena duen erakunde publikoko langileak (txipa) – SINADURA	QCP-n	1.3.6.1.4.1.14777.52.2.1.1



Ezizena duten entitate publikoko langileak (software)	QCP-n	1.3.6.1.4.1.14777.52.2.2
<b>Profesionalaren ziurtagiriak</b>		
Korporatibo kualifikatua (txipa)	QCP-n	1.3.6.1.4.1.14777.51.2.1
Korporatibo kualifikatua (software)	QCP-n	1.3.6.1.4.1.14777.51.2.2
Korporatibo kualifikatua (HSM)	QCP-n	1.3.6.1.4.1.14777.51.2.3
<b>Erakundearen zigilu elektronikoko ziurtagiriak</b>		
Erakundearen zigilua (edukiontzia)	QCP-l	1.3.6.1.4.1.14777.51.5.2
Erakundearen zigilua (HSM)	QCP-l	1.3.6.1.4.1.14777.51.5.3
<b>Administrazioen zigilu elektronikoko ziurtagiriak</b>		
Administrazioaren zigilua (software)	QCP-l	1.3.6.1.4.1.14777.52.3.2
Administrazioaren zigilua (HSM)	QCP-l	1.3.6.1.4.1.14777.52.3.3
<b>Denbora-zigilatzearen ziurtagiriak</b>		
Denbora-zigilatzearen ziurtagiriak		1.3.6.1.4.1.14777.53.1.3

### 1.3 Gako publikoaren azpiegiturako (PKI) parte-hartzaileak.

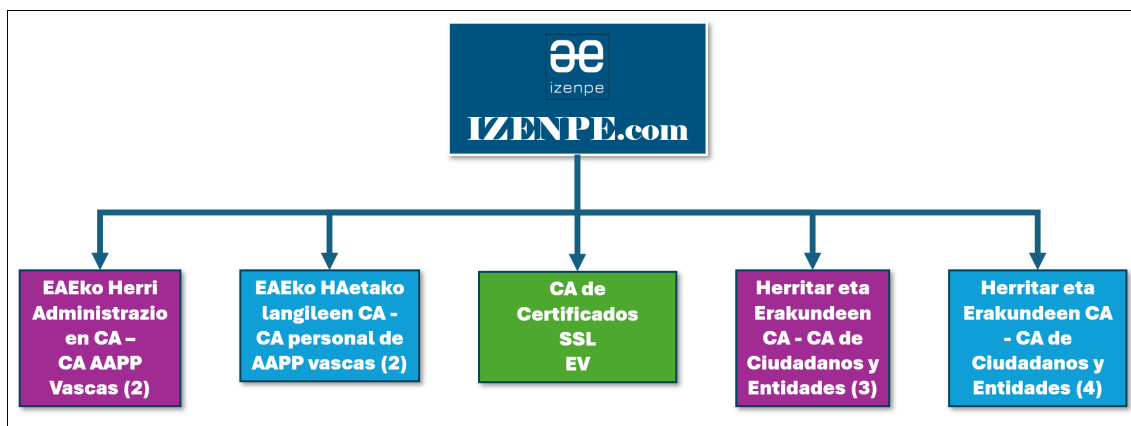
21. Ziurtapen-erakundearen kudeaketan eta funtzionamenduan parte hartzen duten rolen artean honako hauek daude:

- Ziurtapen-agintaritzak.
- Erregistro-erakundeak.
- Ziurtagirien harpidedunak eta sinatzaileak.
- Konfiantza duten alderdiak.
- Beste parte-hartzaile batzuk.

#### 1.3.1 Ziurtapen-agintaritzak.

22. Izenpek honako Ziurtapen Agintaritza hauek ditu:

##### 1.3.1.1 2007an sortutako Izenpe.com hierarkia.



#### Oinarrizko CA ziurtagiria.

CN	izenpe.com
BALIO-ALDIA	2007/12/13tik 2037/12/13ra
HASH SHA256	25:30:CC:8E:98:32:15:02:BA:D9:6F:9B:1F:BA:1B:09:9E:2D:29:9E:0F:45:48:BB:91:4F:36:3B:C0:D4:53:1F
GAKO-MOTA	RSA 4096 bits / SHA-256 with RSA

#### Menpeko CA ziurtagiria

CN	EAEko Herri Administrazioen CA - CA AAPP Vascas (2)
BALIO-ALDIA	2010/10/20tik 2037/12/13ra
HASH SHA256	CD:6E:B9:37:EE:17:A9:FC:FF:60:A7:90:F8:BD:E0:CA:9A:BC:A0:7B:3E:F4:60:74:DD:19:78:F0:BC:A4:D4:49
GAKO-MOTA	RSA 4096 bits / SHA-256 with RSA

#### Menpeko CA ziurtagiria

CN	EAEko HAetako langileen CA - CA personal de AAPP vascas (2)
BALIO-ALDIA	2010/10/20tik 2037/12/13ra
HASH SHA256	25:30:3C:FD:0B:F1:BA:A1:EF:24:8C:29:F0:73:FF:FC:2E:7C:81:58:2E:E2:3B:45:C7:F1:C3:B3:2E:34:1A:D8
GAKO-MOTA	RSA 4096 bits / SHA-256 with RSA



#### Menpeko CA ziurtagiria

CN	SSL EV ziurtagirien CA
BALIO-ALDIA	2018/7/6tik 2028/7/6ra
HASH SHA256	DB:47:63:39:CC:BF:CC:9E:4B:D1:D6:CB:60:6C:A2:7F:00:67:9E:1E:F8:A5:81:E7:23:63:09:B9:D6:3F:FE:37
GAKO-MOTA	RSA 4096 bits / SHA-256 with RSA

#### Menpeko CA ziurtagiria

CN	Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (3)
BALIO-ALDIA	2010/10/20tik 2037/12/13ra
HASH SHA256	5A:49:B1:5A:E6:0F:F6:27:DA:27:2A:87:43:D6:71:62:BA:CA:10:96:16:82:03:21:3A:CF:82:27:AF:4C:49:42
GAKO-MOTA	RSA 4096 bits / SHA-256 with RSA

#### Menpeko CA ziurtagiria

CN	Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (4)
BALIO-ALDIA	2010/10/20tik 2037/12/13ra
HASH SHA256	7E:D1:93:61:AD:73:4D:70:3F:BA:DF:02:9F:52:EC:3B:66:48:D8:DD:56:BA:BA:08:84:ED:4F:85:9B:5B:93:75
GAKO-MOTA	RSA 4096 bits / SHA-256 with RSA

#### 1.3.1.2 2020an sortutako hierarkia.





### 2020ko OINARRIZKO CA ziurtagiria

CN		ROOT CA QC IZENPE
BALIO-ALDIA		2045/09/23
HASH SHA256		[d4a81325ebf2e5c19c779192c63db76404c8dafd] (CRT)
GAKO-MOTA		SHA2:

### Menpeko CA ziurtagiria

CN		SUBCA QC IZENPE - TSA
BALIO-ALDIA		2045/09/23
HASH SHA256		[fa6cf62e148806df05f536bc71dfe34b364023e8] (CRT)
GAKO-MOTA		SHA2:

### 1.3.1.3 2024an sortutako hierarkia



### 2024ko OINARRIZKO CA ziurtagiria

CN		ROOT CA SSL IZENPE 2024
BALIO-ALDIA		2049/09/24
HASH SHA256		68E93296DEEB4254C18C49C4E80F5D8FA3D38A93:
GAKO-MOTA		ECC(384 Bits)



#### Menpeko CA ziurtagiria

CN	SUBCA SSL 2024
BALIO-ALDIA	2045/09/23
HASH SHA256	E3A0E57B82D88AE25E0A488C51C1E40E2AC0DB18:
GAKO-MOTA	ECC(384 Bits)

#### 1.3.1.4 2025an sortutako hierarkia

##### 2025eko OINARRIZKO CA ziurtagiria

CN	ROOT CA QC IZENPE 2025
BALIO-ALDIA	2050/09/25
HASH SHA256	D2A934AE739B8B8B0C1D3857C324DE595EEB1DCAFD086A4A7E99DC08D77AF0CA
GAKO-MOTA	ECC(384 Bits)

##### Menpeko CA ziurtagiria.

CN	CA ADMINISTRAZIO PUBLIKOA - ADMINISTRAZIO PUBLIKOA 2025
BALIO-ALDIA	2045/09/25
HASH SHA256	7E4E551152F06C51DB576236162514BAFD7ABCE1A3A4141A1A7949BDCFE1A432
GAKO-MOTA	ECC(384 Bits)

##### Menpeko CA ziurtagiria.

CN	CA HERRITARRAK ETA ENPRESAK - HERRITARRAK ETA ENPRESA 2025
BALIO-ALDIA	2045/09/25
HASH SHA256	D852490ED91838B06F6885E17153738DEBFE9A5FF9DDB96BA0E36E5D4572EFEE
GAKO-MOTA	ECC(384 Bits)



#### Menpeko CA ziurtagiria.

CN	CA QC IZENPE - TSA 2025
BALIO-ALDIA	2045/09/25
HASH SHA256	9850D9462094CD18854E39B9241DBA89FA4AFB4084AB942F0D3ABCEBA8FA3529
GAKO-MOTA	ECC(384 Bits)

#### 1.3.2 Erregistro-erakundeak.

23. DPCG hau Izenpek ziurtagiriak jaulkitzeko eta kudeatzeko prozeduretan erabiltzen dituen Erregistro-erakundeei aplikatzen zaie.
24. Erregistro-erakundeek honako eginkizun hauek betetzen dituzte: ziurtagiri-eskatzaileak, harpidedunak eta sinatzaileak identifikatzea; ziurtagirietan jasotzen diren inguruabarren egiaztagiri-dokumentazioa aztertzea; eta ziurtagiriak jaulkitzeko, indargabetzeko eta berritzeko eskaerak balioztatzea eta onestea.
25. Hauek izango dira erregistro-erakunde: Izenpe eta/edo Izenperekin dagokion lege-tresna izenpetzen duten erakunde erabiltzaileak.

#### 1.3.3 Ziurtagirien harpidedunak.

26. Ziurtagiri bat eskatzen duen pertsonak izango du harpidedunaren izaera.
27. **Sinatzaileak** dira beren titulartasuneko ziurtagiriei lotutako sinadura sortzeko datuak beren erabilera eskusiboan dituzten pertsona fisikoak.
28. Batzuetan, harpidedunaren eta sinatzailearen figurak ez datoz bat: pertsona juridikoek beren langile, bazkide edo langileentzako ziurtagiriak eska ditzakete, eta ziurtagiri horietan pertsona fisikoak "sinatzaile" gisa hartzen dira, eta pertsona juridikoa "harpidedun" gisa.
29. **Zigilu-sortzaileak** pertsona juridikoak dira, eta haiek sortzen dituzte zigilu elektronikoak, non pertsona juridikoaren identitatea ageri baita (merkataritza-enpresa, fundazioa, administrazio publikoa...).

#### 1.3.4 Konfiantzazko hirugarrenak.

30. DPCG honen barruan, Izenpek eskaintzen dituen zerbitzuak jasotzen dituzten pertsona fisiko edo juridikoak dira konfiantzazko hirugarrenak, eta, ondorioz, DPCG honek ezarritakoa aplikatzen zaie.
31. Ziurtagirietan eta haiekin sortutako sinadura eta zigiluetan konfiantza jarri aurretik, hirugarrenek egiaztatu egin behar dituzte, DPCG honetan ezarritakoaren arabera: Ziurtagiri balioduna erabili dela egiaztatuko da. Sinadurak edo zigiluak ziurtagiriaren balio-epean sortu direla baieztatuko da. DPCG honetan ezarritako jarraibideak eta argibideak bete direla egiaztatuko da.



32. Hirugarrenek zaintza-neurri egokiak hartu beharko dituzte ziurtagiri-mota bakoitzaren erabileran, fede oneko eta leialtasun-printzipioen arabera jardunez, eta saihestu egin beharko dituzte jokabide iruzurti edo ez-zuhurrak, besteak beste, ziurtagiri edo denbora-zigilu batekin lotutako konfiantzazko esparruaren barruan bidalitako mezuak ukatzeko asmoz.

#### 1.3.5 Beste partaide batzuk

33. Izenpe Denbora Zigiluaren Agintaritza da, denbora-zigilu elektronikoak sortzeko Konfiantzazko Zerbitzua eskaintzen duenean, dagokion DPCPre arabera.

### 1.4 Ziurtagiriaren erabilerak.

34. Ondoren zehazten dira Izenpek jaulkitako ziurtagirien erabilera baimenduak eta debekatuak.

#### 1.4.1 Ziurtagiriaren erabilera egokiak

##### 1.4.1.1 Ziurtagirikualifikatuak

35. Sinadura elektronikoko ziurtagiri kualifikatuek harpidedunaren eta sinatzailearen identitatea bermatzen dute. Sinadura sortzeko gailu seguru batekin erabiltzen direnean, sinadura elektronikoko kualifikatuari eusteko egokiak dira; hau da, ziurtagiri kualifikatuan oinarritzen den eta gailu kualifikatu baten bidez sortu den sinadura elektronikoko aurreratua, eIDAS Erregelamenduaren arabera, balio juridiko osoz eskuzko sinaduraren parekoa dena, inolako baldintza osagarririk bete beharrik gabe.

36. Sinadura elektronikoko ziurtagiri kualifikatuak eIDAS Erregelamenduaren 28. artikulua eta I. Eranskinaren arabera kualifikatuak dira.

37. Ziurtagiri-mota jakin batean hala definitzen bada, sinadura elektronikoko ziurtagiri kualifikatuak erabiltzailearen autentifikazio-mezuak sinatzeko ere erabil daitezke, bereziki SSL edo TLS bezeroaren erroak, gakoaren berreskurapenik gabeko zifratzea, edo bestelako erabilerak. Sinadura elektronikoko horren ondorioz, ziurtagiriaren harpidedunaren identitatea bermatzen da.

38. Horrez gain, ziurtagiri horiek hainbat autentifikazio-moduren eta sinadura elektronikoko aurreratuaren euskarri gisa ere erabil daitezke, sinatzeko gako pribatua modu fidagarrian babesten duten aplikazio informatikoekin konbinatuta.

39. Zigilu elektronikoen ziurtagiria aitortzen elektronikoko bat da, zigilu baten baliozkotze-datuak pertsona juridiko batekin lotzen dituena eta pertsona horren izena berresten duena. Zigilu elektronikokoak sortzeko aukera ematen dute. Zigilu horiek dokumentu elektronikoko bat pertsona juridiko batekin egin duela frogatzen dute, eta dokumentuaren jatorriari eta osotasunari buruzko ziurtasuna ematen dute.

40. Zigilu elektronikoko ziurtagiri kualifikatuak eIDAS Erregelamenduaren 38. artikulua eta III. Eranskinaren arabera kualifikatuak dira.

41. Webguneen autentifikaziorako ziurtagiriek webgune bat egiaztatzea ahalbidetzen dute, eta webgunea ziurtagiria jaso duen pertsona fisiko edo juridikoarekin lotzen dute. Izenpek ematen dituen web-ziurtagiriek kualifikatutzat hartzeko eIDAS Erregelamenduaren IV. eranskineko baldintzak betetzen dituzte.



42. Organoaren zigilu elektronikoaren ziurtagiriak administrazio publikoei igortzen zaizkie organoa identifikatzeko eta dokumentuak elektronikoki zigilatzeke, Sektore Publikoaren Araubide Juridikoaren urriaren 1eko 40/2015 Legean aurreikusitakoaren arabera.
43. Izenperen ziurtagiri kualifikatuek ETSI EN 319 411-2 arau teknikoari jarraitzen diote.

#### 1.4.1.2 Ziurtagiri ez-kualifikatua.

44. Ziurtagiri ez-kualifikatuek ez dute harpidedunaren eta, hala badagokio, sinatzailearen identitatea modu fidagarrian bermatzen, eta sinatzeko erabiltzen badira, sinadura sortzeko gailu arrazoiz seguru batekin batera erabili beharko dira. Kasu horretan, ez dira sinatzailearen eskuzko sinaduraren parekoak izango.
45. Ziurtagiri ez-kualifikatuak, ziurtagiri-motan hala zehaztuta badago, autentifikazio-mezuak sinatzeko ere erabil daitezke, bereziki SSL edo TLS bezeroen erronkak, gakoan berreskurapenik gabeko zifratzea edo beste.
46. Izenperen ziurtagiri ez-kualifikatuek ETSI EN 319 411-1 arau teknikoari jarraitzen diote.

#### 1.4.1.3 Ziurtagirien erabilera-eremua.

47. Erabilera-eremuari dagokionez, bi egoera bereizten dira:
  - Izenpek jaulkitako eta oro har publikoari zuzendutako ziurtagiriak harpidedunek edo, hala badagokio, sinatzaileek erabiliko dituzte, ziurtagiri horien erabilera onartu duten erakunde erabiltzaileekin eta erakunde publiko eta pribatuekin dituzten harremanetan.
48. Ziurtagiri bakoitzaren erabilera-eremuari buruzko berezitasunak PDS dokumentuan kontsulta daitezke, eta halakorik bada, DPC berezietan ere bai.
  - Izenpek jaulkitako eta erakunde erabiltzaileek eskatu dituzten ziurtagiriak pertsona fisiko edo juridiko gisa duten ezaugarrien esparruan erabiliko dira, eIDAS Erregelamenduan ezarritakoaren arabera. Hala ere, sinatzaileek ziurtagiri horiek beste erabilera batzuetarako ere erabili ahal izango dituzte, betiere aurreko atalean adierazitako erabilera-mugak errespetatzen badira.

#### 1.4.1.4 Herritar fisikoaren ziurtagiria.

##### 1.4.1.4.1 Ziurtagiri kualifikatua

- **Deskribapena:** pertsona fisikoaren ziurtagiria.
- **Balio-aldia:** gehienez 4 urte.
- **Euskarria:** txartelean edo HSM bidez (urrunko sinadura) jaulkitakoa.

Deskribapen laburra	Euskarria	Politika-identifikatzailea	OID politika	Sinadura-mota eIDAS
Herritarraren ziurtagiria	Txartela	QCP-n	eIDAS profila	Aurreratua



			1.3.6.1.4.1.14777.2.18.1 1.3.6.1.4.1.14777.51.1.1	
BakQ Herritarraren ziurtagiria	HSM	QCP-n	1.3.6.1.4.1.14777.2.18.3 1.3.6.1.4.1.14777.51.1.3	Aurreratua

#### 1.4.1.4.2 Ziurtagiri ez-kualifikatuak

##### 49. BaK ziurtagiria.

- **Deskribapena:** pertsona fisikoei identifikatzeko eta sinatzeko aukera ematen die. Erabiltzailearen NAN/AIZ/pasaportearekin bat datorren erreferentzia-zenbakiak eta pasahitzak osatzen dute. Ziurtagiri ez-kualifikatu bat da, Izenperen gordailu zentralizatu batean ematen dena eta sinadura ekitaldietarako balio duena. Bak ziurtagiriak barne hartzen duen ETSI LCP politika dela eta, ziurtagiria jaulki ahal izateko ez da aurrez aurreko identifikaziorik behar.
- **Balio-aldia:** gehienez 4 urte.
- **Euskarria:** HSM bidez (urruneko sinadura) jaulkitakoa.

##### 50. Izenpe Mobile ziurtagiria.

- **Deskribapena:** pertsona fisikoen identifikazioa egiteko eta pertsona horrekin lotutako Izenperen gordailu zentral seguru batean biltegitratutako ziurtagiri kualifikatu baten erabilera baimentzeko bitartekoa da. Osagai hauek ditu:
  - Ziurtagiri ez-kualifikatu bati lotutako gailu mugikor batean instalatutako aplikazio bat, komunikazio seguruen prozesuak errazten dituena.
  - Aplikaziora sartzeari ahalbidetzen duen pasahitz bat edo faktore biometriko bat.
- **Balio-aldia:** gehienez 4 urte.
- **Euskarria:** software bidez jaulkitakoa.

##### 51. Autonomoaren ziurtagiria.

- **Deskribapena:** pertsona fisikoaren ziurtagiria, pertsona horrek autonomo gisa Euskadiko foru-ogasunekin dituen harremanetarako.
- **Balio-aldia:** gehienez 4 urte.
- **Euskarria:** software bidez jaulkitakoa.

Deskribapen laburra	Euskarria	Politika-identifikatzaileak	OID politika	Sinadura-mota eIDAS
BaK	HSM	LCP	1.3.6.1.4.1.14777.5.2.5	Oinarrizkoa



Izenpe Mobile	APP edukiontzia	NCP	1.3.6.1.4.1.14777.5.2.5.4	NA (sinatzeko, BaKQ edo profesionalaren ziurtagiria erabiltzen da)
Autonomoa	Software	LCP	1.3.6.1.4.1.14777.5.2.7.2	Oinarrizkoa

#### 1.4.1.5 Erakunde baten ordezkari den pertsona fisikoaren ziurtagiria.

##### 1.4.1.5.1 Ziurtagiri kualifikatua

- **Deskribapena:** pertsona juridiko baten izenean eta ordezkartzan jarduteko gaitasuna duen pertsona fisiko bati jaulkitako ziurtagiria.
- **Balio-aldia:** gehienez 4 urte.
- **Euskarria:** txartelean, software-edukiontzian edo urrunetik HSM bidez jaulkitakoa.

Deskribapen laburra	Euskarria	Politika-identifikatzailea	OID politika	Sinadura-mota eIDAS
Erakundearen ordezkaria	Txip kriptografikoa	QCP-n	1.3.6.1.4.1.14777.2.12 1.3.6.1.4.1.14777.51.3.1	Aurreratua
	Izenpe-ren software-edukiontzia	QCP-n	1.3.6.1.4.1.14777.2.16 1.3.6.1.4.1.14777.51.3.2	Aurreratua
	Txip kriptografikoa	QCP	1.3.6.1.4.1.14777.2.12.5 1.3.6.1.4.1.14777.51.3.5	Kualifikatua

#### 1.4.1.6 Nortasun juridikorik gabeko erakunde baten ordezkari den pertsona fisikoaren ziurtagiria.

- **Deskribapena:** nortasun juridikorik gabeko erakunde baten izenean eta ordezkartzan jarduteko gaitasuna duen pertsona fisiko bati jaulkitako ziurtagiria.
- **Balio-aldia:** gehienez 4 urte.
- **Euskarria:** txartelean, software-edukiontzian edo urrunetik HSM bidez jaulkitakoa.

##### 1.4.1.6.1 Ziurtagiri kualifikatua.

Deskribapen laburra	Euskarria	Politika-identifikatzailea	OID politika	Sinadura-mota eIDAS
	HSM	QCP-n	1.3.6.1.4.1.14777.2.15	Aurreratua



SPJ erakundearen ordezkaria			1.3.6.1.4.1.14777.51.4.3	
	Txip kriptografikoa	QCP-n	1.3.6.1.4.1.14777.2.13 1.3.6.1.4.1.14777.51.4.1	Aurreratua
	Txip kriptografikoa	QCP	1.3.6.1.4.1.14777.2.13.5 1.3.6.1.4.1.14777.51.4.5	Kualifikatua
	Izenpe-ren software- edukiontzia	QCP-n	1.3.6.1.4.1.14777.2.17 1.3.6.1.4.1.14777.51.4.2	Aurreratua

#### 1.4.1.7 Langile publikoaren ziurtagiria

##### 1.4.1.7.1 Ziurtagiri kualifikatua

- **Deskribapena:** administrazio publikoen zerbitzuko langileei jaulkitako ziurtagiria. Sektore Publikoaren Araubide Juridikoaren urriaren 1eko 40/2015 Legearen esparruan emana.
- **Balio-aldia:** gehienez 4 urte.
- **Euskarria:** txartelean, software-edukiontzian edo urrunetik HSM bidez jaulkitakoa.

Deskribapena	Euskarria	Politika-identifikatzailea	OID politika	eIDAS sinadura-mota
Enplegatu publikoa	Txartel kriptografikoa	QCP-n	1.3.6.1.4.1.14777.4.14.1 1.3.6.1.4.1.14777.52.1.1	Aurreratua
	Izenpe-ren software-edukiontzia	QCP-n	1.3.6.1.4.1.14777.4.14.2 1.3.6.1.4.1.14777.52.1.2	Aurreratua
	HSM	QCP-n	1.3.6.1.4.1.14777.4.14.3 1.3.6.1.4.1.14777.52.1.3	Aurreratua

#### 1.4.1.8 Ezizena duen administrazio publikoko langilearen ziurtagiria.

##### 1.4.1.8.1 Ziurtagiri kualifikatua

- **Deskribapena:** administrazio publikoetan zerbitzua ematen duten langileei emandako ziurtagiria, ziurtagiriaren titularraren datu pertsonalak ez jasotzeko ezaugarriarekin, baizik eta “Ogasuneko eta Administrazio Publikoetako Ministerioko ziurtagiri elektronikoen profilak” dokumentuaren arabera ezizen bat erabiliz, “2015eko urriaren 1eko 40/2015 Legea, Sektore Publikoaren Araubide Juridikoarena” delakoaren esparruan.
- **Balio-aldia:** gehienez 4 urte.
- **Euskarria:** txartelean edo software-edukiontzian jaulkitakoak.



Deskribapen laburra	Euskarria	Politika-identifikatzailea	OID politika	Sinadura-mota eIDAS
Ezizena duen enplegatu publikoa (sinadura)	Txartel kriptografikoa	QCP-n	1.3.6.1.4.1.14777.4.13.1.1 1.3.6.1.4.1.14777.52.2.1.1	Aurreratua
Ezizena duen enplegatu publikoa	Izenpe-ren software-educiontzia	QCP-n	1.3.6.1.4.1.14777.4.13.2 1.3.6.1.4.1.14777.52.2.2	Aurreratua

#### 1.4.1.8.2 Ziurtagiri ez-kualifikatuak

- **Deskribapena:** autentifikazio- eta zifratze-funtzioetarako ziurtagiria, sinadura kualifikatuaren ziurtagiriarekin batera jaulkitzen dena.
- **Balio-aldia:** gehienez 4 urte.
- **Euskarria:** txartelean jaulkitakoak.

