

Ziurtapen Digitaleko Zerbitzuaren Konfiantzazko Jardunbideen Adierazpena

Erreferentzia: IZENPE-ZPD
Bertsio zk.: v7.6
Data: 2024/07/23



Bertsioen historia

7.0 bertsioaren aurreko bertsioetako aldaketak www.izenpe.eus webguneko atal honetan kontsulta daitezke: “Ziurtapen praktiken deklarazioari buruzko eguneratzeak eta jakinarazpenak”



Bertsioa	Data	Izandako aldaketen laburpena
7.0	2021/07/14	Eguneraketen dokumentua ordezkatzeko aldaketen taula gehitu da ZPD dokumentuko 4.9.12 atala eguneratu da, gako pribatuko konpromisoa frogatzeko eskuragarri dauden metodoak adierazteko.
7.1	2022/01/13	Honako epigrafe hauek eguneratu dira: <ul style="list-style-type: none">– 6.2.1 Modulu kriptografikoen estandarrak– 9.3.3 Informazio konfidentziala babesteko erantzukizuna: araudiaren eguneraketa.– 9.16.6: Beste estipulazio batzuk.
7.2	2022/09/01	Honako epigrafe hauek eguneratu dira: <ul style="list-style-type: none">– 1.1.1 Oinarrizko CA 2007 hierarkia (CN=izenpe.com): sinadura motaren balioa Kualifikatua izatetik Aurreratua izatera pasatu da txip kriptografikoan indarrean diren OIDetan
7.3	2022/10/21	Honako epigrafe hauek eguneratu dira: <ul style="list-style-type: none">– 1.1.1 Oinarrizko CA 2007 hierarkia (CN=izenpe.com): politikaren identifikatzailearen balioa eguneratu da QCP-n izan dadin txip kriptografikoetan indarrean diren OIDetan eta SSL EV ziurtagirien politika eguneratu da: QEVCP-w
7.4	2023/09/13	1.4.1 Akatsen zuzenketa 1.6.2 Akatsen zuzenketa 2.3 Idazketaren eguneraketa 6.1.2 FIPSen eguneraketa 6.1.3 Banaketa-metodoen eguneraketa 7.1 Ziurtagirien profilaren eguneraketa



7.5	2023/11/08	<p>4.9.8 atala eguneratzea: CRLak sortzen direnetik argitaratzen direnera arte emandako denbora</p> <p>Jarraibideen gidaren nagusitasunari buruzko 9.16.6 puntua eguneratzea</p>
7.6	2024/07/23	<p>Sarrera eguneratzea: araudiak</p> <p>1.1.1 koadroa eguneratzea</p> <p>1.1.2 koadroa eguneratzea</p> <p>1.1.5 koadroa sartzea</p> <p>1.1.3 eguneratzea (Erroko CA berria)</p> <p>1.4.1 eguneratzea (Proba-ziurtagiriak)</p> <p>1.5.1 eguneratzea (Egoitzaren helbidea)</p> <p>1.5.2 eguneratzea (Posta)</p> <p>4.2.1 eguneratzea (Identifikazio baten indarraldia ezartzea)</p> <p>5.5.2 eguneratzea (Akatsa zuzentzea: jaulkitze-dataren ordeztu, amaiera-data)</p> <p>6.3.2 eguneratzea (Erroko CA berriaren indarraldia)</p> <p>9.4.4.4 eguneratzea (Kontrol-agintaritzaren datuen babesaren arloan)</p> <p>9.8.4 idazketa eguneratzea</p>



Aurkibidea

Edukia

Honako epigrafe hauek eguneratu dira:	3
– 6.2.1 Modulu kriptografikoen estandarrak	3
– 9.3.3 Informazio konfidentziala babesteko erantzukizuna: araudiaren eguneraketa.	3
– 9.16.6: Beste estipulazio batzuk.	3
Honako epigrafe hauek eguneratu dira:	3
– 1.1.1 Oinarrizko CA 2007 hierarkia (CN=Izenpe.com): sinadura motaren balioa Kualifikatua izatetik Aurreratua izatera pasatu da txip kriptografikoan indarrean diren OIDetan	3
Honako epigrafe hauek eguneratu dira:	3
– 1.1.1 Oinarrizko CA 2007 hierarkia (CN=Izenpe.com): politikaren identifikatzailearen balioa eguneratu da QCP-n izan dadin txip kriptografikoetan indarrean diren OIDetan eta SSL EV ziurtagirien politika eguneratu da: QEVCP-w	3
1.4.1 Akatsen zuzenketa	3
1 Sarrera	18
1.1 Helburua	19
1.1.1 Oinarrizko CA 2007 hierarkia (CN=Izenpe.com)	19
1.1.2 Oinarrizko CA 2020 kualifikatuen hierarkia (CN=ROOT CA QC IZENPE)	23
1.1.3 Oinarrizko CA 2020 kualifikatu gabekoen hierarkia (CN= ROOT CA NQC IZENPE)	26
1.1.4 Oinarrizko CA barneko SSL hierarkia (CN=Izenpe.com) ¡Error! Marcador no definido.	
1.2 Dokumentuaren izena eta identifikazioa	27
1.3 PKI gako publikoko azpiegituraren parte hartzaileak	28
1.3.1 Ziurtapen-agintaritzak	28
1.3.2 Erregistro-entitateak	29
1.3.3 Ziurtagirien harpidedunak	29
1.3.4 Konfiantzako hirugarren batzuk	29



1.3.5	Beste parte-hartzaile batzuk.	30
1.4	Ziurtagiriaren erabilerak	30
1.4.1	Ziurtagiriaren erabilera egokiak	30
1.4.2	Ziurtagiriaren erabilera debekatuak	32
1.5	Politiken administrazioa	32
1.5.1	Dokumentazioaren kudeaketaz arduratzen den entitatea	32
1.5.2	Harremanetarako datuak	32
1.5.3	Ziurtapen Praktiken Deklarazioaren egokitzapenaren arduradunak	32
1.5.4	Ziurtapen Praktiken Deklarazioa onartzeko prozedura	33
1.6	Definizioak eta akronimoak	33
1.6.1	Definizioak	33
1.6.2	Akronimoak	37
2	Argitalpena eta informazio-biltegiaren arduradunak	39
2.1	Informazio-biltegia	39
2.2	Ziurtapen-informazioaren argitalpena	39
2.2.1	Argitalpen- eta jakinarazte-politika	39
2.2.2	Ziurtapen Praktiken Deklarazioan argitaratzen ez diren elementuak	39
2.3	Argitalpen-maiztasuna	39
2.4	Biltegirako sarrera kontrolatzea	40
3	Izenak	41
3.1.1	Izen motak	41
3.1.2	Izenen esanahia	41
3.1.3	Goitizenak	41
3.1.4	Izenen formatuak interpretatzeko arauak	41
3.1.5	Izen-bakartasuna	42



3.1.6	Izenen eta marka erregistratuen tratamenduaren arloko gatazkak ebaztea	42
3.2	Identitatea baliozkotzea	42
3.2.1	Gako pribatuaren jabetza frogatzeko metodoak	42
3.2.2	Erakundearen identitatea kautotzea	42
3.2.3	Pertsona fisiko eskatzailearen nortasuna kautotzea	43
3.2.4	Egiaztatu gabeko harpidedunaren informazioa	43
3.2.5	Agintaritza baliozkotzea	43
3.2.6	Elkarreragineko irizpideak	43
3.3	Gakoak berriro jaulkitzeko eskaeretarako identifikatzea eta kautotzea	43
3.3.1	Ohiko berritzea	43
3.3.2	Ezeztatze baten ondorengo berritzea	43
3.4	Ezeztatzeko eskaeretarako identifikatzea eta kautotzea	43
4	Ziurtagirien bizi-zikloaren baldintza operatiboak	44
4.1	Ziurtagiria eskatzea	44
4.1.1	Eskaeraren egiaztapena	44
4.1.2	Inskribatzeko prozesua eta erantzukizunak.	44
4.2	Eskaerak prozesatzea	45
4.2.1	Identifikatzeko eta kautotzeko eginkizunak egitea	45
4.2.2	Eskaerak onartzea edo baztertzea	45
4.2.3	Eskaera prozesatzeko denbora	45
4.3	Ziurtagiria jaulkitzea	45
4.3.1	CAren jardunak ziurtagiriak jaulkitzean	46
4.3.2	Jaulkipena jakinaraztea harpidedunari	46
4.4	Ziurtagiria onartzea	46
4.4.1	Ziurtagiria onartzeko prozesua	46
4.4.2	CAk ziurtagiria argitaratzea	46



4.4.3	CAk beste entitate batzuei ziurtagiria jaulki izana jakinaraztea	46
4.5	Gako-parea eta ziurtagiriaren erabilera	46
4.5.1	Harpidedunaren gako pribatua eta ziurtagiriaren erabilera	46
4.5.2	Ziurtagirietan konfiantza duten hirugarren batzuek gako publikoa eta ziurtagiria erabiltzea	48
4.6	Ziurtagiria berritzea	49
4.6.1	Ziurtagiria berritzeko inguruabarrak	49
4.6.2	Nork eska dezake ziurtagiria berritzea?	49
4.6.3	Ziurtagiria berritzeko eskaeren tratamendua	49
4.6.4	Harpidedunari jakinaraztea	49
4.6.5	Ziurtagiri berritua onartzeko prozedura	49
4.6.6	Ziurtagiria argitaratzea	49
4.6.7	Beste entitate batzuei jakinaraztea	49
4.7	Ziurtagiria berritzea, haren gakoak berriro sortuta	49
4.7.1	Ziurtagiriaren gakoak berriro sortzeko inguruabarrak	50
4.7.2	Nork eska dezake?	50
4.7.3	Ziurtagiria berritzeko eskaeren tratamendua, gakoak berriro sortuta	50
4.7.4	Harpidedunari jakinaraztea	50
4.7.5	Ziurtagiri berritua onartzeko prozedura	50
4.7.6	Ziurtagiria argitaratzea	50
4.7.7	Beste entitate batzuei jakinaraztea	50
4.8	Ziurtagiria aldatzea	50
4.8.1	Ziurtagiria aldatzeko inguruabarrak	50
4.8.2	Nork eska dezake ziurtagiria aldatzea?	51
4.8.3	Ziurtagiria aldatzeko eskaerak prozesatzea	51
4.8.4	Ziurtagiriaren aldaketa jakinaraztea	51



4.8.5	Ziurtagiriaren aldaketa onartzea dakarren jokabidea	51
4.8.6	Ziurtagiri aldatua argitaratzea	51
4.8.7	Ziurtagiriaren aldaketa beste erakunde batzuei jakinaraztea	51
4.9	Ezeztatzea	51
4.9.1	Ezeztatzeko inguruabarrak	51
4.9.2	Nork eska dezake ziurtagiria ezeztatzeko?	52
4.9.3	Ezeztatzeko eskaeren tratamendua	52
4.9.4	Ezeztatzea eskatzeko graziazko epea	53
4.9.5	Ezeztatzea prozesatzeko CAren epea	53
4.9.6	Konfiantzako hirugarren batzuek ezeztatzeak egiaztatzeko betebeharra	53
4.9.7	CRLak sortzeko maiztasuna	53
4.9.8	CRLak sortzen direnetik argitaratzen direnera arte emandako denbora	53
4.9.9	Ziurtagirien egoera online egiaztatzeko sistemaren erabilgarritasuna	53
4.9.10	Online ezeztatzea egiaztatzeko eskakizunak	54
4.9.11	Ezeztatzeak ohartarazteko beste modu batzuk	54
4.9.12	Arriskupean dagoen gakoaren eskakizun bereziak	54
4.9.13	Eteteko inguruabarrak	54
4.9.14	Nork eska dezake etetea?	55
4.9.15	Etetea eskatzeko prozedura	55
4.9.16	Etenaldiari buruzko mugak	55
4.10	Ziurtagirien egoera-zerbitzuak	55
4.10.1	Ezaugarri operatiboak	55
4.10.2	Zerbitzuaren erabilgarritasuna	55
4.10.3	Aukerako ezaugarriak	55
4.11	Harpidetzari amaiera ematea	55
4.12	Gakoak zaintzea eta berreskuratzea	55



4.12.1	Gakoak zaintzeko eta berreskuratzeko praktikak eta politikak	55
4.12.2	Saioko gakoa babesteko eta berreskuratzeko praktikak eta politikak	55
5	Segurtasun fisikoaren, prozeduren eta langileen kontrolak	56
5.1	Segurtasun fisikoko kontrolak	56
5.1.1	Instalazioen kokalekua eta eraikuntza	56
5.1.2	Sarbide fisikoa	56
5.1.3	Elektrizitatea eta aire egokitua	57
5.1.4	Urarekiko esposizioa	57
5.1.5	Suteen prebentzioa eta horien aurkako babesa	57
5.1.6	Euskarriak biltegitzea	57
5.1.7	Hondakinen tratamendua	57
5.1.8	Instalazioetatik kanpoko babeskopia	57
5.2	Prozeduren kontrolak	57
5.2.1	Konfiantzazko eginkizunak	57
5.2.2	Zeregin bakoitzerako pertsona kopurua	58
5.2.3	Eginkizun bakoitzean identifikatzea eta kautotzea	58
5.2.4	Eginkizunetan zereginak bereiztea	58
5.3	Langileen kontrolak	58
5.3.1	Historialei, kalifikazioei, esperientziari eta kautotzei buruzko baldintzak	58
5.3.2	Historiala ikertzeko prozedurak	58
5.3.3	Trebakuntza-baldintzak	58
5.3.4	Trebakuntza eguneratzeko baldintzak eta maiztasuna	59
5.3.5	Lan-txandaketen segida eta maiztasuna	59
5.3.6	Baimendu gabeko konexioen zigorrak	59
5.3.7	Langileak kontratatzeke baldintzak	59
5.3.8	Langileei dokumentazioa ematea	59



5.4	Audit	60
5.4.1	Erregistratutako gertaera motak	60
5.4.2	Log fitxategien prozesamenduaren maiztasuna	60
5.4.3	Audit logaren atxikipen-aldia	60
5.4.4	Audit logaren babesa	60
5.4.5	Audit-logaren backup prozedura	61
5.4.6	Log-fitxategiak biltzea	61
5.4.7	Log-fitxategiak sortzea eragin duen ekintzaren jakinarazpena	61
5.4.8	Puntu ahulen azterketa	61
5.5	Erregistroak artxibatzea	61
5.5.1	Artxibatutako erregistroen mota	61
5.5.2	Fitxategiaren atxikipen-aldia	61
5.5.3	Fitxategiaren babesa	61
5.5.4	Artxiboaren backup prozedurak	61
5.5.5	Erregistroen denbora zigilatzeko eskakizunak	61
5.5.6	Artxibatzeke sistema	62
5.5.7	Artxiboaren informazioa lortzeko eta egiaztatzeke prozedurak	62
5.6	CAren gakoak aldatzea	62
5.7	Gorabeheren kudeaketa eta larrialdietarako plana	62
5.7.1	Gorabeherak kudeatzeko prozedurak	62
5.7.2	Datu eta software ustelen aurrean jarduteke plana	63
5.7.3	CAren gako pribatua arriskuan dagoenerako prozedura	63
5.7.4	Hondamendi baten ondoren, negozioaren jarraipena	64
5.8	CAren edo RAren amaiera	64
5.8.1	Ziurtapen-entitatea	64
5.8.2	Erregistro-entitatea	65



6	Segurtasun teknikoko kontrolak	66
6.1	Gako-parea sortu eta instalatzea	66
6.1.1	Gako-parea sortzea	66
6.1.2	Gako pribatua harpidedunari banatzea	66
6.1.3	Gako publikoa ziurtagiriaren jaulkitzaileari banatzea	66
6.1.5	Gakoen tamaina	67
6.1.6	Gako publikoa sortzeko eta kalitatea egiaztatzeko parametroak	67
6.1.7	Gakoen erabilera baimenduak (KeyUsage field X.509v3)	68
6.2	Gako pribatua babestea	68
6.2.1	Modulu kriptografikoen estandarrak	68
6.2.2	Gako pribatua pertsona batek baino gehiagok kontrolatzea (m-tik n)	68
6.2.3	Gako pribatuaren zaintza	68
6.2.4	Gako pribatuaren babeskopia	69
6.2.5	Gako pribatua artxibatzea	69
6.2.6	Izenpek gako pribatuen segurtasun-kopia bat egin ahal izango du, bikoiztutako datuen segurtasun-maila jatorrizko datuen maila berekoa dela bermatuta, eta bikoiztutako datuen kopuruak ez duela gainditzen zerbitzuaren jarraitutasuna bermatzeko beharrezkoa en gutxienekoa. Sinadura sortzeko datuak ez dira bikoizten beste ezertarako. Gako pribatuaren transferentzia, modulu kriptografikora edo modulu kriptografikotik	¡Error! Marcador no definido.
6.2.7	Gako pribatua modulu kriptografikoan biltegitzea	69
6.2.8	Gako pribatua aktibatzeke metodoa	70
6.2.9	Gako pribatua desaktibatzeke metodoa	70
6.2.10	Gako pribatua deuseztatzeke metodoa	70
6.2.11	Modulu kriptografikoaren kalifikazioa	70
6.3	Gako-parea kudeatzearen beste alderdi batzuk	70
6.3.1	Gako publikoa artxibatzea	70
6.3.2	Ziurtagiriaren eragiketa-aldiak eta gako-parearen erabilera-aldiak	70
6.4	Aktibatzeke datuak	71



6.4.1	Aktibatzekeo datuak sortzea eta instalatzea	71
6.4.2	Aktibatzekeo datuak babestea	71
6.4.3	Aktibatzekeo datuen beste alderdi batzuk	71
6.5	Segurtasun informatikoko kontrolak	71
6.5.1	Segurtasun informatikorako berariazko eskakizun teknikoak	71
6.5.2	Segurtasun informatikoaren mailaren ebaluazioa	72
6.6	Bizi-zikloaren kontrol teknikoak	72
6.6.1	Sistemen garapen-kontrolak	72
6.6.2	Segurtasunaren kudeaketa-kontrolak	73
6.6.3	Bizi-zikloaren segurtasun-kontrolak	73
6.7	Sareko segurtasunaren kontrolak	73
6.8	Denbora-iturria	73
7	Ziurtagiriaren profilak eta ezeztatutako ziurtagiriaren zerrendaren profilak	74
7.1	Ziurtagiriaren profila	74
7.1.1	Bertsio-zenbakia	74
7.1.2	Ziurtagiriaren luzapenak	74
7.1.3	Algoritmo-objektuen identifikatzaileak	74
7.1.4	Izenen formatuak	74
7.1.5	Izenen murrizketak	74
7.1.6	Ziurtagiriaren politikaren objektu-identifikatzailea	74
7.1.7	“Politika-murrizketak” luzapenaren erabilera	75
7.1.8	Politika-kalifikatzaileen sintaxia eta semantika	75
7.1.9	“certificate policy” luzapenerako tratamendu semantikoa	75
7.2	Ezeztatutako ziurtagiriaren zerrendaren profila	75
7.2.1	Bertsio-zenbakia	75



7.2.2	Zerrendako elementuen ezeztatutako ziurtagirien eta luzapenen zerrenda	76
7.3	OCSP profila	76
7.3.1	Bertsio-zenbakia	76
7.3.2	OCSPren luzapenak	76
7.3.3	OCSParen beste alderdi batzuk	76
8	Betetzearen ikuskapenak	77
8.1	Ikuskapenaren maiztasuna	77
8.2	Ikuskatzailearen kualifikazioa	77
8.3	Ikuskatzailearen eta ikuskatutako enpresaren arteko harremana	77
8.4	Ikuskatu beharreko elementuak	77
8.5	Urritasunen ondoriozko erabakiak hartzea	77
8.6	Emaitzen berri ematea	78
9	Beste lege- eta jarduera-gai batzuk	79
9.1	Tarifak	79
9.1.1	Ziurtagiriak jaulkitzeko edo berritzeko tarifak	79
9.1.2	Ziurtagiriak jasotzeko tarifak	79
9.1.3	Ziurtagirien egoerari buruzko informazioa eskuratzeko tarifa	79
9.1.4	Beste zenbait zerbitzutarako tarifak	79
9.1.5	Itzultze-politika	79
9.2	Finantza-erantzukizuna	79
9.2.1	Erantzukizun zibileko aseguruak	79
9.2.2	Beste aktibo batzuk	79
9.2.3	Azken entitateentzako aseguruak eta bermeak	79
9.3	Informazioaren konfidentzialtasuna	80
9.3.1	Informazio konfidentzialaren irismena	80
9.3.2	Irismenaren barruan ez dagoen informazioa	80



9.3.3	Informazio konfidentziala babesteko erantzukizuna	81
9.4	Datu pertsonalak babestea	81
9.4.1	Pribatutasun-plana	81
9.4.2	Pribatu gisa tratatutako informazioa	82
9.4.3	Pribatutzat jotzen ez den informazioa	82
9.4.4	Informazio pribatua babesteko erantzukizuna	82
9.4.4.1	Datuak babesteko ordezkaria	82
9.4.4.2	Tratamendu-jardueren erregistroa	82
9.4.4.3	Interesdunen eskubideak	83
9.4.4.4	Agintaritzekin lankidetzan jardutea	83
9.4.4.5	Segurtasun-urraketen jakinarazpena	83
9.4.5	Informazio pribatua erabiltzeko oharra eta adostasuna	83
9.4.6	Prozesu judizialaren edo administratiboaren araberako zabalkundea	84
9.4.7	Informazioa zabaltzeko beste egoera batzuk	84
9.5	Jabetza intelektualeko eskubideak	84
9.5.1	Ziurtagirien jabetza	84
9.5.2	Ziurtapen Praktikaren jabetza	84
9.5.3	Izenen gaineko informazioaren jabetza	84
9.5.4	Gakoen eta horiei dagokien materialaren jabetza	84
9.6	Betebeharrak eta bermeak	84
9.6.1	CAren betebeharrak	85
9.6.1.1	Zerbitzua egiteko betebeharrak	85
9.6.1.2	Jardun fidagarriko betebeharrak	85
9.6.1.3	Identifikazio-betebeharrak	86
9.6.1.4	Erabiltzaileei informatzeko betebeharrak	86
9.6.1.5	Egiaztapen-programen inguruko betebeharrak	87



9.6.1.6 Ziurtapen-zerbitzuaren arautze juridikoaren inguruko betebeharrak	87
9.6.2 Erregistro-entitatearen betebeharrak	88
9.6.3 Titularren betebeharrak	88
9.6.4 Konfiantza duten aldeen betebeharrak	89
9.6.5 Beste parte-hartzaile batzuen betebeharrak	90
9.7 Bermeei uko egitea	90
9.8 Erantzukizunen muga	90
9.8.1 Ziurtapen-agintaritzaren erantzukizunak	90
9.8.2 Erregistro-agintaritzaren erantzukizunak	91
9.8.3 Harpidedunen betebeharrak	91
9.8.4 Ziurtagirietan konfiantza duten hirugarrenen erantzukizunak	92
9.9 Kalte-ordainak	93
9.10 Baliozkotze-aldia	93
9.10.1 Epea	93
9.10.2 Amaiera	93
9.10.3 Amaieraren ondorioak	93
9.11 Banako jakinarazpenak eta komunikazioa parte-hartzaileekin	93
9.12 Dokumentu honen aldaketak	93
9.12.1 Aldaketetarako prozedura	93
9.12.2 Jakinarazteko aldia eta mekanismoa	94
9.12.3 OIDA zer inguruabarretan aldatu behar den	94
9.13 Erreklamazioak eta auzien ebazpena	94
9.14 Araudi aplikagarria	94
9.15 Aplikatzekoa den araudia betetzea	95
9.16 Askotariko estipulazioak	96
9.16.1 Akordio osoa	96



9.16.2	Esleipena	96
9.16.3	Bereizgarritasuna	96
9.16.4	Betetzea	96
9.16.5	Ezinbestea	96
9.16.6	Beste estipulazio batzuk	96
10	I. ERANSKINA. CA-EN ZIURTAGIRIEN PROFILAK	98
10.1	OINARRIZKO ZIURTAPEN-AGINTARITZAK	98
10.2	MENDEKO ZIURTAPEN AGINTARITZAK	100
10.2.1	subCA CN=lzenpe.com	100
10.2.2	SUBCA CN = ROOT CA QC IZENPE	106
10.2.3	subCA CN = ROOT CA NQC IZENPE	109



1 Sarrera

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

Premisa horietatik abiatuta, Eusko Jaurlaritzak eta foru-aldundiek, beren informatika sozietateen bidez, 2022ko ekainean, “Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, IZENPE, SA” (aurrerantzean, IZENPE) merkataritza-sozietatea sortu zen.

