ZIURTAPEN-POLITIKA

SSL / TLS

2019ko azaroa

1.6 bertsioa

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

www.izenpe.com
info@izenpe.com
Tel.: 945 017 490

AURKIBIDEA

1 SARRERA 3
1.1 ZIURTAGIRIEN DESKRIBAPENA 3
1.2 IDENTIFIKAZIOA 5
1.3 KOMUNITATEA ETA ERABILERA-ESPARRUA 5
1.4 XEDAPEN OROKORRAK 5
2 ESKAKIZUN OPERATIBOAK 7
2.1 BEHARREZKO DOKUMENTAZIOAREN ZERRENDA 7
2.2 ESKAERA-PROZEDURA 7
2.3 ZIURTAGIRIA JAULKITZEA ETA EMATEA 10
2.4 ZENBATEKOA 11
2.5 ZIURTAGIRIA EGIAZTATZEA 11
2.6 ZIURTAGIRIAK EZEZTATZEA 11
2.7 ZIURTAGIRIA BERRITZEA 13
2.8 IKUSKAPENAK ETA GORABEHERAK 13
3 ALDAKETAREN KUDEAKETA 14
4 ALDAKETEN KONTROLA 15
4.1 0 BERTSIOTIK 1.0 BERTSIORA 15
4.2 1.0 BERTSIOTIK 1.1 BERTSIORA 15
4.3 1.1 BERTSIOTIK 1.2 BERTSIORA 15
4.4 1.2 BERTSIOTIK 1.3 BERTSIORA 16
4.5 1.3 BERTSIOTIK 1.4 BERTSIORA 16
4.6 1.4 BERTSIOTIK 1.5 BERTSIORA 17
4.7 1.5 BERTSIOTIK 1.6 BERTSIORA 17

1 SARRERA

Dokumentu honek *Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, SA* (aurrerantzean IZENPE) enpresak jaulkitako ziurtagiriei dagokien ziurtapen-politika jasotzen du.

Xedea da ziurtagiri mota horretarako zehaztea eta osatzea IZENPEren Ziurtapen Praktiken Deklarazioan oro har xedatzen dena, eta *CA/Browser Forum*-aren berariazko *Baseline Requirements (aurrerantzean BR)* eta *EV guidelines (aurrerantzean EVBR)* dokumentuetan web-guneetarako ziurtagiriak jaulkitzeko xedatzen dena, baita ETSIren zehaztapenetan xedatzen dena ere (www.etsi.org).

Hartara, ETSIk ezarritako honako ziurtapen-politika hauek hartzen ditu aintzat IZENPEk:

- DVCP (Domain Validation Certificates Policy): "SSL DV" ziurtagirietan
- OVCP (Organizational Validation Certificates Policy): "SSL OV" ziurtagirietan
- EVCP (Extended Validation Certificates Policy): "EV egoitza", "SSL EV", "SSL kualifikatua" eta "Egoitza kualifikatua" ziurtagirietan.

Google Certificate Transparency proiektuaren esparruan, egindako SSL ziurtagiri guztiak IZENPErekin hitzarmena duten Log Servers hornitzaileen CT zerbitzuan emango dira argitara.

1.1 Ziurtagirien deskribapena

Ziurtagiri horien bidez, IZENPEren xedea da bere harpidedunek segurtasun gehigarria eskaini ahal izatea haien web-zerbitzuetan.

Ziurtagiri motari dagokionez, IZENPEk honelako ziurtagiriak jaulkitzen ditu:

SSL	EGOITZA ELEKTRONIKOA
SSL DV SSL OV SSL EV SSL kualifikatua	EV egoitza Egoitza kualifikatua

Ziurtagiri mota horiek web-zerbitzarietan datu-komunikazioak TLS/SSL bidez ezartzea dute xede.

Aukera ematen dute erabiltzailearen eta web-gunearen arteko komunikazioak zifratzeko eta, horrela, informazioa Internet bidez zifratzeko beharrezkoak diren zifratze-gakoen trukea errazteko.

– *SSL MOTAKO ZIURTAGIRIAK,*

IZENPEk egindako balidazioaren arabera, ziurtagiria honelakoa izan daiteke:

- *SSL DOMAIN VALIDATED (**SSL DV**),*

  Ziurtagiri hori, kualifikatu gabetzat jotzen dena, web-gunea barnean hartzen duen domeinuaren titulartasuna identifikatzeko erabiliko da, Interneteko erabiltzaile bati zentzuzko bermea eskainiz.

  Ziurtagiri horiek 1 edo 2 urtez izan daitezke baliozkoak.