Deskribapen laburra	Euskarria	Politika-identifikatzailea	OID politika	Sinadura-mota eIDAS
Ezizena duen enplegatu publikoa	txartela	NCP+	1.3.6.1.4.1.14777.4.13.1.2 autentifikazioa 1.3.6.1.4.1.14777.52.2.1.2	e/a
		e/a	1.3.6.1.4.1.14777.4.13.1.3 zifratzea 1.3.6.1.4.1.14777.52.2.1.3	e/a

#### 1.4.1.9 Pertsona fisiko profesionalaren ziurtagiria.

##### 1.4.1.9.1 Ziurtagiri kualifikatua

- **Deskribapena:** erakunde bateko langileei jaulkitako ziurtagiria.
- **Balio-aldia:** gehienez 4 urte.
- **Euskarria:** txartelean, software-educiontzian edo urrunetik HSM bidez jaulkitakoa.



Deskribapen laburra	Euskarria	Politika-identifikatzailea	OID politika	Sinadura-mota eIDAS
Profesionala-Korporatibo kualifikatua	Txartela	QCP-n	1.3.6.1.4.1.14777.2.19.1 1.3.6.1.4.1.14777.51.2.1	Aurreratu a
	Izenpe-ren software- edukiontzia	QCP-n	1.3.6.1.4.1.14777.2.19.2 1.3.6.1.4.1.14777.51.2.2	Aurreratu a
	HSM	QCP-n	1.3.6.1.4.1.14777.2.19.3 1.3.6.1.4.1.14777.51.2.3	Aurreratu a

#### 1.4.1.9.2 Ziurtagiri ez-kualifikatuak

##### 52. Profesionala-Korporatibo ez-kualifikatua

- **Deskribapena:** ziurtapen-maila ertainarekin identifikatzen du erakunde jardulea ziurtagiriaren harpidedun gisa, baita bertan kargu edo postu bat betetzen duen pertsona ere, sinatzaile den aldetik.
- **Balio-aldia:** gehienez 4 urte.
- **Euskarria:** txartelean jaulkitakoa.

##### 53. Profesionala-Korporatibo pribatu ez-kualifikatua,

- **Deskribapena:** ziurtapen-maila ertainarekin identifikatzen du erakunde pribatu jardulea ziurtagiriaren harpidedun gisa, baita bertan kargu edo postu bat betetzen duen pertsona ere, sinatzaile den aldetik.
- **Balio-aldia:** gehienez 4 urte.
- **Euskarria:** txartelean jaulkitakoak.

Deskribapen laburra	Euskarria	Politika-identifikatzailea	OID politika	Sinadura-mota eIDAS
Korporatibo ez-kualifikatua	Txip kriptografikoa	NCP+	1.3.6.1.4.1.14777.1.1.1	Oinarrizkoa
Korporatibo pribatu ez-aitortua	Txip kriptografikoa	NCP+	1.3.6.1.4.1.14777.5.2.2	Oinarrizkoa

#### 1.4.1.10 Erakundearen (pertsona juridikoa eta SPJ) zigilu elektronikoko ziurtagiria.

- **Deskribapena:** erakundearen identifikazioa ahalbidetzen du, baita, kasuan kasu, eskatzeko pertsonaren identitatea ere.



Dokumentu elektroniko bat erakundeak eman duela frogatzea ahalbidetzen du, dokumentuaren jatorria eta osotasuna ziurtatuz.

Pertsona juridikoei eta nortasun juridikorik gabeko erakundeei jaulkitzen zaie.

Harpideduna erakundea izango da. Eskatera egiten duen pertsona fisikoa izango da, erakundearen izenean jarduteko gaitasuna duena, eta ziurtagiria eskatzen duena.

Ziurtagiriaren barruan pertsona fisikoaren informazioa ager daiteke, argi eta garbi hala adierazten bada.

- **Balio-aldia:** gehienez 3 urte.
- **Euskarria:** software bidez edo urrunetik HSM bidez jaulkitakoa.

#### 1.4.1.10.1 Ziurtagiri kualifikatua

Deskribapen laburra	Euskarria	Politika-identifikatzailea	OID politika	Sinadura-mota eIDAS
Entitatearen zigilua	Izenpe-ren software- edukiontzia	QCP-I	1.3.6.1.4.1.14777.2.11 1.3.6.1.4.1.14777.51.5.2	Aurreratua
	HSM	QCP-I	1.3.6.1.4.1.14777.2.20 1.3.6.1.4.1.14777.51.5.3	Aurreratua

#### 1.4.1.11 Administrazioaren zigu elektronikoko ziurtagiria (organoaren zigu)

- **Deskribapena:** aukera ematen du administrazioa, organoa, organismo publikoa edo zuzenbide publikoko erakundea identifikatzeko, bai eta, hala badagokio, organoaren titularrak nor den jakiteko ere.

Sektore Publikoaren Araubide Juridikoaren urriaren “1eko 40/2015 Legearen esparruan emana”.

Administrazio, organo, organismo publiko edo zuzenbide publikoko erakundea izango da harpideduna.

Ziurtagiriak maila ertainekoak dira.

- Ziurtagiria harpidedunak erabiliko du, bere erakundeak automatizatutako jardura-prozedura gisa zehaztutako zerbitzuetan eta hirugarrenek, DPCG honetan ezarritako baldintza eta mugak betez, onartzen dituzten zerbitzuetan.
- **Balio-aldia:** gehienez 3 urte.
- **Euskarria:** software bidez edo urrunetik HSM bidez jaulkitakoa.

#### 1.4.1.11.1 Ziurtagiri kualifikatua



Deskribapen laburra	Euskarria	Politika-identifikatzailea	OID politika	Sinadura-mota eIDAS
Administrazioaren zigilua	Izenpe-ren software-educiontzia	QCP-l	1.3.6.1.4.1.14777.4.11.2 1.3.6.1.4.1.14777.52.3.2	Aurreratua
	HSM	QCP-l	1.3.6.1.4.1.14777.4.11.3 1.3.6.1.4.1.14777.52.3.3	Aurreratua

#### 1.4.1.12 Webgunearen autentifikazio-ziurtagiria (zerbitzari segurua).

##### 1.4.1.12.1 Ziurtagiri kualifikatua

- **Deskribapena:** webgunearen autentifikazio-ziurtagiria.
- **Balio-aldia:** 395 egun arte<sup>2</sup>.
- **Euskarria:** software bidez jaulkitakoa.

Deskribapen laburra	Euskarria	Politika-identifikatzailea	OID politika
SSL kualifikatua	Software	QEVCP-w	1.3.6.1.4.1.14777.6.1.3
SSL kualifikatua	Software	QEVCP-w	1.3.6.1.4.1.14777.50.3.2

##### 1.4.1.12.2 Ziurtagiri ez-kualifikatuak

Deskribapen laburra	Euskarria	Politika-identifikatzailea	OID politika
SSL DV	Software	DVCP	1.3.6.1.4.1.14777.1.2.4
SSL OV	Software	OVCP	1.3.6.1.4.1.14777.1.2.1
SSL DV	Software	DVCP	1.3.6.1.4.1.14777.50.1.2
SSL OV	Software	OVCP	1.3.6.1.4.1.14777.50.2.2
SSL DV	Software	DVCP	1.3.6.1.4.1.14777.14.1.2

<sup>2</sup>Balio-aldia Cabforum.org araudiarekin bat dator



#### 1.4.1.13 Aplikazio-ziurtagiria.

##### 1.4.1.13.1 Ziurtagiri ez-kualifikatua.

- **Deskribapena:** aplikazio informatiko batek erabiltzen du sinadura digitalari lotutako datu elektronikoen egiazkotasuna eta osotasuna ziurtatzeko.
- **Balio-aldia:** gehienez 3 urte.
- **Euskarria:** software bidez jaulkitakoa.

Deskribapen laburra	Euskarria	Politika-identifikatzailea	OID politika
Aplikazioa	Izenpe-ren software- edukiontzia	NCP	1.3.6.1.4.1.14777.1.2.2

#### 1.4.1.14 IOT gailuarentzako ziurtagiria.

##### 1.4.1.14.1 Ziurtagiri ez-kualifikatua.

- **Deskribapena:** IoT ekosistemako objektuentzako identitatea sortzen duen ziurtagiria, eta sinatutako dokumentuen osotasuna eta jatorria bermatzen dituena.
- **Balio-aldia:** gehienez 10 urte.
- **Euskarria:** software bidez jaulkitakoa.

Deskribapen laburra	Euskarria	Politika-identifikatzailea	OID politika
Gailua	Software	NCP	1.3.6.1.4.1.14777.1.3.2

#### 1.4.1.15 Denbora zigilatze TSA/TSU ziurtagiria.

##### 1.4.1.15.1 Timestamp ziurtagiria.

- **Deskribapena:** pertsona juridiko baten zigilu elektronikoko ziurtagiria da, eta aktibatutako erabilera denbora-zigilatze elektronikorako.
- **Balio-aldia:** gehienez 5 urte.
- **Euskarria:** software bidez jaulkitakoa.

DESKRIBAPEN LABURRA	EUSKARRIA	POLITIKA-IDENTIFIKATZAILEA	OID POLITIKA
TSU ziurtagiria	Software	NA	1.3.6.1.4.1.14777.10.1 1.3.6.1.4.1.14777.53.1.3



#### 1.4.2 Ziurtagiriaren erabilera debekatuak

54. Ziurtagiriak soilik beren funtzio eta helburu zehatzetarako erabili behar dira, eta ezin dira beste funtzio edo helburu batzuetan erabili.
55. Era berean, ziurtagiriak aplikagarri den legeriarekin bat etorri soilik erabili behar dira.
56. Ziurtagiriak ez dira diseinatu, eta ezin dira erabilpen edo salmenta berrirako zuzenduta egon arriskutsuak diren egoerak kontrolatzeko tresna moduan, edo akatsik gabeko jarduerak behar dituzten erabileretan, hala nola zentral nuklearretako funtzionamenduan, nabigazio-sistemetako edo aireko komunikazioetako sistemetan, edo armamentuen kontrol-sistemetako erabileran, non hutsegite batek heriotza, kalte pertsonal edo ingurumen-kalte larriak eragin ditzakeen zuzenean.
57. Azken erabiltzailearen ziurtagiriak ezin dira inolako gako publikoaren ziurtagiri-mota sinatzeko erabili, ezta ziurtagiriak indargabetzeko zerrendak sinatzeko edo ziurtagiriak jaulkitzeko, berritzeko, eteteko edo indargabetzeko eskaerak sinatzeko erabili ere.

### 1.5 Politiken kudeaketa.

#### 1.5.1 Dokumentazioaren kudeaketarako arduraduna den erakundea.

58. Izenpe da (egoitza: Beato Tomás de Zumárraga kalea, 71, 1. solairua, CP 01008, Gasteiz. IFZ: A-01337260) DPCG hau aplikagarri duten ziurtagiriak jaulkitzen dituen ziurtapen-erakundea.

#### 1.5.2 Harremanetarako datuak.

Hornitzailearen izena	Ziurtapen eta Zerbitzu Enpresa - Empresa de Certificación y Servicios Izenpe SA
Posta-helbidea	Tomas Zumarraga Dohatsuaren kalea, 71, 1. solairua. 01008 Vitoria-Gasteiz
Helbide elektronikoa	<a href="mailto:izenpe@izenpe.eus">izenpe@izenpe.eus</a>
Telefono	900 840 123

59. Segurtasun-arazoak jakinarazteko, hala nola gakoa arriskuan jartzearen susmoa, ziurtagirien erabilera okerra, iruzurra edo beste gai batzuk, jarri harremanetan [incidencias@izenpe.eus](mailto:incidencias@izenpe.eus) helbidearekin.
60. Kontsultatu “4.9.3 Baliogabetze-eskaeren tratamendua.” atala baliogabetze-kanalak ezagutzeko.

#### 1.5.3 DPCGaren egokitzapenaren arduradunak

61. Izenperen Segurtasun Batzordea da adierazitako DPCG hau onartzeaz arduratzen den organoa, baita haren aldatetak, DPC bereziak eta PDS dokumentuak onartzeaz ere, baldin badaude.



#### 1.5.4 DPCGren onarpen-prozedura

62. Dokumentu honen azken aldaketak, DPCPak eta PDSak Izenperen Segurtasun Batzordeak onartzen ditu, ezarritako baldintzak betetzen direla egiaztatu ondoren.

## 1.6 Definizioak eta akronimoak.

### 1.6.1 Definizioak.

- **Ziurtapen Agintaritza (CA):** Erregistro Agintaritzaren eskaeraren arabera, modu automatizatuan eta Erregistro Agintaritzaren bermearekin, ziurtagiriak jaulkitzen dituen erakundea.
- **Erregistro Agintaritza (RA):** ziurtagirien eskatzaileak, harpidedunak eta gako-edukitzaileak identifikatzeko lanak egiteaz arduratzen den erakundea; ziurtagirietan dagoen informazioa egiaztatzen duen dokumentazioa egiaztatzen du, eta ziurtagiriak egiteko, ezeztatze eta berritzeko eskaerak baliozkotzen eta onartzen ditu. Erabiltzaileak erregistro-agintaritzara jo behar du ziurtagiri bat eskatzeko, erregistro-agintaritzari lotutako ziurtatze-agintaritzaren bermearekin.

- **Denbora Zigilatze Agintaritza (TSA):** denbora-zigiluak igortzen dituen agintaritza.

- **Ziurtagiria:** ziurtapen-zerbitzuen hornitzaile batek modu elektronikoa sinatutako dokumentu elektronikoa da, eta sinadura egiaztatze datuak sinatzaile bati lotzen dizkio, eta haren identitatea egiaztatzen du.

- **Oinarrizko ziurtagiria:** Izenperen hierarkian sartzen den ziurtapen-agintaritzaren harpideduna den ziurtagiria da, eta ziurtapen-agintaritza horren sinadura egiaztatze datuak barne hartzen ditu, ziurtapen-zerbitzuen hornitzaile gisa dituen sinadura sortzeko datuekin sinatuta. PKI hierarkiaren lehen eta oinarrizko ziurtagiria da. Automatikoki sinatzen du eta bitarteko edo azpiko CA agintaritzen ziurtagiriak sinatzeko balio du, zeinak azken ziurtagirien igorleak baitira.

Izenperen erakunde igorleek hierarkia bat osatzen dute, non ziurtagiri-mota guztientzat oinarrizko erakunde komun bat baitago eta azpiko hainbat erakunde baitaude, ziurtagiri-mota desberdinetarako.

- **Ziurtagiri kualifikatua:** eskatzaileen identitatea eta gainerako inguruabarrak egiaztatzeari eta ematen dituen ziurtatze-zerbitzuen fidagarritasunari eta bermeei dagokienez, eIDAS programan ezarritako baldintzak betetzen dituen konfiantzazko zerbitzu-emaile batek emandako ziurtagiri elektronikoa.
- **Ziurtagiri ez-kualifikatuak:** ziurtagiri arruntak dira, eta ez dute kualifikatutako ziurtagiriaren balio juridikorik.
- **Gakoa:** zifratze- eta deszifratze-operazioak kontrolatzeko erabiltzen diren sinbolo-sekuentzia.
- **Konfidentzialtasuna:** dokumentu elektronikoa bat erabiltzaile guztientzat eskuragarria ez izateko gaitasuna, salbu eta pertsona jakin batzuentzat. Horrela, komunikazioak besteek ez entzutea lor dezakegu, eta adierazitako hartzaileak bakarrik irakur ditzakeen dokumentuak bidali.
- **Kriptografia:** matematikaren adar bat da, eta irakurtzen den informazioa zuzenean irakurri ezin den informazio bihurtzen du, hau da, deszifratu egin behar da irakurri ahal izateko.



- **Sinadura sortzeko datuak (gako pribatua):** gako pribatu bat zenbaki bakar eta sekretu bat da, pertsona bakar bati dagokiona, eta, beraz, pertsona bere gako pribatuaren bidez identifika daiteke. Kode hori asimetrikoa da bere gako publikoarekin. Gako batek egiazta eta deszifra dezake besteak sinatu edo zifratu duena.
- **Sinadura egiaztatzeko datuak (gako publikoa):** gako publiko bat zenbaki bakar bat da, pertsona bakar bati dagokiona, baina, gako pribatua ez bezala, guztiek jakin dezakete. Prozedura matematikoen bidez gako pribatuarekin erlazionatzen da eta sinadura elektronikoak enkriptatu eta egiaztatzeko balio du.
- **Konfiantza Globaleko Praktiken Adierazpena (DPCG):** Izenpek adierazpen hori jendearen eskura jartzen du, erraz eskuratzeko moduan, bide elektronikoak erabilia eta doan. eIDASen esparruan, hauek zehaztuko dira: konfiantzazko zerbitzu-emaileek sinadura eta ziurtagiri elektronikoak sortzeko eta egiaztatzeko datuen kudeaketari dagokionez betetzeko konpromisoa hartu duten betebeharrak; ziurtagirien indarraldia eskatzeko, emateko, erabiltzeko eta iraungitzeko aplikatu beharreko baldintzak; segurtasun-neurri teknikoak eta antolaketa-neurriak; ziurtagirien indarraldiari buruzko informazio-profilak eta -mekanismoak, eta, hala badagokio, dagozkien erregistro publikoekin koordinatzeko prozedurak, aipatutako erregistroetan inskribatutako ahalordeei buruzko informazioa berehala trukatzeko aukera emango dutenak.
- **Ziurtagirien direktorioa:** ITU-T-ren X.500 estandarrari jarraitzen dion informazio-biltegia. Hala, Izenpek ziurtagirien direktorio eguneratu bat du, emandako ziurtagiriak adierazteko.
- **Sinadura sortzeko gailu kualifikatua:** sinadura elektronikoak sortzeko gailua, eIDAS Erregelamenduaren II. eranskinean zerrendatutako baldintzak betetzen dituenak.
- **Sinadura elektronikoak:** beste datu elektroniko batzuei erantsitako edo haiekin modu logikoan lotutako datuak, sinatzaileak sinatzeko erabiltzen dituenak.
- **Sinadura elektroniko aurreratua:** eIDAS Erregelamenduaren 26. artikuluan jasotako baldintzak betetzen dituen sinadura elektronikoak.
- **Sinadura elektroniko kualifikatua:** sinadura elektroniko aurreratua, sinadura elektronikoak sortzeko gailu kualifikatu baten bidez sortzen dena eta sinadura elektronikoak ziurtagiri kualifikatu batean oinarritzen dena.
- **Sinatzailea:** sinadura sortzeko gailu bat duen pertsona da, eta bere izenean edo ordezkatzeko duen pertsona fisiko edo juridiko baten izenean jarduten du.
- **Hash edo hatz-marka digitala:** mezu bati hash funtzio bat aplikatu ondoren lortzen den tamaina finkoko emaitza, hasierako datuei unibokoki lotuta dagoena.
- **HSM (Segurtasun kriptografikoko modulua):** gako kriptografikoak sortzen eta babesten dituen segurtasun-gailua da.
- **Gako publikoen azpiegitura (PKI, Public Key Infrastructure):** PKI batek zehazten du zer erakunde sartuko diren ziurtapen-sisteman, zer eginkizun duten erakunde horiek, zer arau eta protokolo bete behar diren sistemaren barruan jardun ahal izateko, nola kodetzen eta transmititzen den informazioa, zer informazio izango duten azpiegiturak kudeatutako objektuek eta dokumentuek. Hori guztia Gako Publikoaren teknologian oinarritzen da (bi gako).
- **Europako Parlamentuaren eta Kontseiluaren 2016/679 (EB) Erregelamendua, 2016ko apirilaren 27koa, datu pertsonalen tratamenduari dagokionez pertsona fisikoak babesteari**



eta datu horien zirkulazio askeari buruzkoa, 95/46/EE Zuzentaraua (DBEO) indargabetzen duena: Datu pertsonalen tratamenduari dagokionez, pertsona fisikoen askatasun publikoak eta oinarrizko eskubideak eta, bereziki, pertsona horien ohorea eta intimitate pertsonala eta familiarra bermatzea eta babestea helburu duen Europako Erregelamendua.

- **Ezeztatutako ziurtagirien zerrendak (CRLak):** zerrenda horretan, ezeztatze bat berehala egiten denetik Izenpek igortzen dituen ezeztatutako ziurtagirien zerrenda agertzen da. Web-zerbitzu bat ere badago, Izenpek ezeztatutako ziurtagirien eguneratze inkremental telematikoa kontsultatzeko aukera ematen duena. Ezeztatutako Ziurtagirien Zerrendak argitaratzeari dagokionez, ziurtagirien erabiltzaile eta harpidedunentzako sarbide segurua eta azkarra bermatzen da.
- **Ziurtagiriaren serie-zenbakia:** balio oso eta bakarra da, ziurtapen-zerbitzuen edozein zerbitzu-emailek emandako ziurtagiriari argi eta garbi lotua.
- **OCSP (Online Certificate Status Protocol):** ziurtagiri elektronikoko baten egoera egiaztatzea ahalbidetzen duen protokolo informatikoa da.
- **OID (Object Identifier):** puntu batez bereizitako osagai ez-negatibo osoek osatutako osagai aldakorren segida da. Objektu erregistratuei esleia dakieke, eta gainerako OI Den artean bakarrak izateko propietatea dute.
- **PIN (Personal Identification Number):** mekanismo horrek babesten duen baliabide batera sartu behar duen subjektuak bakarrik jakin dezakeen karaktere-sekuentzia.
- **Gako-edukitzaileak:** autentifikazio-gakoen eta sinadura elektronikoen zaintza duten edo haien erantzule diren pertsona fisikoak dira.
- **Konfiantzazko zerbitzuen emaile kualifikatua (TSP):** konfiantzazko zerbitzuen emailea, eIDAS Erregelamenduaren arabera kualifikatutako konfiantzazko zerbitzu bat edo batzuk ematen dituena, gainbegiratze-organismoak kualifikazioa eman dionean.
- **Egiaztapen aurreratuko zerbitzua:** zerbitzuaren Erakunde Erabiltzaileak Izenpek jaulkitako ziurtagirien erabileraz baliatzeko aukera du, ziurtagirien egoera OCSP (Online Certificate Status Protocol) protokoloan oinarrituz egiaztatuz.
- **Argitalpen zerbitzua:** ziurtapen-sistemarekin lotutako dokumentazioa argitaratzen den zerbitzua da, eta ziurtagirien erabiltzaileentzat eskuragarri egon behar duena.
- **Denbora-zigilu zerbitzua:** erakunde erabiltzaileari informazio jakin bat une jakin batean existitzen zela bermatzen dion zerbitzua.
- **Zerbitzari segurua:** web-zerbitzari bat da, non komunikazioa amaieratik amaierara modu seguruan zifratuta bidaltzen den. Operazio hau egiteko, zerbitzariak ziurtagiri bat izan behar du.
- **Ziurtagiriaren eskatzailea:** pertsona bat da, bere izenean edo erakunde baten izenean ziurtagiri bat jaulkitzeko eskaera egiten duena.
- **SSL (Secure Socket Layer):** Interneteko nabigatzaile baten eta web-zerbitzari baten arteko informazioa zifratuta transmititzeko protokolo bat da.
- **Ziurtagiriaren harpideduna:** pertsona bat da, bere nortasun pertsonala elektronikoki sinatutako datuekin lotuta dagoena, ziurtapen-zerbitzuen hornitzaileak ziurtagiri gako publiko baten bidez.



- **Txartel kriptografikoa:** sinadura sortzeko gailu segurutzat hartzen den txartela da, harpidedunak sinadura eta autentifikaziorako gako pribatua gordetzeko, sinadura elektronikoak sortzeko eta datu-mezuak deszifratzeko erabiltzen duena.
- **Konfiantza duten hirugarrenak:** Izenpek jaulkitako ziurtagiriak jasotzen dituzten pertsona fisiko edo juridikoak dira. Ziurtagirietan konfiantza duten hirugarrenak dira, eta, beraz, DPCGk ezarritakoa aplikatu behar zaie ziurtagiri horietan konfiantza izatea erabakitzen dutenean.
- **Ziurtagirien erabiltzaileak:** ziurtagiri elektronikoak jaulkitze, kudeaketa eta erabilerako zerbitzuen azken erabiltzaileak pertsona eta erakundeak dira.
- **Zigilu-sortzailea:** zigilu elektroniko bat sortzen duen pertsona juridikoa.
- **Zigilu elektronikoa:** formatu elektronikoko datuak, formatu elektronikoko beste datu batzuekin zerikusirik ez dutenak edo modu logiko batean haiekin zerikusia dutenak, azken horien jatorria eta osotasuna bermatzeko.
- **Zigilu elektroniko aurreratua:** eIDAS Erregelamenduaren 36. artikuluan jasotako eskakizunak betetzen dituen zigilu elektronikoa.
- **Zigilu elektroniko kualifikatua:** zigilu elektroniko aurreratua da, zigilu elektroniko kualifikatuak sortzeko gailu batekin sortua, eta zigilu elektronikoko ziurtagiri kualifikatu batean oinarritua.
- **Zigilu elektronikoa sortzeko datuak:** zigilu elektronikoa sortzen duen pertsonak zigilu hori sortzeko erabiltzen dituen datu bakarrak.
- **Zigilu elektronikoko ziurtagiria:** zigilu baten baliozkotze-datuak pertsona juridiko bati lotzen dizkion adierazpen elektronikoa, eta pertsona horren izena bermatzen duena.
- **Zigilu elektronikoaren ziurtagiri kualifikatua:** zigilu elektronikoaren ziurtagiria, konfiantzazko zerbitzuen emaile kualifikatu batek emana, eIDAS Erregelamenduaren III. eranskinean ezarritako baldintzak betetzen dituena.
- **Zigilu elektronikoa sortzeko gailua:** zigilu elektroniko bat sortzeko erabiltzen den ekipo edo programa informatikoa.
- **Zigilu elektronikoa sortzeko gailu kualifikatua:** zigilu elektronikoak sortzeko gailua, mutatis mutandis betetzen dituena eIDAS Erregelamenduaren II. eranskinean zerrendatutako baldintzak.
- **Denbora-zigilu elektronikoa:** formatu elektronikoa dauden datuak, beste datu batzuk une jakin batekin lotzen dituztenak, une horretan azken datu horiek existitzen zirenean frogatuta emanez.
- **Denbora-zigilu elektroniko kualifikatua:** eIDAS Erregelamenduaren 42. artikuluan ezarritako baldintzak betetzen dituen denbora-zigilu elektronikoa.