Euskal Autonomia Erkidegoko Administrazio Publikoetako Sozietate Informatikoek IZENPE tresna edo erakundea erabili dute konfiantzazko zerbitzuen garapenean duten interes komuna kudeatzeko, eta baliabide ezin hobea da herritarren eta administrazioaren arteko harremanak sinplifikatzeko bidean aurrera egiteko.

910/2014 (EB) Erregelamenduak Konfiantzazko Zerbitzugile Kualifikatu izateko aukera aurreikusten du (910/2014 (EB) Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2014ko uztailaren 23koa, barne-merkatuko transakzio elektronikoetarako konfiantzazko zerbitzuei buruzkoa, zeinaren bidez indargabetzen baita 1999/93/EE Zuzentaraua, Europako Parlamentuaren eta Kontseiluaren 2024ko apirilaren 11ko 2024/1183 Erregelamenduaren bidez aldatua identitate digitalaren Europako esparrua ezartzeari dagokionez).

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

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

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

Era berean, zerbitzuak eraginkortasunez garatzeko eta ezartzeko helburuarekin, Izenpek informazioaren segurtasuna kudeatzeko sistema ezarri du konfiantza-zerbitzuekin lotzen diren prozesuetarako, betiere ISO 27001 estandarren arabera.

IZENPEK ETSIren (Telekomunikazio Estandarren Europako Institutua) estandarren jarraibideei jarraitzen die, ziurtagiri kualifikatuak eta kualifikatu gabeak, sinadurak baliozkotzeko zerbitzu kualifikatua eta denbora-zigiluak emateko. Web-autentifikazioko ziurtagirien (SSLak) kasuan,



gainera, CA/Browser Forumez onartutako gidei jarraitzen zaie (www.cabforum.org helbidean daude eskuragarri).

Arau hauetan definitzen diren zehaztapen teknikoek (ETSI TS) oinarrizko baldintzak ezartzen dituzte, ziurtagiri kualifikatuak eta kualifikatu gabeak eta denbora-zigiluak jaulkitzen dituzten konfiantzako zerbitzugileen kudeaketa eta ziurtapen-jardunbideei dagokienez, 910/2014 Erregelamenduaren eta 2024/1183 Erregelamenduaren lege-esparruaren barruan: EN 319 411-1, ziurtagirien jaulkipenerako; EN 319 411-2 ziurtagiri kualifikatuen jaulkipenerako, eta EN 319 421 denbora-zigiluen jaulkipenerako.

Azken erabiltzailearen konfiantzako zerbitzuen eta produktuen eskuragarritasuna eskatzen duen ETSI EN 319 401 estandarrari jarraituta, Izenpek lan egiten du herritar guztiek, eta batez ere Izenperekin harremanetan dauden pertsona desgaituek edo adinekoek, baldintza-berdintasunean balia ahal izan ditzaten informazioa eta zerbitzu elektronikoak, haien inguruabar pertsonalak, bitartekoak edo ezagupenak edozein izanik ere. Ondorio horretarako ETSI EN 301 549 estandarraren gomendioak izango dira kontuan.

Edonola ere, Izenperen webgunearen, produktuen edo zerbitzuen erabilgarritasunaren arloko edozein kontsulta egin dezakezu info@izenpe.com helbide elektronikoaren bidez edo www.izenpe.eus webgunean eskura dagoen formularioaren bidez.

Ziurtapen Praktiken Deklarazio hau (ZPD) RFC 3647aren arabera egituratuta dago.

1.1 Helburua

Izenpek honako zerbitzu kualifikatu hauek egiteko azpiegitura bat kudeatzen du:

- a) Sinadura elektronikoko ziurtagiri elektronikoko kualifikatuak egiteko.
- b) Zigilu elektronikoko ziurtagiri elektronikoko kualifikatuak egiteko.
- c) Webguneak kautotzen dituzten ziurtagiri elektronikoko kualifikatuak egiteko.
- d) Denborako zigilu elektronikoko kualifikatuak egiteko zerbitzua.

Eta honako zerbitzu kualifikatu gabe hauek:

- a) Sinadura elektronikoko ziurtagiri elektronikoko kualifikatu gabeak egiteko.
- b) Webguneak kautotzen dituzten ziurtagiri elektronikoko kualifikatu gabeak egiteko.
- c) Entrega elektronikoko ziurtatua egiteko.
- d) Sinadura elektronikoak baliozkotzeko.
- e) Zigilu elektronikoak baliozkotzeko.

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

1.1.1 Oinarrizko CA 2007 hierarkia (CN=Izenpe.com)

HERRITARRAK



Deskribapen laburra	Euskarria	Politikaren identifikatzailea	OID politika	eIDAS, identifikazio-maila	Sinadura mota eIDAS
B@K	HSM	NCP	1.3.6.1.4.1.14777.5.2.5	Txikia	Oinarritzkoa
B@KQ	HSM	QCP-n	1.3.6.1.4.1.14777.2.18.3	Oinarritzkoa (Giltzarekin)	Aurreratua
Herritarren Ziurtagiria	Txip kriptografikoa	QCP-n	eIDAS profila 1.3.6.1.4.1.14777.2.18.1	Handia	Aurreratua
			eIDAS aurreko profila 1.3.6.1.4.1.14777.2.6	Handia	Kualifikatua
Izenpe Mobile	APP edukitzailea	NCP	1.3.6.1.4.1.14777.5.2.5.4	Oinarritzkoa	Ez aplikagarri (sinatzeko, BAKQrena erabiltzen da)
NQC goitizena	Softwarea	NCP	1.3.6.1.4.1.14777.5.2.7.2	Oinarritzkoa	Aurreratua

ERAKUNDEAREN ORDEZKARIA					
Deskribapen laburra	Euskarria	Politikaren identifikatzailea	OID politika	eIDAS, identifikazio-maila	Sinadura mota eIDAS
Erakundearen ordezkaria	HSM	QCP-n	1.3.6.1.4.1.14777.2.14	Oinarritzkoa (Giltzarekin)	Aurreratua
	Txip kriptografikoa	QCP-n	1.3.6.1.4.1.14777.2.12	Handia	Aurreratua
	IZENPEren software-edukitzailea	QCP-n	1.3.6.1.4.1.14777.2.16	Oinarritzkoa	Aurreratua

NORTASUN JURIDIKORIK GABEKO ERAKUNDEKO ORDEZKARIA					
Deskribapen laburra	Euskarria	Politikaren identifikatzailea	OID politika	eIDAS, identifikazio-maila	Sinadura mota eIDAS
Nortasun Juridikorik	HSM	QCP-n	1.3.6.1.4.1.14777.2.15	Oinarritzkoa (Giltzarekin)	Aurreratua



Gabeko erakundeko ordezkaria	Txip kriptografikoa	QCP-n	1.3.6.1.4.1.14777.2.13	Handia	Aurreratua
	IZENPEren software-educitzailea	QCP-n	1.3.6.1.4.1.14777.2.17	Oinarrizkoa	Aurreratua

PROFESIONALA					
Deskribapen laburra	Euskarria	Politikaren identifikatzailea	OID politika	eIDAS, identifikazio-maila	Sinadura mota eIDAS
Erakunde publikoko langileak	Txip kriptografikoa	QCP-n	1.3.6.1.4.1.14777.4.14.1	Handia	Aurreratua
	IZENPEren software-educitzailea	QCP-n	1.3.6.1.4.1.14777.4.14.2	Oinarrizkoa	Aurreratua
	HSM	QCP-n	1.3.6.1.4.1.14777.4.14.3	Oinarrizkoa (Giltzarekin)	Aurreratua
Erakunde publikoko langile goitizendunak	Txip kriptografikoa	QCP-n	Sinadura: 1.3.6.1.4.1.14777.4.13.1.1	Handia	Aurreratua
		NCP+	Kautotzea: 1.3.6.1.4.1.14777.4.13.1.2	Handia	Ez aplikagarria
		Ez aplikagarria	Zifratua: 1.3.6.1.4.1.14777.4.13.1.3	Handia	Ez aplikagarria
Korporatibo kualifikatua	Txip kriptografikoa	QCP-n	1.3.6.1.4.1.14777.2.19.1	Handia	Aurreratua
	IZENPEren software-educitzailea	QCP-n	1.3.6.1.4.1.14777.2.19.2	Oinarrizkoa	Aurreratua
	HSM	QCP-n	1.3.6.1.4.1.14777.2.19.3	Oinarrizkoa (Giltzarekin)	Aurreratua
Korporatibo kualifikatu gabea	Txip kriptografikoa	NCP+	1.3.6.1.4.1.14777.1.1.1	Ez aplikagarri (kualifikatu gabea)	Aurreratua
Erakunde publikoetako langileak (eIDAS aurrekoak)	Txip kriptografikoa	QCP public + SSCD	1.3.6.1.4.1.14777.4.1	Ez aplikagarria	Aitortua



Aitortutako korporatibo publikoa (eIDAS aurrekoak)	Txip kriptografikoa	QCP public + SSCD	1.3.6.1.4.1.14777.4.2	Ez aplikagarria	Aitortua
Aitortu gabeko korporatibo publikoa (eIDAS aurrekoak)	Txip kriptografikoa	NCP+	1.3.6.1.4.1.14777.1.1.1	Ez aplikagarria	Aurreratua
Aitortutako korporatibo pribatua (eIDAS aurrekoak)	Txip kriptografikoa	QCP public + SSCD	1.3.6.1.4.1.14777.2.2	Ez aplikagarria	Aitortua
Aitortu gabeko korporatibo pribatua (eIDAS aurrekoak)	Txip kriptografikoa	NCP+	1.3.6.1.4.1.14777.5.2.2	Ez aplikagarria	Aurreratua

ERAKUNDEAREN ZIGILUA

Deskribapen laburra	Euskarria	Politikaren identifikatzailea	OID politika	eIDAS, identifikazio-maila	Sinadura mota eIDAS
Erakundearen zigilua	Izenperen software-educitzailea	QCP-I	1.3.6.1.4.1.14777.2.11	Oinarrizkoa	Aurreratua
	HSM	QCP-I	1.3.6.1.4.1.14777.2.20	Oinarrizkoa	Aurreratua

ADMINISTRAZIO-ZIGILUA

Deskribapen laburra	Euskarria	Politikaren identifikatzailea	OID politika	eIDAS, identifikazio-maila	Sinadura mota eIDAS
Administrazio-zigilua	Izenperen software-educitzailea	QCP-I	1.3.6.1.4.1.14777.4.11.2	Oinarrizkoa	Aurreratua
	HSM	QCP-I	1.3.6.1.4.1.14777.4.11.3	Oinarrizkoa	Aurreratua



ZERBITZARI SEGURUA (SSL/TLS)			
DESKRIBAPEN LABURRA	EUSKARRIA	POLITIKAREN IDENTIFIKATZAILEA	OID POLITIKA
SSL DV	Softwarea	DVCP	1.3.6.1.4.1.14777.1.2.4
SSL OV	Softwarea	OVCP	1.3.6.1.4.1.14777.1.2.1
SSL Kualifikatua	Softwarea	QEVCP-w	1.3.6.1.4.1.14777.6.1.3

APLIKAZIOA			
DESKRIBAPEN LABURRA	EUSKARRIA	POLITIKAREN IDENTIFIKATZAILEA	OID POLITIKA
Aplikazioa	Izenperen software- edukitzailea	NCP	1.3.6.1.4.1.14777.1.2.2

KODE-SINADURA			
DESKRIBAPEN LABURRA	EUSKARRIA	POLITIKAREN IDENTIFIKATZAILEA	OID POLITIKA
Kode-sinadura	Txip kriptografikoa	NCP+	1.3.6.1.4.1.14777.1.3.1

IOT GAILUA			
DESKRIBAPEN LABURRA	EUSKARRIA	POLITIKAREN IDENTIFIKATZAILEA	OID POLITIKA
Gailua	Softwarea	NCP	1.3.6.1.4.1.14777.1.3.2

1.1.2 Oinarrizko CA 2020 kualifikatuen hierarkia (CN=ROOT CA QC IZENPE)

HERRITARRAK					
Deskribapen laburra	Euskarria	Politikaren identifikatzailea	OID politika	eIDAS, identifikazio-maila	Sinadura mota eIDAS
B@KQ	HSM	QCP-n	1.3.6.1.4.1.14777.8.1.3	Oinarrizkoa (Giltzarekin)	Aurreratua
Herritarren Ziurtagiria	Txip kriptografikoa	QCP-n-qscd	1.3.6.1.4.1.14777.8.1.1	Handia	Kualifikatua



ERAKUNDEAREN ORDEZKARIA					
Deskribapen laburra	Euskarria	Politikaren identifikatzailea	OID politika	eIDAS, identifikazio-maila	Sinadura mota eIDAS
Erakundearen ordezkaria	HSM	QCP-n	1.3.6.1.4.1.14777.8.3.3	Oinarrizkoa (Giltzarekin)	Aurreratua
	Txip kriptografikoa	QCP-n-qscd	1.3.6.1.4.1.14777.8.3.1	Handia	Kualifikatua
	Izenperen software-edukitzailea	QCP-n	1.3.6.1.4.1.14777.8.3.2	Oinarrizkoa	Aurreratua

NORTASUN JURIDIKORIK GABEKO ERAKUNDEKO ORDEZKARIA					
Deskribapen laburra	Euskarria	Politikaren identifikatzailea	OID politika	eIDAS, identifikazio-maila	Sinadura mota eIDAS
Nortasun Juridikorik Gabeko erakundeordezkaria	HSM	QCP-n	1.3.6.1.4.1.14777.8.4.3	Oinarrizkoa (Giltzarekin)	Aurreratua
	Txip kriptografikoa	QCP-n-qscd	1.3.6.1.4.1.14777.8.4.1	Handia	Kualifikatua
	Izenperen software-edukitzailea	QCP-n	1.3.6.1.4.1.14777.8.4.2	Oinarrizkoa	Aurreratua

PROFESIONALA					
Deskribapen laburra	Euskarria	Politikaren identifikatzailea	OID politika	eIDAS, identifikazio-maila	Sinadura mota eIDAS
	Txip kriptografikoa	QCP-n-qscd	1.3.6.1.4.1.14777.9.1.1	Handia	Kualifikatua



Erakunde publikoko langileak	Izenperen software-educitzailea	QCP-n	1.3.6.1.4.1.14777.9.1.2	Oinarrizkoa	Aurreratua
	HSM	QCP-n	1.3.6.1.4.1.14777.9.1.3	Oinarrizkoa (Giltzarekin)	Aurreratua
Erakunde publikoko langile goitizendunak	Txip kriptografikoa	QCP-n-qscd	Sinadura 1.3.6.1.4.1.14777.9.2.1	Handia	Kualifikatua
		NCP+	Kautotzea 1.3.6.1.4.1.14777.9.2.2	Handia	Ez aplikagarria
		Ez aplikagarria	Zifratua 1.3.6.1.4.1.14777.9.2.3	Handia	Ez aplikagarria
Korporatibo kualifikatua	Txip kriptografikoa	QCP-n-qscd	1.3.6.1.4.1.14777.8.2.1	Handia	Kualifikatua
	Izenperen software-educitzailea	QCP-n	1.3.6.1.4.1.14777.8.2.2	Oinarrizkoa	Aurreratua
	HSM	QCP-n	1.3.6.1.4.1.14777.8.2.3	Handia (txartel birtual arekin)	Oinarrizkoa (Giltzarekin)

ERAKUNDEAREN ZIGILUA					
Deskribapen laburra	Euskarria	Politikaren identifikatzailea	OID politika	eIDAS, identifikazio-maila	Sinadura mota eIDAS
Erakundearen zigilua	Izenperen software-educitzailea	QCP-I	1.3.6.1.4.1.14777.8.5.2	Oinarrizkoa	Aurreratua
	HSM	QCP-I	1.3.6.1.4.1.14777.8.5.3	Oinarrizkoa	Aurreratua

ADMINISTRAZIO-ZIGILUA					
Deskribapen laburra	Euskarria	Politikaren identifikatzailea	OID politika	eIDAS, identifikazio-maila	Sinadura mota eIDAS
Administrazio-zigilua	Izenperen software-educitzailea	QCP-I	1.3.6.1.4.1.14777.9.3.2	Oinarrizkoa	Aurreratua



	HSM	QCP-I	1.3.6.1.4.1.14777.9.3.3	Oinarrizkoa	Aurreratua
--	-----	-------	-------------------------	-------------	------------

1.1.3 Oinarrizko CA 2020 kualifikatu gabekoen hierarkia (CN= ROOT CA NQC IZENPE)

HERRITARRAK					
Deskribapen laburra	Euskarria	Politikaren identifikatzailea	OID politika	eIDAS, identifikazio-maila	Sinadura mota eIDAS
B@K	HSM	NCP	1.3.6.1.4.1.14777.11.1.2	Txikia	Oinarrizkoa
Mobile	APP edukitzailea	NCP	1.3.6.1.4.1.14777.11.3.4	Oinarrizkoa	Ez aplikagarri (sinatzeko, BAKQrena erabiltzen da)
NQC goitizena	Softwarea	NCP	1.3.6.1.4.1.14777.11.2.2	Oinarrizkoa	Aurreratua

PROFESIONALA					
Deskribapen laburra	Euskarria	Politikaren identifikatzailea	OID politika	eIDAS, identifikazio-maila	Sinadura mota eIDAS
Profesionala, kualifikatugabea	Txip kriptografikoa	NCP+	1.3.6.1.4.1.14777.11.4.2	Ez aplikagarri (kualifikatugabea)	Aurreratua

APLIKAZIOA			
DESKRIBAPEN LABURRA	EUSKARRIA	POLITIKAREN IDENTIFIKATZAILEA	OID POLITIKA
Aplikazioa	Izenperen software-edukitzailea	NCP	1.3.6.1.4.1.14777.12.1.2



IOT GAILUA			
DESKRIBAPEN LABURRA	EUSKARRIA	POLITIKAREN IDENTIFIKATZAILEA	OID POLITIKA
Gailua	Softwarea	NCP	1.3.6.1.4.1.14777.12.2.2

BARNEKO ZERBITZARI SEGURUA (SSL/TLS)			
DESKRIBAPEN LABURRA	EUSKARRIA	POLITIKAREN IDENTIFIKATZAILEA	OID POLITIKA
SSL DV	Softwarea	DVCP	1.3.6.1.4.1.14777.14.1.2

1.1.4 Erroko CAren hierarkia 2024 (CN=ROOT CA SSL IZENPE 2024)

ZERBITZARI SEGURUA (2024)			
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 kualifikatua	Software	QCP-w	1.3.6.1.4.1.14777.6.1.3

1.2 Dokumentuaren izena eta identifikazioa

Dokumentu honi “Izenperen Ziurtapen Praktiken Deklarazioa” deritza eta barne mailan “ZPD” akronimoa erabiltzen da.

Dokumentu honetan ez dira jorratzen ziurtapen-praktiken eta -politiken alderdi bereizgarriak, ezta Izenpek konfiantzako zerbitzuak egiteko inplementatzen dituen zerbitzarian sinatzeko zerbitzuarenak edo denbora-zigilatze politikarenak ere. Berezitasun horiek dagozkien dokumentuetan garatzen dira, eta honako Ziurtapen Praktiken Deklarazio hau da horien aplikazio-esparru nagusia.

Ziurtapen Politika Partikularrak Ziurtapen Praktiken Deklarazio honen eduki nagusian xedatutakoari nagusituko zaizkio, betiere alderdi partikularrei dagokienez eta aztergai dituzten ziurtagiri eta/edo zerbitzu motei dagokienez.

Izenperen segurtasun-batzordeak erregularitasunez berrikusten ditu Erakundeak izan ditzakeen arriskuak, eta ziurtapen-politiketako bakoitzean definitutako zerbitzuen segurtasuna bermatzeko beharrezkoak diren tratamendu-planak onartzen ditu.



Ziurtapen Praktiken Deklarazio honen mendeko ziurtapen-deklarazio partikularretan islatuko dira erabilera-baldintzak, mugak, erantzukizunak, jabetzak eta ziurtagiri mota bakoitzaren berariazko beste edozein informazio.

Prozedura horiek oinarritzen dira, batik bat, European Telecommunications Standards Institute (ETSI) institutuaren arauetan.

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

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

1.3 PKI gako publikoko azpiegituraren parte hartzaileak

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

- Ziurtapen Agintaritzek.
- Erregistro-entitateek.
- Ziurtagirien harpidedunak edo titularrak.
- Konfiantza duten aldeak.
- Beste parte-hartzaile batzuk.

1.3.1 Ziurtapen-agintaritzak

Izenpek honako ziurtapen-agintaritza hauek ditu:

- CN = Izenpe.com
 - CA, Herritar / Entitate kualifikatuak
 - CA, Herritar / Entitate kualifikatu gabeak
 - CA, Herri Administrazio kualifikatu gabeak
 - CA, Herri Administrazio kualifikatuak
 - CA, SSL EV
 - CA SSL EV 2018
- CN = ROOT CA QC IZENPE
 - CN= SUBCA QC IZENPE – TSA
 - CN= SUBCA QC IZENPE - ADMINISTRAZIO PUBLIKOA-ADMINISTRACION PUBLICA
 - CN= SUBCA QC IZENPE - HERRITARRAK ETA ENPRESA-CIUDADANIA Y EMPRESA
- CN= ROOT CA NQC IZENPE
 - CN= CA NQC IZENPE - PERTSONA FISIKOA-PERSONA FISICA



- CN= CA NQC IZENPE - GAILUA-DISPOSITIVO
- CN= CA NQC IZENPE - TEKNIKOA-TECNICA
- CN= CA NQC IZENPE - SSL EZ PUBLIKOA-SSL NO PUBLICO
- CN = ROOT CA SSL IZENPE 2024
 - CN= SUBCA SSL 2024

I. eranskinean jaso dira ziurtagiri bakoitzaren profilak.

1.3.2 Erregistro-entitateak

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

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

Erregistro-entitateak izango dira Izenpe bera edota Izenperekin dagokion lege-tresna sinatzen duen entitate erabiltzailea.

1.3.3 Ziurtagirien harpidedunak

Ziurtagiri baten harpidedunak ez du zertan sinatzailea bera izan, gerta baitaiteke sinatzailea erakunde baten ordezkari edo kide gisa jardutea —kasu horretan, erakunde hori joko da erakunde harpideduntzat—, edo zigilu elektronikoen edo web-kautotzearen ziurtagiriak izatea. Dena dela, Ziurtapen Politika Partikularren Deklarazio bakoitzean zehaztuko da sinatzailearen eta harpidedunaren arteko balizko bereizketa hori.

Sinatzaileak pertsona fisikoak dira, eta haiek soilik erabil ditzakete titular diren ziurtagiriekin lotzen diren sinadura sortzeko datuak.

1.3.4 Konfiantzako hirugarren batzuk

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

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

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



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

1.3.5 Beste parte-hartzaile batzuk.

Izenpe da Denbora Zigilatze Agintaritzaren denbora-zigilu elektronikoa sortzeko konfiantzako zerbitzua egiten duenean, betiere dagokion Praktika Partikularren Deklarazioaren mende.

1.4 Ziurtagiriaren erabilerak

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

1.4.1 Ziurtagiriaren erabilera egokiak

Ziurtagiri kualifikatuak

Sinadura elektronikoko ziurtagiri kualifikatuak harpidedunaren identitatea eta gako pribatuaren edukizailearen identitatea bermatzen dituzte.