- *SSL ORGANIZATION VALIDATED (**SSL OV**),*

  Ziurtagiri hori, kualifikatu gabetzat jotzen dena, erakundearen egiaztapenaren eta domeinuaren titularitasuna identifikatzeko erabiliko da, eta Interneteko erabiltzaile bati zentzuzko bermea eskainiko dio sartzen ari den web-gune horren titularitasuna ziurtagirian identifikatutako erakundearena dela.

  Ziurtagiri horiek 1 edo 2 urtez izan daitezke baliozkoak.

- *BALIDAZIO HEDATUA DUEN SSL (**SSL EV**),*

  Ziurtagiri hori, kualifikatu gabetzat jotzen dena, erakundearen egiaztapenaren eta domeinuaren titularitasuna identifikatzeko erabiliko da, eta Interneteko erabiltzaile bati berme sendoa eskainiko dio sartzen ari den web-gune horren titularitasuna ziurtagirian identifikatutako erakundearena dela.

  Ziurtagiri horiek 1 edo 2 urtez izan daitezke baliozkoak.

- *SSL KUALIFIKATUA (**SSL KUALIFIKATUA**),*

  Ziurtagiri hori kualifikatutzat joko da, 1999/93/EE Zuzentaraua indargabetzen duen Europako Parlamentuaren eta Kontseiluaren identifikazio elektronikoari eta barne-merkatuko transakzio elektronikoetarako konfiantzako zerbitzuei buruzko uztailaren 23ko 910/2014 Araudiaren arabera. Ziurtagiria erakundearen egiaztapenaren eta domeinuaren titularitasuna identifikatzeko erabiliko da, eta Interneteko erabiltzaile bati berme sendoa eskainiko dio sartzen ari den web-gune horren titularitasuna ziurtagirian identifikatutako erakundearena dela.

  Ziurtagiri horiek 1 edo 2 urtez izan daitezke baliozkoak.

– *EGOITZA ELEKTRONIKOA MOTAKO ZIURTAGIRIAK*

  Sektore publikoaren araubideari buruzko urriaren 1eko 40/2015 Legearen esparruan, IZENPEk mota hauetako ziurtagiriak jaulkitzen ditu:

- ***EV BALIDAZIO HEDATUA DUEN EGOITZA ELEKTRONIKOA (EGOITZA EV),***

  Egoitza elektronikoko ziurtagirian definitutako ezaugarriez gain, balidazio hedatuaren (EV) xedea da Herri Administrazioaren edo administrazio-organoaren edo -entitatearen kautotze-maila hobea eskaintzea, betiere balidazio zorrotzago baten indarrez.

  Identifikazio eta sinadura elektronikoko eskeman definitutako ziurtatze-mailen arabera, IZENPEk jaulkitako *egoitza elektronikoko ziurtagiria* maila ertaineko ziurtagiria da.

  Ziurtagiri horiek 2 urtez dira baliozkoak.

- ***EGOITZA ELEKTRONIKO KUALIFIKATUA (EGOITZA KUALIFIKATUA)***

  Ziurtagiri hau kualifikatutzat joko da, 1999/93/EE Zuzentaraua indargabetzen duen Europako Parlamentuaren eta Kontseiluaren identifikazio elektronikoari eta barne-merkatuko transakzio elektronikoetarako konfiantzako zerbitzuei buruzko uztailaren 23ko 910/2014 Araudiaren arabera.

Balidazio hedatuaren (EV) xedea da Herri Administrazioaren edo administrazio-organoaren edo -entitatearen kautotze-maila hobea eskaintzea, betiere balidazio zorrotzago baten indarrez.

Identifikazio eta sinadura elektronikoko eskeman definitutako ziurtatze-mailen arabera, IZENPEk jaulkitako *egoitza elektronikoko ziurtagiria* maila ertaineko ziurtagiria da.

Ziurtagiri horiek 2 urtez dira baliozkoak.

1.2 Identifikazioa

Ziurtagiriak identifikatu ahal izateko, IZENPEk honako objektu-identifikatzaile hauek (OID) esleitu dizkie.

ZIURTAGIRIA	OID IZENPE	OID CA/B FORUM
SSL DV	1.3.6.1.4.1.14777.1.2.4	2.23.140.1.2.1
SSL OV	1.3.6.1.4.1.14777.1.2.1	2.23.140.1.2.2
SSL EV	1.3.6.1.4.1.14777.6.1.1	2.23.140.1.1
SSL kualifikatua	1.3.6.1.4.1.14777.6.1.3	2.23.140.1.1
Egoitza EV	1.3.6.1.4.1.14777.6.1.2	2.23.140.1.1
Egoitza kualifikatua	1.3.6.1.4.1.14777.6.1.4	2.23.140.1.1

Ziurtagirien serieko zenbakiek entropiako 64 bit izango dute gutxienez.