### 1.6.2 Akronimoak

- **ARL:** Ziurtapen Agintaritzen indargabetze-zerrenda.
- **CA:** Ziurtapen Agintaritzaren.
- **CN:** Common Name (izen arrunta).



- CRL: Certificate Revocation List (Ezeztatutako Ziurtagirien Zerrenda).
- DN: Distinguished Name (Izen bereizia).
- DPCG: Konfiantza Globaleko Praktiken Adierazpena.
- QSCD: Sinadura Sortzeko Gailu Kualifikatua.
- ETSI: European Telecommunications Standards Institute.
- GN: ziurtagiriko titularraren izen propioa.
- HSM: Hardware Security Module (Segurtasun Modulu Kriptografikoa).
- LRA: Tokiko Erregistro Agintaritza.
- OCSP: Online Certificate Status Protocol (Data eta ordu jakin batetik aurrera Ezeztatutako Ziurtagirien Argitalpen Zerbitzua).
- OID: Object Identifier (Objektu-identifikatzaile bakarra).
- PIN: Personal Identification Number (Identifikazio pertsonaleko zenbakia)
- PKCS: Public Key Cryptography Standards (RSA Laboratorios enpresak garatutako PKI estandarrak).
- PKI: Public Key Infrastructure (Gako Publikoaren Azpiegitura).
- PSC: Konfiantzazko Zerbitzu Hornitzailea.
- ETSI EN 319411-1 arauan (*General requirements*) definitutako ziurtapen-politikak:
  - NCP: Ziurtapen-politika estandarizatua, edozein transakziotan erabiltzen diren ziurtagiriak jaulkitzen dituzten hornitzaileek onartutako jardunbide egokien arabera betetzen duena.
  - NCP+: Ziurtapen-politika estandarizatu hedatua, NCP politikaren praktikak betetzen dituena, baina ziurtagiriak erabiltzeko gailu kriptografiko segurua behar duena.
  - OVCP: Erakundearen ziurtapen-politika balioztatua, erakunde eskatzaileak baliozkotzeko CABForum-en eskakizunak betetzen dituzten web-autentifikazioko ziurtagirietarako.
  - DVCP: Domeinu egiaztaturako ziurtapen-politika, web-autentifikazioko ziurtagirietarako, domeinuak egiaztatzeko CABForum-en eskakizunekin bat datorrena.
- Ziurtapen-politika kualifikatuak, ETSI EN 319411-2 arauan (*Requirements for trust service providers issuing EU qualified certificates*) definituta daudenak.
  - QCP-n: Pertsona fisikoentzako ziurtapen-politika kualifikatua, eiDAS Erregelamenduaren 26. eta 28. artikuluek xedatutako ziurtagiri kualifikatuetan oinarritutako sinadura elektronikoa aurreratuei dagokiena.
  - QCP-l: Pertsona juridikoentzako ziurtapen-politika kualifikatua, eiDAS Erregelamenduaren 36. eta 38. artikuluetan ezarritako ziurtagiri kualifikatuetan oinarritutako zigilu elektronikoa aurreratuei dagokiena.



- QCP-n-qscd: Pertsona fisikoentzako ziurtapen-politika kualifikatua, eiDAS Erregelamenduaren 3.12 artikuluan definitutako sinadura elektronikoko kualifikatuak aipatzen dituena.
  - QCP-l-qscd: Pertsona juridikoentzako ziurtapen-politika kualifikatua, eiDAS Erregelamenduaren 3.27 artikuluan definitutako zigilu elektronikoko kualifikatuak aipatzen dituena.
  - QEVCP-w: Web-autentifikaziorako ziurtagiri kualifikatuei buruzko ziurtapen-politika kualifikatua, eiDAS Erregelamenduaren 3.38 eta 45. artikuluetan definituta eta ETSI EN 319 411-2 arauaren 4.2.2.5 atalean deskribatua.
- RA: Erregistro Agintaritzaren zerbitzaria.
  - SSL: Secure Socket Layer .
  - TSA: Denbora Zigilatzeko Agintaritzaren zerbitzaria.



## 2 Informazio-biltegien argitalpena eta arduradunak.

---

### 2.1 Informazio-biltegia

63. Izenpek informazio publikoaren biltegi bat du [www.izenpe.eus](http://www.izenpe.eus) helbidean, eguneko 24 orduetan eta asteko 7 egunetan eskuragarri.

### 2.2 Ziurtapen-informazioaren argitalpena.

64. Izenpek bermatzen du DPCG, DPCP, PDS eta konfiantzazko zerbitzuen erabilerarako baldintza eta terminoen eskuragarritasuna [www.izenpe.eus](http://www.izenpe.eus) webgunean.

65. Izenpek bermatzen du erabiltzaileek eta harpidedunek ziurtagiriaren egoerari buruzko informazioa eskuratzeko aukera dutela modu seguru, azkar eta doakoan. Sarbide hori bi modutara egin daiteke:

- Online kontsulta (OCSP): Izenpek igorritako ziurtagirien egoera kontsultatzeko zerbitzu azkar eta segurua eskaintzen du, ziurtagirietan konfiantza duten hirugarrenen eskura.
- Offline kontsulta (CRL): Ezeztatutako Ziurtagirien Zerrenden (CRL) argitalpenaren bidez egiten da.

66. Izenpek proba-inguruneak eskaintzen ditu software-hornitzaileek beren produktuak SSL/TLS ziurtagiriekiko ekoizpen-ingurunean probatu ahal izan ditzaten. Izenpek hainbat gune mantentzen ditu, gutxienez honako hauek dituztenak: ziurtagiri final aktibo bat, iraungitakoa eta ezeztatutakoa. Kontsultatu web-autentifikaziorako ziurtagirien DPG berezia.

#### 2.2.1 Argitalpen- eta jakinarazpen-politika

67. Zerbitzuaren zehaztapenetan edo baldintzetan egindako aldaketak Izenpek erabiltzaileei jakinaraziko dizkie [www.izenpe.eus](http://www.izenpe.eus) webgunearen bidez. Egoera jakinetan, komunikaziorako kanal osagarriak ezar daitezke.

68. DPCG eta Erabilera Baldintzak eta Terminoak dokumentuei dagokienez, Izenpek bertsioren historial publikoa mantenduko du [www.izenpe.eus](http://www.izenpe.eus) webgunean.

#### 2.2.2 Ziurtapen Globaleko Praktiken Adierazpenean argitaratu gabeko elementuak.

69. Osagai, azpiosagai eta elementuen zerrenda, isilpekoak direlako jendearen eskura ez daudenak, DPCG honen “9.2.5 Irismenean ez dagoen informazioa.” atalean aipatutakoak dira.

### 2.3 Argitalpen-maiztasuna.

70. DPCG onartzen den unean argitaratzen da, eta urteko berrikuspenean aldaketarik ez badago. Aldaketak dokumentu honetan ezarritako irizpideen arabera arautzen dira.

71. Ziurtagirien egoerari buruzko informazioa dokumentu honetako “4.9.7 CRLen sorreraren maiztasuna.” eta “4.9.9 Online baliogabetze-berrespenaren eskakizunak.” ataletan ezarritakoaren arabera argitaratzen da.



#### **2.4 Biltegiako sarbide-kontrola.**

72. Izenpek aukera ematen du bere biltegiari argitaratutako informazioa irakurtzeko, eta kontrolak ezartzen ditu baimenik ez duten pertsonak zerbitzu honetako erregistroak gehitu, aldatu edo ezabatu ez ditzaten eta gordetako informazioaren osotasuna eta benetakotasuna babesteko.

73. Izenpek sistema fidagarriak erabiltzen ditu informazio-biltegiari sartzeko, eta, beraz:

- Baimendutako pertsonak bakarrik egin ditzakete oharrak eta aldaketak.
- Informazioaren egiazkotasuna egiaztatu ahal izatea.
- Ziurtagiriak kontsultatzeko moduan daude.
- Segurtasun-baldintzetan eragina izan dezakeen edozein aldaketa tekniko detektatu ahal izatea.



### 3 Identifikazioa eta autentifikazioa.

---

#### 3.1 Izenak.

##### 3.1.1 Izen-motak

74. Erakundearen azken ziurtagiriek guztiak izen bereizi bat daukate Subject Name eremuan.
75. Subject eremuko izen bereizi hori osatzen duten atributuak ziurtagiriaren profilari buruzko atalean jasotzen dira.
76. *Common Name* eremuaren balio autentikatua harpidedunaren izena da, eta hala badagokio, sinatzailearena.
77. Subject Alternative Name luzapenean normalean ziurtagiriaren harpidedun gisa agertzen den pertsona beraren identitate alternatiboak sartzen dira.

##### 3.1.2 Izenen esanahia.

78. Subject Name eremuko izen bereizi (DN) guztiak esanguratsuak dira. Ziurtagiriaren harpidedunari lotutako atributuen deskribapena giza irakurketarako egokia da (ikus dokumentu honetako izenen Izenen formatuak. atala).

##### 3.1.3 Ezizenak.

79. Ziurtagiriek ez dute onartzen sinatzailearentzako ezizenik erabiltzea, salbuespen gisa, ezizena duen enplegatu publikoaren ziurtagirietan izan ezik.

##### 3.1.4 Izen-formatuak interpretatzeko arauak.

80. Ziurtagiri bateko subject-ak pertsona fisikoa edo juridikoa, edo gailua identifikatzen du. Izenpek badu izen edo ezizen horien eta izendatutako erakundeen arteko lotura egiaztatzen duen froga. Izenek ezin dute izan engainagarriak. Horrek ez ditu kanpoan uzten "3.1.5 Izenen bakartasuna" atalean zehaztutako ezizen-ziurtagiriak.
81. Webguneen autentifikazio-ziurtagirietan, kontuan hartu beharko dira CABForum-en eskakizunak (Baseline Requirements eta EV Guidelines).

##### 3.1.5 Izenen bakartasuna

82. Harpidedunen eta hala badagokio sinatzaileen izenak ziurtagiri-mota bakoitzeko bakarrak izan behar dira. Common Name (CN) eremuan izenen bakartasunari eta espazioen erabilerari buruzko baldintzak bete behar dira. Izenpek ezizen-ziurtagiriak jaulki ditzake, baina ezin dira izan CA edo menpeko CA ziurtagiriak. Ziurtagiri-mota bakoitzaren profil-xehetasunak hemen kontsulta daitezke: [www.izenpe.eus](http://www.izenpe.eus).

##### 3.1.6 Marka erregistratuen izenei eta tratamenduari buruzko gatazkak ebaztea.

83. Ziurtagiri-eskatzaileek ez dute jaulkipen-eskaeretan hirugarrenen eskubideak urratzea ekar dezakeen izenik sartu behar etorkizuneko harpidedunarentzat.
84. Izenpek ez du zehazten ziurtagiri-eskatzaile batek eskubiderik duen ziurtagiri-eskaera batean agertzen den izenaren gainean. Era berean, ez du epaile edo bitartekari gisa jarduten, eta ez du beste inola ere konpontzen pertsonen edo erakundeen izenen edo domeinu-izenen jabetzari buruzko eztabaidarik.
85. Izenpek eskubidea du ziurtagiri-eskaera bat atzera botatzeko, izen-gatazka dela eta.



### 3.1.7 Jaulkitzailea (Issuer).

86. Eremu honetan Izenperen identifikazioa dago, ziurtagiria sinatu eta igorri duen ziurtapen-erakundearena.
87. Eremuak ezin du hutsik egon eta nahitaez izen bereizi bat du (DN), atributu-multzo batez osatua, izen edo etiketa bat eta lotutako balio bat.
88. Menpeko CAen issuer eremua bat dator ziurtagiri horiek jaulki dituen CAren subject eremuarekin.

### 3.1.8 Gaia (Subject).

89. Eremu honetan Izenpek jaulkitako ziurtagiriaren harpidedunaren edo titularraren identifikazioa dago (eremu horretako Issuer eremuan identifikatutako CA).
90. Eremuak ezin du hutsik egon eta nahitaez izen bereizi bat du (DN). Izen bereizi batek atributu-multzo bat du, izen edo etiketa bat eta horri lotutako balio bat.

## 3.2 Identitatearen balidazioa.

### 3.2.1 Gako pribatuaren jabetza egiaztatzeko metodoak.

91. Gako-parea hauek sortzen badute:
  - Erregistro-erakunde batek, eta gakoak txartel kriptografiko batean badaude kokatuta: gako pribatuaren jabetza txartel kriptografikoa eta dagokion ziurtagiria eta barruan gordetako gako-parea entregatu eta onartzeko prozedura fidagarriaren bidez frogatzen da.
  - Erregistro-erakunde batek, eta gakoak HSM batean badaude: gako pribatuaren jabetza HSMn gordetzeko prozedura fidagarriaren bidez frogatzen da, bai eta harpidedunak edo, hala badagokio, sinatzaileak gakoetarako sarbide eskusiboaren bidez ere.
  - Ziurtagiriaren sinatzaileak berak: gako pribatuaren jabetza frogatzeko, ziurtagiria behar bezala erabili behar da.
  - Gailu mugikorreko gakoaren edukiontzia bidez: gako pribatuaren jabetza egiaztatzeko, gako-parea sortzeko eta ziurtagiria emateko prozedura fidagarria erabiltzen da.

### 3.2.2 Erakundearen identitatearen autentifikazioa

92. Izenpe Batzordearen 2015eko irailaren 8ko 2015/1502 (EB) Betearazpen Erregelamenduaren zehaztapenetan oinarritzen da; erregelamendu hori identifikazio elektronikorako bitartekoaren segurtasun-mailetarako gutxieneko espezifikazio eta prozedura teknikoak ezartzeari buruzkoa da, eIDAS Erregelamenduaren 8. artikulua 3. apartatua xedatutakoaren arabera.
93. [www.izenpe.eus](http://www.izenpe.eus) webgunean argitaratzen da erakunde bakoitzak zer dokumentazio aurkeztu behar duen bere konfigurazio juridikoaren arabera.
94. Erakundearen identitatea erakunde-motaren arabera eskatzen diren agirien bidez egiaztatuko da.
95. Informazio gehiago: PDSetan.



#### 3.2.2.1 Domeinuaren balidazioa.

96. Webguneen autentifikazio-ziurtagirietan, dagokion PDSan deskribatzen da web-domeinuaren baliozkotzea.

#### 3.2.3 Pertsona fisiko eskatzailearen identitatearen autentifikazioa..

97. Izenpe Batzordearen 2015eko irailaren 8ko 2015/1502 (EB) Betearazpen Erregelamenduaren zehaztapenetan oinarritzen da; erregelamendu hori identifikazio elektronikorako bitartekoen segurtasun-mailetarako gutxieneko espezifikazio eta prozedura teknikoak ezartzeari buruzkoa da, eIDAS Erregelamenduaren 8. artikulua 3. apartatua xedatutakoaren arabera.

98. Informazio gehiago Identitatea Egiatzatzeko Zerbitzuaren Praktiken Adierazpenean eta PDSetan.

99. Izenpek eskatzailearen identitatea egiaztatuko du,

- Aurrez aurre.
- Emate-eskaera notario bidez sina dadin legitimatzea.
- Indarrean dagoen ziurtagiri kualifikatu baten bidez
- Bideo bidezko urruneko identifikazioarekin.

#### 3.2.4 Sinatzailearen balioztatu gabeko informazioa

100. Oro har, ziurtagirietako informazioa eman aurretik egiaztatzen da, eta informazio-iturriekin alderatzen da. PDSak daudenean, horri buruz zehaztutakoa hartuko da kontuan.

#### 3.2.5 Autoritatearen balidazioa.

101. Dagokion lege-tresna sinatuko da; bertan, erregistroa eskuordetzeko baldintzak eta operadoreen erantzukizunak zehaztuko dira.

102. Erregistro-agintariek honako hauek egin beharko dituzte:

- Operadoreak egiaztatu.
- Izenpek emandako ziurtagiri kualifikatu bat eman.
- Prestakuntza nahikoa jaso dutela ziurtatu.
- Izenperi dokumentazioa bidaltzen zaiola ziurtatu.

#### 3.2.6 Interoperaziorako irizpideak.

103. Ez dago interaktibitate-harremanik Izenperekin zerikusirik ez duten ziurtapen-agintaritzekin.

### 3.3 Gakoak berriz ematea eskatzeko identifikazioa eta autentifikazioa.

#### 3.3.1 Berritze arrunta.

#### 3.3.2 Baliogabetze baten ondoko berritzea.

104. Ziurtagiria baliogabetu ondoren berritzeko prozesua hasierako jaulkipen-prozesuaren berdina izango da.



### **3.4 Baliogabetze-eskaerarako identifikazioa eta autentifikazioa.**

105. Baliogabetze-eskaeraren autentifikazio-baldintzak dagokion PDS dokumentuan garatzen dira.



## 4 Ziurtagirien bizi-zikloaren eskakizun operatiboak.

---

Dokumentu honetako DPCG honek Izenpek jaulkitako ziurtagiriek betebeharreko eskakizun operatibo komunak arautzen ditu.

Izenpek kanpoko CA batekin cross-certification bat egingo balu, CA horri DPCG, PDS eta DPSV dokumentuetan jasotako eskakizun guztiak betetzea eskatuko dio.

### 4.1 Ziurtagiri-eskaera.

106. Ez da beharrezkoa izango ziurtagiri-eskaera berria egitea, ziurtagiria berriz jaulkitzen den kasuetan jaulkipen- edo banaketa-akats teknikoek ondorioz baliogabetu bada, edo ziurtagiriarekin zerikusia duen dokumentazioaren akatsen ondorioz.

107. Ziurtagiri bakoitzaren edukian ezarritako muga teknikoek barruan, dagokion identifikazio-datuak zehaztasunez jasoko dira.

#### 4.1.1 Eskaeraren egiaztapena.

108. Ziurtagiria jaulki aurretik, Izenpek eskaeran jasotako datuak egiaztatuko ditu, DPCG, DPCP eta PDS dokumentuetan adierazitakoaren arabera.

#### 4.1.2 Izena emateko prozesua eta erantzukizunak.

109. Ziurtagirian jasotako informazioa identifikatzeko eta egiaztatzeko lanak, bai eta jaulkipen-, baliogabetze- eta berritze-eskaeren baliozkotzea eta onarpena, Izenperen erregistro-erakundeek edo Izenpek legezko tresna egokia sinatzen duen erakunde erabiltzaileek egingo dituzte. Azken horiek (erakunde erabiltzaileek) betebeharrak hauek izango dituzte:

- Eskatzailearen, harpidedunaren eta sinatzailearen identitatea eta bestelako inguruabar pertsonalak egiaztatzea, ziurtagirietan jasotakoak edo ziurtagirien xedeetarako garrantzitsuak direnak, prozedura hauen arabera.
- Ziurtagirien jaulkipenarekin, berritzearekin, baliogabetzearekin edo berraktibazioarekin lotutako informazio eta dokumentazio guztia gordetzea.
- Ziurtagiriak baliogabetzeko eskaerak Izenperi azkar eta modu fidagarrian jakinaraztea, behar den arduraz jardunez.
- Izenpek artxiboetarako sarbidea izatea eta bere funtzioak betetzeko prozeduren auditoria egitea ahalbidetzea, baita horretarako beharrezko informazioa mantentzea ere.
- Izenperi jakinaraztea jaulkipen-, berritze-, berraktibazio-eskaerak eta ziurtagiriei eragiten dien edozein beste alderdi.
- Ziurtagirien indarraldian eragina izan dezaketen baliogabetze-arrazoiak egiaztatzea, dagokion zorrotasunarekin.
- Ziurtagiriak jaulkitzeko, berritzeko eta baliogabetzeko kudeaketa-lanetan, Izenpek ezarritako prozedurak eta indarreko legeria betetzea.
- Ziurtagiri-motak hala eskatzen badu, harpidedunari eta/edo sinatzaileari sinadura elektronikoaren sorrerako eta egiaztapenerako prozedura teknikoak eskura jartzeko eginkizuna bere gain hartzea.



## 4.2 Eskaeren kudeaketa.

### 4.2.1 Identifikazio- eta autentifikazio-funtzioak betetzea.

110. Harpideduna behar bezala identifikatzea Izenperen ardura da, DPSV dokumentuan ezarritakoaren arabera. Eskaerak onartu edo baztertzea.
111. Ziurtagiri-eskaera bat jasotakoan, Erregistro Agintaritzak (RA) eskatzaileak emandako informazioa egiaztatu beharko du, harpidedunaren nortasunaren baliozkotzea barne.
112. Informazioa ez bada zuzena, RAK eskaera ukatuko du, eta eskatzailearekin harremanetan jarriko da arrazoia jakinarazteko. Informazioa zuzena bada, ziurtagiria jaulkiko da.
113. Zerbitzari baten autentifikaziorako domeinu-izena duen ziurtagiria eskatzen denean, Izenpek aztertuko du RFC 6844 arauan ezarritako CAA erregistroa (Certification Authority Authorization). CAA erregistroak Izenperi ziurtagiri horiek jaulkitzea baimentzen ez badio, ziurtagiria ez da jaulkiko. Hala ere, eskatzaileei aukera emango zaie berriz eskaera egiteko, gorabehera hori konponduta.

### 4.2.2 Eskaerak prozesatzeko denbora.

114. Eskaera onartzen denetik ziurtagiria jaulkitzen den arte ez da igaro behar hilabetetik gorako denbora-tartea. Nolanahi ere, DPCP edo PDS bakoitzak zehaztuko du alderdi hau bere edukian.

## 4.3 Ziurtagiriaren jaulkipena.

115. Ziurtagiri bat jaulkitzeak eskaeraren azken eta osoko onarpena dakar. Izenpek ziurtagiria jaulkiko du dokumentu honetan (DPCG), dagozkion DPCP eta PDSetan ezarritakoaren arabera. Halaber, Izenpek harpidedunari (edo sinatzaileari, ziurtagiri profesionalen kasuan) emango dizkio ziurtagiriak eta/edo desblokeatzeko kodeak, gakoak Izenpek sortzen baditu.
116. Eskatzaileak ez badu jakinarazpenik jaso ziurtagiriaren jaulkipenez, Izenperekin harremanetan jarri beharko du.

### 4.3.1 CAren jarduerak jaulkipenean zehar

117. Izenpek ziurtagiri-mota bakoitzerako ezarritako jaulkipen-prozedurak beteko ditu, DPCG, DPCP eta DPSV dokumentuetan jasotakoaren arabera.

### 4.3.2 Ziurtagiriaren jaulkipena egingo da dagokion DPCP edo PDS dokumentuan jasotako baldintzen arabera.

118. Izenpek ziurtagiriaren jaulkipena jakinaraziko dio harpidedunari eta/edo sinatzaileari.

### 4.3.3 Ziurtagiria egiaztatzea

119. Sinatzaileak behar bezala funtzionatzen duela egiaztatuko du, eta, behar izanez gero, funtzionamendu-akatsen berri emango dio Izenperi.
120. Funtzionamendu-akatsak arrazoi teknikoengatik badira (besteak beste, ziurtagiriaren euskarriak gaizki funtzionatzeagatik, ziurtagirian akats teknikoa egiteagatik, etab.) edo ziurtagirian dauden eta Izenperi aplikatu dakizkiokeen datuetan akatsak egonez gero, Izenpek ziurtagiria baliogabetuko du eta beste bat jaulkiko du, horren ondoriozko kostuak bere gain hartuta.



#### 4.4 Ziurtagiriaren onarpena

121. Ziurtagiriaren onarpenak esan nahi du harpidedunak onartzen duela Izenperen eta harpidedunaren arteko eskubideak eta betebeharrak arautzen dituen kontratuan jasotako baldintzak eta terminoak, eta ezagutzen duela DPCG hau, Izenpek ematen dituen ziurtapen-zerbitzuak teknikoki eta operatiboki arautzen dituen dokumentua.

##### 4.4.1 Ziurtagiriaren onarpen-prozesua

122. Ziurtagiri-eskaeraren dokumentua sinatzean, onartzen dira baita ere erabilera-baldintzak eta terminoak, [www.izenpe.eus](http://www.izenpe.eus) webgunean eskuragarri daudenak.

##### 4.4.2 Ziurtagiria CAk argitaratzea.

123. Ziurtagiria harpidedunak onartu eta sortu ondoren, Izenperen barne-biltegietan argitaratuko da.

124. Edozeinek eskura dezake ziurtagiriaren egoerari buruzko informazioa, VA edo CRL kontsultatuz.

##### 4.4.3 CAk beste erakunde batzuei ziurtagiriaren jaulkipena jakinaraztea.

125. Zerbitzari Seguruaren ziurtagiriak (SSL) Certificate Transparency Log Server zerbitzuan (CT) argitaratzen dira, Googleren gidalerroen arabera. Gainerako ziurtagiriak ez zaizkio ezein erakunderi jakinarazten.