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

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

Zigilu elektronikoko ziurtagiriak pertsona juridiko batekin lotzen ditu zigilu bat baliozkotzeko datuak, eta pertsona horren izena berresten du. Zigilu elektronikoa sortzeko aukera ematen dute, eta, hartara, dokumentu elektronikoa jakin bat pertsona juridiko batek jaulki duela frogatzen dute eta dokumentuaren jatorriari eta integritateari buruzko ziurtasuna gehitzen dute.

Izenpek jaulkitzen dituen zigilu elektronikoko ziurtagirik eIDAS1, eIDAS2 araudiaren III. Eranskinaren betekizunak betetzen dituzte ziurtagiri kualifikatutzat jotzeko.

Webgunea kautotzeko ziurtagirik webgune jakin bat kautotzeko aukera ematen dute, eta ziurtagiria jaulki zaion pertsona juridikoarekin edo fisikoarekin lotzen dute webgunea. Izenpek egindako web-autentifikazioko ziurtagirik eIDAS1 eta eIDAS2ko IV. eranskineko baldintzak betetzen dituzte kualifikatutzat jotzeko.

Organo-zigilu elektronikoen ziurtagiriak administrazio publikoei ematen zaizkie organoa identifikatzeko eta dokumentuak elektronikoki zigilatzeke, sektore publikoaren bitarteko elektronikoen bidezko jardunaren eta funtzionamenduaren erregelamendua onartzen duen martxoaren 30eko 203/2021 Errege Dekretuan aurreikusitakoaren arabera.



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

Ziurtagiri kualifikatu gabea

Ziurtagiri kualifikatu gabeek ez dute fedez bermatzen harpidedunaren identitatea eta, hala badagokio, gako pribatuaren edukitzailearen identitatea; edonola ere, sinatzeko erabiliz gero, sinadura sortzeko gailu behar bezain seguru batekin batera erabili beharko da. Horrelakoetan, ez da sinatzaileak eskuz idatzitako sinaduraren baliokide izaten.

Ziurtagiri kualifikatuak, dagokion ziurtagiri motan hala definitzen bada, kautotze-mezuak sinatzeko ere erabil daitezke, bereziki SSL edo TLS bezeroen testiguak, gako-berreskurapen gabeko zifratzeak eta beste zenbait.

Izenperen ziurtagiri ez kualifikatuek ETSI EN 319 411-1 arau teknikoari jarraitzen diote.

Ziurtagirien erabilera-esparrua

Erabilera-esparruari dagokionez bi kasu bereizten dira:

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

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

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

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

Proba-ziurtagiria

Trafiko juridikoaren segurtasun-arrazoia direla eta, proba-ziurtagiriak honako identifikazio-datu hauekin emango dira, besterik adierazi ezean:

Nortasun agiri nazionalaren zenbakia (NAN): 0000000T

Atzerritarraren identifikazio-zenbakia (AIZ): X0000000T, Y0000000R, Z0000000W

Izena:Nombre

Lehen Abizena: ApellidoUno

Bigarren Abizena: ApellidoDos

Behar izanez gero, proba-ziurtagiriak sortu ahal izango dira beste datu batzuekin; kasu horretan, aurrez gainbegiratze-organo eskudunari jakinaraziko zaio.



Datu horiekin emandako ziurtagiriak euskal sektore publikoko aplikazioen probak egiteko baino ez dira erabiliko.

1.4.2 Ziurtagiriaren erabilera debekatuak

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

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

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

1.5 Politiken administrazioa

1.5.1 Dokumentazioaren kudeaketaz arduratzen den entitatea

IZENPE (sozietatearen egoitza: Beato Tomás de Zumarraga 71, 1.a; IFZ: A-01337260) Ziurtapen Jardunbideen Adierazpen hau aplikatzen zaien ziurtagiriak ematen dituen Konfiantzazko Zerbitzugilea da.

1.5.2 Harremanetarako datuak

Zerbitzu-emailearen izena	Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe SA
Posta-helbidea	Tomas Zumarraga Dohatsuaren kalea, 71-1. 01008 Vitoria-Gasteiz
Posta elektronikoko helbidea	izenpe@izenpe.eus
Telefonoa	900 840 123

Segurtasun-arazoen berri emateko, hala nola gakoa arriskuan dagoen susmoa, ziurtagirien erabilera desagokia, iruzurra edo bestelako arazoren baten berri emateko, jar zaitez harremanetan seguridad@izenpe.eus helbidearekin.

Kontsultatu "4.9.3 Ezeztatzeko eskaeren tratamendua atala ezeztatzeko bideak ezagutzeko.

1.5.3 Ziurtapen Praktiken Deklarazioaren egokitzapenaren arduradunak

Izenperen Segurtasun Batzordea arduratzen da Ziurtapen Praktiken Deklarazio hau onartzeaz, baita hari egin beharreko aldaketak onartzeaz ere.



1.5.4 Ziurtapen Praktiken Deklarazioa onartzeko prozedura

Dokumentu honetan egindako azken aldaketak Izenperen Segurtasun Batzordeak onartuko ditu, ezarritako baldintzak betetzen direla egiaztatu eta gero.

1.6 Definizioak eta akronimoak

1.6.1 Definizioak

- **Datuak Babesteko Espainiako Agentzia (APD):** zuzenbide publikoko erakunde bat da, berezko izaera juridikoa du eta ahalmen publiko eta pribatu osoa. Askatasun osoz burutzen ditu bere funtzioak, Administrazio Publikoen mende egon gabe. Helburu nagusia datuak babesteari buruzko legedia betetzen dela zaintzea eta legediaren aplikazioa kontrolatzea da.
- **Ziurtapen Agintaritza (CA):** Ziurtapen Agintaritza behar diren ziurtagiriak jaulkitzen dituen entitatea da, Erregistro Agintaritzak hala eskatu ondoren, modu automatizatuan eta Tokiko Erregistro Autoritatearen baieztapena jaso ondoren.
- **Erregistro Agintaritza (RA):** Erregistro Agintaritza arduratzen da ziurtagirien gakoen eskatzaileak, harpidedunak eta edukitzaileak identifikatzeaz, baita ziurtagirietan jasotzen diren inguruabarrak egiaztatzen dituen dokumentazioa egiaztatzeaz eta ziurtagiriak jaulkitzeko, ezeztatzeko eta berritzeko eskaerak baliozkotzeaz eta onartzeaz. Erabiltzaileak Erregistro Agintaritzara joan behar du ziurtagiri bat eskatzeko, Erregistro Agintaritzarekin lotuta dagoen Ziurtapen Agintaritzaren bermearekin.
- **Denbora Zigilatze Agintaritza (TSA):** denbora-zigiluak jaulkitzen dituen agintaritza.
- **Ziurtagiria:** Ziurtapen Zerbitzuen Egileak elektronikoki sinatutako dokumentu elektronikoa da, sinadura egiaztatzeko datuak sinatzailearekin lotzen ditu eta haren identitatea baieztatzen du.
- **Oinarrizko ziurtagiria:** harpidedun gisa Izenperen hierarkiako Ziurtapen Agintaritza bat duen ziurtagiria. Agintaritza horren sinadura egiaztatzeko datuak Ziurtapen Zerbitzuen Egile gisa daude sinatuta, agintaritzarenak diren sinadura sortzeko datuekin. Izenpeko entitate jaulkitzaileek hierarkia bat osatzen dute, horrela, oinarrizko entitate bat dago, komuna edozein ziurtagiritarako, eta mendeko entitate bat baino gehiago, ziurtagiri mota desberdinetarako.
- **Ziurtagiri kualifikatua:** Ziurtapen Zerbitzuen Egile batek emandako ziurtagiri elektronikoak dira. Ziurtapen Zerbitzuen Egile horrek eIDAS-ean ezarritako baldintzak betetzen ditu, identitateari eta eskatzaileen inguruko bestelakoei dagokienez, eta ematen dituzten ziurtapen-zerbitzuen bermeei dagokienez.
- **Ziurtagiri kualifikatu gabeak:** ziurtagiri arruntak dira, ziurtagiri kualifikatuen legeaizatespenik gabekoak.
- **Kodea:** zifratze- eta deszifratze-eragiketak kontrolatzeko erabilitako sinbolo-sekuentzia.
- **Konfidentzialtasuna:** konfidentzialtasuna dokumentu elektroniko bat pertsona-zerrenda jakin bati izan ezik gainerako erabiltzaile guztiei eskura ezin egiteko gaitasuna da. Horrela, komunikazioak beste batzuek entzun ezin izateko moduan egitea eta



dokumentuak adierazitako hartzaileak soilik irakurri ahal izateko moduan igortzea lortu dezakegu.

- **Kriptografia:** kriptografia matematikaren adar bat da, eta aztertzen duena da nola eraldatu informazio irakurgarria zuzenean ezin irakurtzeko moduan, hau da, irakurtzeko deszifratu behar izateko moduan.
- **Sinadura sortzeko datuak (gako pribatua):** gako pribatua zenbaki bakar eta sekretua da eta pertsona bakar bati dagokio, horrela, pertsona bere gako pribatuaren bitartez identifika daiteke. Gakoa asimetrikoa da gako publikoarekiko. Gako batek beste gako batek sinatu edo zifratu duena egiaztatu eta deszifratu dezake.
- **Sinadura egiaztatzeko datuak (gako publikoa):** gako publikoa pertsona bakar bati dagokion zenbaki bakarra da baina, gako pribatua ez bezala, edonork jakin dezake. Prozedura matematikoen bitartez gako pribatuarekin lotu eta sinadura digitalak zifratzeko eta egiaztatzeko balio du.
- **Ziurtapen Praktiken Deklarazioa (ZPD):** Izenpek edonorentzat eskuragarri duen deklarazioa, erraz lortu daitekeena, elektronikoki eta dohainik. Segurtasun-dokumentuaren balioa du eta bertan zehazten dira —eIDAS arauaren esparruan— zein diren Ziurtapen Zerbitzuen Egileen betebeharrak, sinadura sortzeko nahiz egiaztatzeko datuak kudeatzeari dagokionez eta ziurtagiri elektronikoak kudeatzeari dagokionez, hala nola, zein diren aplikagarri diren baldintzak ziurtagiria eskatzean, jaulkitzean, erabiltzean nahiz iraungitzean, zein diren segurtasun-neurri teknikoak eta antolakuntzari dagozkionak, zein diren ziurtagirien indarraldiari buruzko profilak eta informazio-mekanismoak. Bertan zehazten da, halaber, koordinazio-prozedurak izan behar direla dagozkien erregistro-publikoekin, ziurtagirietan aipatzen den ahalmenaren indarraldiari buruzko informazioa —erregistro horietan aginduz jaso beharko dira— berehala elkarri trukatzeko.
- **Ziurtagirien direktorioa:** ITU-Tren X.500 estandarraren araberako informazio-biltegia. Horrela, Izenpek ziurtagirien direktorio eguneratua mantentzen du eta direktorio horrek egindako ziurtagiriak emango ditu aditzera.
- **Sinadura elektronikoak sortzeko gailua:** eIDAS arauaren II. eranskinean zerrendatzen diren betekizunak betetzen dituen sinadura elektronikoak sortzeko gailua.
- **Sinadura elektronikoak:** sinatzaileak sinatzeko erabiltzen dituen formatu elektronikoko datuak, beste datu elektroniko batzuei erantsiak edo horiekin modu logikoan lotuak.
- **Sinadura elektroniko aurreratua:** eIDAS1 eta eIDAS2 arauaren 26. artikuluan aintzat hartzen diren betekizunak betetzen dituen sinadura elektronikoak.
- **Sinadura elektroniko kualifikatua:** sinadura elektroniko aurreratua, sinadura elektronikoak sortzeko gailu kualifikatu bidez sortzen dena eta sinadura elektronikoko ziurtagiri kualifikatu batean oinarritzen dena.
- **Sinatzailea:** sinadura sortzeko gailua duen pertsona, eta nor bere izenean edota ordezkatzan duen pertsona fisiko edo juridikoaren izenean jarduten du.
- **Hash edo hatz-marka:** mezu bati hash funtzioa aplikatu ostean lortzen den emaitza, tamaina zehatzekoa, eta hasierako datuetara modu unibokoan lotuta dagoena.



- **HSM (segurtasun-modulu kriptografikoa):** gako kriptografikoak sortzen eta babesten dituen segurtasun-gailua da.
- **Gako Publikoen Azpiegitura (PKI, Public Key Infrastructure):** PKIak ziurtapen-sistema zein entitatek osatuko duten zehazten du, entitate horiek zein betekizun betetzen duten, zein arau eta protokolori jarraitu behar zaion sistema barnean lan egiteko, informazio digitala nola kodetzen den eta nola transmititzen den, eta zein izango den azpiegiturak kudeatzen dituen objektu eta dokumentuetako informazioa. Horrek guztiak Gako Publikoko teknologia izango du oinarri (bi gako).
- **Europako Parlamentuaren eta Kontseiluaren 2016/679 Araudia, 2016ko apirilaren 27koa, pertsona fisikoak babesteari buruzkoa, datu pertsonalen tratamenduari eta datu horien zirkulazio libreari dagokionez. Erregelamendu horrek 95/46/EB Zuzentaraua indargabetzen du.** Europar Batasuneko Araudi horren helburua da datu pertsonalak baliatzerakoan pertsona fisikoaren askatasun publikoak eta oinarrizko eskubideak bermatu eta babestea, batez ere, pertsona horien ohorea eta intimitate pertsonal eta familiara.
- **Ezeztatutako Ziurtagirien Zerrenda (CRLak):** Izenpek jaulkitzen dituen ziurtagiri ezeztatuek osatzen duten zerrenda da, eta berehalako ezeztatze bat gertatzen den bezain laster geratzen da jasota zerrendan. Bada beste web-zerbitzu iraunkor bat ere, Izenpek ezeztatutako ziurtagirien eguneratze inkremental telematikoak kontsultatzeko aukera eskaintzen duena. Ezeztatutako Ziurtagirien Zerrendak argitaratzeari dagokionez, sarbide azkarra eta segurua bermatzen zaie erabiltzaileei eta ziurtagirien harpidedunei.
- **Ziurtagiriaren serie-zenbakia:** balio osoa eta bakarra da, eta modu unibokoan dago edozein Ziurtapen Zerbitzuen Egilek jaulkitako ziurtagiri bati lotuta.
- **OCSP (Online Certificate Status Protocol):** ziurtagiri elektronikoen baten egoera frogatzen duen protokolo informatikoa da.
- **OID (Object Identifier):** aldagai oso ez negatiboek —puntu batez banatuta— osatzen duten sekuentzia. Erregistratutako objektuei egokitu dakieke, eta bakarrak dira gainerako OID guztien artean.
- **PIN (Personal Identification Number):** mekanismo honen beraren babespean dagoen baliabide batera sartu behar duen subjektuak bakarrik ezagutu behar duen karaktere-sekuentzia.
- **Ziurtapen-politika:** Ziurtapen Praktiken Deklarazioari erantsitako dokumentua da, eta bertan jasotzen da zein den ziurtagirien aplikazio-eremua, karaktere teknikoak, ziurtapen-zerbitzuak ematerakoan jarraitutako prozeduretarako arauak, baita ziurtagirien erabilpen-baldintzak ere.
- **Gakoen edukitzaileak:** sinadura digitaleko gakoak eta kautotzeko gakoak dituzten eta horiek zaintzeaz arduratzen diren pertsona fisikoak izango dira.
- **Konfiantzako zerbitzuen egile kualifikatua (TSP):** konfiantzako zerbitzuen egilea, eIDAS arauaren arabera konfiantzako zerbitzu bat edo batzuk egiten dituen eta ikuskapen-organismoaren eskutik kualifikazioa lortu duena.



- **Egiaztapen Aurreratuko Zerbitzua:** zerbitzu honek aukera ematen dio zerbitzuaren Entitate Erabiltzaileari Izenpek jaulkitako ziurtagiriak erabiltzeko. Horretarako, ziurtagirien egoera begiratzen du, OCSP (Online Certificate Status Protocol) protokoloaren bidez.
- **Argitalpen-zerbitzua:** ziurtapen-sistemarekin lotutako dokumentazioa argitaratzen duen zerbitzua da, eta ziurtagirien erabiltzaile guztientzat egon behar du erabilgarri.
- **Denbora zigilatze zerbitzua:** entitate erabiltzaileari aukera ematen dio bermatzeko denbora-tarte jakin batean informazio jakin bat bazegoela.
- **Zerbitzari segurua:** web-zerbitzari bat da eta, bertan, komunikazioa zifratuta doa batetik bestera, modu seguruan. Eragiketa hori egin ahal izateko, zerbitzariak ziurtagiri bat izan behar du.
- **Ziurtagiriaren eskatzailea:** nor bere buruaren izenean, edota erakunde batenean, ziurtagiri bat jaulkitzea eskatzen duen pertsona da.
- **SSL (Secure Socket Layer):** protokolo honek bide ematen du zifratutako informazioa Interneteko nabigatzaile baten eta zerbitzari baten artean transmititzeko.
- **Ziurtagiriaren harpideduna:** Ziurtapen Zerbitzuen Egileak ziurtatutako gako publikoaren bitartez identitate pertsonala elektronikoki sinatutako datuei lotua duen pertsona.
- **Txartel kriptografikoa:** Sinadura Sortzeko Gailu Seguru gisa hartzen den txartela da, eta harpidedunak, besteak beste sinatzeko eta kautotzeko erabiltzen diren gako pribatuak biltzeko, sinadura elektronikoak sortzeko eta datu-mezuak deszifratzeko erabil dezake.
- **Hirugarrengoen konfiantza duten hirugarren batzuk:** Izenpek jaulkitako ziurtagiriak jasotzen dituzten pertsona fisikoak edo juridikoak dira. Ziurtagirietan konfiantza duten hirugarren batzuk dira eta, hirugarrenak diren heinean, Ziurtapen Praktiken Deklarazioan ezarritakoa zaie aplikagarri, baldin eta ondorioetarako ziurtagiri horietan benetan konfiantza badute.
- **Ziurtagirien erabiltzaileak:** ziurtagirien erabiltzaile diren azken entitateak ziurtagiri digitalak jaulki, kudeatu eta erabiltzeko zerbitzuak jasotzen dituzten pertsona eta erakundeak dira.
- **Zigilu baten sortzailea:** zigilu elektronikoa bat sortzen duen pertsona juridikoa.
- **Zigilu elektronikoa:** formatu elektronikoko datuak, formatu elektronikoko beste datu batzuei eranstean zaizkienak edo horiekin modu logikoan lotzen direnak, azken horien jatorria eta integritatea bermatzeko.
- **Zigilu elektronikoa aurreratua:** eIDAS arauaren 36. artikuluan aintzat hartzen diren betekizunak betetzen dituen denbora elektronikoa
- **Zigilu elektronikoa kalifikatua:** zigilu elektronikoa aurreratua, zigilu elektronikoak sortzeko gailu kualifikatu bidez sortzen dena eta zigilu elektronikoko ziurtagiri kualifikatu batean oinarritzen dena.
- **Zigilu elektronikoa sortzeko datuak:** zigilu elektronikoko egileak zigilu elektronikoa sortzeko erabiltzen dituen datu bakarrak.



- **Zigilu elektronikoko ziurtagiria:** deklarazio elektronikoa, zigilu bat baliozkotzeko datuak pertsona juridiko batekin lotzen dituena, eta pertsona horren izena berresten duena.
- **Zigilu elektronikoko ziurtagiri kualifikatua:** konfiantzako zerbitzuen egile kualifikatu batek jaulkitako zigilu elektronikoetako ziurtagiria, eIDAS arauaren III. eranskinean ezarritako betekizunak betetzen dituena.
- **Zigilu elektronikoa sortzeko gailua:** zigilu elektronikoa sortzeko erabiltzen den tresna edo programa informatiko konfiguratu.
- **Zigilu elektronikoa sortzeko gailu kualifikatua:** eIDAS arauaren II. eranskinean zerrendatzen diren betekizunak mutatis mutandis betetzen dituen zigilu elektronikoak sortzeko gailua.
- **Denbora-zigilu elektronikoa:** formatu elektronikoko datuak, formatu elektronikoko beste datu batzuk une jakin batekin lotzen dituztenak eta azken datu horiek une horretan bazeudela frogatzen dutenak.
- **Denbora-zigilu kualifikatu elektronikoa:** eIDAS arauaren 42. artikuluan ezartzen diren betekizunak betetzen dituen denbora-zigilu elektronikoa.

1.6.2 Akronimoak

ARL: ziurtapen-agintaritzak ezeztatzeko zerrenda.

CA: ziurtapen-agintaritza.

CN: Common Name (izen arrunta).

CRL: Certificate Revocation List (ezeztatutako ziurtagirien zerrenda).

DN: Distinguished Name (izen bereizgarria).

ZPD: Ziurtapen Praktiken Deklarazioa

QSCD: Sinadura sortzeko gailu kualifikatua

ETSI: European Telecommunications Standards Institute.

GN: ziurtagiri baten edukitzailearen izen berezia

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

LRA: tokiko erregistro-agintaritza.

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

OID: Object Identifier (objektu-identifikatzaile bakarra).

PIN: Personal Identification Number (identifikazio pertsonaleko zenbakia).

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

PKI: Public Key Infrastructure (gako publikoen azpiegitura)

PSC: Konfiantzazko Zerbitzuen Egilea

RA: erregistro-agintaritza.



SSL: Secure Socket Layer

TSA: Denbora Zigilatzeko Agintaritzaren zerbitzaria

eIDAS1: 1999/93/EE Zuzentaraua indargabetzen duen Europako Parlamentuaren eta Kontseiluaren identifikazio elektronikoari eta barne-merkatuko transakzio elektronikoetarako konfiantzako zerbitzuei buruzko 2014ko uztailaren 23ko 910/2014 araudia.

eIDAS2: 2024/1183 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2024ko apirilaren 11koa, zeinaren bidez aldatzen baita 910/2014 Erregelamendua identitate digitalaren Europako esparrua ezartzeari dagokionez.



2 Argitalpena eta informazio-biltegiaren arduradunak

2.1 Informazio-biltegia

IZENPE informazio publikoko biltegia du www.izenpe.com webgunean, eta asteko zazpi egunetan eta eguneko 24 orduetan dago eskuragarri.

2.2 Ziurtapen-informazioaren argitalpena

Izenpek bermatzen du ZPDa, ziurtagirien berariazko politikak eta ziurtagiriak erabiltzeko terminoak eta baldintzak eskuragarri egongo direla www.izenpe.eus web-orrian.

Izenpek bermatzen du erabiltzaileak eta harpidedunak segurtasunez, azkar eta dohainik sartu ahal izango direla ziurtagiriaren egoerari buruzko informaziora. Bi modutan sartu ahal izango da:

- Online kontsulta (OCSP): Izenpek aukera ematen du jaulkitako ziurtagirien egoera azkar eta modu seguruan kontsultatzeko. Ziurtagirietan konfiantza duten hirugarrenek ere kontsulta dezakete egoera.
- Offline kontsulta (CRL): ezeztatutako ziurtagirien zerrendak (CRL) argitaratuta.

Izenpek testak egiteko webguneak ditu, software-hornitzaileek SSL/TLS ziurtagiriak dituzten haien produktuak produkzio ingurune batean proba ditzaten. Izenpek zenbait webgune ditu, gutxienez amaierako ziurtagiri bizi, iraungi eta ezeztatu. Berariazko politikan kontsultatu horietako bakoitzaren ibilbidea.

2.2.1 Argitalpen- eta jakinarazte-politika

Zerbitzuaren zehaztapenetan edo baldintzetan egindako aldaketak www.izenpe.com helbidearen bidez jakinaraziko dizkie Izenpek erabiltzaileei. Izenpek egoera espezifikotarako komunikazio-bide gehigarriak ezarri ahal izango ditu.

ZPDa eta Ziurtagiriak Erabiltzeko Terminoak eta Baldintzak mugarik gabe eskuragarri egongo dira www.izenpe.com web-orrian, indarrean dagoen bertsioa ez ezik, aurreko guztiak ere bai.