1.3 Komunitatea eta erabilera-esparrua

Erabiltzailetzat hartuko dira,

- Ziurtagiriaren eskatzailea, ziurtagiri bat eskatzen duen pertsona juridikoa. Behin ziurtagiria jaulki denean, harpidedun deritza.
- Ziurtagirien harpideduna, ziurtagirian identifikatutako pertsona juridikoa.

Erabilera-esparrua. Ziurtagiriak ziurtagiriaren erakunde titularraren berezko eskumenen esparruan erabiliko dira.

1.4 Xedapen orokorrak

Identifikazio-betebeharrak

IZENPEk –berez edo berarekin dagokion lege-tresna harpidetu duten entitateen bidez– egiaztatzen ditu, ziurtagirien eskatzaileen eta harpidedunen nortasuna eta beste zeinahi datu pertsonal. IZENPEk ez du inola ere eskuordetuko titulartasunaren egiaztapena edo domeinuaren gaineko kontrola.

CA/Browser Forum-aren dokumentuetan adierazten dena betetzearen eskakizuna hartuko du barnean aldeen arteko legezko tresnak.

Ziurtagiri-harpidedunaren betebeharrak

Harpidedunaren betebeharrak jasotzen dira Ziurtapen Praktiken Deklarazioan eta Gako Publikoa Dibulgatzeko Akordioan (PDS).

2 ESKAKIZUN OPERATIBOAK

2.1 Beharrezko dokumentazioaren zerrenda

- ✓ Behar bezala beteta aurkeztu beharko da ziurtagiria jaulkitzeko eskaera, eta modu elektronikoan sinatuko da IZENPEren ordezkari-ziurtagiri batekin edo erakunde publikoko langilearen ziurtagiri batekin —bertan eskatzailearen kargua adierazi beharko da—. Entitatearen lege-ordezkariak SSL/TLS ziurtagiriak eskatzeko ahalmena eskuordetzen duenean, ez da sinadurarik beharko. Eskuordetze hori modu elektronikoan sinatu beharko du lege-ordezkariak, IZENPEren ordezkari-ziurtagiri batekin edo erakunde publikoko langilearen ziurtagiri batekin —bertan eskatzailearen kargua adierazi beharko da—.

- ✓ SSL-DV ziurtagirien eskaeren kasuan izan ezik, eratze-informazioa Merkataritza Erregistroan kontsultatzeko moduan ez daukaten entitate ez-publikoek dokumentazio hau aurkeztu beharko dute:

    - o Dagokion erregistroan argitaratu izanaren kopia
    - o IFKren kopia

2.2 Eskaera-prozedura

- ➢ ESKATZAILEAK ziurtagiria jaulkitzeko eskaera eta beharrezko dokumentazioa bidali beharko du,

    - o Bide telematikoz, certservidor@izenpe.eus helbide elektronikora
    - o Edo IZENPEren web-gunean horretarako antolatutako aplikazioaren bidez.

  Ziurtagiriak jaulkitzeko eskaeraren sinadurarekin, eskatzaileak Gako Publikoaren Azpiegitura Dibulgatzeko Akordioaren (PDS) baldintzak onartzen ditu.

- ➢ Honako dokumentazio hau baliozkotuko da,

SSL DV SSL OV SSL kualifikatua Egoitza kualifikatua	➢ Domeinuaren erabileraren titulartasuna edo eskubidea. Modu hauetako edozein bidez egin ahal izango da: a) Domeinuaren kontaktuari mezu elektronikoa bidaliz. IZENPEK eskatzaileari kode bakarra eta ausazkoa igorriko dio, mezu elektroniko bidez, whois-eko kontaktuan agertzen den helbidera (Registrant, administratzailea edo teknikaria). Erakunde eskatzailearen edozein pertsonak erantzun dezake, ausazko kodea adierazita. b) Domeinuaren kontaktuari mezu elektroniko eraikia bidaliz. IZENPEk mezu elektroniko bat igorriko die honako helbide hauetako bati edo batzuei: “admin”,“administrator”, “webmaster”, “hostmaster” edo “postmaster”, eta gero “@” sinboloa eta SSL ziurtagiria eskatzen duen domeinuaren izena. Igortzen den mezu elektronikoan kode bakarra eta ausazkoa txertatzen da. Erakunde eskatzaileko edozein pertsonak erantzun diezaioke mezu elektronikoari, ausazko kodea adierazita. c) DNSan adostutako aldaketaren bidez. Eskatzaileak aldaketa bat egiten du SSL ziurtagiria nahi duen domeinuaren DNS erregistroan. Eskatzaileak IZENPEk igorritako kode bakarra eta ausazkoa erantsi beharko du CNAME, TXT edo CAA eremu batean, DNS erregistroan. Eskatzaileak aldaketa egin duenean,