#### 4.5 Gako-parea eta ziurtagiriaren erabilerak

##### 4.5.1 Harpidedunaren gako pribatua eta ziurtagiriaren erabilera.

126. Bere gakoak zaintzen dituen harpidedunak:

- Ziurtagirien euskarriak ondo erabiltzea eta zaintzea bermatuko du.
- Ziurtagiria modu egokian erabiliko du eta, bereziki, erabilera-mugen arabera jardungo du.
- Gako pribatua behar bezala zainduko du, baimenik gabeko erabilerak saihesteko, DPCGren 6.1, 6.2 eta 6.4 ataletan ezarritakoaren arabera.
- Izenperi eta ziurtagirian konfiantza izan dezakeen edozein pertsonari berehala jakinaraziko dio, atzerapenik gabe:
  - Bere gako pribatuaren galera, lapurreta edo arriskua.
  - Gako pribatuaren gaineko kontrola galtzea, aktibazio-datuak arriskuan jartzeagatik (adibidez, gailu kriptografikoaren PIN kodea) edo beste edozein arrazoiengatik.
  - Ziurtagiriaren edukian dauden zehaztasun-gabeziak edo aldaketak, horiek baliogabetze-arrazoia badira, ziurtagiriaren baliogabetzea eskatuz.
- Ziurtagiriaren balio-epea amaitzen denean, gako pribatua erabiltzen uzteko konpromisoa hartuko du.
- Sinatzaileei transferituko dizkie haien betebeharrak espezifikoak.



- Ez du kontrolatuko, manipulatu edo egingo ziurtapen-zerbitzuen ezarpen teknikoari buruzko atzeranzko ingeniarietzako egintzarik, ziurtapen-erakundearen aurretiazko idatzizko baimenik gabe.
- Ez du nahita arriskuan jarriko ziurtapen-zerbitzuen segurtasuna.
- Ez ditu erabiliko ziurtagirietan jasotako gako publikoei dagozkien gako pribatuak beste ziurtagiriaren bat sinatzeko, Ziurtapen Erakunde bat balitz bezala.
- Ziurtagirian zerrendatutako gako publikoari dagokion gako pribatua erabiliz sinadura elektronikoak sortzen dituen ziurtagiri kualifikatuen harpidedunak aitortu behar du, dagokion tresna juridikoan, sinadura elektroniko horiek eskuz idatzitako sinaduren baliokideak direla, betiere gailu kriptografikoa erabiltzen bada, eIDAS Erregelamenduan adierazitakoaren arabera.

#### 127. Bere gakoak Izenperen gordeta dituen harpidedunak:

- Ziurtagiria modu egokian erabiliko du, eta bereziki, ziurtagiriaren erabilera-mugak beteko ditu.
- Aktibazio-gakoa behar bezala zainduko du, baimenik gabeko erabilerak saihesteko, DPCGren 6.1, 6.2 eta 6.4 ataletan ezarritakoaren arabera.
- Izenperi eta ziurtagirian konfiantza izan dezakeen edozein pertsonari berehala jakinaraziko dio, atzerapenik gabe:
  - Gako pribatuaren gaineko kontrola galtzea, aktibazio-datuak arriskuan jartzeagatik edo beste edozein arrazoirengatik.
  - Ziurtagiriaren edukian dauden zehaztasun-gabeziak edo aldaketak, horiek baliogabetze-arrazoia badira, ziurtagiriaren baliogabetzea eskatuz.
- Ziurtagiriaren balio-epea amaitzen denean, gako pribatua erabiltzen uzteko konpromisoa hartuko du.
- DPCG honetan zehaztutako betebeharrak onartuko ditu.
- Ez du kontrolatuko, manipulatu edo egingo ziurtapen-zerbitzuen ezarpen teknikoari buruzko atzeranzko ingeniarietzako egintzarik, ziurtapen-erakundearen aurretiazko idatzizko baimenik gabe.
- Ez du nahita arriskuan jarriko ziurtapen-zerbitzuen segurtasuna.
- Ziurtagirian zerrendatutako gako publikoari dagokion gako pribatua erabiliz sinadura elektronikoak sortzen dituen ziurtagiri kualifikatuen harpidedunak aitortu behar du, dagokion tresna juridikoan, sinadura elektroniko horiek eskuz idatzitako sinaduren baliokideak direla, betiere sinadura sortzeko gailu kualifikatu bat erabiltzen bada, eIDASen agindutakoaren arabera.

#### 4.5.2 Gako publikoaren eta ziurtagiriaren erabilera – Hirugarrenen konfiantza

128. Ziurtagirietan konfiantza duten erabiltzaile egiaztatzaileek honako betebeharrak dituzte:



- Modu independentean aholkatzea, ziurtagiria aurreikusitako erabilerarako egokia den ala ez zehazteko.
- Ziurtagiriaren erabilera-baldintzak ezagutzea, DPCG dokumentuan ezarritakoaren arabera.
- Jaulkitako ziurtagirien baliozkotasuna edo baliogabetzea egiaztatzea, ziurtagiriaren egoerari buruzko informazioa erabiliz.
- Ziurtagiri-hierarkiako ziurtagiri guztiak egiaztatzea, sinadura elektronikoko batean edo hierarkiako beste edozein ziurtagiritan konfiantza izan aurretik.
- Ziurtagiriaren erabilera-murrizketak kontuan hartzea, haiek ziurtagiriaren beraren barruan egon ala ez.
- Edozein kontratu edo beste tresna juridikotan ezarritako neurriak eta oharrak kontuan hartzea, haien izaera juridikoa edozein izanik ere.
- Ziurtagiriari buruzko edozein gertaera edo egoera anomalo jakinaraztea, baliogabetze-arrazoi izan daitezkeenak.
- Ez monitorizatzea, manipulazioak ez egitea edo alderantzizko ingeniari-tza-prozedurarik ez gauzatzea, Izenperen ziurtagiriaren zerbitzuen ezarpen teknikoaren gainean, aurrezko idatzizko baimenik gabe.
- Ez arriskuan jartzea nahita ziurtagiriaren zerbitzuen segurtasuna.
- Sinadura elektronikoko horiek eskuz idatzitako sinaduren baliokideak direla onartzea, eIDAS Erregelamenduaren arabera.

#### 4.6 Ziurtagiriak berritzea

129. Ziurtagiria berritzeko, harpidedunari beste ziurtagiri bat egin behar zaio, ziurtagirian agertzen den informazioa aldatu gabe. Ziurtagiri-motaren arabera, balio-epea desberdina izan daiteke. Jaulkipen-kostuak [www.izenpe.eus](http://www.izenpe.eus) webgunean adierazita daude.

130. Ziurtagiria iraungi aurreko 60 eguneko epean, berritu ahal izango da.

131. Izenpek aurreikusitako jaulkipen- eta entrega-prozeduraren arabera izapidetuko du berritze-prozesua.

##### 4.6.1 Ziurtagiria berritzeko inguruabarrak.

132. Izenpek ahalegin arrazoizkoak egiten ditu harpidedunei ziurtagiriaren iraungitze hurbila jakinarazteko. Jakinarazpena normalean ziurtagiriaren iraungitze-dataren aurreko 60 egunetan egingo da.

##### 4.6.2 Nork eska dezake berritzea

133. Edozein harpidedunek eska dezake bere ziurtagiria berritzeko, DPCG honetan deskribatutako baldintzak betetzen badira. Izenpek ez du ziurtagiririk automatikoki berritzen.

##### 4.6.3 Ziurtagiriaren berritze-eskaeren tratamendua.

134. Harpidedunak Izenperekin harremanetan jarri eta berritze-eskaera egin ahal izango du. Izenpek eskaera nola formalizatu jakinaraziko dio.



#### 4.6.4 Harpidedunari jakinaraztea.

135. Ziurtagiri berrien eskaeretakako jakinarazpen-prozedura bera erabiliko da.

#### 4.6.5 Berritutako ziurtagiri baten onarpen-prozedura.

136. Ziurtagiri berrien eskaeretakako erabiltzen den onarpen-prozedura bera aplikatuko da.

#### 4.6.6 Ziurtagiria argitaratzea.

137. Ziurtagiria berritu ondoren, ziurtagiri berria argitaratuko da ziurtagiri berrien barne-biltegi berean.

#### 4.6.7 Beste erakunde batzuei jakinaraztea.

138. 4.4.3 atalean jasotakoaren arabera egingo da.

### 4.7 Ziurtagiriaren gakoak berritzea eta berreskuratzea.

139. “Re-key” prozesuak ziurtagiri berri bat sortzea dakar, gako publiko eta serie-zenbaki berri batekin, baina aurreko ziurtagiriaren subject edukia mantenduz. Ziurtagiri berriak baliozkotasun-datu berriak eta gako-pare berria izango ditu, baina subject bera mantenduko du.

140. Gakoak ziurtagiriaren berritze-prozesuan berrituko dira, DPS dokumentuan jasotakoaren arabera.

#### 4.7.1 Ziurtagiriaren gakoak berriz sortzeko inguruabarrak.

141. Ziurtagiriaren gakoak berriz sortuko dira ziurtagiria berritzeko prozesuaren barruan, DPCGko 3.2 atalean adierazitakoaren arabera. Ziurtagiriaren gakoak arriskuan daudenean ere berregin ahal izango dira.

#### 4.7.2 Nork eska dezake.

142. Izenpek CAen ziurtagirien gakoak birsor ditzake, CA berria edo azpikategoria sortzeko zeremonia-dokumentuaren arabera. Halaber, VA eta TSA zerbitzuen ziurtagirien gakoak birsor ditzakezu, barne-prozeduran ezarritakoaren arabera.

143. Edozein harpidedunek eska dezake bere ziurtagiria berritzeko, DPCG honetan deskribatutako baldintzak betetzen badira.

#### 4.7.3 Gakoak berriro sortuz berritzeko eskaeren tratamendua.

144. Harpidedunak Izenperekin harremanetan jarri eta berritze-eskaera egin ahal izango du. Izenpek jakinaraziko dio nola formalizatu bere eskaera. Harpidedunari jakinaraztea.

145. Ziurtagiri berrien eskaeretakako jakinarazpen-prozedura bera erabiliko da.

#### 4.7.4 Berritutako ziurtagiriaren onarpen-prozedura.

146. Ziurtagiri berrien eskaeretakako erabiltzen den onarpen-prozedura bera aplikatuko da.

#### 4.7.5 Ziurtagiria argitaratzea.

147. Ziurtagiria berritu ondoren, ziurtagiri berria argitaratu ahal izango da beharrezkotzat jotzen diren ziurtagiri-biltegietan.

148. Beste erakunde batzuei jakinaraztea.

149. 4.4.3 atalean jasotakoaren arabera egingo da.



#### 4.8 Ziurtagiria aldatzea

150. Ziurtagiriko daturen bat aldatu beharra dagoenean, Izenpek ziurtagiria baliogabetuko du eta berri bat jaulkiko du.

##### 4.8.1 Ziurtagiriaren aldaketarako inguruabarrak.

151. Ez da aurreikusten ziurtagiriaren aldaketa.

##### 4.8.2 Nork eska dezake ziurtagiriaren aldaketa

152. Ez da aurreikusten ziurtagiriaren aldaketa.

##### 4.8.3 Ziurtagiriaren aldaketa-eskaeren tratamendua.

153. Ez da aurreikusten ziurtagiriaren aldaketa.

##### 4.8.4 Ziurtagiriaren aldaketaren jakinarazpena.

154. Ez da aurreikusten ziurtagiriaren aldaketa.

155. Ziurtagiriaren aldaketa onartutzat jotzeko jokabidea.

156. Ez da aurreikusten ziurtagiriaren aldaketa.

##### 4.8.5 Aldatutako ziurtagiriaren argitalpena.

157. Ez da aurreikusten ziurtagiriaren aldaketa.

##### 4.8.6 Ziurtagiriaren aldaketa beste erakunde batzuei jakinaraztea.

158. Ez da aurreikusten ziurtagiriaren aldaketa.

#### 4.9 Baliogabetua.

##### 4.9.1 Baliogabetzeko egoerak

159. Izenpek ziurtagiriak baliogabetuko ditu honako kasu hauetan:

- Sinatzaileak, honek ordezkaturako pertsona fisiko edo juridikoak, baimendutako hirugarren batek edo pertsona juridiko baten zigilua edo SSL ziurtagiria eskatzen duen pertsona fisikoak hala eskatzen duenean.
- Sinatzailearen edo ziurtapen-zerbitzuen hornitzailearen sinadura sortzeko datuak urratzen edo arriskuan jartzen direnean, edo sinatzaileak edo hirugarren batek datu horiek modu desegokian erabiltzen dituenean.
- Epai judizial edo administratibo baten bidez agintzen denean.
- Sinatzailea hiltzen denean edo nortasun juridikoa azkentzen zaionean, ordezkaturak hiltzen denean edo nortasun juridikoa azkentzen zaionean, sinatzailea edo ordezkaturak erabat edo zati batean ezgaituta geratzen denean, ordezkaturak amaitzen denean, ordezkaturako pertsona juridikoa desegiten denean edo pertsona juridiko bati egindako ziurtagirietan islatzen diren sinadura sortzeko datuen zaintza edo erabilera-baldintzak aldatzen direnean.



- Izenpek jarduera uzten duenean, salbu eta, sinatzailearen alde aurreko baimenarekin, hark jaulkitako ziurtagiri elektronikoen kudeaketak beste ziurtagiri-zerbitzuen emaile bati transferitzen bazaizkio.
- Ziurtagiria lortzeko aurkeztutako datuak aldatzen direnean, edo ziurtagiria jaulkitzeko egiaztatutako inguruabarrak aldatzen direnean.
- Ziurtagiria galtzen, lapurtzen edo hondatzen denean, euskarrian kalteak gertatzen direlako, edo ziurtagiriaren euskarriaren aldaketa bat gertatzen bada eta hori ez badago aurreikusita ziurtapen-politikan.
- Alderen batek bere betebeharrak betetzen ez dituenean.
- Ziurtagiria jaulkitzeko prozesuan akats bat gertatzen denean, ezarritako prozedurarekin bat ez datorrelako edo arazo teknikoak direla medio.
- Sinadura sortzeko datuak arriskuan egon ez arren, Izenpek jaulkitako ziurtagirien segurtasuna edo fidagarritasuna arriskuan egon daitekeenean.
- Ziurtagiriaren jaulkipenean eta/edo banaketan akats teknikoak gertatzen direnean.
- Ziurtagiria eskatuta hiru hilabete igarotzen direnean eskatzaileak hartzen ez badu.
- Izenpek ziurtagiri baten jaulkipen-eskaera jasotzen duenean, eta politika berari dagokion eta bakartasun-irizpide bera duen beste ziurtagiri baliodun bat existitzen bada, eskatzailearen baliogabetze-eskaera jaso ondoren, aurreko ziurtagiria baliogabetuko da.

#### 4.9.2 Nork eska dezake baliogabetzea

160. Ziurtagiria baliogabetzeko eskatu ahal izango dute,

- Harpidedunak.
- Erakunde harpidedunaren legezko ordezkariak edo baimendutako hirugarrenak.
- Langileen arduradunak edo baimendutako hirugarrenak.
- Eskatzaileak.
- Izenpek, dokumentu honetan jasotako arrazoi teknikoengatik.

#### 4.9.3 Baliogabetze-eskaeren tratamendua.

161. Ezeztapenaren eskatzaileak Izenperen aurrean izapidetuko du *ezeztatze*ko eskaera.

162. Ezeztatzea eskatzailea, harpideduna edo sinatzailea ez den beste pertsona batek eskatzen badu, ezeztatzearen aurretik edo aldi berean, Izenpek sinatzaileari eta ziurtagiriaren harpidedunari jakinaraziko die bere ziurtagiria baliogabetu dela eta zergatik ezeztatu den.

163. Eskatzaileak ziurtagiria baliogabetu ahal izango du honako kanal hauen bidez:

- Aurrez aurre honako hauetan:
  - Aurrez aurre, Izenperen aurrean, hitzordua eskatuz [www.izenpe.eus](http://www.izenpe.eus) helbidearen bidez.
  - Izenpek dagokion tresna juridikoa sinatu duen erakunde harpidedunaren aurrean.



- On line baliogabetzeko aplikazioan sartzeko aukera: <https://servicios.izenpe.com/gestionCertificados/>
- Posta elektronikoz, EU TSLn (Trusted Service List) sartutako CA batek emandako ziurtagiri kualifikatu batekin sinatutako ezeztapen-eskaeraren inprimakia [izenpe@izenpe.eus](mailto:izenpe@izenpe.eus) helbidera bidaliz.

164. Baliogabetze-eskaera autentikatua, bai eta baliogabetzea justifikatzen duen informazioa ere, erregistratu eta artxibatu egingo dira.

#### 4.9.4 Baliogabetze-eskaeraren barkamen-epea.

165. Prozesu honek ez du barkamen-epetik, izan ere, baliogabetzea berehala egiten da baliogabetze-eskaeraren harrera egiaztatzen denean.

#### 4.9.5 CAk baliogabetzea prozesatzeko duen denbora-epea.

166. Izenpe-k lanegun bateko eskaera jaso eta hurrengo 24 orduetan baliogabetuko du ziurtagiria, eta posta elektronikoz jakinaraziko die eskatzaileari eta harpidedunari ziurtagiriaren egoera-aldaketaren berri.

167. “4.9.3 Baliogabetze-eskaeren tratamendua.” atalean adierazitakoa bete ondoren, eta RAK (edo “4.9.1 Baliogabetzeko egoerak” atalean zehaztutako kasuetan Izenpek) baliogabetzea behar bezala izapidetu ondoren, baliogabetzea berehala egingo da eraginkor.

#### 4.9.6 Konfiantzazko hirugarrenek baliogabetzeak egiaztatzeko betebeharra.

168. Ziurtagiriaren egoera egiaztatzea derrigorrezkoa da ziurtagiria erabiltzen den bakoitzean, bai CRL (Ziurtagiri Baliogabetuen Zerrenda) kontsultatuz, bai OCSP (Online Certificate Status Protocol) zerbitzua erabiliz.

169. Izenpek informazioa eskaintzen die egiaztatzaileei CRL eta/edo OCSP non eta nola aurkitu adierazteko.

#### 4.9.7 CRLen sorreraren maiztasuna.

170. Izenpek CRL (Ziurtagiri Baliogabetuen Zerrenda) bat jaulkitzen du berehala, baliogabetze bat gertatzen den unetik bertatik.

171. CRLn CRL berri bat jaulkitzeko programatutako unea adierazten da, baina CRL bat jaulki ahal izango da aurreko CRLan adierazitako epea baino lehen. Baliogabetzerik gertatzen ez bada, CRL eguneratu egiten da egunero.

172. Azken erakundearen ziurtagiriaren CRLa gutxienez 24 orduero jaulkitzen da edo baliogabetze bat gertatzen denean, eta 10 egunetik beherako balio-epea du.

173. CAren ziurtagiriaren CRLa (ARL) urtean behin jaulkitzen da edo baliogabetze bat gertatzen denean.

174. Iraungitako ziurtagiri baliogabetuak CRLetik kentzen dira. Hortik aurrera, baliogabetzearen erregistroa Izenperen barne-erregistroetan gordeko da 15 urtez.

#### 4.9.8 CRLen sorkuntza eta argitalpenaren arteko denbora-tartea.

175. CRLa sortu eta gehienez 30 segundora argitaratu behar da.

176. Argitalpena berehalakoa da, baina zerbitzariak gehienez 1 orduz cachean eduki dezake.

177. Ziurtagiriaren egoera online egiaztatzeko sistemaren eskuragarritasuna



178. Izenpek Erakunde Erabiltzaileei denbora errealeko egiaztapen-zerbitzua eskaintzen die, OCSP (Online Certificate Status Protocol) bidez. Erabiltzaile-aplikazioek ziurtagiriaren egoera egiaztatu ahal izango dute.

179. Zerbitzua eskuragarri dago egunean 24 orduz, asteko 7 egunetan.

#### 4.9.9 Online baliogabetze-berrespenaren eskakizunak.

180. Sarbide libreko CRL zerbitzua erabiltzeko, baldintza hauek bete behar dira:

- Beti egiaztatzea azken CRLa, ziurtagirian bertan jasotako “CRL Distribution Point” luzapenean agertzen den URL helbidean deskarga daitekeena.
- Erabiltzaileak egiaztatzea ziurtapen-hierarkiaren kateko dagozkion CRLak.
- Erabiltzaileak ziurtatu behar du baliozkotu nahi duen ziurtagiria eman duen agintaritzak sinatuko duela ezeztatze-zerrenda.

181. Iraungitako ziurtagiri baliogabetuak CRLetik kentzen badira ere, ziurtagiriaren egoerari buruzko informazioa online kontsultatzeko aukera eskainiko da, ziurtagiria iraungita egon arren.

182. Sarbide libreko OCSP zerbitzua erabiltzeko, baldintza hauek bete behar dira:

- Ziurtagirian bertan jasotako “Authority Info Access” luzapenean dagoen URL helbidea egiaztatzea.
- Erabiltzaileak ziurtatzea OCSP erantzuna ziurtagiria jaulki duen CAk sinatu duela.

#### 4.9.10 Baliogabetze-ohartarazpenen bestelako bideak.

183. Izenpek ziurtagiria baliogabetzen denean mezu elektronikoko bat bidaltzen dio ziurtagiriaren harpidedunari, informazio gisa.

#### 4.9.11 Gakoa arriskuan: eskakizun bereziak.

184. Ziurtagiriaren gako pribatua arriskuan badago, harpidedunak/sinatzailea horren berri eman beharko dio IZENPERi, ziurtagiria baliogabetzeko eta ziurtagiria erabiltzeari uzteko eska dezan.

185. Izenperi 1.5.2 atalean adierazitako incidencias@izenpe.eus posta-kontuaren bidez gako pribatu bat arriskuan dagoela jakinaraztean, froga bat aurkeztu behar da, eta posta elektronikokoaren gaian hau adierazi: “Gakoak arriskuan”. Hori frogatzeko, metodo hauek erabil ditzakete aldeak:

- Arriskuan jarritako gako pribatua bidaltzea, edo gako pribatuak sinatutako eta gako publikoak egiaztatzeko moduko desafio-erantzuna bidaltzea, baita gako publikoa bera ere.
- Ahultasunei eta / edo segurtasun-gorabeheren iturriei buruzko erreferentziak ematea, haien arabera gakoak arriskuan dagoela egiaztatu badaiteke.

186. Izenpek gakoak arriskuan daudela behar bezala frogatzen duten bestelako ebidentziak onartu ahal izango ditu.

187. IZENPERen CA baten gako pribatua arriskuan jarriz gero, dokumentu honen 5.7.3 atalean ezarritakoaren arabera jokatu da.



#### 4.9.12 Ziurtagiria eteteko inguruabarrak

188. Izenpek ez du bere ziurtagirietako bakar bat ere etetea onartzen.

#### 4.9.13 Nork eska dezake etetea

189. Izenpek ez du bere ziurtagirietako bakar bat ere etetea onartzen.

#### 4.9.14 Etete-eskaera egiteko prozedura.

190. Izenpek ez du ziurtagiriak etetea onartzen.

#### 4.9.15 Etete-epearen mugak.

191. Izenpek ez du ziurtagiriak etetea onartzen.

### 4.10 Ziurtagirien egoerari buruzko zerbitzuak.

#### 4.10.1 Funtzionamendu-ezaugarriak

192. Izenpek CRL (Ziurtagiri Baliogabetuen Zerrenda) zerbitzua eskaintzen du doan, sarbide-murrizketarik gabe. Horrez gain, ziurtagiriak egiaztatzeko OCSP (Online Certificate Status Protocol) bidezko zerbitzua ere eskaintzen du.

#### 4.10.2 Zerbitzuaren eskuragarritasuna

193. Izenpek egunean 24 orduz, asteko 7 egunetan eskaintzen die baliogabetze-zerbitzua erakunde erabiltzaileei.

#### 4.10.3 Aukerako ezaugarriak.

194. Ez daude aurreikusita.

### 4.11 Harpidetza amaitzea.

195. Ziurtagiria ez da baliozkoa haren balio-epea amaitzen denean edo baliogabetua izan denean.

196. Ziurtagiri kualifikatuek gehienez ere 5 urteko indarraldia izan dezakete, Konfiantzazko zerbitzu elektronikoen alderdi jakin batzuk arautzen dituen azaroaren 11ko 6/2020 Legearen<sup>3</sup> arabera.

197. Web-autentifikaziorako ziurtagiriek beren balio-epea izango dute, Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates<sup>4</sup> araudiaren arabera.

---

<sup>3</sup> 2020ko azaroaren 11ko 6/2020 Legea, konfiantzazko zerbitzu elektronikoen alderdi jakin batzuk arautzen dituen, 4.2 artikulua.

<sup>4</sup> <https://cabforum.org>



#### **4.12 Gakoen zaintza eta berreskurapena**

4.12.1 Gakoak zaintzeko eta berreskuratzeko jardunbideak eta politikak.

198. Izenpek ez ditu ziurtagirien titularren gako pribatuak berreskuratuko.

4.12.2 Saio-gakoa babesteko eta berreskuratzeko jardunbideak eta politikak.

199. Ez da aurreikusten.



## 5 Segurtasun fisikoko kontrolak, prozedurazkoak eta langileekin lotutakoak.

### 5.1 Segurtasun fisikoko kontrolak.

200. Izenpek segurtasun fisikoko kontrolak ezartzen ditu zerbitzuak eskaintzen dituen instalazio guztietan.

#### 5.1.1 Instalazioen kokapena eta eraikuntza.

201. Informazioa prozesatzen den instalazioek honako baldintza fisiko hauek betetzen dituzte:

- Informazioa prozesatzeko instalazioak dituen eraikina solidoa da fisikoki, kokalekuaren kanpo-hormak sendoak dira eta segurtasun-kamerez zainduta daude beti, eta behar bezala baimendutako pertsoneri bakarrik uzten diete sartzen.
- Ate eta leiho guztiak itxita daude, eta baimenik gabeko sarreretatik babestuta.