2.2.2 Ziurtapen Praktiken Deklarazioan argitaratzen ez diren elementuak

Ziurtapen Praktiken Deklarazio honetako “9.3.2 Irismenaren barruan ez dagoen informazioa atalean lehendik dauden osagaiei, azpiosagaiei eta elementuei, baina horien konfidentziasuna gordetzeko publikoarentzat erabilgarri ez daudenei, egiten zaie erreferentzia.

2.3 Argitalpen-maiztasuna

Ziurtapen Praktiken Deklarazioa onartzen den unean ematen da argitara eta urteko berrikusketan aldaketarik izango ez balitz. Ziurtapen Praktiken Deklarazioan egin beharreko aldaketak dokumentu honek diotenaren arabera egin behar dira.

Ziurtagirien egoerari buruzko informazioa dokumentu honetako “4.9.7 behean eta “4.9.10 Online ezeztatzea egiaztatzeko eskakizunak atalek diotenaren arabera argitaratu behar da.



2.4 Biltegirako sarrera kontrolatzea

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

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

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



3 Izenak

3.1.1 Izen motak

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

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

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

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

Igorlea

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

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

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

Gaia

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

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

Ziurtagiri bakoitzerako berariazko dokumentazioan ezartzen da ziurtagiri bakoitzaren profil zehatza.

3.1.2 Izenen esanahia

Subject Name eremuko izen bereizgarri (DN) guztiak adierazgarriak dira. Ziurtagiriaren harpidedunari lotzen zaizkion atributuen deskribapena gizakiek irakurtzeko modukoa da (ikus dokumentu honetako 7.1.4 Izenen formatuak atala).

3.1.3 Goitizenak

Ziurtapen Politika Partikularren Deklarazio bakoitzak zehaztuko du alderdi hori, politika horien mende egindako ziurtagirietarako.

3.1.4 Izenen formatuak interpretatzeko arauak

Ziurtagiri batean subject-ak eta jaulkitzailearen izenak pertsona (fisikoa edo juridikoa) edo gailua identifikatzen du, eta esanahia izan beharko du, RAK izen edo goitizen horien eta dagozkien entitateen arteko loturaren ebidentzia baitu. Izenak ezin izango dira engainagarriak izan. Horrek ez ditu baztertzen “3.1.5 Izen-bakartasuna atalean definitzen diren goitizen-ziurtagiriak.



3.1.5 Izen-bakartasuna

Harpidedunen eta, hala badagokio, gakoan edukitzaileen izenak bakarrak dira ziurtagiri mota bakoitzerako. Common name-ak (CN) izenean espazioetako eta bakartasuneko eskakizunak bete beharko ditu. Izenpek goitizen-ziurtagiriak jaulki ditzake, baina ezin izango dira CA ziurtagiriak edo mendeko CA ziurtagiriak izan. Ziurtagiri mota bakoitzaren profilaren xehetasunak kontsulta daitezke www.izenpe.eu webgunean.

3.1.6 Izenen eta marka erregistratuaren tratamenduaren arloko gatazkak ebaztea

Ziurtagiri-eskatzaileek ziurtagiriak jaulkitzeko eskaeretan izena jartzean, ez dute jarri behar etorkizuneko harpidedunak hirugarrenen eskubideak urratzeko moduko izenik.

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

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

3.2 Identitatea baliozkotzea

3.2.1 Gako pribatuaren jabetza frogatzeko metodoak

Gako-parea

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

3.2.2 Erakundearen identitatea kautotzea

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



3.2.3 Pertsona fisiko eskatzailearen nortasuna kautotzea

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

3.2.4 Egiaztatu gabeko harpidedunaren informazioa

Ziurtapen Politika Partikularren Deklarazio bakoitzak zehaztuko du alderdi hori, politika horien mende egindako ziurtagirietarako.

3.2.5 Agintaritza baliozkotzea

Ziurtapen Politika Partikularren Deklarazio bakoitzak zehaztuko du alderdi hori, politika horien mende egindako ziurtagirietarako.

3.2.6 Elkarreragineko irizpideak

Ez dago FNMT-RCMaz kanpoko Ziurtapen Agintaritzekiko elkarreragin-harremanik.

3.3 Gakoak berriro jaulkitzeko eskaeratarako identifikatzea eta kautotzea

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

3.3.1 Ohiko berritza

Ziurtapen Politika Partikularren Deklarazio bakoitzak zehaztuko du alderdi hori, politika horien mende egindako ziurtagirietarako.

3.3.2 Ezeztatze baten ondorengo berritza

Ziurtagiri bat ezeztatu ondoren, ziurtagiria berritu nahi izanez gero, ziurtagiri horren hasierako jaulkipeneko prozesu bera bete beharko da.

3.4 Ezeztatzeko eskaeratarako identifikatzea eta kautotzea

Ezeztatzeko eskaera baten kautotze-baldintzak dagokien politikan garatuko dira.



4 Ziurtagirien bizi-zikloaren baldintza operatiboak

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

Ziurtagiri mota bakoitzerako berariazko erregulazioa dagokion politikan kontsultatu beharko da.

4.1 Ziurtagiria eskatzea

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

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

4.1.1 Eskaeraren egiaztapena

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

4.1.2 Inskribatzeko prozesua eta erantzukizunak.

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

- Eskatzailearen, harpidedunaren eta sinatzaileen nortasuna eta bestelako inguruabar pertsonalak egiaztatzea, ziurtagirietan jasotakoak edo ziurtagirien xedeetarako garrantzitsuak direnak, prozedura hauen arabera.
- Kudeatzen dituen ziurtagirien jaulkipenari, berritzeari, ezeztatzeari edo berraktibatzeari buruzko dokumentazio eta informazio guztia gordetzea.
- Izenperi garaiz ematea ziurtagiriak azkar eta modu fidagarrian ezeztatzeko eskaeren berri.
- Izenperi artxiboak erabiltzen uztea, baita jardueretarako erabiltzen diren prozeduren eta horretarako behar den informazioaren mantentze-lanen ikuskapena egiten ere.
- Izenperi ematea ziurtagiriak jaulkitzeko, berritzeko edo berraktibatzeako eskaeren berri, baita hark jaulkitzen dituen ziurtagiriei buruzko beste zeinahi alderdiren berri ere.
- Garaiz begiratzea ziurtagirien iraunaldian eragina izan dezaketen ezeztatzeko zergatiak.



- Ziurtagiriak jaulki, berritu eta ezeztatzeko Izenpek ezarritako prozedurak eta gai horretaz indarrean dagoen legeriak agindutakoa betetzea.
- Ziurtagiri motak eskatzen badu, bere gain hartu ahal izango du sinadura elektronikoa sortzeko eta egiaztatzeko prozedura teknikoak harpidedunaren eta/edo gakoan edukitzailearen esku jartzeko eginkizuna.

4.2 Eskaerak prozesatzea

4.2.1 Identifikatzeko eta kautotzeko eginkizunak egitea

Izenperen erantzukizuna da harpideduna behar bezala identifikatzea. Prozesu hori ziurtagiria jaulki aurretik egin beharko da, eta bi prozesuen artean ezin da hilabete baino gehiago igaro.

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

4.2.2 Eskaerak onartzea edo baztertzea

Ziurtagiria eskatu ondoren, RAK eskatzaileak emandako informazioa egiaztatu beharko du, harpidedunaren identitatearen baliozkotzea barne.

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

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

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

4.2.3 Eskaera prozesatzeko denbora

Ziurtapen Politika Partikularren Deklarazio bakoitzak zehaztuko du alderdi hori, politika horien mende egindako ziurtagirietarako.

4.3 Ziurtagiria jaulkitzea

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

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



4.3.1 CAren jardunak ziurtagiriak jaulkitzean

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

4.3.2 Jaulkipena jakinaraztea harpidedunari

Izenpek ziurtagiriaren jaulkipenaren berri emango dio harpidedunari.

4.4 Ziurtagiria onartzea

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

Harpidedunak/Sinatzaileak 15 eguneko epea du, ziurtagiria ematen zaionetik, ziurtagiriak behar bezala funtzionatzen duela egiaztatzeko eta, beharrezkoa izanez gero, Izenperi itzultzeko.

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

4.4.1 Ziurtagiria onartzeko prozesua

Ziurtagiria eskatzeko dokumentuaren sinadurarekin batera onartuko dira ziurtagiria erabiltzeko terminoak eta baldintzak, www.izenpe.com webgunean eskuragarri daudenak.

4.4.2 CAk ziurtagiria argitaratzea

Harpidedunak ziurtagiria onartu eta sortu ostean, Izenperen barneko biltegietan emango da argitara ziurtagiri hori. Edonork eskura dezake ziurtagiriaren egoerari buruzko informazioa, VA edo CRLa kontsultatuta.

4.4.3 CAk beste entitate batzuei ziurtagiria jaulki izana jakinaraztea

Zerbitzari seguruko ziurtagiriak (SSL) argitara emango dira Izenperen Certificate Transparency Log Server (CT) zerbitzuan, Google-en politikaren arabera. Gainerako ziurtagiriak ez zaizkio inolako entitateri jakinaraziko.

4.5 Gako-parea eta ziurtagiriaren erabilera

4.5.1 Harpidedunaren gako pribatua eta ziurtagiriaren erabilera

Bere gakoak zaintzen dituen harpidedunak,



- Ziurtagirien euskarriak ongi erabili eta gordeko direla bermatuko du.
- Ziurtagiria egoki erabiliko du, eta, zehazki, ziurtagirien erabilera-mugak aintzat hartuko ditu.
- Arretaz zainduko du gako pribatua, baimendu gabeko erabilerak saihestearren, Ziurtapen Praktiken Deklarazioko 6.1, 6.2 eta 6.4 atalek agintzen dutenaren arabera.
- Izenperi eta harpidedunaren ustez konfiantza izan dezakeen edozein pertsonari honakoak jakinaraziko dio, atzerapenik gabe (atzeratzeko arrazoirik egon ezean):
 - Gako pribatua galdu, norbaitek ostu edo arriskuan jarri izana.
 - Gako pribatuaren kontrola galdu izana, aktibatze-datuak (gailu kriptografikoaren PIN kodea, adibidez) arriskuan jartzeagatik edo beste edozein arrazoirengatik.
 - Ziurtagiriaren edukian dauden okerrak edo izandako aldaketak (harpidedunak dakizkienak edo jakin litzakeenak). Aldaketak ziurtagiria ezeztatzea badakar, horretarako eskaera egin behar du harpidedunak.
- Gako pribatua erabiltzeari utziko dio ziurtagiriaren balio-epea amaitu ondoren.
- Gakoen edukitzaileei jakinaraziko die zein betebeharrak dagozkien.
- Ez du ziurtagiri-zerbitzuen ezartze teknikoak kontrolatuko, manipulatu edo atzeranzko ingeniartzako ekintzarik ez egingo, aurrez Ziurtapen Entitatearen idatzizko baimenik eduki gabe.
- Ez du ziurtagiri-zerbitzuen segurtasuna arriskuan nahita jarriko.
- Ez ditu ziurtagirietako gako publikoei dagozkien gako pribatuak erabiliko inongo ziurtagiri izenpetzeko, ziurtapen-entitatea balitz bezala.
- Ziurtagirian zerrendatutako gako publikoari dagokion gako pribatua erabiliz sinadura digitalak sortzen dituen ziurtagiri kualifikatuen harpidedunak aitortu egin behar du, dagokion bitarteko juridikoaz, sinadura elektronikoko horiek eskuz idatzitako sinaduren baliokide direla, gailu kriptografikoa erabiltzen denean, betiere eIDASek adierazitakoaren arabera.

Bere gakoak Izenpen gordetzen dituen harpidedunak,

- Ziurtagiria egoki erabiliko du, eta, zehazki, ziurtagirien erabilera-mugak aintzat hartuko ditu.
- Arretaz zainduko du aktibatze gakoak, baimendu gabeko erabilerak saihestearren, Ziurtapen Praktiken Deklarazioko 6.1, 6.2 eta 6.4 sailek agintzen dutenaren arabera.
- Izenperi eta harpidedunaren ustez konfiantza izan dezakeen edozein pertsonari honakoak jakinaraziko dio, atzerapenik gabe (atzeratzeko arrazoirik egon ezean):
 - Gako pribatuaren kontrola galdu izana, aktibatze-datuak arriskuan jartzeagatik edo beste edozein arrazoirengatik.



- Ziurtagiriaren edukian dauden okerrak edo izandako aldaketak (harpidedunak dakizkienak edo jakin litzakeenak). Aldaketak ziurtagiria ezeztatzea badakar, horretarako eskaera egin behar du harpidedunak.
- Gako pribatua erabiltzeari utziko dio ziurtagiriaren balio-epea amaitu ondoren.
- Ziurtapen Praktiken Deklarazio honetan adierazten diren betebeharrak onartuko ditu.
- Ez du ziurtagiri-zerbitzuen ezartze tekniko kontrolatuko, manipulatu edo atzeranzko ingeniartzako ekintzarik ez egingo, aurrez Ziurtapen Entitatearen idatzizko baimenik eduki gabe.
- Ez du ziurtagiri-zerbitzuen segurtasuna arriskuan nahita jarriko.
- Ziurtagirian zerrendatutako gako publikoari dagokion gako pribatua erabiliz sinadura digitalak sortzen dituen ziurtagiri kualifikatuen harpidedunak aitortu egin behar du, dagokion bitarteko juridikoaz, sinadura elektronik horiek eskuz idatzitako sinaduren baliokide direla, sinadura sortzeko gailu kualifikatu bat erabiltzen denean, betiere eIDAS arauak agintzen duenaren arabera.

4.5.2 Ziurtagirietan konfiantza duten hirugarren batzuek gako publikoa eta ziurtagiria erabiltzea

Ziurtagirien erabiltzaile egiaztatzaileak honako betebeharrak dituzte:

- Eman nahi zaion erabilerarako ziurtagiria egokia den ala ez jakiteko, informazioa iturri independenteetatik jasotzea.
- Ziurtagiriak erabiltzeko baldintzak ezagutzea, Ziurtapen Praktiken Deklarazioan aurreikusitakoaren arabera.
- Emandako ziurtagirien baliozkotasuna edo ezeztapena egiaztatzea, eta, horretarako, ziurtagirien egoerari buruzko informazioa erabiltzea.
- Ziurtagirien hierarkiako ziurtagiri guztiak egiaztatzea, sinadura digitalean edo hierarkiako ziurtagiriren batean konfiantza jarri baino lehen.
- Kontuan izatea ziurtagiria erabiltzeko dauden mugak, nonahi daudelarik ere: ziurtagirian bertan nahiz egiaztatzailearen kontratuan.
- Kontuan izatea kontratuan edo beste nonbait finkatutako badaezpadako neurri guztiak, haren izaera juridikoa edozein delarik ere.
- Ziurtagiriari buruzko gertaera edo egoera irregular guztiak jakinaraztea, ziurtagiria ezeztatzeko arrazoia izan daitezkeenak.
- Ziurtagiri-zerbitzuen ezartze tekniko ez kontrolatzea, manipulatu edo atzeranzko ingeniartzako ekintzarik ez egitea, aurrez Izenperen idatzizko baimenik gabe.
- Ziurtagiri-zerbitzuen segurtasuna arriskuan nahita ez jartzea.
- Sinadura elektronik horiek eskuz egindako sinaduren baliokideak direla onartzea, eIDAS1 eta eIDAS2 arauaren arabera.



4.6 Ziurtagiria berritzea

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

4.6.1 Ziurtagiria berritzeko inguruabarrak

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

4.6.2 Nork eska dezake ziurtagiria berritzea?

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

4.6.3 Ziurtagiria berritzeko eskaeren tratamendua

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

4.6.4 Harpidedunari jakinaraztea

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

4.6.5 Ziurtagiri berritua onartzeko prozedura

Ziurtapen berriko eskaerarako erabiltzen den prozesu bera erabili beharko da.

4.6.6 Ziurtagiria argitaratzea

Ziurtagiria berritu ostean, ziurtagiri berria ziurtagiri-biltegi berean emango da argitara.

4.6.7 Beste entitate batzuei jakinaraztea

4.4.3. puntuan jasotakoaren arabera.

4.7 Ziurtagiria berritzea, haren gakoak berriro sortuta

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

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



4.7.1 Ziurtagiriaren gakoak berriro sortzeko inguruabarrak

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

4.7.2 Nork eska dezake?

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

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

4.7.3 Ziurtagiria berritzeko eskaeren tratamendua, gakoak berriro sortuta

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

4.7.4 Harpidedunari jakinaraztea

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

4.7.5 Ziurtagiri berritua onartzeko prozedura

Ziurtapen berriko eskaeretakako erabiltzen den prozesu bera erabili beharko da.

4.7.6 Ziurtagiria argitaratzea

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

4.7.7 Beste entitate batzuei jakinaraztea

4.4.3. puntuan jasotakoaren arabera.

4.8 Ziurtagiria aldatzea

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

4.8.1 Ziurtagiria aldatzeko inguruabarrak

Ez da aldaketarik erabaki.



4.8.2 Nork eska dezake ziurtagiria aldatzea?

Ez da aldaketarik erabaki.

4.8.3 Ziurtagiria aldatzeko eskaerak prozesatzea

Ez da aldaketarik erabaki.

4.8.4 Ziurtagiriaren aldaketa jakinaraztea

Ez da aldaketarik erabaki.

4.8.5 Ziurtagiriaren aldaketa onartzea dakarren jokabidea

Ez da aldaketarik erabaki.

4.8.6 Ziurtagiri aldatua argitaratzea

Ez da aldaketarik erabaki.

4.8.7 Ziurtagiriaren aldaketa beste erakunde batzuei jakinaraztea

Ez da aldaketarik erabaki.

4.9 Ezeztatzea

4.9.1 Ezeztatzeko inguruabarrak

Honako egoera hauetan ezeztatuko ditu ziurtagiriak Izenpek:

- Ziurtagiriak ezeztatzea sinatzaileak, edo hori ordezkatzeko duen pertsona fisikoak edo juridikoak eskatuta edota hirugarren baimendu batek edo pertsona juridikoko ziurtagiri elektronikoa eskatu duen pertsona fisiko batek eskatuta.
- Sinatzailearen edo ziurtapen-zerbitzuen egilearen sinadura sortzeko datuak urratzen direnean edo arriskuan jartzen direnean, edo sinatzaileak edo hirugarren batek datu horiek bidegabe erabiltzen dituenean.
- Ebazpen judizial edo administratiboren batek hala agintzen duenean.
- Sinatzailearen nortasun juridikoa iraungitzea edo hiltzea, ordezkatuaren nortasun juridikoa iraungitzea edo hiltzea, sinatzailearengan edo ordezkatuarengan gerora ezintasun iraunkorra edo partziala agertzea, ordezkari zari amaiera ematea, ordezkariaren pertsona juridikoa desagitea, edo pertsona juridiko batek egindako ziurtagirietan islatzen diren sinadura sortzeko datuak zaindu eta erabiltzeko baldintzak aldatzea.
- Izenpek jardura eteten badu, baldin eta, sinatzailearen aurretiko onarpena dela medio, hark jaulkitako ziurtagiri elektronikoen kudeaketak ez bazaizkio transferitzen beste ziurtapen-zerbitzuen egileren bati.
- Ziurtagiria lortzeko emandako datuak aldatzea edo ziurtagiria emateko egiaztatutako inguruabarrak aldatzea.
- Ziurtagiria galtzen bada edo lapurtzen badute, edo erabiltzeko ez dela geratzen bada ziurtagiriaren euskarria hondatu delako edo Ziurtapen Politikak aurreikusten ez duen beste euskarri batera aldatu delako.



- Aldeetakoren batek dagozkion betebeharrak betetzen ez dituenean.
- Ziurtagiria jaulkitzean akatsen bat gertatu bada, ezarritako prozedurari ez egokitzeagatik edo jaulkitze-prozesuan arazo teknikoak sortzeagatik.
- Sinadura sortzeko datuen hitzarmenetik kanpoko gorabeherak direla medio, Izenpek jaulkitako ziurtagiriaren fidagarritasuna eta sistemen segurtasuna arriskuan jartzen bada.
- Ziurtagiria edo harekin lotzen den dokumentazioa jaulkitzean eta/edo banatzean akats teknikoren bat gertatzen bada.
- Ziurtagiria eskatu zen egunetik hiru hilabete iragan direnean eskatzaileak jaso duen arte.
- Izenpek ziurtagiria jaulkitzeko eskaera bat jasotzen duenean, eta politika bereko eta bakartasun-irizpide bereko beste ziurtagiri bat dagoenean, ezeztatu egingo da indarrean dagoen ziurtagiria, baina eskatzaileak ezeztatze eskaera egin ondoren.

4.9.2 Nork eska dezake ziurtagiria ezeztatzeko?

Honako hauek eska dezakete ziurtagiria ezeztatzea:

- Harpidedunak.
- Entitate harpidedunaren lege-ordezkariek edo hirugarren baimenduak.
- Langileen arduradunak edo hirugarren baimenduak.
- Eskatzaileak.
- Izenpek, dokumentu honetan aintzat hartzen diren kausa teknikoetan.

4.9.3 Ezeztatze eskaeren tratamendua

Ezeztapenaren eskatzaileak IZENPEren aurrean izapidetuko du Ezeztatze Eskaera. Ezeztapena eskatzailea, harpideduna edo sinatzailea ez den pertsona batek eskatzen badu, ezeztapenaren aurretik edo aldi berean, IZENPEk bere ziurtagiriaren ezeztapena eta zergatik egin den jakinaraziko die gakoan edukitzaileari eta ziurtagiriaren harpidedunari.

Eskatzaileak honako bide hauetatik ezeztatu ahal izango du ziurtagiria:

- Bertaratuta:
 - Izenperen aurrean, www.izenpe.com bidez hitzordua eskatuta.
 - Edo erakunde harpidedunaren aurrean, betiere Izenpek aginduzko lege-tresna harpidetu badu horrekin.
- On line, www.izenpe.com helbidean.
- Posta elektronikoa bidez, ziurtagiri kualifikatuz sinatutako ezeztatze-eskaeraren formularioa, izenpe@izenpe.eus helbidera bidaliz.

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



4.9.4 Ezeztatzea eskatzeko graziako epea

Ez da prozesu horrekin lotzen den graziako eperik, ezeztatze eskaera modu egiaztatuan jaso bezain pronto egiten baita ezeztatzea.

4.9.5 Ezeztatzea prozesatzeko CAren epea

“4.9.3 Ezeztatze eskaeren tratamendua” atalean aditzera emandakoa egin ostean, eta RAK (edo Izenpek “4.9.1 Ezeztatze inguruabarrak” atalean adierazitako kasuetan) behar bezala tramitatutako ezeztatzearen ondoren, berehala ezeztatuko da ziurtagiria.

4.9.6 Konfiantzako hirugarren batzuek ezeztatzeak egiaztatze betebeharra

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

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

4.9.7 CRLak sortzeko maiztasuna

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

CRLan adierazten da beste CRL bat jaulkitzeko programatuta dagoen unea, nahiz eta aurreko CRLan adierazitako epea amaitu baino lehen ere CRL bat jaulki daitekeen. Ziurtagiririk berritzen ez bada, ziurtagiriak ezeztatze zerrenda egunero birsortuko da.

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

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

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

4.9.8 CRLak sortzen direnetik argitaratzen direnera arte emandako denbora

CRLa sortzen denetik, 30 segundokoa da gehieneko latentzia-denbora.

Argitaratze-denbora beheralakoa da, baina horiek erakusten dituen zerbitzariak ordubetez azter ditzake.

4.9.9 Ziurtagirien egoera online egiaztatze sistemaren erabilgarritasuna

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

Zerbitzua eguneko 24 orduetan erabili daiteke, asteko 7 egunetan.



4.9.10 Online ezeztatzea egiaztatzeko eskakizunak

Sarbide libreko CRLen zerbitzua erabiltzeak honakoa eskatzen du:

- Jaulkitako azken CRLa beti egiaztatzea —hori ziurtagirian bertan jasotzen den URL helbidean, “CRL Distribution Point” luzapenean, deskargatu ahal izango da—.
- Erabiltzaileak, horrez gain, hierarkiaren ziurtapen-kateko CRLa(k) ere egiaztatzea.
- Erabiltzaileak ziurtatzea baliozkotu nahi den ziurtagiria jaulki duen agintaritzak sinatzen duela ezeztatzeke zerrenda.