	IZENPEk aldaketa egiaztatuko du. d) Web-gunean adostutako aldaketaren bidez. Eskatzaileak IZENPEk igorritako kode bakarra eta ausazkoa jasoko duen fitxategia "/.well-known/pki-validation" bidean argitaratu beharko du. Eskatzaileak aldaketa egin duenean, IZENPEk aldaketa egiaztatuko du. e) DNS CAAren kontaktuari mezu elektronikoa bidaliz. IZENPEk mezu elektroniko bidez bidaliko dio kode bakarra eta ausazkoa eskatzaileari, DNS CAA erregistroan agertzen den helbidera. Erakunde eskatzailearen edozein pertsonak erantzun dezake, ausazko kodea adierazita. f) DNS TXTaren kontaktuari mezu elektronikoa bidaliz. IZENPEk mezu elektroniko bidez bidaliko dio kode bakarra eta ausazkoa eskatzaileari, DNS TXT erregistroan agertzen den helbidera. Erakunde eskatzailearen edozein pertsonak erantzun dezake, ausazko kodea adierazita. g) DNS Lookup bidez. IZENPEk domeinuaren DNS lookup kontsulta egingo du eta A eremuaren edo AAAA eremuaren IP helbidea aterako du. Gero, egiaztatuko da eskatzaileak esleituta duela lortutako IP helbidea; horretarako, Internet Assigned Numbers Authority (IANA) bidez edo Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC) bidez egingo da bilaketa. IZENPEk kontaktuari mezu elektroniko bat igorriko dio, eta mezuan kode bakarra eta ausazkoa jasoko da. Erakunde eskatzailearen edozein pertsonak erantzun dezake, ausazko kodea adierazita. ➢ SSL ziurtagiri oro jaulki aurretik, IZENPEk ziurtagiriaren CN eta subjectAltName luzapenetako DNS izen bakoitzerako CAA erregistro bat dagoen baliozkotzen du, betiere RFC 6844aren zehaztapenen arabera. Ziurtagiria jaulkitzen bada, baliozkotzea CAA erregistroaren TTLaren aurretik egingo da, baina inola ere ez 8 ordu baino tarte handiagoz. IZENPEk "issue" eta "issuewild" tag-ak prozesatzen ditu. Jaulkipen-baimena duten domeinuak identifikatzen dituzten IZENPEren CAA erregistroak “izenpe.com” eta “izenpe.eus” dira. ➢ SSL DV eta SSL OV egiaztagirien kasuan, wildcard-ak onartuko dira host izenetan edo azpidomeinuetan, betiere entitate eskatzaileak domeinu osoaren legezko kontrola egiaztatzeko aukera badu. Hala izan ezean, eskaera baztertuko da. Esate baterako, ezin izango dira jaulki “*.co.uk” edo “*.local”, baina bai “*.adibide.com” Adibide, SA. enpresari. ➢ IZENPEk bere barneko datu-basean baliozkotzen du ukatuen zerrenda. ➢ IZENPEk Mcafee TrustedSource bidez egiaztatzen ditu arrisku handiko eskaerak.
SSL OV SSL kualifikatua Egoitza kualifikatua	➢ Erakundearen izen ofiziala egiaztatzea; – Entitate publikoan: idazkariak/letratuak egindako ziurtagiria, erregistroko ziurtagiria / aldizkari ofizialaren informazio-ohar sinplea edo erreferentzia, betiere jaulkitzeko eskaeraren aurreko 13 hilabeteetan. – Entitate pribatua: dagokion erregistroko jatorrizko ziurtagiria edo informazio-ohar sinplea.