#### 5.1.2 Sarbide fisikoa

##### 5.1.2.1 Datuak Prozesatzeko Zentroa.

202. Izenperen instalazioek sarbide fisikoa kontrolatzeko sistema oso bat dute:

- Lurzorutik sabairaino hedatzen den segurtasun-perimetroa, baimenik gabeko sarbideak saihesteko.
- Instalazioetarako sarbide fisikoaren kontrola:
  - Sarbidea baimendutako langileei soilik baimentzen zaie.
  - Gune segururako sarbide-eskubideak aldizka berrikusi eta eguneratu egiten dira.
  - Langile guztiek ikusgai daramaten identifikazio-elementuren bat eraman behar dute, eta langileei gomendatzen zaie beste inori identifikazioa eskatzeko, ez badaramate.
  - Izenpeko operazioarekin loturarik ez duen langilea, instalazioetan lanean ari bada, gainbegiratu egingo da.

203. Sarbideen log-fitxategi bat modu seguruan mantentzen da. Izenperen sarrerako ateei sarbide-mekanismo espezifikokoak dituzte. Telebista-zirkuitu itxi bat, Izenpek ziurtatze-zerbitzua emateko erabiltzen dituen elementuak monitorizatzen dituena.

##### 5.1.2.2 Erregistro Agintaritzak (RAk).

204. RAek segurtasun-irizpide egokiak betetzen dituzte, bai Segurtasun Politikan, bai Izenperen Hornitzaileen Segurtasun Politikan ezarritakoak.

#### 5.1.3 Elektrizitatea eta aire girotua.

205. Datuak Prozesatzeko Zentroak energiako eta aire girotuko sistema egokiak ditu, funtzionamendu-ingurune fidagarria bermatzeko.

206. Halaber, Izenperen instalazioek etenik gabeko elikadura-funtzionalitatea dute (SAI eta ekipo elektrogenoa), eta funtzionalitate horrek sistemak modu ordenatuan ixteko behar den denboran mantentzen ditu ekipoak martxan, baldin eta energia-akats batek edo aire girotuak sistemak erortzea eragiten badu.



#### 5.1.4 Ureztatze-arriskuaren aurkako babesa

207. Izenpek beharrezko neurriak hartu ditu urak eragindako kalteetatik eratorritako arriskuak gutxitzeko.

#### 5.1.5 Suteen prebentzioa eta babesa.

208. Izenperen Datuak Prozesatzeko Zentroak hesi fisikoak ditu, benetako lurzorutik benetako sabairaino, baita suteak automatikoki detektatzeko sistemak ere, helburu hauekin:

- Sute baten berri ematea Izenpeko zaintza-zerbitzuari eta langileei.
- Sute baten hasiera zaintza-zerbitzuari eta Izenpeko langileei jakinaraztea. Haizagailuen sistemaren deskonexioa, sute-kontrako konporten itxiera, energia elektrikoaren etetea eta itzalketa-instalazio automatikoaren aktibazioa bezalako funtzioak betetzea.

#### 5.1.6 Euskarrien biltegitratzea.

209. Babeskopien euskarriak modu seguruan biltegitratzen dira.

#### 5.1.7 Hondakinen tratamendua.

210. Informazio-euskarrien suntsipen-prozedurak arautzen dituen politika ezarri da.

211. Informazio konfidentziala duten euskarriak suntsitu egiten dira, halako moldez non informazioa ezin izango baita berreskuratu bota ondoren.

#### 5.1.8 Instalazioetatik kanpoko babeskopien biltegitratzea.

212. Izenpek babeskopien euskarriak instalazioetatik kanpo biltegitratzen ditu, istripuen aurrean babestuta eta kokapen nagusian gertatzen den edozein hondamendiren aurrean kaltetu ez daitezen, distantzia nahikoan kokatuta.

## 5.2 Prozeduren kontrolak.

### 5.2.1 Konfiantzazko rolak

213. "Konfiantzazko rol" gisa ulertzen da segurtasun-arazoak sor ditzakeen funtzio bat esleituta daukan rola, funtzio hori behar bezala betetzen ez bada, nahigabe edo nahita.

214. Konfiantzazko roletan esleitutako funtzioak behar bezala gauzatuko direla ziurtatzeko, bi ikuspegi kontuan hartzen dira:

- Teknologiaren diseinu eta konfigurazioa, erroreak saihesteko eta jokabide desegokia eragozteko moduan prestatua.
- Funtzioen banaketa hainbat pertsonaren artean, horrela jarduera maltzurak gauzatzeko zenbait pertsonaren konplizitatea behar izatea bermatuz.

215. Izenpek antolaketan garatutako rolen definizio osoa du. Rol guztientzat, funtzio eta erantzukizunak zehaztuta daude.

### 5.2.2 Pertsona-kopurua zeregin bakoitzeko.

216. Sistema babesteko, rol bakoitzari pertsona ezberdinak esleitzen zaizkio, salbuespen bakarra operadorearen rola da, zeina administratzaileak bete dezakeen.

217. Gainera, rol berera hainbat pertsona esleitu daitezke.



### 5.2.3 Rol bakoitzerako identifikazioa eta autentifikazioa

218. Konfiantzazko rolek autentifikazio segurua eskatzen dute, eta beti erabiltzaile pertsonalekin egiten da.

219. Izenpek rol bakoitzari buruzko dokumentazio espezifikoa dauka, non funtzio horien esleipena zehazten den.

### 5.2.4 Rol desberdinetako zereginen bereizketa.

220. Izenpek CWA 14167 segurtasun-politikari jarraitzen dio (Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures), eta bere segurtasun-ereduan definituta dago.

## 5.3 Langileen kontrolak.

### 5.3.1 Historiala, kualifikazioa, esperientzia eta autentifikazioari buruzko eskakizunak.

221. Izenpek beharrezko esperientzia eta kualifikazioa duten langileak kontratatzen ditu, betebeharreko zerbitzuak modu egokian burutzeko.

222. Konfiantzazko roletan diharduten langile guztiak inpartzialtasunari eragin diezaioketen interes-gatazketatik libre daude.

### 5.3.2 Historialaren ikerketa-prozedurak.

223. Izenpek, bere langile-prozeduren barruan, pertsona bat kontratatu aurretik dagokion ikerketa egiten du. Legezko murrizketengatik, ez da aurreikusten aurrekari penalak egiaztatzea.

### 5.3.3 Prestakuntza-baldintzak

224. Izenpeko langileek beharrezko prestakuntza jasotzen dute, beren eginkizunak behar bezala eta gaitasun profesional egokiarekin burutzeko. Urtero gutxienez prestakuntza-saio bat egiten da, eta bertan, gutxienez, honako puntu hauek jorratzen dira:

- DPCGren kopia bat ematea.
- Segurtasunarekiko kontzientziaketa.
- Software eta hardwarearen erabilera, rol bakoitzerako zehaztuta.
- Rol bakoitzerako segurtasun-prozedurak.
- Rol bakoitzerako ustiapen- eta administrazio-prozedurak.
- Hondamendien berreskurapenerako prozedurak.
- Gorabeherak kudeatzeko prozedura.
- Pribatutasunaren eta datuen babesaren inguruko kontzientziaketa.

225. RAKo operadoreentzako prestakuntza eta kontzientziaketa espezifikoa egingo da gutxienez haien alta ematean, eta ondoren Izenpek ezarritako maiztasunarekin errepetatuko da.

### 5.3.4 Prestakuntza-eguneratzeen eskakizunak eta maiztasuna.

226. Izenperen jardueran aldaketa esanguratsurik gertatzen bada, prestakuntza-plan bat eskatuko da, eta planaren exekuzioa dokumentatuko da. "Konfiantzazko Rolak" barruko



langileek urtean behin gutxienez prestakuntza saioa jaso behar dute, beren gaitasun-maila egokia mantentzeko. Prestakuntza honek beti barne hartu behar du edukien berrikuspena.

#### 5.3.5 Lanpostuen txandakatze-sekuentzia eta maiztasuna.

227. Langileen txandakatzea lanpostuaren beharren arabera edo langilearen eskaeraz egiten da.

#### 5.3.6 Baimendu gabeko jardueren aurkako zigorrak.

##### 5.3.6.1 Informazioaren segurtasun-gorabeherak

228. Izenpek Informazio Segurtasunaren Intzidentzien Kudeaketa Plana dauka.

##### 5.3.6.2 Zigor-prozesua.

229. Izenpek diziplina-erregimen propioa du, zigor-prozedura definitzen duena.

#### 5.3.7 Langileen kontratazioaren eskakizunak.

230. Zerbitzuen operazioarekin lotutako funtzioak betetzeko azpikontrataturako langile guztiak Izenperen Hornitzaileen Segurtasun Politikaren eskakizunen menpe daude.

#### 5.3.8 Langileei dokumentazioa ematea.

231. Konfiantzazko rolek in lotutako langile guztiek jasotzen dute:

- DPCGren kopia bat.
- Rol bakoitzaren betebeharrak eta prozedurak definitzen dituen dokumentazioa.
- Sistemako osagai desberdinen ustiapenari buruzko eskuliburuaren sarbidea dute.

### 5.4 Auditoria.

232. Izenperen softwareak, Erregistro-Entitateek eta erabiltzaileek eragindako gertaera esanguratsuak berreraikitze log-fitxategiak erabiliko dira. Log-ak baliozko froga izan daitezke une jakin bateko sinadura baten baliozkotasuna egiaztatze, gatazka edo arbitraje-prozesu batean.

#### 5.4.1 Erregistratzen diren gertaeren motak.

233. Honako log hauek gordetzen dira:

- Ziurtagiri-eskaera berriak.
- Ukatutako ziurtagiri-eskaerak.
- Kontuetarako sarbide-urratzeak.
- Ziurtagirien sinadura.
- Ziurtagiriak baliogabetzea.
- Kontuetako saio-hasierak.
- CRLen sinadura.

234. CAtan egindako aldaketak.

- Ziurtagirien iraungitzea.



235. Zerrenda hau ez da osatua, eta ziurtagirien kudeaketarekin edo administrazio-funtzioekin zuzenean lotutako gertaerak soilik barne hartzen ditu. Bereziki, beste sistema batzuetan erregistratzen diren gertaera teknikoak ez dira hemen sartzen.

236. Gertaera bakoitzaren data eta ordua grabatzeko, denbora-oinarri fidagarri bat erabiltzen da.

#### 5.4.2 Logen prozesamendu-maiztasuna.

237. Logak etengabe prozesatzen dira, eta segurtasun-arduradunak hiru hilean behin ikuskatzen ditu. Auditoretza-txostenak honako alderdi hauek jasotzen ditu:

- Baimendu gabeko sarbide-saiakeren zerrenda.
- CA bakoitzean sortutako erroreak.
- Administrazioaile erabiltzaileen zerrenda.
- Windows makinetan instalatutako softwarearen zerrenda.

#### 5.4.3 Audit logaren atxikipen-epea.

238. Log-fitxategietan sortutako informazioa online mantentzen da artxibatu arte. Behin artxibatuta, log fitxategiak 15 urtez mantentzen dira.

#### 5.4.4 Audit logaren babeseta.

239. Logeko informaziorako sarbidea esleitzen zaie beren funtzioaren barruan sarbidea behar duten langileei. Auditorearen rola dutenek sarbidea dute. Egunkaria datu-basean gordetzen da, eta sarbidea hainbat mailatan babestuta dago.

240. Ez da onartzen log-erregistroak baimenik gabe ezabatzea edo aldatzea. Log-datuen galera saihesteko kontingentzia-neurriak ezarrita daude.

#### 5.4.5 Audit logaren babeskopia egiteko prozedura.

241. Logak datu-basean daudenez, egunero egiten den datu-basearen babeskopian sartzen dira, "Babeskopien Politika"ren arabera.

#### 5.4.6 Logen bilketa.

242. CA eta RAen log-fitxategiak Izenperen barne-sistemetan gordetzen dira.

243. Logen jatorriari egindako ekintzen jakinarazpena

244. Ez da aurreikusten gertaeraren jatorriari log-fitxategien ekintzen jakinarazpena egitea.

#### 5.4.7 Zaugarritasunen analisia.

245. Hiru hilean behin egiten da zaugarritasunen analisia bat, bai kanpoko, bai Izenperen barne-sistemetan. Urtero penetrazio-proba bat ere egiten da.

### 5.5 Erregistroak artxibatzea.

#### 5.5.1 Artxibatutako erregistro-motak.

246. Artxibatzen diren datu edo fitxategi motak, besteak beste, honako hauek dira:

- Erregistro-prozedurarekin eta ziurtagiri-eskaerekin lotutako datuak;
- Aurreko atalean deskribatutako auditoria-erregistroak;



- Gakoen historia.

#### 5.5.2 Artxihoaren atxikipen-epea.

247. Zerbitzu kualifikatuei buruzko informazio eta dokumentazio guztia 15 urtez gordetzen da, ziurtagiria amaitzen den egunetik edo emandako zerbitzua amaitzen den egunetik zenbatzen hasita, eta ziurtagiriei eta kualifikatu gabeko zerbitzuei buruzkoa, berriz, 7 urtez (ziurtagiria amaitzen den egunetik edo emandako zerbitzua amaitzen den egunetik zenbatzen hasita).

#### 5.5.3 Artxihoaren babes

248. "Artxihoaren Kudeaketa Prozedurak" zehazten du paperezko zein formatu elektronikoko erregistroak ezin direla manipulatu ezta beren edukia suntsitu ere, eta horretarako ezarri beharreko babes-neurriak.

#### 5.5.4 Artxihoaren babeskopia egiteko prozedurak.

249. "Babeskopien Politika" eta "Kontingentzia Plana" daude ezarrita, eta hauek definitzen dituzte gorabehera baten aurrean jarduteko irizpideak eta estrategiak. Jarduketa-estrategia osoaren diseinua aktiboen inbentarioan eta arriskuen analisisian oinarritzen da.

#### 5.5.5 Erregistroen denbora-zigilurako eskakizunak.

250. Izenpek erabiltzen dituen informazio-sistemek bermatzen dute gertaeren denbora-erregistroa. Erabilitako denbora-instantziak data eta ordu fidagarriaren iturri seguru batetik datozen. Sistema guztiak sinkronizatuta daude iturri honekin (ikus Denbora-iturria.).

#### 5.5.6 Artxiho-sistema.

251. Artxiho-sistema Izenperen instalazioetan eta zerbitzuaren ematean parte hartzen duten entitateetan kokatzen da.

#### 5.5.7 Artxiho-informazioa eskuratzeko eta egiaztatze prozedurak.

252. Informazio horretarako sarbidea baimendutako langileetara mugatuta dago, eta sarbide fisiko zein logikoen aurkako babes ezarrita dago, DPCG honetako 5. eta 6. atalean ezarritakoaren arabera.

### 5.6 CAren gakoak aldatzea.

253. CA baten gako pribatuaren konpromisoa saihesteko arriskua minimizatzeko, gakoak aldatu egin behar da erabilitako algoritmoen segurtasun-mailaren arabera. Behin aldaketa eginda, gako berria sinadura-funtzioetarako bakarrik erabili behar da. Gako zaharra, baliozkoa izaten jarrai dezakeena, erabilgarri egon behar da aurreko sinadurak egiaztatze, gako horrekin sinatutako ziurtagiri guztiak iraungi arte. Gako zaharra bakarrik mantendu behar da hura erabiliz sinatutako ziurtagiriak jasotzen dituzten CRLak sinatzeko erabiltzen bada, eta babes-maila bera aplikatuko zaio gako berriari ezarritakoarekin. CA berri baten gakoaren sorrera-prozedura "CA berriaren Sorreraren Zeremonia eta CA zaharraren Migrazio Dokumentuan" jasota dago. 6.1.5 atalean erabiltzen diren gakoaren tamainak eta algoritmoak zehazten dira.



## 5.7 Gertaeren kudeaketa eta kontingentzia-plana.

### 5.7.1 Salaketak kudeatzeko prozedura.

254. “Kontingentzia Plana” izeneko dokumentu batean jasotzen dira Izenpek eskaintzen dituen ziurtapen-zerbitzuak erabilteztina edo degradatua bihurtzen dituen gertakari nahita edo istripuzko baten aurrean egin beharreko ekintzak, erabiliko diren baliabideak eta inplikaturako langileak. Helburua da ez-erabilgarritasun denbora ahalik eta txikiena izatea.

255. Kontingentzia Planaren helburu nagusiak honako hauek dira:

- Berreskurapenerako jardueren eraginkortasuna maximizatzea, hiru fase ezarrita:
  - Jakinarazpen/Ebaluazio/Aktibazio fasea: gertakaria detektatzeko, kalteak ebaluatzeko eta plana aktibatzeke.
  - Berreskurapen fasea: zerbitzuak behin-behinean eta partzialki berrabiarazteko, jatorrizko sistemari izandako kalteak konpondu arte.
  - Birgaitze fasea: sistema eta prozesuak ohiko funtzionamendura itzultzeko.
- Ziurtapen-zerbitzuen parte-hartzearekin jarraitzeko beharrezko jarduerak, baliabideak eta prozedurak identifikatzea, CPD alternatibo batean, ohiko operatibitatearen etenaldi luzeetan.
- Izenpeko langile izendatuei erantzukizunak esleitzea, eta etenaldi luzeetan ohiko operatibitatea berreskuratzeko gida bat eskaintzea.
- Estrategia planifikatuan parte hartzen duten eragile guztien arteko koordinazioa bermatzea (barne-sailak, kanpoko harremanetarako puntuak eta hornitzaileak).

256. Izenperen Kontingentzia Plana aplikagarria da konfiantzazko zerbitzuen berreskurapenerako beharrezko funtzio, eragiketa eta baliabide guztietan, eta konfiantzazko zerbitzuekin lotutako Izenpeko langile guztiei aplikatzen zaie.

257. Planak Izenperen operazioen berreskurapenean parte hartuko duten talde zehatzak ezartzen ditu.

258. Kalte-ebaluazioa eta ekintza-plana Kontingentzia Planean bertan deskribatzen dira.

259. Algoritmoak, erabilitako gako-tamainen konbinazioak edo beste edozein egoera tekniko sistemaren segurtasun tekniko nabarmen murrizten badute, Kontingentzia Plana aplikatuko da. Eraginaren azterketa bat egingo da. Azterketa horretan segurtasun-arazoaren kritikotasuna, eragin-esparrua eta intzidentziaren aurrean aplikatu beharreko berreskurapen-estrategia aztertuko dira. Gutxienez, honako puntu hauek zehaztuko dira eraginaren azterketa-txostenean:

- Kontingentziaren deskribapen xehatua: denbora-esparrua, ezaugarriak, etab.
- Kritikotasuna eta eragin-esparrua
- Proposatutako irtenbidea edo irtenbideak
- Aukeratutako konponbidearen ezarpen-plana, eta gutxienez honako hauek jasoko ditu:
  - Erabiltzaileei jakinaraztea, eraginkorra den komunikazio-bidez. Jakinarazpena hartzaileei, harpidedunei eta egiaztatzaileei (hirugarren fidagarriak) egingo zaie.



- Webgunean argitaratuko da gertatutako kontingentzia.
- Kaltetutako ziurtagirien baliogabetzea.
- Berritze-estrategia.

#### 5.7.2 Datu edo software hondatuen aurrean jarduteko plana.

260. Izenperen Larrialdi Planean halako egoeren aurrean jarduteko estrategia jasotzen da.

#### 5.7.3 CAren gako pribatuaren konpromisoaren aurreko prozedura

261. Errebokazioa eragin zuten faktoreak konpondutakoan, Erro-CAk hau egin dezake:

- CA igorlearentzat ziurtagiri berri bat sortzea.
- Ziurtatu CAk igortzen dituen ziurtagiri eta CRL guztiak gako berri berriarekin sinatzen direla.

262. Ziurtagiri baliogabetua ARLn (Ziurtapen Agintarien Baliogabetze Zerrenda) argitaratuko da.

263. Kontingentzia hori “Izenperen kontingentzia-planean eta negozio-jarraitutasuneko planean” jasota dago, eta, bestek beste, ekintza hauek zehazten ditu:

- Kaltetutako zerbitzua emateari uztea.
- Kaltetutako ziurtagiri guztiak baliogabetzea.
- Sinatzaileei, erabiltzaileei eta hirugarrenei jakinaraztea. Era berean, konfiantzazko hitzarmenak dituzten TSPei, nabigatzaile-fabrikatzaileei eta, oro har, Izenperekin zerbitzua erabiltzeko kontratuzko harremanen bat duen edozein erakunderi egindako jakinarazpena ere sartuko da.
- DPCGn eta indarrean dagoen legerian ezarritakoaren arabera, "TSPren Jarduerak Eteteko Plana" abiarazteko beharra aztertuko da.

#### 5.7.4 Hondamendi baten ondorengo negozioaren jarraipena.

264. CAren jarduera eten egingo da berreskurapen-prozedura amaitu arte, eta zerbitzua behar bezala berriro funtzionatzen hasi arte, bai zentro nagusian, bai alternatiboan.

265. “Izenperen Kontingentzia eta Negozioaren Jarraipen Plana” aktibatuko da.

## 5.8 CA edo RAren amaiera.

### 5.8.1 Ziurtapen Erakundea.

266. Izenpek "Jarduera Eteteko Plana" du, egoera hori gertatuz gero aplikatu beharreko prozedura jasotzen duena.

267. Bere jarduera eteteko asmoa badu, Izenpek jakinarazpena egingo dio harpidedunari, bidalketa eta jasotzea bermatzen duen edozein bide erabiliz, gutxienez 2 hilabeteko aurreabisuz, ziurtapen-zerbitzuen hornitzaile gisa jardutea utziko duela adieraziz. Jakinarazpen horretan adieraziko da 2 hilabeteko epean indarrean dauden ziurtagiri guztiak baliogabetuko direla.

268. CA baten amaiera iristen bada (iraungitzeagatik edo baliogabetzeagatik), ziurtagiriaren egoerari buruzko kontsultei OCSP zerbitzuaren bidez erantzungo zaie. CA amaitzen denean, CA horrek jaulkitako ziurtagiriei buruzko OCSP erantzunak Izenperen indarrean



dagoen beste CA batek sinatuko ditu. Izenperen CRLek ez dute ziurtagiri iraungirik jasotzen, DPCGko 4.9.7 atalean (CRLen sorrera-maiztasuna) ezarritakoaren arabera.

269. Izenpek bere jarduera uzten badu, azken CRL baten bidez emango du ziurtagirien baliogabetze-informazioa, "99991231235959Z" nextUpdate balioarekin, ETSI EN 319 411-1 arauko 6.3.9 atalean ezarritakoaren arabera.
270. Jakinarazpena egingo zaie TSPei, nabigatzaileen fabrikatzaileei eta Izenpek ziurtagirien erabilerarako kontratu-harremana duen edozein erakunderi.
271. Izenpek DPCG honetan ezarritako denboran mantenduko du erregistroei, baliogabetze-egoerari eta log fitxategien artxiboari buruzko informazioa. Transferentzia beste erakunde bati eginez gero, behar diren berme guztiekin egiteko neurriak hartuko dira.
272. Izenpeko Zuzendaritza Nagusiari edo Administrazio Kontseiluak izendatutako pertsonen dagokie jakinarazpen horren erantzukizuna, eta hark erabakiko du zein den mekanismo egokiena.
273. Izenpek Gainbegiratze Erakundeari jakinaraziko dio bere jardueraren amaiera, baliogabetuko diren ziurtagiriei buruzko informazioa barne. Jakinarazpen hori konfiantzazko zerbitzuak emateko arloan eskumena duen ministerioaren egoitza elektronikoko jakinarazpenak bidaltzeko plataformaren bidez egingo da, jarduera utzi baino gutxienez 3 hilabete lehenago.
274. Izenperekin zerbitzuak emateko kontratua (identifikazioa, jaulkipena, aterpetxea, etab.) duten hirugarrenen edozein prestazio amaitutzat emango da.
275. Izenpek edo Izenperekin zerbitzua transferitzea adosten duen erakunde batek bere ziurtagiri kualifikatu guztien baliozkotasunari buruzko informazioa eskainiko du, baita ziurtagiria iraungita dagoenean ere (ziurtagiria jaulki zuen mendeko CAren iraungitze-datara arte).

#### 5.8.2 Erregistro Erakundea.

276. Behin erregistro-erakundeak bere gain hartzen dituen funtzioak egiteari uzten dionean, Izenperi transferituko dizkio mantentzen dituen erregistroak, informazioa artxibatuta edukitzeko betebeharra dagoen bitartean; bestela, informazioa ezeztatu eta suntsitu egingo da.



## 6 Segurtasun teknikoko kontrolak

---

### 6.1 Gako-pareen sorrera eta instalazioa.

#### 6.1.1 Gako-parearen sorrera.

277. Root eta Sub CAen gako kriptografikoak dagokion babes-profilaren gainean FIPS 140-2 (3. maila edo handiagoa) eta Common Criteria EAL 4+ betetzen dituen hardware-modulu kriptografiko batean (HSM) sortu behar dira.

278. Baliozkotasun-agintaritzaren (VA) gako kriptografikoak HSM batean sortu behar dira, eta horrek ere FIPS 140-2 (3. maila edo handiagoa) bete behar du.

279. TSAren gako kriptografikoak FIPS 140-2 (3. maila) edo FIPS 140-3 (3. maila edo handiagoa) betetzen dituen hardware-modulu kriptografiko batean (HSM) sortu behar dira.

280. Gako kriptografiko guztiak ETSI TS 119 312 estandarrean zehaztutako algoritmo eta gutxieneko gako-luzeraren gomendioak jarraituz sortu behar dira. Izenpek gakoak sortzen dituen ziurtagiri kualifikatuetan, gakoak txartel kriptografikoan edo hardware kriptografikoan sortuko dira.