Ezeztatzen diren ziurtagiriak CRLtik kenduko dira, baina ziurtagiriaren egoerari buruzko informazioa eskaintzen jarraituko da online egiaztatzearen bitartez, iraungita egonik ere.

Sarbide libreko OCSP zerbitzua erabiltzeak honakoa eskatzen du:

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

4.9.11 Ezeztatzeak ohartarazteko beste modu batzuk

Ziurtagiri bat ezeztatzen denean, Izenpek informaziorako mezu elektronikoa bidaltzen dio ziurtagiriaren harpidedunari.

4.9.12 Arriskupean dagoen gakoaren eskakizun bereziak

Ziurtagiriaren gako pribatua erabiltzeko konpromisoa badago, harpidedunak/sinatzaileak horren berri eman beharko dio IZENPERi, ziurtagiria baliogabetzeko eta ziurtagiria erabiltzeari uzteko eska dezan.

Izenperi 1.5.2 atalean adierazitako seguridad@izenpe.eus posta-kontuaren bidez gako pribatu bat arriskuan egotearen berri emanez gero, arrisku horren froga bat gehitu behar da edozein kasutan, eta posta elektronikoaren gaien honako hau adierazi: “Gakoak arriskuan”. Hori frogatzeko, alderdiek honako metodo hauek erabil ditzakete:

- Arriskuan dagoen gako pribatua bidaltzea edo gako pribatuak sinatutako eta gako publikoak egiazta dezakeen erroka-erantzuna, gako publikoarekin berarekin batera.
- Urrakortasunei eta/edo segurtasun-gorabeheren iturriei buruzko erreferentziak bidaltzea, haien bidez egiaztatu ahal izateko gakoaren arriskua.

Izenpek gakoak arriskuan egotea behar bezala egiaztatzeko bestelako ebidentziak onar ditzake.

Izenperen CA baten gako pribatua arriskupean badago, dokumentu honen 5.7.3 atalak dioena egin behar da.

4.9.13 Eteteko inguruabarrak

Izenpek ez du bere ziurtagirietako bat bera ere etetea onartzen.



4.9.14 Nork eska dezake etetea?

Izenpek ez du bere ziurtagirietako bat bera ere etetea onartzen.

4.9.15 Etetea eskatzeko prozedura

Izenpek ez du bere ziurtagirietako bat bera ere etetea onartzen.

4.9.16 Etenaldiari buruzko mugak

Izenpek ez du bere ziurtagirietako bat bera ere etetea onartzen.

4.10 Ziurtagirien egoera-zerbitzuak

4.10.1 Ezaugarri operatiboak

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

4.10.2 Zerbitzuaren erabilgarritasuna

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

4.10.3 Aukerako ezaugarriak

Erabaki gabeak.

4.11 Harpidetzari amaiera ematea

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

Berriazko politikan adierazten da ziurtagiri bakoitzaren iraungitzea.

4.12 Gakoak zaintzea eta berreskuratzea

4.12.1 Gakoak zaintzeko eta berreskuratzeko praktikak eta politikak

Izenpek ez ditu ziurtagirien titularren gako pribatuak berreskuratuko.

4.12.2 Saioko gakoa babesteko eta berreskuratzeko praktikak eta politikak

Erabaki gabe.



5 Segurtasun fisikoaren, prozeduren eta langileen kontrolak

5.1 Segurtasun fisikoko kontrolak

Izenpek segurtasun fisikoko kontrolak dauzka zerbitzuak egiten dituen leku guztietan.

5.1.1 Instalazioen kokalekua eta eraikuntza

Informazioa prozesatzen den tokiek honako baldintza fisiko hauek betetzen dituzte:

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

5.1.2 Sarbide fisikoa

Datuak prozesatzeko zentroa

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

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

Sarbideen log fitxategi bat dago, leku seguruan gordeta.

Izenpera sartzeko ateen sarbide-mekanismoak dauzkate.

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

Erregistro-agintaritzak (RAK)

RAek Izenperen Segurtasun Politikan zein Hornitzaileen Segurtasun Politikan definitutako beharrezko segurtasun-irizpideak betetzen dituzte.



5.1.3 Elektrizitatea eta aire egokitua

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

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

5.1.4 Urarekiko esposizioa

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

5.1.5 Suteen prebentzioa eta horien aurkako babesa

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

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

5.1.6 Euskarriak biltegitratzea

Babeskopien euskarriak modu seguruan biltzen dira.

5.1.7 Hondakinen tratamendua

Informazio-euskarriak deuseztatzeko prozedurak arautuko dituen politika ezarri da.

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

5.1.8 Instalazioetatik kanpoko babeskopia

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

5.2 Prozeduren kontrolak

5.2.1 Konfiantzazko eginkizunak

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

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



- Lehenbizikoa erroreak saihesteko eta jarrera desegokiak debekatzeko teknologia diseinatzea eta konfiguratzeko da.
- Bigarrena funtzioak zenbait laguneren artean banatzea da, asmo txarreko jarduerak gauzatzeko zenbait lagunekin adostea beharrezkoa izateko.

Izenpek antolakundean garatu diren eginkizunen definizio osoa du. Horietarako guztietarako eginkizunak eta erantzukizunak definituta daude.

5.2.2 Zeregin bakoitzerako pertsona kopurua

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

Gainera, eginkizun baterako lagun bat baino gehiago esleiri daitezke.

5.2.3 Eginkizun bakoitzean identifikatzea eta kautotzea

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

Izenpek bakoitzaren eginkizunak zehazten dituen berariazko dokumentazioa du.

5.2.4 Eginkizunetan zereginak bereiztea

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

5.3 Langileen kontrolak

5.3.1 Historialei, kalifikazioei, esperientziari eta kautotzei buruzko baldintzak

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

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

5.3.2 Historiala ikertzeko prozedurak

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

5.3.3 Trebakuntza-baldintzak

Funtzioak betetzean beren trebetasuna ziurtatzeko beharrezkoa den trebakuntza jasoko dute Izenperen langileek. Urtean behin, gutxienez, egingo dira prestakuntza-jardunak, honako puntu hauekin gutxienez:



- Ziurtapen Praktiken Deklarazioaren kopia bat emango zaie.
- Segurtasunaren gaineko kontzientziazioa.
- Softwarearen eta hardwarearen funtzionamendua eginkizun jakin bakoitzerako.
- Segurtasun-prozedurak eginkizun jakin bakoitzerako.
- Funtzionamenduko eta administrazioko prozedurak eginkizun jakin bakoitzerako.
- Hondamenak konpontzeko prozedurak.
- Gertakariak kudeatzeko prozedura.

RAko langileentzako prestakuntza eta kontzientziazio espezifikoa egingo da, gutxienez alta hartzen dutenean eta, gero, Izenpek finkatzen duen aldizkakotasun batez.

5.3.4 Trebakuntza eguneratzeko baldintzak eta maiztasuna

Izenperen funtzionamenduan aldaketa garrantzitsu bat egiten den bakoitzean trebakuntza-plana egingo da eta planaren egikaritzea dokumentatuko da. “Trusted Roles”eko langileek gutxienez urtean behin jaso beharko du prestakuntza, trebakuntza-mailari eutsi ahal izan diezaioten. Prestakuntza horrek edukia berrikustea hartu beharko du barnean.

5.3.5 Lan-txandaketen segida eta maiztasuna

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

5.3.6 Baimendu gabeko konexioen zigorrak

Informazioaren segurtasuneko gertakariak

Izenpek segurtasun-larrialdiak kudeatzeko plana du.

Zigor Prozesua

Zigor-prozesua definitzen duen barne-erregimen diziplinarioa dago.

5.3.7 Langileak kontratatzeke baldintzak

Izenpek bere zerbitzuen jardunarekin lotuta azpikontratatzten dituen langile guztiek Izenperen Hornitzaileen Segurtasun Politikaren eskakizunak bete beharko dituzte.

5.3.8 Langileei dokumentazioa ematea

Konfiantzazko eginkizunekin lotutako langile guztiek honako hauek jasotzen dituzte:

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



5.4 Audit

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

5.4.1 Erregistratutako gertaera motak

Honako log hauek biltegitzen dira:

- Ziurtagiri-eskaera berriak
- Baztertutako ziurtagiri-eskaerak
- Kontuetarako sarbideen urraketak
- Ziurtagirien sinadura
- Ziurtagiriak ezeztatzea
- Kontuen logon-a
- CRLen sinadura
- CAetako aldaketak
- Ziurtagirien iraungipena

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

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

5.4.2 Log fitxategien prozesamenduaren maiztasuna

Arlo teknikoak etengabe prozesatzen eta ikuskatzen ditu logak hiru hilean behin. Ikuskapen-txostenak alderdi hauek hartzen ditu barnean:

- Baimendu gabe sartzeko egindako saioen zerrenda
- CA bakoitzean izan diren huts-egiteak

5.4.3 Audit logaren atxikipen-aldia

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

5.4.4 Audit logaren babesa

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

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



5.4.5 Audit-logaren backup prozedura

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

5.4.6 Log-fitxategiak biltzea

CAren, RAre eta LRAren log-fitxategiak Izenperen barne-sistemetan gordetzen dira.

5.4.7 Log-fitxategiak sortzea eragin duen ekintzaren jakinarazpena

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

5.4.8 Puntu ahulen azterketa

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

5.5 Erregistroak artxibatzea

5.5.1 Artxibatutako erregistroen mota

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

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

5.5.2 Fitxategiaren atxikipen-aldia

Emandako zerbitzu kualifikatuei buruzko informazio eta dokumentazio guztia 15 urtez gordetzen da (ziurtagiria azkentzen den edo emandako zerbitzua amaitzen den egunetik aurrera), eta ziurtagiriei eta kualifikaziorik gabeko zerbitzuei buruzkoa, berriz, 7 urtez (ziurtagiria azkentzen den edo emandako zerbitzua amaitzen den egunetik aurrera).

5.5.3 Fitxategiaren babesa

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

5.5.4 Artxiboaren backup prozedurak

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

5.5.5 Erregistroen denbora zigilatze eskakizunak

Izenpek erabilitako informazio-sistemek horiek egin direneko denbora-tarteak erregistratzea bermatzen dute. Sistemetako denbora-uneak data- eta ordu-sistema seguru batek sortzen ditu. Sistema guztiek iturri horrekin sinkronizatzen dute beren denbora-unea.



5.5.6 Artxibatzeko sistema

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

5.5.7 Artxiboaren informazioa lortzeko eta egiaztatzeko prozedurak

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

5.6 CAren gakoak aldatzea

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

5.7 Gorabeheren kudeaketa eta larrialdietarako plana

5.7.1 Gorabeherak kudeatzeko prozedurak

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

Larrialdietarako Planaren helburu nagusiak hauek dira:

- Berreskuratze-lanen eraginkortasuna areagotzea, hiru fase hauek erabiliz:
 - Jakinarazteko/ebaluatze/aktibatze fasea, kalteak ebaluatze eta plana aktibatze.
 - Berreskuratze fasea, behin-behingo eta partzialki zerbitzuak berriro martxan jartzeko, harik eta jatorrizko sisteman izandako kalteak konpondu arte.
 - Konpontze fasea, sistema eta prozesuak bere ohiko martxara itzularazteko.
- Ohiko martxaren etenaldi luzeetan ordeko DPZ batean ziurtapen-zerbitzuak partzialki egiteko behar diren jarduerak, baliabideak eta prozedurak identifikatzea.
- Erantzukizunak esleitzea Izenpek jarritako langileei, eta gida bat prestatzea etenaldi luzeetan ohiko martxa berreskuratze.



- Planifikatu den larrialdirako estrategian esku hartzen duten eragile guztien koordinazioa bermatzea (entitateko sailak, kanpoko harremanak eta saltzaileak).

Ziurtapen-zerbitzuak egiteko beharrezkoak diren eginkizun, eragiketa eta baliabide guztiei aplikatu behar zaie Izenperen Larrialdietarako Plana. Ziurtapen-zerbitzuetan diharduten Izenpeko langileei aplikatu behar zaie aipatu plana.

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

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

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

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

5.7.2 Datu eta software ustelen aurrean jarduteko plana

Izenperen Larrialdietarako Planak egoera horien aurrean jarduteko estrategia jasotzen du.

5.7.3 CAren gako pribatua arriskuan dagoenerako prozedura

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

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

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

Larrialdi hori Izenperen negozioaren jarraipenerako planean hartzen da aintzat, eta honako ekintza hauek zehazten ditu, besteak beste:

- 1) Eraginpean dagoen zerbitzua egiteari uztea.



- 2) Eraginpean egon daitezkeen ziurtagiriak ezeztatzea.
- 3) Harpidedunei, erabiltzaileei eta hirugarrenei jakinaraztea. Era berean, barnean hartuko du konfiantza-hitzarmena duten TSPEi jakinaraztea, nabigatzaileen fabrikatzaileei jakinaraztea eta, oro har, Izenperekin zerbitzua erabiltzeko kontratu-harremana duen edozein entitateri jakinaraztea.
- 4) ZPDaren arabera eta indarrean dagoen legeriaren arabera, TSParen jarduerak bertan behera uzteko plana egikaritzeko beharra aztertzea.

5.7.4 Hondamendi baten ondoren, negozioaren jarraipena

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

Izenperen Larrialdietarako eta Negozioaren Jarraipenerako Plana aktibatuko da.

5.8 CAren edo RAren amaiera

5.8.1 Ziurtapen-entitatea

Izenpek jarduerak uzteko plan bat du, eta bertan inguruabar horretan abian jarriko den prozedura zehazten da.

Jarduera etetea erabakiz gero, Izenpek harpidedunari jakinarazi behar dio ziurtapen-zerbitzuak egiteari uztekotan dela, jarduera eten baino bi hilabete lehenago, gutxienez. Harpidedunak jakinarazpena jasoko duela bermatzen duen bideren bat erabili behar du Izenpek hura bidaltzeko. Komunikazio horretan jakinaraziko da 2 hilabeteko epean ezeztatuko direla indarrean dauden ziurtagiri guztiak.

CA bat amaitzen bada berau iraungitzeagatik edo ezeztatzeagatik, OCSP zerbitzuaren bidez erantzungo zaie ziurtagiriaren egoerari buruzko galderari. CA amaitutakoan, CA horrek jaulkitako ziurtagiriei buruzko OCSParen erantzunak indarrean dagoen Izenperen beste CA batek sinatuko ditu. Izenperen CRLak ez ditu ziurtagiri iraungiak barnean hartzen, Ziurtapen Praktiken Deklarazio honen 4.9.7 CRLak sortzeko maiztasuna atalean adierazten denez.

Izenpek jarduerari uzten badiu, "99991231235959Z" nextUpdate bat izango duen last CRL baten bidez emango da ziurtagiriak ezeztatzearen informazioa, ETSI EN 319 411-1aren 6.3.9 atalaren zehaztapenen arabera.

Jarduerari utziko zaiola jakinaraziko zaie TSPEi, nabigatzaileen fabrikatzaileei eta, oro har, Izenperekin zerbitzua erabiltzeko kontratu-harremana duen edozein entitateri.

Izenpek beharrezko denboraz mantenduko du erregistroari, ezeztatze-egoerari eta log-fitxategiei buruzko informazio oro, Ziurtapen Praktiken Deklarazio honen zehaztapenen arabera. Beste entitate bati eskualdatuz gero, beharrezkoak diren neurriak hartuko dira transferentzia hori beharrezko berme guztiekin egin dadin.

Izenperen Zuzendaritza Nagusiak edo Administrazio Kontseiluak izendatutako pertsonak (edo pertsonak) du (edo dute) jakinarazpen horren erantzukizuna, eta hark erabakiko du horretarako mekanismorik egokiena zein den.

Izenpek bere jarduera bertan behera uzten duela jakinarazi beharko dio gainbegiratze-organismoari, eta jakinaraziko dio zer ziurtagiriren indarraldia amaituko den eta ziurtagiri horien



informazioa emango dio. Komunikazio hori konfiantzako zerbitzuak eskaintzeko eremuan eskumena duen Ministerioaren egoitza elektronikoak jakinarazpenak bidaltzeko duen plataformaren bidez egingo da gutxienez jarduerari utzi baino 2 hilabete lehenago.

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

Izenpek —edo Izenpek eskuordetuta, zerbitzu horiek jasoko dituen entitate 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-entitatea

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



6 Segurtasun teknikoko kontrolak

6.1 Gako-parea sortu eta instalatzea

6.1.1 Gako-parea sortzea

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

.

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

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

ETSI TS 119 312 arauan definitzen diren gako luzera minimoaren eta algoritmoaren gomendioak kontuan izanik sortu beharko dira gako kriptografiko guztiak. Izenpek gakoak sortzen dituen ziurtagiri kualifikatuen kasuetan, gakoak txartelean, token kriptografikoan edo hardware kriptografikoan sortuko dira.

Ziurtagiri kualifikatu hauetan, gakoak sortzen dituen azken erabiltzailea den kasuetan, gakoak honako gailu hauetan sortu ahal izango dira:

- Bezeroen gakoaren edukitzailean (adibidez web-zerbitzarian)
- Izenperen edukitzaile seguruan
- Izenperen telefono mugikorrerako app-aren edukitzailean

6.1.2 Gako pribatua harpidedunari banatzea

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

6.1.3 Gako publikoa ziurtagiriaren jaulkitzaileari banatzea

Gako publikoa, gakoak sortzeko eta zaintzeko gailuaren gainean sortutako gako pribatuarekin batera sortua, ziurtapen-agintaritzari ematen zaio, ziurtapen-eskaera bidalita.

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

- Izenpek sortutako gakoak (txartela, tokena, HSMA): gailu kriptografikoan bertan edo edukitzaile seguruan biltzen direnak.
- Telefono mugikorrean sortutako gakoak: Izenperen app-aren edukitzailean biltegitratzen direnak.

6.1.4 Zerbitzari Seguruko Ziurtagiriko gakoak (SSL): Izenpe Ziurtapen-entitatearen gako publikoa ziurtagirien erabiltzaileei banatzea



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

6.1.5 Gakoen tamaina

Gakoen tamaina kasuen arabera izango da:

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

TSU zerbitzarien gakoen tamaina 4096rekin jaulkitzen da.

6.1.6 Gako publikoa sortzeko eta kalitatea egiaztatzeko parametroak

Izenpek ziurtagiriak sinatzeko erabiltzen duen algoritmo-identifikatzailea (AlgorithmIdentifier) SHA2 da (hash algoritmoa), RSArekin batera (sinadura-algoritmoa). Algoritmo-identifikatzaile hori "Identifier for SHA-2 checksum with RSA encryption for use with Public Key Cryptosystem One defined by RSA Inc." da. Erabilitako padding-eskema emsa-pkcs1-v2.1 da (RFC 3447, 9.2 sekzioaren arabera).

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

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

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

- Larrialdiaren deskribapen zehatza, denbora-esparrua eta abar.
- Larritasuna, esparrua.
- Proposatutako irtenbidea edo irtenbideak.
- Hautatutako irtenbidea zabaltzeko plana. Plan horretan, gutxienez, honako puntu hauek hartuko dira kontuan:
 - Erabiltzaileei jakinaraztea, eraginkorra dela uste den bidea erabilia. Ziurtagirietako eskatzaileei nahiz harpidedunei eta egiaztatzaileei (fidagarriak diren hirugarrenak) jakinaraziko zaie.
 - Sortutako kontingentziaren berri web-orrian ematea.



- Kaltetutako ziurtagiriak ezeztatzea.
- Berritze-estrategia.

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

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

Oinarritzko CA gakoak erabiltzen dira mendeko CAen ziurtagiriak eta ARLak sinatzeko. Mendeko CAen edo CA jaulkitzaileen gakoak soilik erabiltzen dira azken erabiltzaileen ziurtagiriak, CRLak, TSU ziurtagiriak eta OCSP ziurtagiriak sinatzeko.

Azken ziurtagirietarako onartzen diren gako-erabilerak definituta daude www.izenpe.eus webgunean eskura dagoen ziurtagiri-profiletako dokumentuan.

6.2 Gako pribatua babestea

6.2.1 Modulu kriptografikoen estandarrak

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

Izenpek HSMa bat garraiatzean eta biltegitratzean manipulatu ez dela egiaztatzeko protokoloak mantentzen ditu.

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

Gailu horiek gailu-ziurtagiri segurua galduko balute eta horrek sinadura kualifikatua galtzea eragingo balu, Izenpek ziurtagiria ezeztatuko du; indarrean den araudi eta/edo organo ikuskatzaileak zehaztatutakoaren arabera, betiere.

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

Izenpek, nolahi ere, gakoak sortzeko erabiltzen dituen harpidedun-gailuak prestatzearen, biltegitratzearen eta banatzearen gaineko kontrola mantentzen du.

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

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

6.2.3 Gako pribatuaren zaintza

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



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

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

6.2.4 Gako pribatuaren babeskopia

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

Bada Izenpek gakoak zaintzen dizkien harpidedunen modulu kriptografikoetako gakoak berreskuratzeko prozedura bat, eta dagozkien prozeduretan definitutako kasuetan aplika daiteke.

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

6.2.5 Gako pribatua artxibatzea

Izenpek gako pribatuen 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 gutxieneko kopurua. Sinadura sortzeko datuak ez dira bikoizten beste ezein helburutarako.

6.2.6 Gako pribatuaren transferentzia, modulu kriptografikora edo modulu kriptografikotik

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

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

- ✓ Txartela / token kriptografikoa

Gakoak sortzen dituen harpideduna bera denean, harpideduna bera izango da gakoaren zaintzaren arduraduna.

6.2.7 Gako pribatua modulu kriptografikoan biltegitratzea

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

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

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

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



6.2.8 Gako pribatua aktibatze metodoa

Ziurtapen Agintaritzen gako pribatuak FIPS140-2 Level 3 segurtasun-eskakizunak betetzen dituen gailu kriptografiko batek sortu eta zainduko ditu.

Azken entitateko ziurtagirien gako pribatuak aktibatze eta erabiltze mekanismoak zehazten dira ziurtagiri bakoitzaren berariazko politikan.

6.2.9 Gako pribatua desaktibatze metodoa

Administrazio eginkizuna betetzen duen pertsona batek ekin diezaiolke Ziurtapen Agintaritzen gakoa desaktibatzeari, eta horretarako sistema geldituko du. Berririko aktibatze "6.2.8. Gako pribatua aktibatze metodoa" atalean deskribatutakoaren arabera jardungo da.

Azken entitateko ziurtagirien gako pribatuak desaktibatze modua zehazten da ziurtagiri bakoitzaren berariazko politikan.

6.2.10 Gako pribatua deuseztatzeko metodoa

CAren gakoak suntsitzeko prozedura bat dago.

CAren gakoak dituen HSMa kentzen bada, ezarritako prozedura beteko da.

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

6.2.11 Modulu kriptografikoaren kalifikazioa

Dokumentu honen 6.2.1 atalean aditzera ematen denaren arabera.

6.3 Gako-parea kudeatzearen beste alderdi batzuk

6.3.1 Gako publikoa artxibatzea

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

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

Izenpek jaulkitako ziurtagirien erabilera-aldiak dira:

- ✓ 2007ko Oinarrizko CAren ziurtagiria 30 urtez da baliozkoa.
- ✓ 2020ko Oinarrizko CAren ziurtagiria 25 urtez da baliozkoa
- ✓ SSL erroko CAren 2024ko ziurtagiriak 25 urterako balio du
- ✓ EVak jaulkitzen dituen mendeko CAren ziurtagiria 10 urtez da baliozkoa, gainerako mendeko CAk baliozkoak dira oinarrizko CA iraungi arte.
- ✓ Oinarrizko zein mendeko CAen ziurtagirien gako-aldaketa eskari bidez egingo da, eta industriak zehaztutako estandarren arabera.



- ✓ Azken erabiltzaileko ziurtagiriek kasuen araberako iraupena izango dute, kontsultatu berriazko politika. Pertsona fisikoaren eta juridikoaren ziurtagiri guztietan, ziurtagiria berritzeak gakoak sortzea ekarriko du.