	➢ Erakundearen merkataritza-izena egiaztatzea: eskatzaileak merkataritza-izena aurkezten badu, izen ofizialaren kasuan egiaztatzeko erabilitako iturri berak erabiliko dira. ➢ Mezu elektroniko bidez egiaztatzea eskatzaileak ziurtagiriaren tramitazioaren berri duela. Erakundeko ordezkariak baimendutako eskatzaileak adierazi beharko ditu. ➢ Entitatearen posta-helbidea egiaztatzea: – Datuak Babesteko Agentzietan. – EUDELen, Euskadiko udalerrietarako. – Erregistro ofizialean. ➢ Herrialdea egiaztatzea: ➢ Datuak Babesteko Espainiako Agentzian (APD). ➢ Eudelen. ➢ Dagokion erregistro publikoan.
SSL kualifikatua Egoitza kualifikatua	➢ Identitatearen identifikazio fiskaleko zenbakia egiaztatzea; – Entitate publikoan: Datuak Babesteko Agentzietan, Aldizkari Ofizialean edo dagokion erregistro ofizialean. – Entitate pribatuan: Datuak Babesteko Agentzietan, jatorrizko erregistro-ziurtagiri bidez edo informazio-ohar sinple bidez. – Enpresan: Datuak Babesteko Agentzietan edo Merkataritza Erregistroan. – Merkataritzakoa ez den / irabazi asmorik ez duen nazioarteko entitatean: entitatea nazioarteko erakunde ezaguna den egiaztatzea. ➢ Existentzia operatiboa egiaztatzea: “Izen ofiziala egiaztatzea”, “Merkataritza-izena egiaztatzea” eta “Posta-helbidea egiaztatzea” ataletan deskribatutako metodo guztiek egiaztatzen dute erakundea egoera aktiboan dagoen. Ezinezkoa izango balitz, on line kontsultatuko zaio QIISi (adib: einforma, DUN & BRADSTREET, eta abar). ➢ Eskaera baimentzen duen pertsonaren, ziurtagiria eskatzen duen pertsonaren eta eskaera sinatzen duen pertsonaren izena, kargua eta ahalmena egiaztatzea. ➢ Dokumentazioa egiaztatzeko sinadura duala.
Egoitza kualifikatua	➢ Egoitza elektronikoaren argitalpen ofiziala egiaztatzea dagokion aldizkari ofizialean.

OHARRAK

- Gaineratutako dokumentazioa eta egiaztatutakoa bat ez badatoz, eskabidean jasoarazi den helbidean entitate eskatzaileak modu egonkorrean diharduela egiaztatuko du IZENPEk.
- Ez da entitatearen indarraldia eskatuko, ezta eskatzeko eskumena ere, baldin eta IZENPEk eskatzaileari jaulki dion eta indarrean dagoen ziurtagiri korporatibo onartua bada edo

entitateko ziurtagiria bada, betiere ziurtagiria azken 825 egunetan jaulki bada (13 hilabete EV ziurtagirien edo ziurtagiri kualifikatuen kasuan).

- Domeinuaren titulartasuna egiaztatzeko erabilitako tokenak eta ausazko balioak 30 egunez dira baliagarriak.
- IZENPEren SSL ziurtagiriak on line aplikazioaren bidez egiaztatzeko, entitateak sortu ahal izango ditu entitaterako ziurtagiriak jaulkitzeko baimenduko dituen langileekin lotzen diren erabiltzaileak.
- IZENPE beti arduratuko da domeinuaren titulartasuna edo erabiltzeko eskubidea egiaztatzeaz.
- IZENPEk egiaztapen gehigarriak egin ahal izango ditu, esate baterako: erakundearen eskaera berrestea, edo eskatzaileari ziurtagiria erakundearen izenean bideratzeko baimena ematea, eta hori betetzen dela urtero berrikustea, kanpo-ikuskapen baten bidez.
- Balidazioa zehaztutakoaren arabera egin ezin denean, dokumentazioko egiaztapen-dokumentuan justifikatu beharko da zergatia.
- Dokumentazioa egiaztatu ostean, IZENPEk dokumentazioko egiaztapen-dokumentuaren bidez jasoaraziko ditu egin diren egiaztapenak.
- EV ziurtagirietan eta ziurtagiri kualifikatuetan, balidazioa duala da.
- IZENPEk EZ du IP helbideak jaulkitzea aintzat hartzen.
- IZENPEk beti egiaztatuko du ez direla CSRak berriro erabiltzen.
- IZENPEk honako iturri hauek joko ditu fidagarritzat:
    - Datuak Babesteko Agentziak.
    - Eudel.
    - Dagokion Erregistro Ofiziala.
    - Aldizkari Ofizialak.
    - Udalaren idazkariak/abokatuak egindako ziurtagiria.
    - ICANN.
    - ccTLD bakoitzari dagokion Whois-a.