281. Ziurtagiri kualifikatu hauetan, erabiltzaile amaierakoa da gakoak sortzen dituenak, eta gako horiek honako gailu hauetan sortu ahal izango dira:

282. Bezeroaren gako-edukiontzian (adibidez: web-zerbitzari batean).

283. Izenperen edukiontzi segurua.

- Mugikorretarako Izenperen aplikazioaren edukiontzia.

#### 6.1.2 Gako pribatuaren banaketa sinatzaileari.

284. Gako pribatua entregatzeko metodoa ziurtagiri-motaren eta gailuaren arabera aldatzen da. Kontsultatu PDS eta/edo DPCP.

#### 6.1.3 Gako publikoa ziurtagiriaren jaulkitzaileari banatzea.

285. Gako publikoa, gako pribatua sortu eta gordetzen duen gailuan sortua, Ziurtagiri Agintaritzari entregatzen zaio ziurtagiri-eskaera baten bidez.

286. Izenpe osatzen edo harekin lankidetzan diharduten erakundeek gako publikoa entregatzeko metodoa honako hau da:

- Izenpek sortutako gakoak (txartela, tokena, HSM): gailu kriptografiko edo edukiontzi seguru berean gordetzen dira.
- Nabigatzailean sortutako gakoak: nabigatzailearen ziurtagiri-edukiontzian gordetzen dira.
- Telefono mugikorrean sortutako gakoak: Izenperen aplikazioaren edukiontzian gordetzen dira.
- Zerbitzari seguruaren ziurtagirien gakoak (SSL): Izenpe.

#### 6.1.4 Ziurtagiriaren jaulkitzailearen gako publikoaren banaketa ziurtagiri-erabiltzaileei.

287. Izenpeko CAren gako publikoak hainbat bide erabiliz banatzen dira, besteak beste, Izenperen webgunearen bidez. DPCG honetako 1.3.1.1 eta 1.3.1.2 ataletan, Root CAen eta CA jaulkitzaileen hatz-markak argitaratzen dira.



#### 6.1.5 Gakoen tamainak.

288. Gakoen tamaina kasuaren arabera zehazten da:

289. 2007, 2020 hierarkia.

- Gutxienez 3072 bit: pertsona fisikoen, juridikoen, gailuen, OCSP zerbitzariaren eta ziurtagiri teknikoaren gakoentzat.
- Gutxienez 3072 bit: 2007tik aurrera igorritako CAentzat.

290. TSUren zerbitzariaren gako-tamaina 4096rekin emititzen da.

291. 2024 hierarkia

292. ECC 256 edo 384 bit.

293. 2025 hierarkia ECC 256 edo 384 bit.

#### 6.1.6 Gako publikoaren sorkuntza-parametroak eta kalitatearen egiaztapena.

294. 2007ko eta 2020ko hierarkian ziurtagiriak sinatzeko Izenpek erabiltzen duen algoritmo-identifikatzailea (AlgorithmIdentifier) SHA2 (hash-algoritmoa) da, RSArekin (sinadura-algoritmoa), eta "Identifier for SHA-2 checksum with RSA encryption for use with Public Key Cryptosystem as defined by RC" identifikatzaileari dagokio. Erabilitako padding eskema emsa-pkcs1-v2.1 da (RFC 3447 arabera 9.2 atala)". 2024ko eta 2025eko hierarkian ECC256 edo 384 erabiltzen du.

295. Azken erabiltzailearen ziurtagiriak RSArekin SHA-256 sinatuta daude. Izenpek gomendatzen du erabiltzaileek RSA + SHA-256 edo handiagoa erabiltzea ziurtagiriarekin sinatzean.

296. Izenpek sektoreak onartutako algoritmo kualifikatuak erabiltzen ditu, sinadura kualifikaturako egokiak direnak. Horretarako kontuan hartzen da ziurtagiriaren balio-eparekin batera CAB/Forum-ek eta ETSI estandarrek emandako gomendioak ere betetzen direla.

297. Algoritmoak, erabilitako gako-tamainen konbinazioak edo sistemaren segurtasun tekniko nabarmen murriztuko duen beste edozein egoera tekniko "Izenperen kontingentzia-plana eta negozioaren jarraitutasun-plana" aplikatuko du, eta inpaktu-azterketa bat egingo da. Azterketa horretan segurtasun-arazoaren kritikotasuna, eragin-esparrua eta intzidentziaren aurrean aplikatu beharreko berreskurapen-estrategia aztertuko dira. Gutxienez, honako puntu hauek zehaztuko dira eraginaren azterketa-txostenean:

- Kontingentziaren deskribapen xehatua: denbora-esparrua, ezaugarriak, etab.
- Kritikotasuna eta eragin-esparrua
- Proposatutako irtenbidea edo irtenbideak
- Aukeratutako konponbidearen ezarpen-plana, eta gutxienez honako hauek jasoko ditu:
  - Erabiltzaileei jakinaraztea, eraginkorra den komunikazio-bidez. Ziurtagirien eskatzaileak, sinatzaileak eta egiaztatzaileak (hirugarren aldeak) barne hartuko dira.
  - Webgunean argitaratuko da gertatutako kontingentzia.
  - Kaltetutako ziurtagirien balio-gabetzea.



- Berritze-estrategia.

#### 6.1.7 Gakoen erabilera onartuak (X.509 v3 KeyUsage field).

298. Ziurtagiri guztiek Key Usage eta Extended Key Usage hedapenak dituzte, gakoen erabilera baimenduak zehaztuz.
299. Root CAren gakoak Sub CAen eta ARLen ziurtagiriak sinatzeko erabiltzen dira. Sub edo igorle diren CAren gakoak erabiltzaile amaierako ziurtagiriak, CRLak, TSU ziurtagiria eta OCSP ziurtagiriak sinatzeko soilik erabiltzen dira.
300. Amaierako ziurtagirientzako gakoen erabilera onartuak [www.izenpe.eus](http://www.izenpe.eus) webgunean eskuragarri dagoen ziurtagiri-profilen dokumentuan zehaztuta daude.

## 6.2 Gako pribatuaren babesa.

### 6.2.1 Modulu kriptografikoen estandarrak.

301. Segurtasun kriptografikoko modulua (HSM) gako kriptografikoak sortzen eta babesten dituen segurtasun-gailua da. HSMek FIPS 140-2 3. maila irizpidea bete behar dute gutxienez, edo Common Criteria EAL 4+ dagokion babes-profilerako.
302. Izenpek protokoloak ditu HSM bat garraiatzean eta biltegitratzean manipulatu ez dela egiaztatzeko.
303. Sinadura elektronikoko kualifikaturako ziurtagiriak dituzten gailu kriptografikoei dagokienez, sinadura sortzeko gailu kualifikatu gisa (QSCD) erabil daitezkeenei dagokienez, CC EAL4+ segurtasun-maila betetzen dute. Hala ere, ITSEC E3 edo FIPS 140-2 ziurtagiri baliokideak (2. maila, gutxienez) ere onargarriak dira.
304. Gailu horiek gailu seguruaren ziurtagiria galtzen badute eta horrek sinadura kualifikatuaren izaera galtzea badakar, Izenpek ziurtagiria baliogabetuko du, betiere gainbegiratze-organoak eta/edo indarrean dagoen araudiak zehaztutakoaren arabera.
305. Erabilitako sinatzaile-gailuetarako Europako erreferentzia-araua da Europako Batzordearen 2016ko apirilaren 25eko 2016/650 Betearazpen Erabakia.
306. Edozein kasutan, Izenpek kontrola mantentzen du gakoak sortzen dituen harpidedun-gailuen prestaketa, biltegitratze eta banaketa prozesuen gainean.

### 6.2.2 Gako pribatuaren gaineko kontrol partekatua (n/m)..

307. CAren gako pribatuak erabiltzeko, gutxienez bi pertsonaren onespina behar da.

### 6.2.3 Gako pribatuaren zaintza.

308. Root CAren gako pribatua FIPS 140-2 (3. maila) eta/edo CC EAL4+ arauak betetzen dituen hardware kriptografiko ziurtatu batean gordetzen da, eta bermatzen da gakoa inoiz ez dela gailu kriptografikotik kanpo ateratzen. Gako pribatuaren aktibazioa eta erabilera goian deskribatutako pertsona anitzeko kontrola eskatzen du.
309. Sub CAen gako pribatuak ere FIPS 140-2 (3. maila) segurtasun-ziurtagiria duten gailu kriptografikoetan gordetzen dira.
310. Sinatzaileak gako pribatua bere gain hartzen badu, berak izango du ardura eksklusiboa gakoa segurtasunez zaintzeko.



#### 6.2.4 Gako pribatuaren babeskopia.

311. Root edo Sub CAren modulu kriptografikoetan gakoaren berreskurapenerako prozedura bat dago, kontingentzia-kasuan aplikatzeko modukoa.

312. Sinatzaileen modulu kriptografikoen gakoak berreskuratzeko prozedura bat dago, eta Izenpek gakoak zaintzen dizkie. Prozedura horiek dagozkien prozeduretan definitutako kasuetan aplika daitezke.

313. Bi kasuetan ere, 6.2.2 atalean ezarritako kontrol berak mantentzen dira.

#### 6.2.5 Gako pribatua artxibatzea

314. Izenpek gako pribatuaren segurtasun-kopia bat egin ahal izango du, eta bermatu beharko du bikoiztutako datuen segurtasun-maila jatorrizko datuen segurtasun-maila bera dela eta bikoiztutako datuen kopuruak ez duela gainditzen zerbitzuaren jarraitutasuna bermatzeko beharrezkoa den gutxienezko kopurua. Sinadura sortzeko datuak ez dira bikoizten beste ezein helburutarako.

#### 6.2.6 Gako pribatuaren transferentzia modulu kriptografikora edo hortik kanpora.

315. Root CAren, Sub CAren, VAren eta TSAren gako pribatuak HSM batean sortzen dira, 5.2.1 puntuan zehaztutakoaren arabera, eta ezin dira esportatu. Kontingentzia-neurri gisa, gako pribatuaren berreskurapena posible da 5.2.4 atalean jasotakoaren arabera.

316. Sinatzaileen modulu kriptografikoen gakoak berreskuratzeko prozedura bat dago, eta Izenpek gakoak zaintzen dizkie. Prozedura horiek dagozkien prozeduretan definitutako kasuetan aplika daitezke.

317. Gakoak bere kabuz sortzen dituen sinatzailearen kasuan, hark izango du gakoaren zaintza-erantzukizuna.

#### 6.2.7 Gako pribatuaren biltegitratzea modulu kriptografikoan.

318. Root CAren eta Sub CAren gakoaren zeremonia-dokumentu bat existitzen da, gako pribatuaren sorrera-prozesuak eta hardware kriptografikoaren erabilera deskribatzen dituena.

319. Izenpek CAren gakoaren sorrerarako ETSI EN 319 411-1 eta CABForum Baseline Requirement Guidelines dokumentuei jarraitzen die.

320. Harpidedunen gakoak txartel kriptografikoan sortzeko, Europako Batzordearen (eIDAS) eta EN 319 411-1 estandarrak jarraitzen ditu.

321. Gako pribatuak modulu kriptografikoetatik kanpo biltegitratzen direnean, babestuta egongo dira, modu fisikoan moduluaren barruan egongo balira bezala babes-maila bera bermatzeko moduan.

#### 6.2.8 Gako pribatuaren aktibazio-metodoa

322. Ziurtapen Agintaritzen gako pribatuak FIPS140-2 (3. maila) segurtasun-baldintzak betetzen dituen gailu kriptografiko batean sortzen eta zaintzen dira.

323. Erakunde amaierako ziurtagirien gako pribatuaren aktibazio- eta erabilera-mekanismoak PDSn eta/edo dagokion DPCPn deskribatzen dira.



### 6.2.9 Gako pribatuaren desaktibazio-metodoa

324. Administratzaile-rola duen pertsona batek ziurtapen-agintaritzaren gakoaren desaktibazioa burutu dezake sistema geldituz. Berraktibatzeke, 6.2.8 Gako pribatuaren aktibazio-metodoa atalean deskribatutakoari jarraituko zaio.

325. Erakunde amaierako ziurtagirien gako pribatuen desaktibazioari dagokionez, PDSn deskribatzen da.

### 6.2.10 Gako pribatuaren suntsiketa-metodoa

326. CAren gakoaren suntsipen-prozedura bat ezarrita dago.

327. CAren gakoak gordetzen dituen HSM kentzen bada, dagokion prozedurari jarraituko zaio.

328. Prozedura hori ez zaie aplikatuko txartel kriptografikoan —edukiontzi seguruan— jaulkitako erabiltzailearen sinadura- edo autentifikazio-gakoei, gailu kriptografiko bera berrerabiliz gakoak berritzen direnean izan ezik; kasu horretan, aurreko gakoa suntsitu egingo da, eta gako berriak sortuko dira euskarri berean.

### 6.2.11 Modulu kriptografikoaren kalifikazioa.

329. Dokumentu honetako 5.2.1 atalean adierazitakoaren arabera.

## 6.3 Gako-parearen kudeaketari buruzko beste alderdi batzuk.

### 6.3.1 Gako publikoa artxibatzea.

330. CAk sortutako ziurtagiriak, eta, beraz, gako publikoak, CAk biltegitratzen ditu indarrean dagoen legediak ezarritako epean.

### 6.3.2 Ziurtagiriaren jardunaldia eta gako-parearen erabilera-epea.

331. Izenpek jaulkitako ziurtagirien erabilera-epeak honako hauek dira:

- 2007ko erroko CAren ziurtagiriak 30 urterako balio du.
- SSL erroko CAren 2020ko ziurtagiriak 25 urterako balio du
- SSL erroko CAren 2024ko ziurtagiriak 25 urterako balio du
- SSL erroko CAren 2025ko ziurtagiriak 25 urterako balio du
- EV motako ziurtagiriak jaulkitzen dituen Sub CA ziurtagiriaren balioa hamar (10) urtekoa da; gainerako Sub CA ziurtagiriak, berriz, Root CAren iraungitze-datara arte dira baliodunak.
- CA ziurtagirien (Root edo Sub) gakoaren aldaketa industriako estandarrek ezartzen dituzten irizpideen arabera egingo da, behar denean.
- Azken erabiltzaileen ziurtagiriak iraupen desberdina dute, motaren arabera. Pertsona fisikoentzako edo zigilua duten ziurtagiri kualifikatuen gehieneko iraupena bost (5) urtekoa da. Web-autentifikazioko ziurtagiriak gehienez 365 eguneko iraupena dute. Pertsona fisikoen eta pertsona juridikoen zigilu-ziurtagirien kasuan, berritzeak beti dakar gakoaren birsorkuntza.



## 6.4 Aktibazio-datuak

### 6.4.1 Aktibazio-datuen sorrera eta instalazioa.

332. Erabiltzailearen azken ziurtagiriak jaulkitzen dituzten Root CAren eta Sub CAren gakoen aktibazio-datuak dagokien Ziurtapen Agintaritzaren gako-sorkuntza ekitaldian sortzen dira.

333. Azken erabiltzaileentzako ziurtagirien gakoen aktibazio-datuei dagokienez, horiek DPS edo DPCP dokumentuetan deskribatzen dira, hala badagokio.

### 6.4.2 Aktibazio-datuen babesa.

334. Root CAren gakoen aktibazio-datuak hainbat txartel fisikotan banatuta daude, eta gutxienez bi pertsona behar dira edozein eragiketa egiteko. Txartelen gakoak kutxa gotorretan gordetzen dira.

335. Sub CAren gakoen aktibazio-datuak ere hainbat txartel fisikotan banatuta daude, eta gutxienez bi pertsona behar dira edozein eragiketa egiteko. Txartelen gakoak kutxa gotorretan gordetzen dira.

336. TSA (Time Stamping Authority) eta VA (Validation Authority) zerbitzuetako gakoak azpiko CAen gakoekin HSM (Hardware Security Module) berean sortzen eta kudeatzen dira. Arau berak aplikatzen dira.

337. Harpidedunek beren aktibazio-datuak isilpean mantentzeko betebeharra dute.

### 6.4.3 Aktibazio-datuen beste alderdi batzuk

338. Ikus daitezke dagozkien dokumentuetan, hala nola PDSetan (Zerbitzuaren Praktika Deklarazioak).

## 6.5 Segurtasun-informatikoko kontrolak

### 6.5.1 Segurtasun informatikoaren eskakizun tekniko espezifikoak

339. Izenperen ziurtapen-zerbitzuaren sistema osatzen duten elementuen kokalekuan hainbat kontrol daude ezarrita (CAak, Izenperen datu-baseak, Izenperen Internet zerbitzuak, CAren operazioa eta sarearen kudeaketa):

340. Eragiketa-kontrolak.

- Eragiketako prozedura guztiak behar bezala dokumentatuta daude dagokien eragiketa-eskuliburuetan.
- Kontingentzia-plan bat dago ezarrita.
- Birusen eta kode maltzurren aurkako babesa duten tresnak ezarrita daude.
- Ekipamenduen mantentze-lanak jarraian egiten dira, erabilgarritasuna eta osotasuna bermatzeko.
- Informazio-euskarrien, euskarri eramangarrien eta ekipamendu zaharkituen babeskopia, ezabatze eta suntsiketa segururako prozedura bat dago ezarrita.

341. Informazio-trukea. Datu-truke hauek enkriptatuta egiten dira, beharrezko konfidentzialtasuna bermatzeko:

- Erregistro-datuen transmisioa ERen (Erregistro Agintaritzak) eta erregistroaren datu-basearen artean.



- Aurre-erregistroaren datuen transmisioa.
- RAen eta CAen arteko komunikazioa.

342. Baliogabetzeen argitalpen-zerbitzuak beharrezko funtzionalitateak ditu 24x7 funtzionamendua bermatzeko.

343. Sarbideen kontrola.

- Erabiltzaile ID bakarrak erabiltzen dira, erabiltzaileak burutzen dituzten ekintzekin lotu eta horien erantzukizuna eskatzeko aukera izan dadin.
- Eskubideak esleitzeko, gutxieneko pribilegio-emakidaren printzipioari jarraitzen zaio.
- Lanpostuz aldatzen diren edo erakundea uzten duten erabiltzaileen sarbide-eskubideak berehala ezabatzea.
- Erabiltzaileei esleitutako sarbide-maila hiru hilean behin berrikustea.
- Pribilegio berezien esleipena “kasuz kasu” egiten da, eta esleipena eragin zuen arrazoia amaitutakoan kentzen dira.
- Kalitate-jarraibideak daude pasahitzetan.
- Operadorearen kontu guztiek, ziurtagiriak jaulkitzeko gaitasuna dutenek, bi faktoreko autentikazioan oinarritutako sarbide-kontrola dute.

344. Izenpek segurtasun-politika eta maila desberdinetan segurtasuna bermatzeko prozedura espezifikoak ditu.

#### 6.5.2 Informatika-segurtasunaren mailaren ebaluazioa.

345. Ziurtapen-zerbitzuak emateko erabiltzen diren produktuek ISO/IEC 15408 estandarrean oinarritutako nazioarteko ziurtagiria dute.

## 6.6 Bizitzaren zikloko kontrol teknikoak

### 6.6.1 Sistemak garatzeko kontrolak.

346. Produkzio-sistemetan softwarea ezartzea kontrolpean dago. Sistema horietan arazoak saihesteko, honako kontrol hauek hartzen dira kontuan:

- Izenperen politikak aplikazioen eta sistemen garapen segururako arauak jasotzen ditu.
- Aldaketak kontrolatzeko prozedura formala dago ezarrita. Aldaketak beharrezkoetara mugatzen dira, eta kontrol zorrotza egiten zaie.
- Sistema eragileak aldatzen direnean, funtsezkotzat jotzen diren negozio-aplikazioak berrikusten dira, Negozioaren Jarraitutasun Planean oinarrituta.
- Sistema-segurtasuneko ingeniartzaren printzipioak ezartzen dira.
- Garapen-ingurunea behar bezala babestuta dago.
- Azpikontratutako garapena Izenpek gainbegiratzen eta kontrolatzen du.
- Garapenean zehar segurtasun funtzionalaren probak egiten dira.



- Informazio-sistema berrien, eguneratzeen eta bertsioen onarpen-probak ezartzen dira.
- Proba-datuak hautatu, babestu eta kontrolatzen dira.

#### 6.6.2 Segurtasuna kudeatzeko kontrolak

347. Izenpek etengabe monitorizatzen du sistemak eta komunikazioak Izenperen Segurtasun Politikaren arabera funtzionatzen dutela ziurtatzeko. Prozesu guztiak erregistratu eta auditatu egiten dira indarrean dagoen legeria eta araudiaren arabera.

#### 6.6.3 Bizitza-zikloaren segurtasun-kontrolak

348. Probetarako, ekoizpeneko datuei ahalik eta gertuen dauden datu-kopuru handia behar da. Ekoizpeneko datu-baseak saihesten dira, batez ere datu pertsonalak dituztenak.

#### 6.7 Sareko segurtasun-kontrolak

349. 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. Barneko eta kanpoko trafikorako IPS sistemak daude erabilgarri.

#### 6.8 Denbora-iturria.

350. Izenpek Armadaren Errege Behatokirako konexio batetik lortzen du denbora bere sistemetatik, NTP protokoloari jarraituz. NTP protokoloaren deskribapena IETF RFC 5905 estandarrean aurki daiteke.

351. Barne-zerbitzu honetan oinarrituta, Izenpek denbora zigilatzeke zerbitzu bat (TSA) eskaintzen du, dokumentu arbitrarioen gainean denbora-zigiluak sortzeko erabil daitekeena, IETF RFC 3161 eta ETSI EN 319 421 arauen arabera. Informazio gehiago Izenperen Denbora Zigiluaren Praktiken Adierazpenean.



## 7 Ziurtagirien profilak eta baliogabetutako ziurtagirien zerrendak.

---

### 7.1 Ziurtagiri-profila

352. Izenpek igorritako ziurtagiriek honako arau hauek betetzen dituzte:

- Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 5280) Mayo 2008.
- Internet X.509 Public Key Infrastructure Authority Information Access Certificate Revocation List (CRL) Extension (RFC 4325) Diciembre 2005.
- Update to DirectoryString Processing in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 4630) Agosto 2006.
- ITU-T Recommendation X.509 (2005): Information Technology – Open Systems Interconnection – The Directory: Authentication Framework.
- ETSI EN 319 412.
- ROOT 3739: Internet X.509 Public Key Infrastructure – Qualified Certificate Profile.

#### 7.1.1 Bertsioaren zenbakia

353. Honako DPCG honen arabera jaulkitako ziurtagiriek X.509 estandarra erabiltzen dute, 3. bertsioa (bertsio-eremua zenbaki honen bidez betetzen da: "2").

#### 7.1.2 Ziurtagiriaren luzapenak.

354. [www.izenpe.eus](http://www.izenpe.eus) webgunean eskuragarri dagoen profil-dokumentuan adierazita daude.

#### 7.1.3 Algoritmoen objektu-identifikatzaileak.

355. RSA.

356. Izenpek RSA gakoa erabiltzen duela adierazi behar du rsaEncryption algoritmoaren identifikatzailearen bidez (OID: 1.2.840.113549.1.1.1). Parametroek presente egon behar dute eta NULL esplizituak izan behar dute.

357. Izenpek ez du beste algoritmo bat erabili behar, adibidez id-RSASSA-PSS algoritmo-identifikatzailea (OID: 1.2.840.113549.1.1.10), RSA gakoa dagoela adierazteko.

358. Behin kodetuta, RSA gakoentzako algoritmo-identifikatzailea BYTEZ BYTE berdina izan BEHAR DU hamaseitar bidez kodetutako honako byte hauekin: 300d06092a864886f70d0101010500 ECDSA.

359. CAk adierazi behar du ECDSA gakoa erabiltzen duela, id-ecPublicKey algoritmoaren identifikatzailearen bidez (OID: 1.2.840.10045.2.1). Parametroek namedCurve kodeketa erabili BEHAR dute.

- P-256 gakoetarako, namedCurve secp256r1 izan BEHAR DU (OID: 1.2.840.10045.3.1.7).
- P-384 gakoetarako, namedCurve secp384r1 izan BEHAR DU (OID: 1.3.132.0.34).
- P-521 gakoetarako, namedCurve secp521r1 izan BEHAR DU (OID: 1.3.132.0.35). Behin kodetuta, ECDSA gakoentzako algoritmo-identifikatzailea bytez byte berdina izan BEHAR DU byte hamaseitar hauekin.
- P-256 gakoetarako: 301306072a8648ce3d020106082a8648ce3d030107.



- P-384 gakoetarako: 301006072a8648ce3d020106052b81040022.
- P-521 gakoetarako: 301006072a8648ce3d020106052b81040023.

#### 7.1.4 Izenen formatuak.

360. Formatuak profilen dokumentuan daude adierazita, hemen eskuragarri: [www.izenpe.eus](http://www.izenpe.eus). CAren profilak dokumentu honen 1.3.1 atalean daude.

#### 7.1.5 Izen-murrizketak.

361. Izenpeko Agintaritza Subordinatuen ziurtagirien profilean ez da sartzen “name constraints” hedapena, beraz, ez da mota horretako murrizketarik ezartzen.

#### 7.1.6 Ziurtagiri-politikaren objektu-identifikatzailea (OID)

362. DPCG honetako 1.2 atalean zehaztutakoaren arabera.

#### 7.1.7 Politika-murrizketen luzapenaren erabilera.

363. Ez da erabiltzen politika-murrizketarik.

#### 7.1.8 Politika-kualifikatzaileen sintaxia eta semantika.

364. Certificate Policies luzapenak politika-kualifikatzaile hauek jasotzen ditu:

- CPS Pointer: Izenperen DPCGrako esteka dauka [www.izenpe.eus](http://www.izenpe.eus)
- User Notice: Testuzko ohartxo bat, aplikazio edo erabiltzaile batek eskatuta bistaritzen dena, hirugarren batek ziurtagiria egiaztatzean.
- Policy Identifier: Ziurtagiriaren OID adierazten du.