6.4 Aktibatzeko datuak

6.4.1 Aktibatzeko datuak sortzea eta instalatzea

Azken entitateko ziurtagiriak jaulkitzen dituzten oinarrizko CAen gakoak zein mendeko CAen gakoak aktibatzeko datuak sortzen dira Ziurtapen Agintaritza horien sorrera-gakoen ekitaldian.

Azken entitateko ziurtagirien gakoak aktibatzeko datuak zehazten dira, hala badagokio, ziurtagiri bakoitzaren berriazko politikan.

6.4.2 Aktibatzeko datuak babestea

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

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

TSaren eta VAren gakoak mendeko CAen gakoaren HSM berean sortzen eta kudeatzen dira. Arau berak aplikatzen dituzte.

Harpidedunek sekretuan mantendu behar dituzte aktibazio-datuak.

6.4.3 Aktibatzeko datuen beste alderdi batzuk

Ikusi ziurtagiri mota bakoitzerako berriazko politika.

6.5 Segurtasun informatikoko kontrolak

6.5.1 Segurtasun informatikorako berriazko eskakizun teknikoak

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

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

Larrialdietarako Plan bat dago.
 - Birusen eta kode kaltegarrien aurka babes-tresnak ezarrita daude.
 - Tresneria etengabe mantentzen da, tresneria une oro erabilgarri eta osorik dagoela ziurtatzearen.
 - Informazio-euskarriak, baliabide nahasgarriak eta tresna zaharkituak ziurtasunez babesteko, ezabatzeko eta deuseztatzeko prozedura dago.



- Datu-trukeak. Datu-truke hauek zifratuta doaz dagokien konfidentziasuna ziurtatzeko.
 - RAen eta erregistroko datu-baseen arteko erregistro-datuen trukea.
 - Aurre-erregistroko datuen trukea.
 - RAen eta CAen arteko komunikazioa.
- Ezeztapenen argitalpen-zerbitzuak behar bezalako funtzionalitateak ditu 24x7 funtzionatzea bermatzeko.
- Sarbide-kontrolak.
 - Erabiltzaile bakarreko IDak erabiliko dira; hartara, egiten dituzten ekintzekin lotuko dira erabiltzaileak eta ekintzen erantzukizuna eskatuko zaie.
 - “Pribilegioak ahalik eta gutxien ematea” printzipioa erabiliko da eskubideak esleitzeko.
 - Lanpostuz aldatzen duten edo erakundea uzten duten erabiltzaileen sarbide-eskubideak berehala ezabatuko dira.
 - Erabiltzaileei esleitutako sarbide-maila hiru hilean behin berrikusiko da.
 - Pribilegio bereziak “kasuak kasu” emango dira eta ezabatu egingo dira hura esleitzea eragin zuen kausa amaitzean.
 - Pasahitzen kalitateari dagozkion zuzentarauak daude.
 - Ziurtagiriak jaulkitzeko ahalmena duten operadore-kontu guztiek faktore bikoitzean oinarritutako sarbide-kontrola dute.

Izenpek segurtasun-politika eta berariazko prozedurak ditu zenbait mailatan segurtasuna bermatzeko.

6.5.2 Segurtasun informatikoaren mailaren ebaluazioa

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

6.6 Bizi-zikloaren kontrol teknikoak

6.6.1 Sistemen garapen-kontrolak

Softwarea produkzio-sistemetan ezartzea kontrolatzen da.

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

- Izenperen politikak aplikazioen eta sistemen garapen segururako arauak hartzen ditu barnean.
- Aldaketak kontrolatzeko prozedura formala existitzen da. Beharrezkoetara mugatzen dira, eta kontrol zorrotzaren mende daude.
- Sistema eragileak aldatzen direnean, Negozioaren Jarraitutasun Planak kritikotzat jotzen dituen negozio-aplikazioak berraztertzen dira.



- Sistema seguruko ingeniartza-printzipioak ezartzen dira.
- Garapen-ingurunea behar bezala babestuta dago.
- Garapen kanporatua ikuskatzen eta kontrolatzen du Izenpek.
- Garapenean segurtasun funtzionaleko probak egiten dira.
- Onarpen-probetako programak ezartzen dira informazio-sistema berrietarako, eguneratzeetarako eta bertsioetarako.
- Proba-datuak hautatzen dira, eta babestuta eta kontrolatuta daude.

6.6.2 Segurtasunaren kudeaketa-kontrolak

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

6.6.3 Bizi-zikloaren segurtasun-kontrolak

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

6.7 Sareko segurtasunaren kontrolak

Sareko segurtasuna maila askotariko zonifikazioaren kontzeptuan oinarritzen da, firewall erredundante ugari erabilia. Sare ez-seguruen bitartez transferitzen den informazio konfidentziala modu zifratuan transferitzen da, SSL/TLS protokoloak erabilia. Barne- eta kanpo-trafikorako IPS sistemak daude.

6.8 Denbora-iturria

Izenpek Armadaren Errege Behategirako konexio baten bidez lortzen du bere sistemen denbora, NTP protokoloari jarraituta. . NTP protokoloaren deskribapena IETF RFC 5905 estandarrean aurki daiteke.

Barne-zerbitzu horretan oinarrituta, denbora zigilatzeke zerbitzua (TSA) eskaintzen du Izenpek, eta zerbitzu hori erabili ahal izango da dokumentu arbitrarioetan denbora-zigiluak sortzeko, betiere IETF RFC 3161 estandarren arabera eta ETSI EN 319 421 estandarren arabera. Informazio gehiago Izenperen Denbora Zigilatzeke Praktiken Deklarazioan.



7 Ziurtagirien profilak eta ezeztatutako ziurtagirien zerrendaren profilak

7.1 Ziurtagiriaren profila

IZENPEK jaulkitako ziurtagiriek honako arau hauei jarraitzen diete:

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

7.1.1 Bertsio-zenbakia

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

7.1.2 Ziurtapenen luzapenak

Ziurtapenen luzapenak profilen dokumentuan adierazten dira, dokumentu hori www.izenpe.com webgunean dago eskuragarri.

7.1.3 Algoritmo-objektuen identifikatzaileak

Ziurtagiria sinatzeko IZENPEK erabiltzen duen algoritmoaren identifikatzailea SHA-256/RSA da, eta identifikatzaile honi dagokio: 1.2.840.113549.1.1.11

7.1.4 Izenen formatuak

Izenen formatuak profilen dokumentuan adierazten dira, dokumentu hori www.izenpe.com webgunean dago eskuragarri. Dokumentu honen 1.3.1 puntuan daude CAen profilak.

7.1.5 Izenen murrizketak

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

7.1.6 Ziurtagiriaren politikaren objektu-identifikatzailea

Ziurtapen Praktiken Deklarazio honetako 1.2. atalean zehaztutakoaren arabera.



7.1.7 “Politika-murrizketak” luzapenaren erabilera

Ez da politika-murrizketarik erabiltzen.

7.1.8 Politika-kalifikatzaileen sintaxia eta semantika

Certificate Policies luzapenak politika-kalifikatzaile hauek ditu:

- **CPS Pointer:** Izenperen Ziurtapen Praktiken Deklaraziorako erakuslea du, <http://www.izenpe.com/cps>
- **User notice:** Hirugarren batek ziurtagiria egiaztatzen duenean, aplikazio edo erabiltzaile batek eskatuta, pantailan bistaritzen den testu-oharra.
- **Policy Identifier:** Ziurtagiriaren OIda adierazten du.

Ziurtagiri guztientzako balio duen User Notice (SSL ziurtagirietarako izan ezik):

USER NOTICE	Ziurtagirian fidatu edo hura erabili aurretik, kontsultatu baldintzak www.izenpe.com -en - Consulte en www.izenpe.com los términos y condiciones antes de utilizar o confiar en el certificado
-------------	---

7.1.9 “certificate policy” luzapenerako tratamendu semantikoa

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

7.2 Ezeztatutako ziurtagirien zerrendaren profila

IZENPEK jaulkitako ziurtagiriek honako arau hauei jarraitzen diete:

- Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 5280), 2008ko maiatzekoa.
- Internet X.509 Public Key Infrastructure Authority Information Access Certificate Revocation List (CRL) Extension (RFC 4325), 2005eko abendukoa.
- Update to DirectoryString Processing in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 4630), 2006ko abuztuko.

RFC 6962 arauan deskribatzen denaren arabera, aurreziurtagiri bat ez da inola ere hartuko RFC 5280 arauan definitutako ezaugarriak dituen ziurtagiritzat.

7.2.1 Bertsio-zenbakia

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



7.2.2 Zerrendako elementuen ezeztatutako ziurtagirien eta luzapenen zerrenda

Erabili diren luzapenak honako hauek dira:

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

7.3 OCSP profila

Izenperen OCSP erantzunak bat datoz RFC 6960 arauarekin (X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP), eta OCSP Responder-ek sinatzen ditu —kontsultatzen ari den ziurtagiria jaulkitzeko erabilitako CAk berak sinatu du horren ziurtagiria—.

7.3.1 Bertsio-zenbakia

3. bertsioa.

7.3.2 OCSPren 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 iraungipena dute
- Izenpek jaulki ez dituen ziurtagirien egoera-eskaeretan REVOKED da erantzuna
- Izenpek jaulkitako ziurtagirien egoera-eskaeretan, eta REVOKED izanez gero, id-pkix-ocsp-extended-revoke luzapena txertatzen da OCSP erantzunean.
- Izenperenak ez diren ziurtagirietan, @Firma-tik lortutako erantzuna itzuliko da.
- Izenpek ez du OCSP Stapling onartzen.



8 Betetzearen ikuskapenak

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

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

8.1 Ikuskapenaren maiztasuna

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

8.2 Ikuskatzailearen kualifikazioa

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

8.3 Ikuskatzailearen eta ikuskatutako enpresaren arteko harremana

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

8.4 Ikuskatu beharreko elementuak

Hauek dira ikuskatu beharreko elementua:

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

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

8.5 Urritasunen ondoriozko erabakiak hartzea

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



8.6 Emaitzen berri ematea

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



9 Beste lege- eta jarduera-gai batzuk

9.1 Tarifak

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

9.1.1 Ziurtagiriak jaulkitzeko edo berritzeko tarifak

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

9.1.2 Ziurtagiriak jasotzeko tarifak

Erabaki gabe.

9.1.3 Ziurtagirien egoerari buruzko informazioa eskuratzeko tarifa

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

9.1.4 Beste zenbait zerbitzutarako tarifak

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

9.1.5 Itzultze-politika

Izenpek ez du itzultze-politkarik.

9.2 Finantza-erantzukizuna

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

9.2.1 Erantzukizun zibileko aseguruia

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

9.2.2 Beste aktibo batzuk

Erabaki gabeak.

9.2.3 Azken entitateentzako aseguruak eta bermeak

Erabaki gabeak.



9.3 Informazioaren konfidentzialtasuna

9.3.1 Informazio konfidentzialaren irismena

Zerbitzuak egiteko, Izenpek eta erregistro-entitateek zenbait informazio bildu eta biltegitatu behar dute, zenbait datu pertsonal ere tarteko direla. Interesatuei beraiei eskatzen zaie informazio hori, haien onarpen esplizituaz. Interesatuaren onarpenik gabe ere jaso daiteke informazioa, datuak babesteko legeriak horretarako baimena ematen duen kasuetan.

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

IZENPEK pribatutasun-politika garatzen du, datu pertsonalak babesteko indarrean dagoen legeriak agintzen duen legez.

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

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

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

9.3.2 Irismenaren barruan ez dagoen informazioa

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

- Jaulkitako ziurtagiriak, edo jaulkitze-bidean direnak.
- Pertsona fisikoa den harpidedun batek Izenpek jaulkitako ziurtagiri batekin duen lotura.
- Ziurtagiriaren harpidedunaren izen-abizenak, baldin eta ziurtagirian harpideduna eta sinatzailea pertsona fisikoa bada, edo sinatzailearenak, baldin eta ziurtagiriaren harpideduna pertsona juridikoa edo administrazio-organoa bada—, baita titularraren



beste edozein inguruabar edo datu pertsonal ere, ziurtagiriaren xedeetarako garrantzizkoa bada.

- Sartzen bada, ziurtagiriaren harpidedunaren helbide elektronikoa, harpideduna pertsona fisikoa den ziurtagirien kasuan, edo sinatzailearena, harpideduna pertsona juridikoa edo administrazio-organoa den ziurtagirien kasuan, edo harpidedunak emandako helbide elektronikoa, gailuetarako ziurtagirien kasuan.
- Ziurtagiriak finkatzen dituen muga eta erabilera ekonomikoak.
- Ziurtagiriaren balio-epaia, baita ziurtagiriaren jaulkitze- eta iraungitze-datak ere.
- Ziurtagiriaren serie-zenbakia.
- Ziurtagiriaren egoera guztiak, baita horietako bakoitzaren hasiera-data ere. Zehazki: sortzeko eta/edo entregatzeko zain, baliozkotua, ezeztatua, etena edo iraungia, baita egoera-aldaketa eragin zuen zergatia ere.
- Ezeztatutako Ziurtagirien Zerrendak (CRLak), baita ezeztatze-egoerei dagozkien gainerako informazioak ere.
- Izenperen Argitalpen Zerbitzuan dagoen informazioa.
- Ziurtapen Praktiken Deklarazioko informazio konfidentzialen atalean ageri ez den gainerako informazio guztia.

9.3.3 Informazio konfidentziala babesteko erantzukizuna

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

Zehazki, ziurtagiriko datuen fidagarritasuna bermatzen duten erregistroak soilik argitaratuko dituzte, baldin eta prozedura judizial batean ziurtapena egiaztatzeko eskatzen badituzte, baita ziurtagiriaren harpidedunaren baimenik gabe ere.

Ziurtagiriak argitaratzean, konfiantzazko zerbitzu elektronikoen alderdi jakin batzuk arautzen dituen 2020ko azaroaren 11ko 6/2020 Legeak eta eIDAS1, eIDAS2 araudiak agintzen duenari jarraituko zaio.

9.4 Datu pertsonalak babestea

Izenpek honako web-gunean argitaratzen du bere tratamendu-jardueren erregistroa, baita datu pertsonalei buruzko gainerako informazioa ere, interesdunek kontsultatu ahal izan dezaten: www.izenpe.eus/datos

9.4.1 Pribatutasun-plana

Izenpek egiten duen datu pertsonalen tratamendua bat dator Europako Parlamentuaren eta Kontseiluaren 2016ko apirilaren 27ko 2016/679 (EB) Erregelamenduan xedatutakoarekin eta Estatuko arlo horretako araudi espezifikoaren arabera aplikatzekoak diren eskakizunekin — 2016/679 ARAUDIA (EB), EUROPAKO PARLAMENTUARENA ETA KONTSEILUARENA, 2016ko



apirilaren 27koa, pertsona fisikoen babesari buruzkoa, datu pertsonalen tratamenduari eta datu horien zirkulazio libreari dagokionez. Araudi horrek 95/46/EE Zuzentaraua (datu pertsonalak babesteari buruzko araudi orokorra) indargabetzen du—.

9.4.2 Pribatu gisa tratatutako informazioa

Izenpek informazio pribatutzat jotzen du konfiantzazko zerbitzuak erabiltzen dituzten pertsona fisikoei buruzko informazio pertsonal oro, betiere ziurtagirietan eta ziurtagirien balio-egoerari buruzko informazio- eta kontsulta-zerbitzuak erabiltzen dituen mekanismoetan sartu behar ez dena.

Nolanahi ere, informazio pribatutzat hartuko da ziurtagiri elektronikoa eskatzeko, berritzeko eta ezeztatzeke prozesuetan bildutako informazio pertsonal oro (hurrengo atalean adierazitako salbuespenarekin), baita konfiantzazko zerbitzuen egilearen esku dauden gako pribatuak eta argi eta garbi informazio pribatutzat identifikatutako informazio oro ere.

Izenpek informazio pribatua babesteko babes egokiak aplikatzen ditu.

9.4.3 Pribatutzat jotzen ez den informazioa

Ez da informazio pribatutzat jotzen ziurtagiri elektronikoei txertatzen zaien informazioa, horien indarraldiari buruzko informazioa, ziurtagirien egoeraren (aktiboa, ezeztatua, iraungia...) hasiera data eta egoera-aldaketa hori eragin zuen arrazoa. Horrenbestez, ziurtagiri elektronikoa, ezeztatutako ziurtagirien zerrendak eta horietako edozein eduki ez dira informazio pribatutzat joko.

9.4.4 Informazio pribatua babesteko erantzukizuna

Izenpek Datu Pertsonalak Babesteari buruzko Araudi Orokorren arabeko segurtasun-neurriak hartzen ditu, ziurtagirien eskatzaileen eta harpidedunen datu pertsonalak eskuratzeari eta tratatzeari dagokionez.

Neurri teknikoak eta antolakuntzakoak ezartzeko, kontuan hartuko dira: teknikaren kostua; aplikazio-kostuak; tratamenduaren izaera, irismena, testuingurua eta helburuak; eta eskubide eta askatasunetarako arriskuak.

9.4.4.1 Datuak babesteko ordezkaria

Izenperen datuak babesteko ordezkariaren datuak www.izenp.eus/datos webgunean argitaratuta daude. Harremanetarako datu horietan helbide elektronikoa bat ere barnean hartzen da, eta interesdunek helbide horretara bidal ditzakete datu pertsonalen tratamenduari eta eskubideen erabilerari buruzko galdera guztiak, Datu Pertsonalak Babesteari buruzko Araudi Orokorren 38.4 artikuluekin bat etorritik.

9.4.4.2 Tratamendu-jardueren erregistroa

Izenpek bere erantzukizunpean egiten dituen tratamendu-jardueren erregistro bat du, eta jarduera horien artean dago erakundeak konfiantzazko zerbitzuen egile gisa egiten duen



jarduerari dagokion “identifikazio-baliabideen kudeaketa”. Erregistro horretan honako informazio hau hartzen da barnean, identifikatutako tratamendu bakoitzerako:

- a) Xedea
- b) Entitate arduraduna
- c) Datu pertsonalen kategoriak
- d) Datuak nork ematen dituen
- e) Nor dagoen datu pertsonalen eraginpean
- f) Nor diren tratamenduaren arduradunak
- g) Datuen komunikazioak
- h) Datuen nazioarteko transferentzia
- i) Ezabatzeko epea
- j) Segurtasun-neurriak

Tratamendu-jardueren erregistro-dokumentua kontsulta daiteke www.izenpe.eus/datos webgunean.

9.4.4.3 Interesdunen eskubideak

Interesdunek datuak eskuratzeko, zuzentzeko, ezabatzeko, tratamendua mugatzeko, aurkakotzeko eta eramateko eskubidea baliatu ahal izango dute, datu pertsonalak babesteari buruzko araudi orokorraren 15. artikulutik 22. artikulura bitartean ezarritakoaren arabera. Horretarako, honela balia daitezke eskubideak:

- Posta bidez: eskaerari NANaren edo AIZren kopia bat gehituz.
- Modu elektronikoa, eskaera pertsona fisikoaren ziurtagiri kualifikatu bidez sinatuta.

9.4.4.4 Agintaritzekin lankidetzan jardutea

Izenpe lankidetzan arituko da Datuak Babesteko Euskal Agintaritzarekin, hala eskatzen zaionean.

9.4.4.5 Segurtasun-uraketek jakinarazpena

Izenpek ahalik eta lasterren jakinaraziko dio Datuak Babesteko Espainiako Agentziari datu pertsonalen arloko edozein segurtasun-uraketa, betiere, arduradunak horren berri izan eta hurrengo 72 orduen barruan, baldin eta uraketa horren eraginpean dauden pertsona fisikoen askatasunak arriskuan jar baditzake.

Segurtasun-uraketak interesdunen eskubideak eta askatasunak arriskuan jar baditzake, Datuak Babesteko Espainiako Agentziari zuzendutako jakinarazpena osatuko da interesdunei zuzendutako jakinarazpen batekin, uraketaren ondorioez babesteko neurriak hartu ahal izan daitezen.

9.4.5 Informazio pribatua erabiltzeko oharra eta adostasuna

Ziurtagirien bizi-zikloarekin lotzen diren prozesuetan (adibidez ziurtagiriak eskatzean, nortasuna egiaztatzean, ziurtagiriak berritzean edo ezeztatzean) pertsona fisikoen informazio pribatua lortzeko, pertsona horien adostasun argia eduki beharko da, hau



da, interesdunaren adierazpen baten bidez edo baiezko ekintza argi baten bidez adierazitako adostasuna.

9.4.6 Prozesu judizialaren edo administratiboaren arabera zabalkundea

Izenpek ez ditu datu pertsonalak argitara emango, administrazio-agintaritzek edo agintaritzak judizialek eskatzen dutenean salbu.

9.4.7 Informazioa zabaltzeko beste egoera batzuk

Erabaki gabeak.

9.5 Jabetza intelektualeko eskubideak

9.5.1 Ziurtagirien jabetza

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

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

Arau berberak aplikatu behar zaizkio ziurtagiriak ezeztatzeko informazio-sistemari.

9.5.2 Ziurtapen Praktiken jabetza

Izenpe da Ziurtapen Praktiken Deklarazio honen jabea.

9.5.3 Izenen gaineko informazioaren jabetza

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

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

9.5.4 Gakoaren eta horiei dagokien materialaren jabetza

Ziurtagirien harpidedunak dira gako-pareen jabeak.

9.6 Betebeharrak eta bermeak

Izenpek, ziurtagiriak ziurtapen-praktiken deklarazio honen arabera jaulkitzen dituen ziurtapen-entitatea den aldetik, bere gain hartzen ditu betebeharrak hauek:



9.6.1 CAren betebeharrak

9.6.1.1 Zerbitzua egiteko betebeharrak

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

- Zerbitzuak jaso dituen pertsonaren sinadura sortzeko datuak ez kopiatzea.
- Jaukitako ziurtagiriak adieraziko dituen eta ziurtagiri horiek indarrean dauden edo indarraldia eten edo iraungi den adieraziko duen sistema bat mantentzea.
- Ziurtagiri kualifikatuei eta une bakoitzean indarrean dauden ziurtapen-jardunbideen adierazpenei buruzko informazio eta dokumentazio guztia erregistratuta edukitzea, edozein bide segururen bidez, gutxienez 15 urtez, iraungitzen diren unetik zenbatzen hasita.
- Sinatzaileak sinadura sortzeko datuak dituela ziurtatzea –ziurtagirian jasotzen diren egiaztatzeari dagozkion datuak–.
- Sinadura sortzeko eta egiaztatzeko datuen osagarritasuna bermatzea, betiere biak ziurtapen-zerbitzuen emaileak sortu baditu.
- Segurtasuneko araudia eta estandarrak betetzea (datu pertsonalak babesteari buruzko araudi orokorra, ISO, ETSI eta Izenperen segurtasun-politika).
- Gordetzeko zerbitzuaren hornitzaileei segurtasuneko araudia eta estandarrak bete ditzaten eskatzea (datu pertsonalak babesteari buruzko araudi orokorra, ISO, ETSI, CABForum eta Izenperen Hornitzaileen segurtasun-politika).

9.6.1.2 Jardun fidagarriko betebeharrak

Izenpek honako hau bermatzen du:

- Ziurtagirian agertzen den identitatea ziurtagirian agertzen den gako publikoari dagokiola, era unibokoan.
- Zerbitzua bizkor eta modu seguruan eskaintzea. Bereziki, ziurtagirien baliozkotasuna kontsultatzeko zerbitzu bizkorra eta segurua erabiltzeko aukera ematen du, eta ziurtagiriak modu seguruan eta berehala iraungiko badira, horren berri emango duela bermatzen du, Ziurtapen Praktiken Deklarazio honek aurreikusten duenarekin bat etorritik. Zerbitzua eguneko 24 orduetan erabil daiteke, asteko 7 egunetan.
- Sinadura elektronikoen arloan indarrean dagoen legeriak finkatzen dituen eskakizun teknikoak eta langileei buruzkoak betetzea:
 1. Ziurtapen-zerbitzuak emateko beharrezko fidagarritasuna frogatzea.
 2. Ziurtagiri bat jaulki edo bere indarraldia amaitu den eguna eta ordua zehaztasunez adierazi ahal izan dadin bermatzea.
 3. Eskaintzen diren ziurtapen-zerbitzuak egiteko behar adinako kualifikazioa, ezagutzak eta esperientzia duten langileak erabiltzea, baita sinadura elektronikoen esparruko segurtasuneko eta kudeaketako prozedura egokiak ere.