Zerrenda horretan agertzen ez bada, honako irizpide hauek hartuko dira kontuan iturri bat fidagarritzat jotzeko:

- Informazioaren antzinatasuna.
- Zer maiztasunarekin eguneratzen den.
- Datuen hornitzailea eta datuak biltzearen arrazoia.
- Irisgarritasun publikoa eta eskuragarritasuna.
- Datuak faltsutzeko edo aldatzeko zailtasuna.

2.3 Ziurtagiria jaulkitzea eta ematea

IZENPE *ziurtagiria jaulkitzeko eskaeran* adierazitako arduradun teknikoarekin jarriko da harremanetan, eskaera teknikoa egin eta posta elektroniko bidez IZENPEri bidal diezaion.

IZENPEren eskaera-aplikazioa erabiliz gero, arduradun teknikoa arduratuko da eskaera teknikoa sartzeaz.

IZENPEk mezu elektroniko ziurtatu bidez edo aplikazioaren bidez igorriko dio ziurtagiria arduradun teknikoari.

2.4 Zenbatekoa

Ziurtagiria jaulki ostean, aplikatzekoa den tarifaren araberako zenbatekoa ordainduko da.

IZENPEk urtero emango ditu argitara aplikatzekoak diren tarifak www.izenpe.com bere web-orrian eta ondorio horretarako antolatutako aplikazioan.

2.5 Ziurtagiria egiaztatzea

Eskatzaileak ziurtagiria jaulki eta 15 lanegun izango ditu behar bezala funtzionatzen duela egiaztatzeko, eta, beharrezkoa bada, IZENPEri funtzionamendu-akatsak dituela jakinarazteko.

Funtzionamendu-akatsak kausa teknikoen ondoriozkoak direnean edo IZENPEri egotz dakizkiokeen ziurtagiriko datuetako erroreak direnean soilik ezeztatuko du IZENPEk ziurtagiria, eta beste bat jaulkiko du ondoriozko gastuak bere gain hartuta.

2.6 Ziurtagiriak ezeztatzea

Ziurtagiria ezeztatzeko eskaera

Honako hauek eska dezakete ziurtagiria ezeztatzea:

- Harpidedunak.
  Entitate hartzailearen legezko ordezkariak, langileen arduradunak edo aurrekoek baimendutako hirugarren batek dute ziurtagiria ezeztatzea eskatzeko baimena.
- Eskatzaileak.
- IZENPE baimenduta dago azken entitateko harpidedunaren ziurtagiriak ezeztatzea eskatzeko, ZPDan aintzat hartutako kausa teknikoen kasuetan.

Prozedura

Ziurtagiria ezeztatzea eskatzen duenak IZENPEren aurrean tramitatuko du *ziurtagiria ezeztatzeko eskaera*.
Ziurtagiria edozein unetan ezeztatu ahal izango da, eta gehienez 24 orduko epean ezeztatuko da.
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.
- Telefono bidez, 902 542 542 telefonora deituta.
  Identifikatzeko honako hau eskatuko da:
  - Eskatzailearen NAN
  - Harreman teknikoaren NAN
  - Eskatzailearen helbide elektronikoa
  - Web-gunearen izen osoa (FQDN)
- On line, www.izenpe.com helbidean.
- Posta elektroniko bidez, ziurtagiri kualifikatuz sinatutako ezeztatze-eskaeraren formularioa bidaliz.

Ezeztatzeko arrazoiak

Ziurtapen Praktiken Deklarazioan kontsulta daitezke (www.izenpe.eus).

Horrez gain, mendeko CAen ziurtagiriak 7 eguneko epean ezeztatuko dira, honako kausa hauen ondorioz:

1. Mendeko CAk idatziz eskatzen badu.
2. Mendeko CAk CA jaulkitzaileari jakinarazten badio jatorrizko ziurtagiriaren eskaera ez zela baimendu eta ez duela atzeraeraginezko baimenik onartzen.
3. CA jaulkitzaileak lortutako ebidentziaren arabera, ziurtagiriaren gako publikoari dagokion mendeko CAren gako pribatua arriskupean badago, edo BRen 6.1.5 eta 6.1.6 ataletako eskakizunak betetzeari utzi badio.
4. CA jaulkitzaileak ziurtagiria oker jaulki zen ebidentzia lortu badu.
5. CA jaulkitzaileak hauteman badu ziurtagiria ez zela ziurtapen-politikaren edo ZPDaren arabera jaulki.
6. CA jaulkitzailea ohartu bada ziurtagirian agertzen den daturen bat okerra edo zehaztugabea dela.
7. CA jaulkitzaileak edo mendeko CAk edozein arrazoiren ondorioz jardunari uzten badio eta ez baditu gaitu beste CA batekin ezeztatze-zerbitzua eskaintzeko akordioak.
8. CA jaulkitzaileak edo mendeko CAk, BRen eskakizunen mende, ziurtagiriak jaulkitzeko duten eskubidea amaitzen bada, edo ezeztatzen bada, salbu CA jaulkitzaileak akordioak gaitu baditu CRL/OCSP biltegia mantentzen jarraitzeko.
9. CA jaulkitzailearen politikak eta/edo ZPDak ezeztatu behar badu.
10. Ziurtagiriaren edukiak edo formatu teknikoak arrisku onartezina badu softwarearen hornitzaileentzat edo hirugarren batzuentzat.
11. Hornitzaileen edo hirugarren batzuen ondorioz (adibidez: CA/Browser Forumek adierazten badu algoritmo / sinadura kriptografiko batek edo gakoaren tamainak arrisku onartezina dakarrela eta ziurtagiri horiek ezeztatu eta ordeztu behar direla denboraldi jakin batez)

Horrez gain, IZENPEren berariazko dokumentazio honetan araututako ziurtagirien kasuan,

1. Harpidedunari, hirugarren batzuei eta Interneteko nabigatzaileei argibide argiak eman beharko dizkiete gako pribatuaren inguruko salaketak edo susmoak aurkezteko, ziurtagirien erabilera okerraren inguruko salaketak edo susmoak aurkezteko, edo ziurtagirien arloko bestelako iruzur, arrisku, erabilera oker edo portaera desegokien inguruko salaketak edo susmoak aurkezteko.
2. IZENPEk jaso eta hurrengo hogeita lau orduren barruan ikertuko ditu arazoen txostenak, eta ziurtagiri horiek ezeztearen gaineko erabakia hartuko du. Dena den, honako irizpide hauek hartuko ditu aintzat:
   - Balizko arazoaren izaera
   - Ziurtagiri baten edo web-orri baten arazoen inguruan jasotako txostenen kopurua
   - Salatzaileen nortasuna
   - Indarrean dagoen legeria

2.7 Ziurtagiria berritzea

Ziurtagiria berritu behar izanez gero, eskatzaileak ziurtagiriak jaulkitzeko ezarritako prozesua jarraitu beharko du. Nolanahi ere, kontuan izan beharko du egiaztapenak 13 hilabetez direla baliozkoak EV ziurtagirietarako eta 39 hilabetez gainerako ziurtagirietarako.

2.8 Ikuskapenak eta gorabeherak

Ikuskapenei eta gorabeheren analisiei dagozkien irizpideak,

- ☐ Kexak edo iradokizunak aurkezteko bideak,
  - Telefono bidez: 902 542 542
  - Mezu elektroniko bidez: info@izenpe.com
  - www.izenpe.eus helbidean dagoen kexa eta iradokizunetarako formularioa beteta.
  - Erregistro-postuetan dauden kexa edo erreklamazioak egiteko inprimakiak beteta.

- ☐ Izandako gorabeheren barne-erregistroa.

  Segurtasun-gorabeherak IZENPEren Segurtasun Batzordeak kudeatzen ditu. IZENPEk ikerketa zabalduko du oharra jaso eta gehienez 24 ordutara, eta egin beharreko ekintzak erabakiko ditu, BRen 4.9.5 ataleko irizpideak kontuan izanik.

- ☐ Ikuskapenen urteko plangintza BRek ezarritako irizpideen arabera egingo da. IZENPEk BRen 8.7 atalean definitutako barne-ikuskapenak ere egingo ditu.
- ☐ IZENPEk gorabeheratzat jotzen dituen kasuak (iruzurrak, phising, eta abar) Anti-Phising Work Group-aren web-gunera bideratuko ditu (www.apwg.org), eta, ziurtagiria jaulki aurretik, eskatzailea edo ordezkaria IZENPEren segurtasun-gorabeheren barneko datu-basean ez daudela egiaztatuko du. Haatik, egoera susmagarrietan ziurtagiriak jaulkitzeko eskubidea du.
- ☐ Ikuskapenak ETSI EN 319 411-1ean oinarrituko dira.

3 ALDAKETAREN KUDEAKETA

Dokumentu honetan egiten diren aldaketak IZENPEren Segurtasun Batzordeak onartuko ditu. Batzorde horrek urtean behin berrikusiko du ZPDa, baita edozein aldaketa egiten denean ere. Berrikuspen horrek ziurtapen-politika guztiak ere hartzen ditu barnean.