365. Ziurtagiri guztietan komuna den User Notice bat (SSL ziurtagiriak izan ezik<sup>5</sup>):

#### USER NOTICE

Kontsulta [www.izenpe.com](http://www.izenpe.com)-en terminoak eta baldintzak ziurtagirian fidatu edo erabili aurretik - Consulte en [www.izenpe.com](http://www.izenpe.com) los términos y condiciones antes de utilizar o confiar en el certificado

#### 7.1.9 “Certificate policy” hedapenaren tratamendu semantikoa.

366. Certificate Policy hedapenak Izenpek ziurtagiriari esleitzen dion politika identifikatzea ahalbidetzen du, eta politika horiek non aurki daitezkeen zehazten du.

## 7.2 Ziurtagiri baliogabetuen zerrendaren profila.

367. Izenpek igorritako ziurtagiriekin honako arau hauek betetzen dituzte:

---

<sup>5</sup> UserNotice eremua debekatuta dago SSL ziurtagirietan, Cabforum-eko BRG 2.0.0 bertsioaz geroztik.



- Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 5280) Mayo 2008.
- Internet X.509 Public Key Infrastructure Authority Information Access Certificate Revocation List (CRL) Extension (RFC 4325) Diciembre 2005.
- Update to DirectoryString Processing in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 4630) Agosto 2006.

368. RFC 6962 dokumentuan deskribatzen den bezala, aurreziurtagiri bat ez da RFC 5280an definitutako ezaugarriekin ziurtagiri bat bezala kontsideratuko.

#### 7.2.1 Bertsioaren zenbakia

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

#### 7.2.2 Ziurtagiri balio gabetuen zerrenda eta bertako elementuen hedapenak.

370. Erabilitako hedapenak honako hauek dira:

Eremua	Nahitaezkoa	Kritikoa
X.509v2 Extensions		
1. Authority key Identifier	Bai	Ez
2. CRL Number	Bai	Ez
3. Issuing Distribution Point	Bai	Ez
4. Invalidity Date	Bai	Ez

### 7.3 OCSP profila.

371. Izenperen OCSP erantzunak bat datoz RFC 6960 arauarekin (X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP), eta OCSP Responder erakundeak sinatzen ditu. Horren ziurtagiria kontsultatzen ari den ziurtagiria eman zuen CA berak sinatu du.

#### 7.3.1 Bertsioaren zenbakia

372. 3. bertsioa.

#### 7.3.2 OCSP luzapenak.

Eremua	Nahitaezkoa	Kritikoa
1. Issuer Alternative Name	Ez	Ez
2. Authority/Subject key Identifier	Ez	Ez
3. CRL Distribution Point	Ez	Ez
4. Key usage	Bai	Bai
5. Enhanced Key usage	Bai	Bai



### 7.3.3 OCSPren beste alderdi batzuk.

- OCSP zerbitzuak GET metodoa onartzen du.
- Ziurtagiriaren egoeraren informazioa etengabe eguneratuta dago.
- OCSP erantzunek 48 orduko balioa dute.
- Izenpek ez dituen ziurtagirien egoerari buruzko eskaeretan, REVOKED erantzuna itzultzen da.
- Izenpek jaulkitako ziurtagirien egoera eskatzen bada, eta egoera REVOKED bada, OCSP erantzunean sartzen da id-pkix-ocsp-extended-revoke luzapena.
- Izenpe ez den beste erakunde batek jaulkitako ziurtagiri baten egoera eskatuz gero, @Firma-tik jasotako erantzuna itzultzen da.
- Izenpek ez du OCSP Stapling onartzen.



## 8 Betetze-auditoriak

---

373. Izenpek urtero informazioaren segurtasun eta pribatutasunaren kudeaketa-plana ezartzen du, ezarritako segurtasun-eskakizunekin bat datorrela egiaztatzeko helburuarekin. ,

### 8.1 Auditoriaren maiztasuna.

374. Segurtasun-eskakizunen betetzea aldizka eta aurrez planifikatuta egiaztatzen da, beste jarduera batzuekin integratuta.

### 8.2 Auditorearen kualifikazioa.

375. Auditoreak egiaztatutako kualifikazioa eta esperientzia ditu Konfiantzazko Zerbitzu Emileen auditoriak egiten. ETSI EN 319 403 arauaren arabera egiaztatu behar da.

### 8.3 Auditorearen eta auditatutako erakundearen arteko harremana.

376. Auditoreak barnekoak edo kanpokoak izan daitezke, baina beti independenteak izango dira ekoizpen-zerbitzuarekiko.

### 8.4 Auditoriaren objektu diren elementuak.

377. Hauek dira auditatu beharreko elementuak:

- Konfiantzazko zerbitzuak..
- Informazio-sistemak.
- Datuak prozesatzeko zentroa babestea.
- Lotutako dokumentazioa.

### 8.5 Erabakiak hartzea, akatsen ondorioz.

378. Izenpek etengabeko hobekuntza-eredu bat ezartzen du, eta betetze-auditorien emaitzak eredu horren arabera lantzen dira. Larritasunaren eta presaren arabera, behaketa, hobekuntza eta desadostasun guztiak jarraipen-sistema batean sartzen dira, eta laguntza-tresna bat eskaintzen da. Emaizten komunikazioa.

379. Auditoria-txostenak Segurtasun Batzordeari ematen zaizkio, azter ditzan.



## 9 Beste gai legal eta jarduerarekin lotutakoak.

---

### 9.1 Tarifak

380. Izenpek bere Administrazio Kontseiluak onartutako tarifekin bat datozen ordain ekonomikoak jasoko ditu.

381. Eskainitako ordainketa-aukerak:

- Elektronikoki sinatutako ziurtagiri-eskaera: Ordainketa-pasabidearen bidez online ordainketa.
- Ordainketa-gutuna banku-erakundearen aurkezteko.
- Aurrez aurreko ordainketa Izenpeko Erregistro Erakunde batean, banku-txartelaren bidez.

382. Euskal Sektore Publikokoak diren entitateen kasuan, dagokion esparru arautzailean zehaztutako irizpideak aplikatuko dira.

#### 9.1.1 Ziurtagirien jaulkipen- edo berritze-tarifak.

383. Erabiltzaileek ziurtagiriak ematearen edo berritzearen truke ordaindu behar dituzten tarifak webgunean daude jasota: <https://www.izenpe.eus>

#### 9.1.2 Ziurtagirietarako sarbidearen tarifak.

384. Ez da aurreikusten.

#### 9.1.3 Ziurtagirien egoerari buruzko informazioa eskuratzeko tarifak.

385. Izenpek ziurtagirien egoeraren informazio-zerbitzuak eskaintzen ditu doan, bai CRL (Ziurtagiri Baliogabetze Zerrenda) bidez, bai OCSP bidez.

#### 9.1.4 Beste zerbitzu batzuen tarifak.

386. Beste zerbitzu batzuetarako aplikatu beharreko tarifak Izenperen eta bezeroen artean adostuko dira.

#### 9.1.5 Itzulketarako politika.

387. Izenpek ez dauka itzulketarako politikarik ezarrita.

### 9.2 Finantza-erantzukizuna

388. Izenpek, Erregistro Entitateek eta erabiltzaile-entitateek nahikoa baliabide dituzte beren jarduerak mantentzeko eta eginkizunak betetzeko.

#### 9.2.1 Erantzukizun zibileko aseguruia.

389. Izenpek erantzukizun zibileko aseguruia du, bere jardueraren ondoriozko akats edo ez-egiteengatik sortutako arriskuak estaltzen dituena, 5.000.000 €-ko kalte-ordain mugarekin erreklamazio eta aseguru-epe bakoitzeko.

#### 9.2.2 Beste aktibo batzuk

390. Ez daude aurreikusita.



### 9.2.3 Amaierako entitateentzako aseguruak eta bermeak.

391. Ez daude aurreikusita.

392. Informazioaren konfidentzialtasuna.

### 9.2.4 Informazio konfidentzialaren esparrua

393. Zerbitzua emateko, Izenpek zenbait informazio jaso eta gorde behar du, eta horien artean datu pertsonalak daude. Informazio hori zuzenean jasotzen da interesdunengandik, eta interesdunaren berariazko baimena lortzen da, edo interesdunaren baimenik gabe, datuak babesteko legeriak informazioa era horretan biltzea ahalbidetzen duen kasuetan.

394. Izenpek ziurtagiriak jaulkitzeko eta mantentzeko, eta beste ziurtapen-zerbitzu batzuk emateko beharrezkoak diren datuak soilik jasotzen ditu, eta ezin dira beste helburu batzuetarako erabili sinatzailearen berariazko baimenik gabe.

395. Izenpek DBEOn eta hura garatzeko araudian ezarritakoaren arabera garatzen du bere jardura.

396. Izenpek ez du datu pertsonalik zabalduko edo lagako, DPCG honetan aurreikusitako kasuetan izan ezik.

397. Honako informazio hauek modu konfidentzian gordetzen dituzte Izenpek eta Erregistro Erakundeek:

- Ziurtagiri-eskaerak, onartuak edo ukatuak, eta ziurtagiriak jaulki eta mantentzeko lortutako bestelako informazio pertsonala.
- Izenpek sortu eta/edo gordetako gako pribatuak.
- Transakzioen erregistroak, transakzio osoak eta auditoria-erregistroak barne.
- Izenpeko eta kanpoko auditoreek sortutako eta/edo mantendutako auditoria-erregistroak.
- Negozioaren jarraitutasun- eta larrialdi-planak.
- Segurtasun-politikak eta -planak.
- Funtzionamendu-dokumentazioa eta bestelako jardura-planak (artxiboa, monitorizazioa eta antzekoak).

### 9.2.5 Irismenean ez dagoen informazioa.

398. Informazio hau ez-konfidentzialtzat jotzen da, eta horrela onartzen dute eragindakoez, Izenperekin loteslea den tresna juridikoan:

- Jaulkitako ziurtagiriak edo jaulkitzeko bidean dauden ziurtagiriak.
- Ziurtagirian aipatutako erabilerak eta muga ekonomikoak.
- Ziurtagiriaren balio-epea, jaulkipen-data eta iraungitze-data barne.
- Ziurtagiriaren serie-zenbakia.
- Ziurtagiriaren egoera edo fase desberdinak eta bakoitzaren hasiera-data, hain zuzen ere: sortzeke eta/edo entregatzeke, baliozkoa, baliogabetua, etenekoa edo iraungia, eta egoera-aldaketaren arrazoia.



- Ziurtagiri Baliogabetuen Zerrendak (CRLak), bai eta baliogabetze-egoerari buruzko gainerako informazioak ere.
- Izenperen Argitalpen Zerbitzuan jasotako informazioa.
- DPCG honetako informazio konfidentzialaren atalean zehaztu ez den beste edozein informazio.

#### 9.2.6 Informazio konfidentziala babesteko erantzukizuna.

399. Izenpek informazio konfidentziala soilik zabalduko du legez aurreikusitako kasuetan.

400. Zehazki, ziurtagirian jasotako datuen fidagarritasuna bermatzen duten erregistroak ebidentzia gisa erabiliko dira epaiketa-prozedura batean beharrezkotzat jotzen bada.

401. Ziurtagiriak argitaratu egingo dira, eIDAS Erregelamenduak eta LSECek ezarritakoaren arabera.

### 9.3 Datu pertsonalen babesa.

402. Izenpek pribatutasunari eta datuen babesari buruzko informazioa argitaratzen du webgunean: [www.izenpe.eus/](http://www.izenpe.eus/).

#### 9.3.1 Pribatutasun-plana

403. Izenpek egiten duen datu pertsonalen tratamendua bat dator DBEOn, DBLOn eta garapen-araudian xedatutakoarekin.

#### 9.3.2 Pribatu gisa hartzen den informazioa.

404. Izenpek konfiantzazko zerbitzuen erabiltzaile diren pertsona fisikoei buruzko informazio pertsonal oro pribatu gisa tratatzen du.

#### 9.3.3 Pribatutzat jotzen ez den informazioa

405. Ez da informazio pribatutzat hartzen ziurtagiri elektronikoetan jasotzen den informazioa, haien baliozkotasun-egoerari buruzko informazioa, egoera horren hasiera-data (aktibo, baliogabetua, iraungia...), ezta egoeraren aldaketa eragin duen arrazoia ere. Beraz, ziurtagiri elektronikoak, Ziurtagiri Baliogabetuen Zerrendak (CRL) eta hauetan jasotako eduki oro ez da informazio pribatu gisa hartzen.

#### 9.3.4 Informazio pribatua babesteko erantzukizuna.

406. Ziurtagirien eskatzaileen eta sinatzaileen datu pertsonaletara sartzeari eta datu horiek tratatzeari dagokionez, Izenpek DBEOren arabera eskatzen diren segurtasun-neurriak hartzen ditu.

407. Neurri tekniko eta antolakuntzakoak ezarriko dira teknologiaren egoera, aplikazio-kostuak, tratamenduaren izaera, irismena, testuingurua eta helburuak, eta pertsonen eskubide eta askatasunetarako arriskuak kontuan hartuta.

#### 9.3.4.1 Datuak babesteko ordezkaria.

408. Izenperen DPDrekin harremanetan jartzeko datuak ([www.izenpe.eus/datos](http://www.izenpe.eus/datos) web-orrian daude argitaratuta). Harremanetarako datu horiek helbide elektroniko bat dute, interesdunek beren datu pertsonalen tratamenduari eta beren eskubideen erabilerari buruzko gai guztiak hara bidal ditzaten, DBEOren 38.4 artikularen arabera.



#### 9.3.4.2 Tratamendu-jardueren erregistroa.

409. Izenpek bere ardurapean egiten dituen tratamendu-jardueren erregistroa dauka, eta horien artean dago “Identifikazio-bitartekoen kudeaketa” izeneko tratamendua, konfiantzazko zerbitzuen hornitzaile gisa duen jarduerarekin lotuta. Erregistro horrek, identifikatutako tratamendu bakoitzerako, informazio hau jasotzen du:

- Xedea
- Erakunde arduraduna
- Datu pertsonalen kategoriak
- Nork ematen ditu datuak
- Nor da datu pertsonalen eragindakoa
- Tratamenduaren arduradunak
- Datuen komunikazioak
- Datuen nazioarteko transferentziak
- Ezabatzeko epea
- Segurtasun-neurriak

410. Tratamendu-jardueren erregistroaren dokumentua hemen kontsultatu daiteke: [www.izenpe.eus/datos](http://www.izenpe.eus/datos).

#### 9.3.4.3 Interesdunen eskubideak.

411. Interesdunek datuak eskuratzeko, zuzentzeko, ezabatzeko, tratamendua mugatzeko, aurka egiteko eta datuen eramangarritasunaren eskubideak baliatu ahal izango dituzte, DBEOren 15etik 22ra bitarteko artikuluetan ezarritakoaren arabera, honako hauen bidez:

- Posta: eskaerarekin batera, NANaren/AIZen kopia bat aurkeztu behar da.
- Bide elektronikoz, eskaera sinatuz pertsona fisikoaren ziurtagiri kualifikatuaren bidez.

#### 9.3.4.4 Auzitegi eta agintariekiko lankidetzak.

412. Izenpe lankidetzan arituko da datuak babesteko agintaritzekin, hala eskatzen zaionean.

#### 9.3.4.5 Segurtasun-urratzeen jakinarazpenak.

413. Izenpek Datuak Babesteko Euskal Agintaritzari (aurrerantzean, DBEA) jakinaraziko dio datu pertsonalen arloko segurtasun-urraketa oro, lehenbailehen eta, betiere, arduradunak urraketa horren berri izan eta hurrengo 72 orduen barruan, baldin eta urraketa horrek eragindako pertsona fisikoen askatasunetarako arriskua ekar badezake.

414. Segurtasun-urraketak interesdunen eskubide edo askatasunetarako arrisku handia ekar dezakeen kasuetan, DBEAr egindako jakinarazpenarekin batera interesdun horiei zuzendutako jakinarazpen bat ere bidaliko da, urraketa horren ondorioetatik babesteko neurriak hartu ahal izan ditzaten.



### 9.3.5 Informazio pribatuaren erabilerari buruzko abisua eta baimena.

415. Ziurtagirien bizi-zikloarekin lotutako prozesuetan (eskaera, nortasuna egiaztatzea, berritzea, baliogabetzea...) pertsona fisikoen informazio pribatua eskuratzea interesdunaren adierazpen bidez edo ekintza afirmatibo argi baten bidez egingo da.

### 9.3.6 Zabalkundea, prozesu judizial edo administratiboaren arabera.

416. Izenpek ez du datu pertsonalik zabalduko, agintari administratibo edo judizialek hala eskatzen ez badute.

### 9.3.7 Informazioa hedatzeko beste inguruabar batzuk

417. Ez daude aurreikusita.

## 9.4 Jabetza intelektualeko eskubideak

### 9.4.1 Ziurtagirien jabetza.

418. Izenpe da egiten dituen ziurtagirien gaineko jabetza intelektualaren eskubideak dituen erakunde bakarra.

419. Kanpoan geratzen dira ziurtapen elektronikoko sistema osatzen duten aplikazioetatik eratorritako jabetza intelektual eta industrialeko eskubideak, hirugarren batenak badira.

420. Arau berberak aplikatu behar zaizkio ziurtagiriak ezeztatzeko informazio-sistemari.

### 9.4.2 DPCGren jabetza.

421. Izenpe da DPCG honen jabea.

### 9.4.3 Izenekin lotutako informazioaren jabetza

422. Harpidedunak, eta hala badagokio, sinatzaileak, ziurtagirian jasotako marka, produktu edo merkataritza-izenari buruzko eskubiderik balego, eskubide horiek beretzat gordetzen ditu.

423. Harpidedunak, eta hala badagokio, sinatzaileak, DPCGren 3. atalean zehaztutako informazioekin osatutako ziurtagiriaren izen bereziaren jabetza dauka.

### 9.4.4 Gakoak eta haiekin lotutako materialaren jabetza.

424. Gako-pareak ziurtagirien harpidedunen jabetzakoak dira.

## 9.5 Betebeharrak eta bermeak.

425. Izenpek, DPCG honen arabera ziurtagiriak igortzen dituen ziurtapen-erakunde gisa, honako betebeharrak hartzen ditu bere gain:

### 9.5.1 CAren betebeharrak

#### 9.5.1.1 Zerbitzuaren ematearen betebeharrak.

426. Izenpek bere ziurtapen-zerbitzuak DPCG honetan xedatutakoaren arabera eskaintzen ditu. Bertan, bere eginkizunak, jarduera-prozedurak eta segurtasun-neurriak zehazten dira. Zehazki, bere gain hartzen du dagokion betebeharrak guztiak betetzea, salbu eta erregistro-erakundeak berariaz burututako jarduketak, baldin eta Izenpe ez bada erakunde hori.

427. Betebeharrak honako hauek dira:



- Ez kopiatzea bere zerbitzuak jaso dituen pertsonaren sinadura-sortzeko datuak.
- Sistemaren mantentzea, non jasoko baitira igorritako ziurtagiriak eta haien egoera: indarrean dauden, etenda dauden edo iraungitako ziurtagiriak.
- Ziurtagiri kualifikatuei eta une bakoitzean indarrean dauden ziurtatze-praktiken deklarazioei buruzko informazio eta dokumentazio guztia edozein bide segururen bidez erregistratuta gordetzea, gutxienez 15 urtez, azkentzen diren unetik zenbatzen hasita, era horretan, harekin egindako sinadurak eta gainerako ziurtagiriei dagozkienak egiaztatu ahal izateko, 7 urtez.
- Sinatzailea bere sinadura sortzeko datuen jabe dela ziurtatzea, eta ziurtagirian ageri diren egiaztapen-datuekin bat datozeela bermatzea.
- Sinadura sortzeko eta egiaztatzeko datuen osagarritasuna bermatzea, betiere biak ziurtapen-zerbitzuen hornitzaileak sortuak badira.
- Segurtasun-araudia eta estandarrak betetzea (DBEO, ISO, ETSI eta Izenperen Segurtasun Politika).
- Ostatu-hornitzaileei eskakizun modura ezartzea araudi eta segurtasun-estandarren betetzea (DBEO, ISO, ETSI, CABForum eta Izenperen Hornitzaileen Segurtasun Politika).

#### 9.5.1.2 Fidagarritasun-operazioaren betebeharrak.

428. Izenpek honako hauek bermatzen ditu:

- Ziurtagirian jasotako identitatea bertan jasotako gako publikokoarekin zalantzarik gabe bat datorrela.
- Zerbitzuaren ematea azkar eta seguru egiten dela. Zehazki, ziurtagirien baliozkotasuna kontsultatzeko zerbitzu azkar eta segurua erabiltzeko aukera eskaintzen da, eta ziurtagirien iraungipena modu seguruan eta berehalakoan jakinarazten dela bermatzen da, DPCG honetan xedatutakoaren arabera. Zerbitzua eskuragarri dagoela astean 7 egun, 24 orduz.
- Sinadura elektronikoko indarreko araudiak ezartzen dituen eskakizun teknikoak eta langile-baldintzak betetzea:
  - Ziurtapen-zerbitzuak emateko behar den fidagarritasuna egiaztatzea.
  - Ziurtagiri bat noiz igorri edo haren balioa noiz amaitu den zehaztasunez zehaztu ahal izatea bermatzea.
  - Ziurtapen-zerbitzuak eskaintzeko behar diren gaitasuna, ezagutzak eta esperientzia dituzten langileak erabiltzea, eta sinadura elektronikoaren eremuan segurtasun- eta kudeaketa-prozedura egokiak aplikatzea.
  - Ziurtapen-prozesuen oinarri diren sistemak eta produktuak fidagarriak izatea, edozein aldaketaren aurka babestuta egotea, eta segurtasun teknikoa (eta, hala badagokio, kriptografikoa) bermatzea, Segurtasun Politikaren arabera.
  - Ziurtagiri faltsutzeen aurkako neurriak hartzea eta 6. atalean adierazitakoaren arabera sortze-prozesuko konfidentzialtasuna bermatzea, baita ziurtagiria sinatzaileari modu seguruan ematea ere.



- Ziurtagiri kualifikatuak biltegitratzeko sistemak fidagarriak erabiltzea, haien autentifikazioa egiaztatzeko aukera emango dutenak eta baimenik gabeko pertsonak datuak aldatzea eragotziko dutenak; halaber, sinatzaileak adierazitako egoeretan edo pertsonentzako sarbide-mugak ezarriko dituztenak, eta segurtasun-baldintza horietan edozein aldaketa hautemateko aukera emango dutenak.
- ISO/IEC 27001ak ezarritako printzipioetan oinarritutako Informazioaren Segurtasunaren Kudeaketa Sistemaren ezarpenari esker, honako neurri hauek barne, segurtasuna modu egokian kudeatzen da:
  - Segurtasun-egiaztapen erregularrak egiteko, ezarritako estandarrak betetzen direla egiaztatzeko.
  - Segurtasun-gertakizunen kudeaketa osoa burutzea, haien detekzioa, konponketa eta hobekuntza bermatzeko.
  - Segurtasunaren arloan interesa duten taldeekin harremanak eta kontaktuak mantentzea, hala nola espezialistak, segurtasun-foroak eta informazioaren segurtasunarekin lotutako elkarte profesionalak.
  - Sistemaren mantentze eta garapena behar bezala planifikatzea, erabiltzaileen eta bezeroen itxaropenak betetzen dituen zerbitzu eta errendimendu egokia beti bermatzeko.

#### 9.5.1.3 Identifikazio-betebeharrak.

429. Ziurtagiri kualifikatuei dagokienez, Izenpek ziurtagiriaren harpideduna identifikatzen du, 2015eko irailaren 8ko 2015/1502 (EB) Erregelamendu Exekutiboak eta DPCG honek ezarritako ziurtasun-mailen arabera.

#### 9.5.1.4 Erabiltzaileak informatzeko betebeharrak.

430. Ziurtagiria ematea eta harpidedunari entregatzea baino lehen, Izenpek dokumentu baten bitartez informatzen du ziurtagiriaren erabilerarekin lotutako termino eta baldintzez, prezioaz —ezarrita badago—, erabilera-mugez eta DPCG honen 2. ataleko erreferentzia juridiko loteslez.

431. Izenpek sinatzaileari jakinaraziko dio ziurtagiriaren indarraldia iraungi egin dela, ziurtagiri elektronikoaren indarraldia amaitu aurretik edo aldi berean, eta zehaztuko dio zergatik eta zer egun eta ordutan geratuko den ziurtagiria indarririk gabe.

432. Izenpek bi hilabete lehenago jakinaraziko die sinatzaileei bere ziurtapen-zerbitzuen emate-jardueraren etenaz, eta, behar izanez gero, kudeaketa transferitzeko proposatzen den hornitzailearen ezaugarriak emango ditu. Sinatzaileei zuzendutako komunikazioak dokumentu honetan jasotakoaren arabera egingo dira.

433. Izenpek bere jarduera etenaren amaierarako plan bat du, non zehazten diren egoerak eta baldintzak, nola burutuko litzatekeen.

#### 9.5.1.5 Balidazio-programen betebeharrak.

434. Izenpek publikoarentzako sarbidea duten ziurtagirien balidazioa egiteko mekanismoak eskaintzen ditu, DPCG honetan deskribatutako sistemak erabiliz.



#### 9.5.1.6 Ziurtapen-zerbitzuaren araudi juridikoari buruzko betebeharrak.

435. Izenpek bere gain hartzen ditu zuzenean ziurtagiriaren barruan jasotako edo erreferentziaren bidez barneratutako betebeharrak guztiak. Erreferentziaren bidezko barneratzea ziurtagiriaren barruan objektu-identifikatzaile bat edo beste dokumentu bati lotura bat sartuz lortzen da.