4. Erabiltzen diren sistemak eta produktuak fidagarriak izatea, aldaketa orenen aurka babestuta daudenak eta jasaten dituzten ziurtatze-prozesuen segurtasun tekniko eta —hala badagokio— kriptografikoa bermatzen dutenak, betiere Segurtasun Politikari jarraituz.
 5. Ziurtagirien faltsifikazioaren aurkako neurriak hartzea eta konfidentzialtasuna bermatzea sinadura (gako pribatua) sortzeko datuen eratze-prozesuan, 6. atalak dioenaren arabera. Gainera, sinatzaileari prozedura seguru baten bidez ematea.
 6. Sistema fidagarriak erabiltzea ziurtagiri kualifikatuak biltegitzeko. Sistema horiek ziurtagiriak kautotzeko aukera eman behar dute, eta baimenik gabeko pertsonak datuak aldatu ahal izatea saihestu beharko dute. Sinatzaileak aditzera eman dituen pertsonak eta kasu jakin batzuetan, soilik, sartu ahal izango dira datu horietara, eta hala bermatu behar du sistema horrek. Gainera, segurtasun-baldintzetan eragina izan dezakeen edozein aldaketa antzeman beharko dute sistema horiek.
- Segurtasunaren kudeaketa egokia, Informazioaren Segurtasuna Kudeatzeko Sistema ezartzeari esker, betiere ISO/IEC 27001 arauak ezarritako printzipioen arabera. Honako neurri hauek, besteak beste, hartu dira aintzat:
1. Segurtasuna aldian behin egiaztatzea, ezarritako estandarrekiko adostasuna ziurtatzearen.
 2. Segurtasun-gertakarien kudeaketa osoa gauzatzea, gertakari horiek hauteman, ebatzi eta optimizatu direla bermatzearen.
 3. Segurtasunaren arloan interes berezia duten taldeekin harreman egokiak izatea, hala nola adituekin, segurtasun-foroekin, eta informazioaren segurtasunaren arloko elkargo profesionalekin.
 4. Sistemen mantentze-lana eta bilakaera behar bezala planifikatzea, erabiltzaileen eta bezeroen iguripenak berme osoz beteko dituen zerbitzua eta etekin egokia ziurtatzearen.

9.6.1.3 Identifikazio-betebeharrak

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

9.6.1.4 Erabiltzaileei informatzeko betebeharrak

- Harpidedunari ziurtagiria jaulki eta eman aurretik, eta www.izenpe.com webgunean eskuragarri dagoen “Erabiltzeko terminoak eta baldintzak eta Gako Publikoko Azpiegitura Dibulgatzeko Akordioa (PKI-PDS)” dokumentuaren aipamenaren bidez, alderdi hauen berri ematen dio Izenpek harpidedunari: ziurtagiria erabiltzeko bete behar diren baldintzen berri, prezioaren berri —finkatuta badago—, erabilera-mugen berri eta Ziurtapen Praktiken Deklarazio honen 2.1.1.6. atalean dauden tresna juridiko lotesleen berri.



- 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.
- Bi hilabete lehenago jakinaraziko die Izenpek sinatzaileei ziurtapen-zerbitzuak egiteari utzi egingo diola, eta, hala badagokio, ziurtagirien kudeaketa eskualdatzen zaion emailearen ezaugarrien berri emango die. Dokumentu honek aurreikusitakoaren arabera egin behar dira sinatzaileekiko komunikazioak.
- Izenpek badu jarduera eteteko amaiera-plan bat, eta, bertan zehazten da etete hori zein baldintzatan egingo litzatekeen.

9.6.1.5 Egiatzapen-programen inguruko betebeharrak

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

9.6.1.6 Ziurtapen-zerbitzuaren arautze juridikoaren inguruko betebeharrak

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

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

- Ziurtapen Praktiken Deklarazio honetako 2.1.4., 2.1.5., 2.1.6., 2.2., 2.3. eta 2.4. atalek diotena betetzeko aginduak.
- Zein Ziurtapen Praktiken Deklarazio den aplikagarri adierazi behar du, eta, hala badagokio, zehaztu egin behar du ziurtagiriak salgai daudela eta sinadura sortzeko nahiz mezuak deszifratzeko gailu segurua erabili behar dela.
- Gako pribatuak jaulkitzeko, ezeztatzeko eta, hala badagokio, berreskuratzeko bete beharreko klausulak.
- Ziurtagirian dagoen informazioa zuzena dela adierazi behar du, harpidedunak kontrakoa jakinarazten ez badu behintzat.
- Sinadura sortzeko gailu segurua hornitzeko erabilitako informazioa biltegitratzeko baimena, betiere harpideduna erregistratzeko, gailu kriptografikoa hornitzeko eta informazio hori beste batzuei uzteko, baldin eta Izenperen eragiketarak baliozko ziurtagiriak ezeztatu gabe amaitzen badira.
- Ziurtagiria erabiltzeko mugak, 1.3.2. atalekoak barne.
- Ziurtagiriak nola baliozkotu jakiteko informazioa, ziurtagiriaren egoera egiaztatzea barne dela, baita ziurtagirian dezenteko konfiantza izateko baldintzei buruzkoa ere.
- Aplikagarri diren erantzukizun-mugak, Izenpek bere gain hartzen dituen edo baztertzen dituen erantzukizunak barne.



- Ziurtagiri-eskaeren informazioa zenbat denboraz gordetzen den.
- Ikuskaritza-erregistroak zenbat denboraz gordetzen diren.
- Auziak konpontzeko aplikagarri diren prozedurak.
- Aplikagarri den legea eta eskumena duen jurisdikzioa.
- Izenpe entitate publikoren baten edo batzuen ziurtapen-politikekiko bateragarri aitortu duten, eta, hala badagokio, zein sistemaren arabera.
- Izenperen ondare-erantzukizuna bermatzeko era.

9.6.2 Erregistro-entitatearen betebeharrak

Izenpek erregistro-entitateko funtzioak hirugarren batekin eskuordetzea baimendu aurretik, hirugarren horrek betebeharrak hartu beharko ditu formaltasunez bere gain dagokion lege-tresnaren bidez:

- Eskatzailearen, harpidedunaren eta sinatzaileen nortasuna eta bestelako inguruabar pertsonalak egiaztatzea, ziurtagirietan jasotakoak edo ziurtagirien xedeetarako garrantzitsuak direnak, prozedura hauen arabera.
- Kudeatzen dituen ziurtagirien jaulkipenari, berritzeari, ezeztatzeari edo berraktibatzeari buruzko dokumentazio eta informazio guztia gordetzea.
- Izenperi garaiz ematea ziurtagiriak azkar eta modu fidagarrian ezeztatze eskaeren berri.
- Izenperi artxiiboak erabiltzen uztea, baita jardueretarako erabiltzen diren prozeduren eta horretarako behar den informazioaren mantentze-lanen ikuskapena egiten ere.
- Izenperi ematea ziurtagiriak jaulkitzeko, berritzeko edo berraktibatze eskaeren berri, baita hark jaulkitzen dituen ziurtagiriei buruzko beste zeinahi alderdiren berri ere.
- Garaiz begiratzea ziurtagirien iraunaldian eragina izan dezaketen ezeztatze zergatiak.
- Ziurtagiriak jaulkitzeko, berritzeko, ezeztatze eta berraktibatze eskaeren ezarritako prozedurak eta gai horretaz indarrean dagoen legeriak agindutakoa betetzea.
- Izenperen Hornitzaileen Segurtasun Politika betetzea.

9.6.3 Titularren betebeharrak

Honako betebeharrak hartu beharko ditu ziurtagiri-eskatzaileak:

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



- Gehienez hiru hilabeteko epean ordaintzea ziurtagiri motari dagokion zenbatekoa, Izenpek adierazitako baldintzetan.

Honako betebeharrak dituzte harpidedunak:

- Informazio osoa eta egokia ematea Izenperi, Ziurtapen Praktiken Deklarazioko eskakizunen arabera, erregistro-prozedurari dagokionez batez ere.
- Ziurtagirietan jarri beharreko informazioaren egiazkotasuna, osotasuna eta gaurkotasuna bermatzea.
- Ziurtagiriak erabiltzeko baldintzak jakitea eta onartzea, baita haiei egiten zaizkien aldaketak ere.
- Ziurtagiriren bat jaulki eta eman aurretik, horretarako onarpena ematea.
- Ziurtagiriaren euskarriak ongi erabili eta gordeko direla bermatzea.
- Ziurtagiria egoki erabiltzea, eta, zehazki, ziurtagiriaren erabilera-mugak aintzat hartzea.
- Arretaz zainduko du gako pribatua, baimendu gabeko erabilerak saihestearren, Ziurtapen Praktiken Deklarazioko 6.1, 6.2 eta 6.4 atalek agintzen dutenaren arabera.
- Izenperi eta harpidedunaren ustez konfiantza izan dezakeen edozein pertsonari honakoak jakinaraziko dio, atzerapenik gabe (atzeratzeko arrazoirik egon ezean):
 - Gako pribatua galdu, norbaitek ostu edo arriskuan jarri izana.
 - Gako pribatuaren kontrola galdu izana, aktibatze-datuak (gailu kriptografikoaren PIN kodea, adibidez) arriskuan jartzeagatik edo beste edozein arrazoiengatik.
 - Ziurtagiriaren edukian dauden okerrak edo izandako aldaketak (harpidedunak dakizkienak edo jakin litzakeenak). Aldaketak ziurtagiria ezetzatzea badakar, horretarako eskaera egin behar du harpidedunak.
- Gako pribatua erabiltzeari utziko dio ziurtagiriaren balio-epea amaitu ondoren.
- Gakoen edukitzaileri jakinaraztea zein betebeharrak dagozkien.
- Ziurtagiri-zerbitzuen ezartze teknikoak ez kontrolatzea, manipulatuzea edo atzeranzko ingeniarietako ekintzarik ez egitea, aurrez Ziurtapen Entitatearen idatzizko baimenik eduki gabe.
- Ziurtagiri-zerbitzuen segurtasuna arriskuan nahita ez jartzea.
- Ziurtagirietako gako publikoei dagozkien gako pribatuak ez erabiltzea inongo ziurtagiri izenpetzeko, ziurtapen-entitatea balitz bezala.

9.6.4 Konfiantza duten aldeko betebeharrak

Ziurtagiriaren erabiltzaile egiaztatzaileak honako betebeharrak dituzte:

- Eman nahi zaion erabilerarako ziurtagiria egokia den ala ez jakiteko, informazioa iturri independenteetatik jasotzea.
- Ziurtagiriak erabiltzeko baldintzak zein diren jakitea, Ziurtapen Praktiken Deklarazioak eta egiaztatzailearen eta Izenperen arteko ziurtapen-zerbitzuak egiteko kontratuak aurreikusten dutenaren arabera.



- Emandako ziurtagirien baliozkotasuna edo ezeztapena egiaztatzea, eta, horretarako, ziurtagirien egoerari buruzko informazioa erabiltzea.
- Ziurtagirien hierarkiako ziurtagiri guztiak egiaztatzea, sinadura digitalean edo hierarkiako ziurtagiriren batean konfiantza jarri baino lehen.
- Kontuan izatea ziurtagiria erabiltzeko dauden mugak, nonahi daudelarik ere: ziurtagirian bertan nahiz egiaztatzailearen kontratuan.
- Kontuan izatea kontratuan edo beste nonbait finkatutako badaezpadako neurri guztiak, haren izaera juridikoa edozein delarik ere.
- Ziurtagiriari buruzko gertaera edo egoera irregular guztiak jakinaraztea, ziurtagiria ezeztatzeko arrazoia izan daitezkeenak.
- Ziurtagiri-zerbitzuen ezartze tekniko ez kontrolatzea, manipulatzeko edo atzeranzko ingeniarietako ekintzarik ez egitea, aurrez Izenperen idatzizko baimenik gabe.
- Ziurtagiri-zerbitzuen segurtasuna arriskuan nahita ez jartzea.

9.6.5 Beste parte-hartzaile batzuen betebeharrak

Izenpek, Denbora Zigilatze Agintaritzaren denaldetik egiten duen zerbitzuan, denbora-erreferentzia aldatzeko ardura du, betiere Armadako Errege Institutu eta Behategiko Ordu Atalak emandakoari dagokionez —eskaera egiten den unean sartzen du denbora-erreferentzia denbora-zigilu elektronikoetan—. Nolanahi ere, ez du zerbitzua erabiltzen duten erakundeek bidalitako datu elektronikoaren egiazkotasunaren eta edukien gaineko ardurarik, horiek jaulkitako denbora-zigilu elektronikoaren xede baitira.

9.7 Bermeei uko egitea

Erabaki gabe.

9.8 Erantzukizunen muga

9.8.1 Ziurtagiri-agintaritzaren erantzukizunak

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

- Izenpe ez da ziurtagirietako informazioek eragindako kalteen erantzule izango, betiere, haien edukiak Ziurtagiri Praktiken Deklarazioa betetzen badu.
- Izenpe ez da ziurtagirien eraginkortasuna agortzearen erantzule izango, betiere, Ziurtagiri Praktiken Deklarazioan aurreikusitako argitalpen-betebeharrak betetzen baditu.
- Izenpe ez da sor daitezkeen kalte zuzen edo zeharkako, berezi, intzidentziako eta emergenteen erantzule izango, ezta eskuratu gabeko irabazien, datu-galeren eta zigor-



kalteen erantzule ere —aurreikusteko modukoak izan edo ez—, baldin eta horiek ziurtagirien, sinadura digitalen edo Ziurtapen Praktiken Deklarazioan eskaintzen edo aurreikusten den bestelako edozein transakzioen edo zerbitzuren erabilera, entrega, baimen, funtzionamendu edo funtzionamendu ezarekin lotuta badaude eta behar ez bezalako erabilerak eragin baditu.

- Izenpe ez da ziurtagirian ageri diren datuen zehaztapen-ezagatik harpidedunari edo fede oneko hirugarren pertsoneri eragindako kalte eta galeren erantzule izango, baldin eta datu horiek dokumentu publiko baten bidez (notariotzakoa, judiziala edo administratiboa) ziurtatu badira, Erregistro Entitateak eman duen dokumentu bidez denean izan ezik.
- Izenpe ez da ziurtagiriez fidatzen diren harpidedunek edo hirugarren pertsonen dituzten betebeharrak ez betetzeagatik harpidedunari edo fede oneko hirugarren pertsoneri eragindako kalteen erantzule izango.

Ziurtagirien indarraldiari buruzko edota ziurtagirien indarraldia iraungitzeari buruzko kontsultaz-zerbitzuan ez sartzek edo berandu sartzek norbaiti kalteak edo galerak eragiten badizkio bere lanean, Izenpek kalte edo galera horiez erantzungo du.

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

9.8.2 Erregistro-agintaritzaren erantzukizunak

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

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

9.8.3 Harpidedunen betebeharrak

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

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

Ziurtagiriak onartzearekin batera, erantzukizun hau hartzen du bere gain harpidedunak: kalte guztietatik salbu uztekoa eta, hala badagokio, kalte-ordainak ordaintzekoa Izenperi, erregistro-entitateei, eta entitate erabiltzaileei kalteak, galerak, zorrak, gastu prozesalak edo zeinahi bestelakoak eragiten dituzten ekintzengatik edo ez-egiteengatik, barne direla Izenperi,



erregistro-entitateei, edo entitate erabiltzaileei ziurtagiriak erabiltzeagatik edo argitaratzeagatik dagozkien ordainsariak. Honako arrazoi hauek eragin dezakete aipatutako erantzukizuna:

- Ziurtapen, entitatearekin lotzen duen tresna juridikoaren aginduak ez betetzeak.
- Baimendu gabeko jendearekiko komunikazio elektronikoetan ziurtagiri digitalak erabiltzeak.
- Harpidedunak datuak faltsutzeak edo akats faktikoak egiteak,
- Zabarkeriagatik edo Izenpe entitate publiko erabiltzaileak edo harpidedunaren ziurtagirian konfiantza eduki dezaketen hirugarrenak engainatzeko asmoz ziurtagirietan funtsezko datuak ez jartzeak.
- Gako pribatuak gordetzeko eta horiek ez galtzeko, inork ez jakiteko, ez aldatzeko edo baimenik gabe ez erabiltzeko betebeharra ez betetzeak.

Ildo horretan, Izenpe ez da izango harpidedunaren berezko betekizun hauek ez betetzeak harpidedunari edo hirugarren pertsoneri fede onez eragindako kalteen erantzule:

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

9.8.4 Ziurtagirietan konfiantza duten hirugarrenen erantzukizunak

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

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

- Egiaztatzea eta kontuan hartzea ziurtagirian agertzen diren murrizketak, haren balizko erabilerei dagokienez eta harekin egin daitezkeen transakzioen banakako zenbatekoari dagokienez.
- Ziurtagiriaren baliozkotasuna egiaztatzea.



- Trusted Service List (TSL) zerrendan kualifikatutako ziurtagiriaren identifikatzaile digitala egiaztatzea.

9.9 Kalte-ordainak

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

9.10 Baliozkotze-aldia

9.10.1 Epea

ZPD argitaratzen den unean sartzen da indarrean.

9.10.2 Amaiera

Gaur egungo ZPDa dokumentuaren beste bertsio bat argitaratzen den unean indargabetuko da. Bertsio berriak oso-osorik ordeztuko du aurreko dokumentua.

9.10.3 Amaieraren ondorioak

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

9.11 Banako jakinarazpenak eta komunikazioa parte-hartzaileekin

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

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

9.12 Dokumentu honen aldaketak

9.12.1 Aldaketetarako prozedura

Dokumentu honetan egiten diren aldaketak Izenperen Segurtasun Batzordeak onartuko ditu. Aldaketa horiek Ziurtapen Praktiken Deklarazioaren dokumentuan jasoko dira. Izenpek bermatzen ditu dokumentu horren mantentze-lanak.

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

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

- Aldaketa teknikoki, legalki eta komertzialki justifikatuko da, eta Izenperen zuzendaritzak abala eman beharko du.



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

9.12.2 Jakinarazteko aldia eta mekanismoa

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

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

- Akats tipografikoak zuzentzea dokumentuan.
- Harremanetako informazioa aldatzea.

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

- Aldaketak zehaztapenetan edo zerbitzu-baldintzetan.
- URLak aldatzea.

9.12.3 OIDA zer inguruabarretan aldatu behar den

Dokumentu honetan deskribatutako prozeduretakoren bat aldatzen den inguruabarretan aldatu beharko da OIDA.

9.13 Erreklamazioak eta auzien ebazpena

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

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

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

9.14 Araudi aplikagarria

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

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



- 6/2020 Legea, azaroaren 11koa, konfiantzako zerbitzu elektronikoen alderdi jakin batzuk arautzen dituena.
- 1999/93/EE Zuzentaraua indargabetzen duen identifikazio elektronikoari eta barnermerkatuko transakzio elektronikoetarako konfiantzako zerbitzuei buruzko 910/2014 Araudia.
- 2024/1183 Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2024ko apirilaren 11koa, zeinaren bidez aldatzen baita 910/2014 Erregelamendua identitate digitalaren Europako esparrua ezartzeari dagokionez
- Administrazio Publikoen Administrazio Prozedura Erkideari buruzko 39/2015 Legea.
- Sektore Publikoaren Erregimen Juridikoari buruzko 40-2015 Legea.
- 3/2018 Lege Organikoa, abenduaren 5koa, datu pertsonalak babesteari eta Eskubide Digitalak Bermatzeari buruzkoa.
- Pertsona fisikoen babesari buruzko 2016/679 Araudia (EB), datu pertsonalen tratamenduari eta datu horien zirkulazio libreari dagokionez. Araudi horrek 95/46/EE Zuzentaraua (datuen babeserako araudi orokorra) indargabetzen du.

Horrez gain, Izenpek aurreikusten dituen konfiantzako zerbitzuetan estandar hauek betetzen dira:

- ETSI EN 319 401: General Policy Requirements for Trust Service Providers
- Konfiantzako eta Ziurtapen Elektronikoko Zerbitzuen Praktiken Deklarazio Orokorra, 5.7. bertsioa
- 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

9.15 Aplikatzekoa den araudia betetzea

Jurisdikzio eskuduna une bakoitzean legeria prozesal espainiarrak agintzen duena izango da. Edonola ere, Izenpek jakinarazi du 9.14. atalean adierazten diren araudiak betetzen dituela.



9.16 Askotariko estipulazioak

9.16.1 Akordio osoa

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

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

9.16.2 Esleipena

Izenpe ez da zerbitzurik ezaren edo zerbitzuko anomalien erantzule izango, ezta zuzenean edo zeharka gerta daitezkeen kalte-galeren erantzule ere, baldin eta hutsegitea edo hondamendia ezinbesteko arrazoen, atentatu terroristaren, sabotajeen edo greba basatien ondoriozkoa bada; hori guztia, zerbitzua ahalik eta lasterren konpontzeko eta/edo berrabiarazteko beharrezkoak diren jarduketak egitea alde batera utzi gabe.

9.16.3 Bereizgarritasuna

Erabaki gabe.

9.16.4 Betetzea

Erabaki gabe.

9.16.5 Ezinbestea

Erabaki gabe.

9.16.6 Beste estipulazio batzuk

Izenpek, konfiantzazko zerbitzuen egilea den heinean, zerbitzuak egingo dizkie hala eskatzen duten interesdun guztiei, Ziurtapen Praktiken Deklarazio honetan aurreikusitako baldintzetan eta eskabidearen xedeari aplikatu dakizkiokeen politika, praktika eta emisio-legeetan aurreikusitako baldintzetan.

Izenperen konfiantzazko zerbitzuek —behar bezala erabili eta konbinatuta— aukera emango diete erabiltzaileei, harpidedunei eta titularrei, besteak beste, aldean arteko identifikaziorako, autentifikaziorako, gaitzespenik ezarako eta konfidentzialtasunerako beharrezkoak diren segurtasun-neurriei buruzko informazioa trukatzeko.

Izenpek bere ziurtapen-zerbitzuak kudeatzen ditu eta SSL ziurtagiriak jaulkitzen ditu, “konfiantzazko ziurtagiriak jaulkitzeko eta kudeatzeko oinarritzko betekizunen” azken bertsioaren arabera, hau da, CA/Browser Forum erakundeak ezarritako eskakizunen arabera (<https://cabforum.org/baseline-requirements-documents/> helbidean kontsulta daitezke), eta CA/Browser Forum erakundeak “balidazio hedatuko ziurtagiriak egiteko eta kudeatzeko gidan”



definitutako betekizunen azken bertsioaren arabera (<https://cabforum.org/extended-validation/> helbidean kontsulta daitezke).

Izenpek bere ziurtapen-politikak eta -praktikak berrikusiko ditu, betekizun horien arabera izan daitezke. Dokumentu honen eta "Emandako Balidazio Ziurtagiriak emateko eta kudeatzeko Gidaren" artean inkoherentziarik badago, gidan bertan ezarritako jarraibideak dokumentu honen gainetik daude.

Izenpek hirugarren batzuei uzten die jaulkitzen dituen ziurtagiri mota guztiak egiaztatzen eta probatzen. Horretarako, zenbait proba-ziurtagiri eskuragarri du www.izenpe.eus webgunean.