ZPDaren aldaketa horiek ziurtagiri bakoitzaren berariazko dokumentazioa eguneratzeko dokumentuan jasoko dira, eta IZENPEk bermatuko du dokumentu hori eguneratuta egongo dela.

Berariazko dokumentazioaren bertsio eguneratuak www.izenpe.eus helbidean kontsultatu ahal izango dira.

4 ALDAKETEN KONTROLA

4.1 0 bertsiotik 1.0 bertsiora

	EPIGRAFEA / ARGIBIDEAK
Aurreko bertsioarekiko eguneratzeak	Eskakizunak 2.2. atalean txertatu dira Eskakizunak 2.1. eta 2.2. ataletan eguneratu dira
Argibideak	Eskakizunak 2.2. atalean eguneratu dira
Formatua eguneratzea	Aurkibidea gehitu da Orri-oina gehitu da
Ezabatzeak	Eskakizunak ezabatu dira 2.1. eta 2.2. ataletan Urtea ezabatu da azalean

4.2 1.0 bertsiotik 1.1 bertsiora

	EPIGRAFEA / ARGIBIDEAK
Aurreko bertsioarekiko eguneratzeak	Domeinua baliozkotzeko eskakizunak eguneratu dira, 2.2.atalean
Ezabatzeak	Grafikoak ezabatu dira 2.3. eta 2.6. ataletan

4.3 1.1 bertsiotik 1.2 bertsiora

	EPIGRAFEA / ARGIBIDEAK
Aurreko bertsioarekiko eguneratzeak	CAA baliozkotzeko eskakizunak eguneratu dira, 2.2.atalean

4.4 1.2 bertsiotik 1.3 bertsiora

	EPIGRAFEA / ARGIBIDEAK
Aurreko bertsioarekiko eguneratzeak	– 1. Sarrera Google Certificate Transparency proiektuaren esparruan, egindako SSL EV eta Egoitza EV ziurtagiri guztiak IZENPErekin hitzarmena duten Log Servers hornitzaileen CT zerbitzuan eman dira argitara. – 1.1. Ziurtagirien deskribapena ▪ Zigilu-ziurtagiriaren erregulazioari dagokion araudia eguneratu da. ▪ Ziurtagirien baliozkotasuna eguneratu da, 1 edo 2 urtekoa izan daiteke. – 1.2. Identifikazioa ▪ OID CA/B FORUM barnean hartu dira. ▪ Ziurtagirien serieko zenbakiek entropiako 64 bit izango dute gutxienez. – 1.3. epigrafea eta hurrengoak Terminologia egokitu da entitate pribatuei EV motako ziurtagiriak egitera. – 14. Xedapen orokorrak ▪ Identifikazio-betebeharrak. Adierazi da IZENPEk beti egiaztatzen duela domeinuaren titulartasuna edo domeinuaren gaineko kontrola. ▪ Ziurtagiriaren harpidedunaren betebeharrak. Gako Publikoa Dibulgatzeko Akordioan (PDS) zehaztutakoak barnean hartu dira. – 1., 2. eta 3. atalak BRak betetzeari buruzko argibideak barnean hartu dira.

4.5 1.3 bertsiotik 1.4 bertsiora

Aurreko bertsioarekiko eguneratzeak	SSL-EV eta Egoitza-EV ziurtagirien politikako OIDa eguneratu da. “1.1 Ziurtagirien deskribapena” atalean adierazi da SSL EV ziurtagiri kualifikatua eta Egoitza EV ziurtagiri kualifikatua kualifikatutzat jotzen direla eIDAS-en arabera. Sarreran adierazi da ziurtagiri guztiak argitaratuko direla CTetan.

Ezabatzeak	Egoitza ziurtagiriaren erreferentzia guztiak ezabatu dira.

4.6 1.4 bertsiotik 1.5 bertsiora

Aurreko bertsioarekiko eguneratzeak	Profil kualifikatuak erantsi dira.

4.7 1.5 bertsiotik 1.6 bertsiora

Aldaketa	Atala
Domeinuaren titulartasuna egiaztatzeko metodo hauek erantsi dira: • Domeinuaren kontaktuari mezu elektroniko eraikia bidaltzea • DNS CAAren kontaktuari mezu elektronikoa bidaltzea • DNS TXT kontaktuari mezu elektronikoa bidaltzea • DNS Lookup	2.2
Ezeztatzeko kausak eta epeak zehaztu dira, azkenetan zein mendeko CAetan	2.6