436. Izenpe eta eskari-emailea, harpideduna edo sinatzailea eta ziurtagirian konfiantza duten hirugarrenen arteko instrumentu juridikoa idatzizkoa eta ulergarria izan behar da, eta gutxienez honako edukia izan behar du:

- DPCG honen 2. atalean ezarritako baldintzak betetzeko aginduak.
- Aplikatzen den DPCGren adierazpena, eta, behar izanez gero, publikoari emandako ziurtagiriak direla eta sinadura-sortzeko edo mezuren deszifratze segururako gailuaren beharra.
- Ziurtagiriaren igorpenari, baliogabetzeari, berritzei eta, behar izanez gero, gako pribatuen berreskuratzeari buruzko klausulak.
- Ziurtagirian jasotako informazioa zuzena dela adieraztea, harpidedunak aurka ez badu jakinarazten.
- Harpidedunaren erregistroan erabilitako informazioa gordetzeko baimena, gailu kriptografiko bat eskaintzeko eta informazio hori hirugarrenengana komunikatzeko, Izenperen jardura amaitzen denean baliozko ziurtagiririk baliogabetu gabe.
- Ziurtagirien erabileraren muga, 1.4 atalean ezarritakoak barne.
- Ziurtagiri bat nola balidatu azalpenak, ziurtagirien egoera egiaztatze eskakizuna barne, eta ziurtagirian modu arrazoizkoan konfiantza egin daitekeen baldintzak.
- Ardura-mugak, Izenpek zein erabileretarako onartzen duen eta zeinetarako baztertzen duen ardura barne.
- Ziurtagirien eskaeraren informazioa artxibatze epea.
- Auditoria-erregistroak artxibatze epea.
- Talka-konponbiderako aplikatzen diren prozedurak.
- Aplikatzen den legeria eta jurisdikzio egokia.
- Izenperen ardura patrimoniala nola bermatzen den.

#### 9.5.2 Erregistro-erakundearen betebeharrak.

437. Izenpek hirugarren bati erregistro-erakundearen funtzioen delegazioa baimendu aurretik, hirugarren horrek formalki hartu beharko ditu honako betebeharrak hauek, dagokion tresna juridikoaren bidez:

- Ziurtagirietan agertzen diren edo ziurtagirien xedeetarako garrantzitsuak diren eskatzailearen, harpidedunaren eta sinatzailearen identitatea eta bestelako inguruabar pertsonalak egiaztatzea.
- Ziurtagiriek lotutako informazio eta dokumentazio guztiak gordetzea, hala nola igorpena, berritzea, baliogabetzea edo berraktibatzea kudeatzen duenak.



- Ziurtagiriak baliogabetzeko eskaerak Izenperi azkar eta modu fidagarrian jakinaraztea, behar den arduraz jardunez.
- Izenpek artxiboetarako sarbidea izatea eta bere funtzioak betetzeko prozeduren auditoria egitea ahalbidetzea, baita horretarako beharrezko informazioa mantentzea ere.
- Izenperi jakinaraztea jaulkipen-, berritze-, berraktibazio-eskaerak eta ziurtagiriei eragiten dien edozein beste alderdi.
- Ziurtagirien indarraldian eragina izan dezaketen baliogabetze-arrazoiak egiaztatzea, dagokion zorrotasunarekin.
- Ziurtagiriak igortze, berritze, baliogabetze eta berraktibatze kudeaketa-funtzioak betetzean Izenpek eta arlo horretako legeria indarrean duten prozedurak betetzea.
- Izenperen Hornitzaileen Segurtasun Politikaren betetzea.

### 9.5.3 Jabeen betebeharrak.

438. Ziurtagiriaren eskatzaileak honako hauek bete beharko ditu:

- Ziurtagirien eskaeran emandako informazioa egia, osoa eta eguneratua dela bermatzea, eta ziurtagirietan agertu behar dela.
- DPCGen dagokion PDSetan ezarritako eskaera-prozedura betetzea.

439. Harpidedunak betebeharrak hauek ditu:

- Izenperi informazio osatua eta egokia ematea, batez ere DPCGren erregistro-prozedurari dagokionez.
- Ziurtagirietan jasotako informazioa egia, osoa eta eguneratua dela bermatzea.
- Ziurtagirien erabilerarako baldintzak ezagutzea eta onartzea, baita horietan egiten diren aldaketak ere.
- Ziurtagiri baten igorpena eta entrega onartzea adieraztea.
- Ziurtagirien euskarriaren erabilera egokia eta zaintza bermatzea.
- Ziurtagiria modu egokian erabiltzea, eta, zehazki, ziurtagirien erabilera-muga betetzea.
- Bere gako pribatuaren zaintzan arduratsua izatea, baimenik gabeko erabilerak saihesteko, DPCGren 6.1, 6.2 eta 6.4 ataletan jasotakoaren arabera.
- Izenperi eta ziurtagirian konfiantza duen pertsona orori jakinaraztea atzerapen bidezko arrazoirik gabe:
  - Bere gako pribatuaren galera, lapurreta edo arriskua.
  - Gako pribatuaren gaineko kontrola galtzea, aktibazio-datuak arriskuan jartzeagatik (adibidez, gailu kriptografikoaren PIN kodea) edo beste edozein arrazoiengatik.
  - Ziurtagiriaren edukian dauden zehaztasun-gabeziak edo aldaketak, horiek baliogabetze-arrazoia badira, ziurtagiriaren baliogabetzea eskatuz.
- Ziurtagiriaren balioaldia amaitu ondoren, gako pribatuaren erabilera etetea.



- Sinatzaileei beren betebeharrak zehatzak transferitzea.
- Izenperen baimen idatzirik gabe, ziurtapen-zerbitzuen inplementazio teknikoak ez monitortzea, manipulatzeko edo haren gaineko alderantzizko ingeniarietako ekintzak egitea.
- Ez arriskuan jartzea nahita ziurtapen-zerbitzuen segurtasuna.
- Ziurtagirietan jasotako gako publikoen dagokien gako pribatuak ez erabiltzea inolako ziurtagiriak sinatzeko, ziurtapen-erakunde baten moduan jardutea saihestuz.

440. Ziurtagiri kualifikatuek beren ziurtagiriaren gako pribatuaren bidez sinadura elektronikoak sortzen badituzte, lege-tresna egokian onartu beharko dute sinadura elektroniko horiek eskuzko sinadurekin parekoak direla, betiere gailu kriptografiko bat erabiliz, eIDAS araudian ezarritakoa betez.

#### 9.5.4 Konfiantza duten aldeen betebeharrak.

441. Ziurtagirietan konfiantza duten erabiltzaile egiaztatzaileek honako betebeharrak dituzte:

- Modu independentean aholkatzea, ziurtagiria aurreikusitako erabilerarako egokia den ala ez zehazteko.
- Ziurtagirien erabilera-baldintzak ezagutzea, DPCG honetan eta egiaztatzailearen eta Izenperen arteko ziurtapen-zerbitzuen kontratuan jasotakoa betez.
- Igorritako ziurtagirien baliozkotasuna edo baliozabetzea egiaztatzea, horretarako ziurtagirien egoerari buruzko informazioa erabiliz.
- Ziurtagiri-hierarkiako ziurtagiri guztiak egiaztatzea, sinadura elektroniko batean edo hierarkiako beste edozein ziurtagiritan konfiantza izan aurretik.
- Ziurtagirian bertan edo egiaztatzailearen kontratuan jasota egon ala ez, ziurtagirien erabileran dauden muga guztiak kontuan hartzea.
- Kontratu batean edo beste tresna juridiko batean ezarritako prebentzio-neurri guztiak kontuan hartzea, haien izaera juridikoa edozein dela ere.
- Ziurtagiriari buruzko edozein gertaera edo egoera anomalo jakinaraztea, baliozabetze-arrazoi izan daitezkeenak.
- Izenperen baimen idatzirik gabe, ziurtapen-zerbitzuen inplementazio teknikoak ez monitortzea, manipulatzeko edo haren gaineko alderantzizko ingeniarietako ekintzak egitea.
- Ez arriskuan jartzea nahita ziurtapen-zerbitzuen segurtasuna.

#### 9.5.5 Beste partaideen betebeharrak.

442. Izenpek, Denbora-Zigilatze Agintaritza gisa bere zerbitzua ematean, erantzukizuna hartzen du erreferentzia denboraren aldagarritasunagatik, Armadaren Errege Institutuko Ordu Sailak emandakoa, zerbitzuaren eskaeraren unean zigilu elektronikoetan sartzen duena, baina ez du erantzukizunik hartzen zerbitzuaren erabiltzaile diren entitateek bidalitako datu elektronikoek adierazten dituzten edukien egiazkotasunagatik, izan ere, hauek dira igorritako zigilu elektronikoaren objektua.



## 9.6 Bermeetatik uko egitea.

443. Ez da aurreikusten.

## 9.7 Arduraren mugak

### 9.7.1 Ziurtapen Agintaritzaren ardura

444. Izenpek erantzukizuna izango du akats edo arduragabekeria egonez gero, DPCG honetan deskribatutako ziurtapen-zerbitzuetan, baita sinadura elektronikoari buruzko legerian ezarritako betebeharrak betetzen ez direnean ere, honako salbuespen hauetan izan ezik:

- Izenpe ez da ziurtagirietan Ziurtapen Praktiken Deklarazioan contenidas informazioek eragindako kalteen erantzule izango, baldin eta haien edukiak DPCG hau betetzen badu funtsean.
- Izenpe ez da ziurtagirietan jasotako informazioek eragindako kalteen erantzule izango, baldin eta ziurtagirien edukiak DPCG hau betetzen badu funtsean.
- Izenpek ez du inolako erantzukizunik izango kalte zuzen zein zeharreatatik, bereziki berezko, sorpresazko, galerazko, datu-galera, kalte punitiboetarako, aurreikusitakoak izan edo ez, ziurtagirien erabilerarekin, entrega, lizentzia, funtzionamendu edo hutsarekin, sinadura elektronikoekin edo DPCG honetan jasotako bestelako transakzio edo zerbitzuen erabilera okerrarekin lotuta sortutako kalteengatik.
- Izenpek ez du erantzukizunik izango harpidedunari edo hirugarren onargarri bati eragindako kalteengatik, ziurtagiriak jasotzen dituzten datuen zehaztasun faltagatik, datu horiek dokumentu publiko notarial, judizial edo administratibo baten bidez frogatu badira, salbu eta datu horiek erregistro-erakundeak aurkeztutako dokumentuari dagokionez.
- Izenpek ez du erantzukizunik izango harpidedunaren edo ziurtagirietan konfiantza duten hirugarren onargarri baten betebeharrak betetzeari uztearen ondoriozko kalteengatik.

445. Izenpek erantzukizuna hartuko du ziurtagirien baliozkotasun kontsulta zerbitzuan edo balio gabetzearen kontsulta zerbitzuan sartzean hutsik edo atzerapenarekin pertsona orori eragindako kalteengatik.

446. Era berean, erantzukizun osoa hartuko du hirugarrenekin, ziurtapen-zerbitzuak emateko beharrezko funtzioak betetzeko horretarako delegatutako pertsonen jokabideagatik.

### 9.7.2 Erregistro-erakundearen erantzukizunak

447. Izenpetik bestelako edozein erakunde, erregistro-erakundetzat jarduten duena, erantzukizuna izango du Izenperen aurrean, bere betebeharrak betetzean sortzen diren kalteengatik, dagokion tresna juridikoan ezarritako terminoetan.

448. Identifikazio-funtzioak ziurtagirien harpidedun diren administrazio publikoek betetzen dituztenean, administrazio publikoen erantzukizun patrimoniala aplikatuko da, Administrazio Publikoen Araudi Juridikoaren eta Administrazio Prozedura Arruntaren Legeak ezarritakoaren arabera.



### 9.7.3 Harpidedunen erantzukizunak

449. Harpidedunak erantzukizuna izango du bere gako pribatuarekin sortutako sinadura elektronikoa batekin autentifikatutako komunikazio elektronikoa guztiengatik, Izenpek emandako egiaztapen-zerbitzuen bidez ziurtagiria baliozkoa dela egiaztatu bada.

450. DPCG honetan jasotakoaren arabera ziurtagiriaren galera edo lapurreta jakinarazi arte, ziurtagiriaren baimenik gabeko eta/edo erabilera okerragatik sortu daitezkeen erantzukizunak beti harpidedunari egokituko zaizkio.

451. Ziurtagiriaren onarpena eginez, harpidedunak konpromisoa hartzen du Izenperi, erregistro-erakundeei eta Erabiltzaile Erakundeei kalte, galerak, zorra, prozesu-gastu edo edozein motatako gastu, baita ordainketa profesionalak ere, ordaintzeko eta babesteko, ziurtagiriaren erabilerak edo argitalpenak eragindako edozein ekintza edo ez-ekintzagatik, eta hurrengo egoeretan sortutakoak:

- Ziurtapen-erakundearen eta haren arteko instrumentu juridikoan ezarritako terminoak betetzeko betebeharra ez betetzeagatik,
- Ziurtagiriaren erabilera baimenik gabeko pertsonen artean komunikazio elektronikoa egiteagatik,
- Harpidedunaren gezurrezko edo akats faktikoengatik,
- Ziurtagirietan oinarritutako datuen bat huts eginez edo Izenpe, Erakunde Publiko Erabiltzaileak edo harpidedunaren ziurtagiriari konfiantza egiten dioten hirugarrenei iruzur egiteko asmoz faltsutzea edo ezkutatzea,
- Gako pribatuak zaintzeko betebeharra ez betetzea eta gako pribatuak ez galtzeko, ez ezagutarazteko, ez aldatzeko edo baimenik gabe ez erabiltzeko arrazoizko diren neurriak hartzea.

452. Horrela, Izenpek ez du erantzukizunik izango harpidedunari edo hirugarren onargarri bati eragindako kalteengatik, honako betebeharrak ez betetzeagatik:

- Izenperi edo Erregistro Entitateari informazio egiazkoa, osoa eta zehatza ematea ziurtagirian jaso behar diren edo ziurtagiria egiteko edo ezeztatzeko beharrezkoak diren datuei buruz, zerbitzu-emaileak datu horiek oker daudela atzeman ezin duenean.
- Izenperi edo Erregistro Erakundeari berehala jakinaraztea ziurtagiriaren egoerarekin lotutako edozein aldaketa.
- Bere sinadura-sortzeko datuak modu arduratsuan gordetzea, konfidentziasuna bermatzeko eta sarrera edo deskubrimendu ezkutuetatik babesteko.
- Ziurtagiriaren sinadura-sortzeko datuen konfidentziasunaren segurtasunari buruz zalantzarik badu, ziurtagiriaren baliogabetzea eskatzeko.
- Sinadura sortzeko datuak ez erabiltzea ziurtagiriaren baliotasun-aldia amaitzen den unetik edo zerbitzu-emaileak indarraldia galdu duela jakinarazten dion unetik.
- Ziurtagirian jasotako erabilera-mugak errespetatzea eta ziurtapen-zerbitzuen sinatzaileari ezarritako baldintzak betez erabiltzea.



#### 9.7.4 Ziurtagirietan konfiantza duten hirugarrenen erantzukizunak

453. Ziurtagiri baliogabe batean edo egiaztatu ezin den sinadura elektronikoko batean konfiantza duten hirugarrenek, arrisku guztiak bere gain hartzen dituzte, eta ezingo diete Izenperi, erregistro-erakundeei, erabiltzaile-erakundeei edo harpidedunei inolako erantzukizunik eskatu, ziurtagiri eta sinadura horietan oinarritutako edozein kontu dela medio.

454. Horren haritik, Izenpek ez du erantzukizunik izango harpidedunari edo hirugarren onargarri bati eragindako kalteengatik, dokumentu sinatuen hartzaileak zainketa-betebehar hauetako bat betetzen ez badu:

- Ziurtagirian jasotako erabilera-mugak eta horrekin egin daitezkeen transakzioen kopuru indibidualizatua egiaztatzea eta kontuan hartzea.
- Ziurtagiriaren baliozkotasuna ziurtatzea.
- Ziurtagiri kualifikatuaren identifikatzailea Trusted Service List (TSL) zerrendan egiaztatzea.

#### 9.8 Kalte-ordainak.

455. Izenpek, harpidedunarekin eta egiaztatzailearekin lotzen duten tresna juridikoetan, bere betebeharrak edo aplikagarri den legeria urratzeagatik kalte-ordainen klausulak jasotzen ditu.

#### 9.9 Balio-aldia.

##### 9.9.1 Indarrean jartzea

456. DPCG argitaratzen den unean jartzen da indarrean.

##### 9.9.2 Amaiera

457. DPCG hau bertan behera geratuko da bertsio berri bat argitaratzen den unean. Bertsio berriak aurreko dokumentua osorik ordezkatuko du.

##### 9.9.3 Amaieraren ondorioak.

458. DPCG zahar baten arabera igorritako indarreko ziurtagirientzat, bertsio berriak lehena ordezkatuko du, biek kontraesanik ez badute.

#### 9.10 Jakinarazpen indibidualak eta partaideekiko komunikazioa.

459. Izenpek harpidedunarekin lotura juridikoa duen tresna batean ezartzen ditu jakinarazpen eta komunikaziorako bitarteko eta epeak.

460. Orokorrean, Izenperen webgunea erabiliko da jakinarazpen eta komunikazio mota guztietarako: [www.izenpe.eus](http://www.izenpe.eus).

#### 9.11 Dokumentu honen aldaketak.

##### 9.11.1 Aldaketetarako prozedura.

461. Dokumentu honetako aldaketak Izenperen Segurtasun Batzordeak onartuko ditu. Aldaketa horiek DPCGren eguneratze dokumentu batean jasoko dira, eta horren mantentze-lana Izenpek bermatzen du.



462. DPCGren bertsio eguneratuak eta egindako aldaketen zerrenda [www.izenpe.eus](http://www.izenpe.eus) helbidean kontsulta daitezke.

463. Izenpek DPCG alda dezake modu unilateralean, honako prozedura honen arabera:

- Aldaketa arrazoi tekniko, juridiko edo komertzial batengatik justifikatua egon behar da, eta Izenperen Segurtasun Batzordeak babestua izan behar du.
- Zehaztapen berrien aldaera tekniko eta juridiko guztiak kontuan hartu behar dira.
- Aldaketak kontrolatzeko sistema bat ezarri behar da, aldaketa horrek bete nahi ziren eskakizunak betetzen dituela bermatzeko.
- Zehaztapen aldaketak erabiltzaileari nola eragiten dion zehaztu behar da, eta beharrezkoa denean, aldaketa horien jakinarazpena egitea aurreikusi behar da.

#### 9.11.2 Jakinarazpenaren epea eta mekanismoa.

464. Izenperen Segurtasun Batzordeak urtean behin berrikusiko du DPCG, baita beharrezko den edozein aldaketa egiteko unean ere. Berrikuspen hau arduradun eta parte-hartzaile diren eremu guztien artean egingo da, bai prestaketarako bai mantentzerako.

465. Izenpe-k dokumentu honetan aldaketak egin ahal izango ditu, erabiltzaileei alde zuzenetik jakinarazi beharrik gabe. Adibidez:

- Dokumentuaren tipografia-akatsen zuzenketak.
- Harremanetarako informazio-aldaketak.

466. Erabiltzaileei jakinarazi behar zaizkien aldaketak, esaterako:

- Zerbitzuaren zehaztapen edo baldintzen aldaketak.
- URLen aldaketak.

#### 9.11.3 OID bat aldatzea beharrezkoa den egoerak.

467. OID aldaketa egingo da dokumentu honetan deskribatutako prozeduren batean aldaketak egonez gero.

### 9.12 Kexak eta gatazken konponbidea.

468. Izenpe kontsumoko arbitraje-sistemari dago lotuta, aplikagarri den legerian ezarritako terminoetan, eta sistemak bi aldeentzat loteslea eta exekutagarria den moduan kexa edo erreklamazioak artatzeko eta konpontzeko bitarteko gisa balio du, herritarren ziurtagirien kasuan eskaerari edo harpidedunari dagokionez.

469. Helburu horrekin, uste da eskatzaileak edo harpidedunak sistema horretara jotzen duela kontsumoko arbitraje-batzordearen aurrean arbitraje-eskaera formalizatzen den unean.

470. Herritarren ziurtagiriak arloko eskaerari edo harpidedunei buruz sor daitezkeen bestelako auziak, kontsumoko arbitraje-sistemari lotuta ez daudenak, jurisdikzio egokiaren mende geratuko dira.

471. Aldeek erabaki dute haien artean sortzen den edozein gatazka Zuzenbide Kolaboratiboko prozesu baten bidez ebazteko dutela, eta, ados jarri ezean, Vitoria-Gasteizko epaitegi eta auzietara jo ahal izango da.



### 9.13 Aplikagarri den araudia.

472. Espainiako sinadura elektronikoari buruzko legea aplikatuko da DPCG honen exekuzioari, prestakuntzari, interpretazioari eta baliozkotasunari dagokienez.

473. Dokumentu honi eta honetatik eratorritako jardueri aplikatzen zaien araudia honako hau da:

- 910/2014 (EB) Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2014ko uztailaren 23koa, barne-merkatuko transakzio elektronikoetarako identifikazio elektronikoari eta konfiantzazko zerbitzuei buruzkoa, 1999/93/EE Zuzentaraua indargabetzen duena
- 6/2020 Legea, azaroaren 11koa, Konfiantzazko zerbitzu elektronikoaren zenbait alderdi arautzekoa.
- 2016/679 (EB) Erregelamendua, pertsona fisikoak datu pertsonalen tratamenduari dagokionez babesteari eta datu horien zirkulazio askeari buruzkoa, 95/46/EE Zuzentaraua indargabetzen duena.
- 3/2018 Lege Organikoa, abenduaren 5koa, Datu Pertsonalak Babestekoa eta Eskubide Digitalak Bermatzekoa.

474. Gainera, Izenpek emandako konfiantzazko zerbitzuen praktikak honako estandar hauei jarraitzen die:

- ETSI EN 319 401: General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1: Policy and security requirements for Trust Service Providers issuing certificates. General requirements.
- ETSI EN 319 411-2: Requirements for trust service providers issuing EU qualified certificates
- ETSI EN 319 412: Electronic Signatures and Infrastructures (ESI); Certificate Profiles
- ETSI EN 319 421: Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
- ETSI EN 319 422: Time-stamping protocol and time-stamp token profiles.
- CABForum Baseline Requirements
- CABForum EV Certificate Guidelines.

### 9.14 Araudi aplikagarria betetzea.

475. Espainiako legediak une oro zehaztuko duen jurisdikzioa izango da egokia.

476. Edozein kasutan, Izenpek 9.14 atalean aipatutako araudiak betetzen dituela adierazten du.

### 9.15 Askotariko arauak.

#### 9.15.1 Akordio osoa

477. DPCG honetako klausula bakoitza bere kabuz baliagarria da eta ez ditu gainerakoak baliogabetzen. Klausula baliogabea edo osagabea beste baliokide batez ordezkatu daiteke.



#### 9.15.2 Esleipena.

478. Izenpek ez du zerbitzuaren hutsune edo akatsengatik erantzukizunik izango, zuzenean zein zeharka sortutako kalteengatik ere ez, bereziki kausa honengatik sortzen bada: indar handiaren kasuak, atentatu terrorista, sabotajeak edo greba basatiak; hori guztia, zerbitzua ahalik eta azkarren konpontzeko eta/edo berrabiarazteko beharrezko ekintzak egiteko eskubidea gordez.

#### 9.15.3 Banakortasuna

479. Ez da aurreikusten.

#### 9.15.4 Betetzea

480. Ez da aurreikusten.

#### 9.15.5 Ezinbestea

481. Ez da aurreikusten.

#### 9.15.6 Beste xedapen batzuk

482. Izenpek, konfiantzazko zerbitzu-emaile gisa, zerbitzuak emango dizkie interesatuta daudenei, DPCG honetan eta eskaeraren helbururako aplikagarri diren DP partikularretan, Praktika eta Legeetan jasotako baldintzetan.

483. Izenperen konfiantzazko zerbitzuak modu egokian erabiltzeak eta konbinatzeak erabiltzaileei, harpidedunei eta jabeei aukera emango die, besteak beste, informazio-trukeetan beharrezko segurtasun-neurriak eskaintzeko, alde guztien identifikazio, autentifikazio, ez-estalki eta konfidentzialtasuna bermatzeko.

484. Izenpek bere ziurtapen-zerbitzuak kudeatzen ditu, eta SSL ziurtagiriak ematen ditu, CA/Browser Forum erakundearen BRGen azken bertsioarekin bat (<https://cabforum.org/baseline-requirements-documents/> helbidean kontsulta daitezke) eta CA/Browser Forum erakundeak "Baliozkotze Hedatuko Ziurtagiriak emateko eta kudeatzeko gidan" definitutako baldintzen azken bertsioarekin bat (<https://cabforum.org/extended-validation/> helbidean kontsulta daitezke), bai eta IZENPE autentifikazio-ziurtagirien webgune partikularrean ere.

485. Izenpek bere politika eta ziurtapen-praktikak berrikusiko ditu aipatutako eskakizunetara egokitzeko. Dokumentu hau eta "Baliozkotze Hedatuko Ziurtagiriak emateko eta kudeatzeko gida" bat ez badatoz bat, gidan bertan zehaztutako jarraibideek lehentasuna dute dokumentu honekiko.

486. Izenpek hirugarrenei aukera ematen die igorritako ziurtagiri mota guztiak egiaztatu eta probatzeko. Horretarako, [www.izenpe.eus](http://www.izenpe.eus) webgunean eskuragarri dauden ziurtagiri-probetarako multzo bat dauka.