10 I. ERANSKINA. CA-EN ZIURTAGIRIEN PROFILAK

- CN = Izenpe.com
 - CA, Herritar / Entitate kualifikatuak
 - CA, Herritar / Entitate kualifikatu gabeak
 - CA, Herri Administrazio kualifikatu gabeak
 - CA, Herri Administrazio kualifikatuak
 - CA, SSL EV
 - CA SSL EV 2018
- CN = ROOT CA QC IZENPE
 - CN= SUBCA QC IZENPE – TSA
 - CN= SUBCA QC IZENPE - ADMINISTRAZIO PUBLIKOA-ADMINISTRACION PUBLICA
 - CN= SUBCA QC IZENPE - HERRITARRAK ETA ENPRESA-CIUDADANIA Y EMPRESA
- CN= ROOT CA NQC IZENPE
 - CN= CA NQC IZENPE - PERTSONA FISIKOA-PERSONA FISICA
 - CN= CA NQC IZENPE - GAILUA-DISPOSITIVO
 - CN= CA NQC IZENPE - TEKNIKOA-TECNICA
 - CN= CA NQC IZENPE - SSL EZ PUBLIKOA-SSL NO PUBLICO
- CN = Izenpe.com (barneko SSL)

10.1 OINARRIZKO ZIURTAPEN-AGINTARITZAK

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

CN=Izenpe.com	
Esparrua/luzapena	Edukia
version	3. bertsioa
serialNumber	00b0b75a16485fbfe1cbf58bd719e67d
signature	sha256WithRSAEncryption
issuer	
CN	Izenpe.com
O	IZENPE SA
C	ES
validity	30 urte
subject	
CN	Izenpe.com
O	IZENPE SA
C	ES
subjectPublicKeyInfo	RSA 4096 bit
extensions	
subjectAltName	
rfc822Name	info@izenpe.com
directoryName	
STREET	Mediterraneo Etorbidea 14 - 01010 Gasteiz



O	IZENPE SA - IFK A01337260- RMerc. Gasteiz T1055 F62 S8
subjectKeyIdentifier	1d1c650ea8f2257bb491cfe4b1b1e6bd55746c05
keyUsage	Ziurtagirien sinadura, CRL sinadura konexiorik gabe, Ziurtagiriak ezeztatzeke zerrendaren sinadura (CRL) (06)

CN = ROOT CA QC IZENPE	
Esparrua/luzapena	Edukia
version	3. bertsioa
serialNumber	Ausazko zenbakia
signature	sha256WithRSAEncryption edo sha512
issuer	Subject eremuaren berdina
validity	25 urte
subject	
CN	ROOT CA QC IZENPE
O	IZENPE SA
C	ES
subjectPublicKeyInfo	RSA 4096 bit
extensions	
subjectKeyIdentifier	a96835c280b1a5d4ba522115171bd89be3868697
oinarrizko mugaketak	Gai mota = Ziurtapen-entitatea (CA) Ibilbidearen luzeraren murrizketa=1
keyUsage	KeyCertSign, cRLSign

CN= ROOT CA NQC IZENPE	
Esparrua/luzapena	Edukia
version	3. bertsioa
serialNumber	Ausazko zenbakia
signature	sha256WithRSAEncryption eta/edo sha512.
issuer	Subject eremuaren berdina
validity	25 urte
subject	
CN	ROOT CA NQC IZENPE
O	IZENPE SA
C	ES
subjectPublicKeyInfo	RSA 4096 bit
extensions	
subjectKeyIdentifier	705c7765e8bd5648b249cd1ccf929550b76ccce6
oinarrizko mugaketak	Gai mota = Ziurtapen-entitatea (CA) Ibilbidearen luzeraren murrizketa=1
keyUsage	KeyCertSign, cRLSign



CN=izenpe.com	
Esparrua/luzapena	Edukia
version	3. bertsioa
serialNumber	
signature	
issuer	Subject eremuaren berdina
validity	10 urte
subject	
CN	izenpe.com
O	IZENPE SA
C	ES
subjectPublicKeyInfo	RSA 4096 bit
subjectKeyIdentifier	eca335fb7005e0f7ffd5a9aa98989b17f4906113
keyUsage	Ziurtagirien sinadura, CRL sinadura konexiorik gabe, Ziurtagiriak ezeztatzeko zerrendaren sinadura (CRL) (06)

10.2 MENDEKO ZIURTAPEN AGINTARITZAK

10.2.1 subCA CN=izenpe.com

- CA, Herritar / Entitate kualifikatuak
- CA, Herritar / Entitate kualifikatu gabeak
- CA, Herri Administrazio kualifikatuak
- CA, Herri Administrazio kualifikatu gabeak
- CA, SSL EV
- CA SSL EV 2018

Herritarra eta entitateak (4)	
version	3. bertsioa
serialNumber	2145c8d9b105500e4cbea542553af2c3
signature	sha256WithRSAEncryption
issuer	CA jaulkitzailearen ziurtagiriaren subject eremuaren berdina
CN	izenpe.com
O	IZENPE SA
C	ES
validity	2037ko abenduaren 13a
subject	
CN	Herritar eta entitateen CA (4)
OU	NZZ Ziurtagiri Publikoa



O	IZENPE SA
C	ES
subjectPublicKeyInfo	RSA 4096 bit
extensions	
subjectAltName	
rfc822Name	info@izenpe.com
directoryName	
STREET	Mediterraneo Etorbidea 14 - 01010 Gasteiz
O	IZENPE SA - IFK A01337260- RMerc. Gasteiz T1055 F62 S8
subjectKeyIdentifier	a4171d4e65d7ef87952e7f8eb875cb058bd38c7d
authorityKeyIdentifier	ID gakoa = 1d1c650ea8f2257bb491cfe4b1b1e6bd55746c05
certificatePolicies	
policyIdentifier	Jaulkipen-zuzentarau guztiak
Zuzentarau-ziurtatzailearen IDa	CPS
cpsURI	http://www.izenpe.eus/cps
authorityInfoAccess	
Sartzeko modua	Online ziurtagiriaren egoera-protokoloa (1.3.6.1.5.5.7.48.1)
Ordezko izena	
URL helbidea	http://ocsp.izenpe.com:8094
cRLDistributionPoints	http://crl.izenpe.com/cgi-bin/arl2
keyUsage	Ziurtagirien sinadura, CRL sinadura konexiorik gabe, Ziurtagiriak ezeztatzeko zerrendaren sinadura (CRL) (06)
Hatz-marka	08d8d62a1a1536c53a0f9a1835bf82c9f0968323

Herritarra eta entitateak (3)	
version	3. bertsioa
serialNumber	72eb2bad7d8b65e34cbea5bf9f2ac3d9
signature	sha256WithRSAEncryption
issuer	
CN	izenpe.com
O	IZENPE SA
C	ES
validity	2037ko abenduaren 13a
subject	
CN	Herritar eta entitateen CA (3)
OU	NZZ Ziurtagiri Publikoa
O	IZENPE SA
C	ES



subjectPublicKeyInfo	RSA 4096 bit
extensions	
subjectAltName	
rfc822Name	info@izenpe.com
directoryName	
STREET	Mediterraneo Etorbidea 14 - 01010 Gasteiz
O	IZENPE SA - IFK A01337260- RMerc. Gasteiz T1055 F62 S8
subjectKeyIdentifier	ecb204f691bd8b523806b3f4007fb137dbbc5197
authorityKeyIdentifier	ID gakoa = 1d1c650ea8f2257bb491cfe4b1b1e6bd55746c05
certificatePolicies	
policyIdentifier	Jaulkipen-zuzentarau guztiak
Zuzentarau-ziurtatzailearen IDa	CPS
cpsURI	http://www.izenpe.eus/cps
authorityInfoAccess	
Sartzeko modua	Online ziurtagiriaren egoera-protokoloa (1.3.6.1.5.5.7.48.1)
Ordezko izena	
URL helbidea	http://ocsp.izenpe.com:8094
cRLDistributionPoints	http://crl.izenpe.com/cgi-bin/ar12
keyUsage	Ziurtagiriaren sinadura, CRL sinadura konexiorik gabe, Ziurtagiriak ezeztatzeke zerrendaren sinadura (CRL) (06)
Hatz-marka	875660a35cb103d7e0bb004424f16dbfbf21e0b4

EAEko Herri Administrazioetako langileen CA (2)	
version	3. bertsioa
serialNumber	693a966783e23bdf4cbea6d0d9543fd7
signature	sha256WithRSASignature
issuer	
CN	izenpe.com
O	IZENPE SA
C	ES
validity	2037ko abenduaren 13a
subject	
CN	EAEko Herri Administrazioetako langileen CA (2)
OU	AZZ Ziurtagiri Publikoa
O	IZENPE SA
C	ES
subjectPublicKeyInfo	RSA 4096 bit
extensions	



subjectAltName	
rfc822Name	info@izenpe.com
directoryName	
STREET	Mediterraneo Etorbidea 14 - 01010 Gasteiz
O	IZENPE SA - IFK A01337260- RMerc. Gasteiz T1055 F62 S8
subjectKeyIdentifier	c6af966850be6fa1e514dcb99d973d8d73e77e9a
authorityKeyIdentifier	ID gakoak = 1d1c650ea8f2257bb491cfe4b1b1e6bd55746c05
certificatePolicies	
policyIdentifier	Jaulkipen-zuzentarau guztiak
Zuzentarau-ziurtatzailearen IDa	CPS
cpsURI	http://www.izenpe.eus/cps
authorityInfoAccess	
Sartzeko modua	Online ziurtagiriaren egoera-protokoloa (1.3.6.1.5.5.7.48.1)
Ordezko izena	
URL helbidea	http://ocsp.izenpe.com:8094
cRLDistributionPoints	http://crl.izenpe.com/cgi-bin/ar12
keyUsage	Ziurtagiriaren sinadura, CRL sinadura konexiorik gabe, Ziurtagiriak ezeztatze zerrendaren sinadura (CRL) (06)
Hatz-marka	93a1446b61994b5b0e99d05b14cd5b322e6c1764

EAEko Herri Administrazioen CA (2)	
Esparrua/luzapena	Edukia
version	3. bertsioa
serialNumber	24c5c8aa566f8ee84cbea7055ce164a4
signature	sha256WithRSAEncryption
issuer	
CN	izenpe.com
O	IZENPE SA
C	ES
validity	2037ko abenduaren 13a
subject	
CN	EAEko Herri Administrazioen CA (2)
OU	AZZ Ziurtagiri Publikoa
O	IZENPE SA
C	ES
subjectPublicKeyInfo	RSA 4096 bit
extensions	
subjectAltName	
rfc822Name	info@izenpe.com



directoryName	
STREET	Mediterraneo Etorbidea 14 - 01010 Gasteiz
O	IZENPE SA - IFK A01337260- RMerc. Gasteiz T1055 F62 S8
subjectKeyIdentifier	c0a94af7472587ffbc5a689ce82d246a889eba3
authorityKeyIdentifier	ID gakoa = 1d1c650ea8f2257bb491cfe4b1b1e6bd55746c05
certificatePolicies	
policyIdentifier	Jaulkipen-zuzentarau guztiak
Zuzentarau-ziurtatzailearen IDa	CPS
cpsURI	http://www.izenpe.eus/cps
authorityInfoAccess	
Sartzeko modua	Online ziurtagiriaren egoera-protokoloa (1.3.6.1.5.5.7.48.1)
Ordezko izena	
URL helbidea	http://ocsp.izenpe.com:8094
cRLDistributionPoints	http://crl.izenpe.com/cgi-bin/arl2
keyUsage	Ziurtagirien sinadura, CRL sinadura konexiorik gabe, Ziurtagiriak ezeztatzeke zerrendaren sinadura (CRL) (06)
Hatz-marka	f79cda11e7917419a0418db84ba743c5313ad7f0

SSL EV ziurtagirien CA	
Esparrua/luzapena	Edukia
version	3. bertsioa
serialNumber	6d71e25b7bb6b6364cbea848e3a4a981
signature	sha256WithRSAEncryption
issuer	
CN	izenpe.com
O	IZENPE SA
C	ES
validity	2020ko urriaren 20a
subject	
CN	SSL EV ziurtagirien CA
OU	EV ziurtagiri publikoa
O	IZENPE SA
C	ES
subjectPublicKeyInfo	RSA 4096 bit
extensions	
subjectAltName	
rfc822Name	info@izenpe.com
directoryName	



STREET	Mediterraneo Etorbidea 14 - 01010 Gasteiz
O	IZENPE SA - IFK A01337260- RMerc. Gasteiz T1055 F62 S8
subjectKeyIdentifier	a6ce69692ea621353b3acf0af12e3f15ac199027
authorityKeyIdentifier	ID gakoa = 1d1c650ea8f2257bb491cfe4b1b1e6bd55746c05
certificatePolicies	
policyIdentifier	Jaulkipen-zuzentarau guztiak
Zuzentarau-ziurtatzailearen IDa	CPS
cpsURI	http://www.izenpe.eus/cps
authorityInfoAccess	
Sartzeko modua	Online ziurtagiriaren egoera-protokoloa (1.3.6.1.5.5.7.48.1)
Ordezko izena	
URL helbidea	http://ocsp.izenpe.com
cRLDistributionPoints	http://crl.izenpe.com/cgi-bin/ar12
keyUsage	Ziurtagiriaren sinadura, CRL sinadura konexiorik gabe, Ziurtagiriak ezeztatzeke zerrendaren sinadura (CRL) (06)
Hatz-marka	6c484d0f4db295ec67ebb3e05e3dc214492a9ab8

SSL EV 2018 ziurtagiriaren CA	
Esparrua/luzapena	Edukia
version	3. bertsioa
serialNumber	687db7171744da235b3f625a7393f8a5
signature	sha256WithRSAEncryption
issuer	
CN	izenpe.com
O	IZENPE SA
C	ES
validity	2028ko uztailaren 6a
subject	
CN	SSL EV ziurtagiriaren CA
OU	EV ziurtagiri publikoa
O	IZENPE SA
C	ES
subjectPublicKeyInfo	RSA 4096 bit
extensions	
subjectAltName	
rfc822Name	info@izenpe.com
directoryName	
STREET	Mediterraneo Etorbidea 14 - 01010 Gasteiz



O	IZENPE SA - IFK A01337260- RMerc. Gasteiz T1055 F62 S8
subjectKeyIdentifier	c6edfe77fb51564dfcabd5e3b10c13a3bf54e39b
authorityKeyIdentifier	ID gakoa = 1d1c650ea8f2257bb491cfe4b1b1e6bd55746c05
certificatePolicies	
policyIdentifier	Jaulkipen-zuzentarau guztiak
Zuzentarau-ziurtatzailearen IDa	CPS
cpsURI	http://www.izenpe.eus/cps
authorityInfoAccess	
Sartzeko modua	Online ziurtagiriaren egoera-protokoloa (1.3.6.1.5.5.7.48.1)
Ordezko izena	
URL helbidea	http://ocsp.izenpe.com
cRLDistributionPoints	http://crl.izenpe.com/cgi-bin/arl2
keyUsage	Ziurtagiriaren sinadura, CRL sinadura konexiorik gabe, Ziurtagiriak ezeztatze zerrendaren sinadura (CRL) (06)
Hatz-marka	c68bade5f069778a003074e619dab2e7928342d5

10.2.2SUBCA CN = ROOT CA QC IZENPE

SUBCA QC IZENPE - TSA	
Esparrua/luzapena	Edukia
version	3. bertsioa
serialNumber	Ausazko zenbakia
signature	sha256WithRSAEncryption eta/edo sha512.
issuer	CA jaulkitzailearen ziurtagiriaren subject eremuaren berdina
validity	OINARRIZKO CAren amaiera-datara arte
subject	
CN	SUBCA QC IZENPE - TSA
organizationIdentifier	VATES-A01337260
O	IZENPE SA
C	ES
subjectPublicKeyInfo	RSA 4096 bit gutxienez
extensions	
authorityKeyIdentifier	keyIdentifier eremua soilik txertatu
subjectKeyIdentifier	Gako publikoaren identifikatzailea
certificatePolicies	
policyIdentifier	Jaulkipen-zuzentarau guztiak
cpsURI	https://www.izenpe.eus/cps
cRLDistributionPoints	http://crl.izenpe.eus/cgi-bin/izrootqc
authorityInfoAccess	
ocsp	http://ocsp.izenpe.eus



CA jaulkitzailea	http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/IZENPE_ROOT_QC.crt
oinarrizko mugaketak	Gai mota = Ziurtapen-entitatea (CA) Ibilbidearen luzeraren murrizketa=0
keyUsage	KeyCertSign, cRLSign

SUBCA QC IZENPE - ADMINISTRAZIO PUBLIKOA	
Esparrua/luzapena	Edukia
version	3. bertsioa
serialNumber	Ausazko zenbakia
signature	sha256WithRSAEncryption eta/edo sha512.
issuer	CA jaulkitzailearen ziurtagiriaren subject eremuaren berdina
validity	OINARRIZKO CAren amaiera-datara arte
subject	
CN	SUBCA QC IZENPE - ADMINISTRAZIO PUBLIKOA
organizationIdentifier	VATES-A01337260
O	IZENPE SA
C	ES
subjectPublicKeyInfo	RSA 4096 bit gutxienez
extensions	
authorityKeyIdentifier	keyIdentifier eremua soilik txertatu
subjectKeyIdentifier	Gako publikoaren identifikatzailea
certificatePolicies	
policyIdentifier	Jaulkipen-zuzentarau guztiak



cpsURI	https://www.izenpe.eus/cps
cRLDistributionPoints	http://crl.izenpe.eus/cgi-bin/izrootqc
authorityInfoAccess	
ocsp	http://ocsp.izenpe.eus
CA jaulkitzailea	http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/IZENPE_ROOT_QC.crt
oinarrizko mugaketak	Gai mota = Ziurtapen-entitatea (CA) Ibilbidearen luzeraren murrizketa=0
keyUsage	KeyCertSign, cRLSign

SUBCA QC IZENPE - HERRITARRAK ETA ENPRESA	
Esparrua/luzapena	Edukia
version	3. bertsioa
serialNumber	Ausazko zenbakia
signature	sha256WithRSAEncryption eta/edo sha512.
issuer	CA jaulkitzailearen ziurtagiriaren subject eremuaren berdina
validity	GINARRIZKO CAren amaiera-datara arte
subject	
CN	SUBCA QC IZENPE - HERRITARRAK ETA ENPRESA
organizationIdentifier	VATES-A01337260
O	IZENPE SA
C	ES
subjectPublicKeyInfo	RSA 4096 bit gutxienez
extensions	
authorityKeyIdentifier	keyIdentifier eremua soilik txertatu
subjectKeyIdentifier	Gako publikoaren identifikatzailea
certificatePolicies	
policyIdentifier	Jaulkipen-zuzentarau guztiak
cpsURI	https://www.izenpe.eus/cps
cRLDistributionPoints	http://crl.izenpe.eus/cgi-bin/izrootqc



authorityInfoAccess	
ocsp	http://ocsp.izenpe.eus
CA jaulkitzailea	http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/IZENPE_ROOT_QC.crt
oinarrizko mugaketak	Gai mota = Ziurtapen-entitatea (CA) Ibilbidearen luzeraren murrizketa=0
keyUsage	KeyCertSign, cRLSign

10.2.3 subCA CN = ROOT CA NQC IZENPE

CA NQC IZENPE - PERTSONA FISIKOA	
Esparrua/luzapena	Edukia
version	3. bertsioa
serialNumber	Ausazko zenbakia
signature	sha256WithRSAEncryption eta/edo sha512.
issuer	CA jaulkitzailearen ziurtagiriaren subject eremuaren berdina
validity	OINARRIZKO CAren amaiera-datara arte
subject	
CN	CA NQC IZENPE - PERTSONA FISIKOA
organizationIdentifier	VATES-A01337260
O	IZENPE SA
C	ES
subjectPublicKeyInfo	RSA 4096 bit gutxienez
extensions	
authorityKeyIdentifier	keyIdentifier eremua soilik txertatu
subjectKeyIdentifier	Gako publikoaren identifikatzailea
certificatePolicies	
policyIdentifier	Jaulkipen-zuzentarau guztiak
cpsURI	http://www.izenpe.eus/cps
cRLDistributionPoints	http://crl.izenpe.eus/cgi-bin/izrootnqc
authorityInfoAccess	
ocsp	http://ocsp.izenpe.eus
CA jaulkitzailea	http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/IZENPE_ROOT_NQC.crt



oinarrizko mugaketak	Gai mota = Ziurtapen-entitatea (CA) Ibilbidearen luzeraren murrizketa=0
keyUsage	KeyCertSign, cRLSign

CA NQC IZENPE - GAILUA	
Esparrua/luzapena	Edukia
version	3. bertsioa
serialNumber	Ausazko zenbakia
signature	sha256WithRSAEncryption eta/edo sha512.
issuer	CA jaulkitzailearen ziurtagiriaren subject eremuaren berdina
validity	OINARRIZKO CAren amaiera-datara arte
subject	
CN	CA NQC IZENPE - GAILUA
organizationIdentifier	VATES-A01337260
O	IZENPE SA
C	ES
subjectPublicKeyInfo	RSA 4096 bit gutxienez
extensions	
authorityKeyIdentifier	keyIdentifier eremua soilik txertatu
subjectKeyIdentifier	Gako publikoaren identifikatzailea
certificatePolicies	
policyIdentifier	Jaulkipen-zuzentarau guztiak
cpsURI	http://www.izenpe.eus/cps
cRLDistributionPoints	http://crl.izenpe.eus/cgi-bin/izrootnqc
authorityInfoAccess	
ocsp	http://ocsp.izenpe.eus
CA jaulkitzailea	http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas/adjuntos/IZENPE_ROOT_NQC.crt
oinarrizko mugaketak	Gai mota = Ziurtapen-entitatea (CA) Ibilbidearen luzeraren murrizketa=0
keyUsage	KeyCertSign, cRLSign

CA NQC IZENPE - TEKNIKOIA



Esparrua/luza pena	Edukia
version	3. bertsioa
serialNumber	Ausazko zenbakia
signature	sha256WithRSAEncryption eta/edo sha512.
issuer	CA jaulkitzailearen ziurtagiriaren subject eremuaren berdina
validity	OINARRIZKO CAren amaiera-datara arte
subject	
CN	CA NQC IZENPE - TEKNIKOA
organizationIdentifier	VATES-A01337260
O	IZENPE SA
C	ES
subjectPublic KeyInfo	RSA 4096 bit gutxienez
extensions	
authorityKeyIdentifier	keyIdentifier eremua soilik txertatu
subjectKeyIdentifier	Gako publikoaren identifikatzailea
certificatePolicies	
policyIdentifier	Jaulkipen-zuzentarau guztiak



cpsURI	http://www.izenpe.eus/cps
cRLDistributionPoints	http://crl.izenpe.eus/cgi-bin/izrootnqc
authorityInfoAccess	
ocsp	http://ocsp.izenpe.eus
CA jaulkitzailea	http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas_adjuntos/IZENPE_ROOT_NQC.crt
oinarrizko mugaketak	Gai mota = Ziurtapen-entitatea (CA) Ibilbidearen luzeraren murrizketa=0
keyUsage	KeyCertSign, cRLSign

CA NQC IZENPE - SSL EZ PUBLIKOA	
Esparrua/luza pena	Edukia
version	3. bertsioa
serialNumber	Ausazko zenbakia
signature	sha256WithRSAEncryption eta/edo sha512.
issuer	CA jaulkitzailearen ziurtagiriaren subject eremuaren berdina
validity	OINARRIZKO CAren amaiera-datara arte
subject	
CN	CA NQC IZENPE - SSL EZ PUBLIKOA
organizationIdentifier	VATES-A01337260



O	IZENPE SA
C	ES
subjectPublicKeyInfo	RSA 4096 bit gutxienez
extensions	
authorityKeyIdentifier	keyIdentifier eremua soilik txertatu
subjectKeyIdentifier	Gako publikoaren identifikatzailea
certificatePolicies	
policyIdentifier	Jaulkipen-zuzentarau guztiak
cpsURI	http://www.izenpe.eus/cps
cRLDistributionPoints	http://crl.izenpe.eus/cgi-bin/izrootnqc
authorityInfoAccess	
ocsp	http://ocsp.izenpe.eus
CA jaulkitzailea	http://www.izenpe.eus/contenidos/informacion/cas_izenpe/es_cas_adjuntos/IZENPE_ROOT_NQC.crt
oinarrizko mugaketak	Gai mota = Ziurtapen-entitatea (CA) Ibilbidearen luzeraren murrizketa=0
keyUsage	KeyCertSign, cRLSign