WEBGUNEETARAKO ZIURTAGIRIEN BERARIAZKO DOKUMENTAZIOA

Ekaina 2015

Bertsio 1.0

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

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

1 Sarrera

Dokumentu honek *Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, SA* (aurrerantzean IZENPE) enpresak jaulkitako ziurtagiriei dagokien *Berariazko dokumentazioa* (edo 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 dokumentuetan *(Baseline Requirements eta EV guidelines* webguneetarako ziurtagiriak jaulkitzeko) xedatzen dena eta ETSIren zehaztapenetan xedatzen dena (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" eta "Egoitza" ziurtagirietan.
- EVCP (Extended Validation Certificates Policy): "Egoitza EV" eta "SSL EV" ziurtagirietan.

Google Certificate Transparency proiektuaren barruan, jaulkitako SSL EV eta Egoitza EV ziurtagiriak IZENPEren CT Log zerbitzuan emango dira argitara, baita Google-en eskakizunak betetzeko IZENPErekin akordioa duten beste log server zerbitzuen beste hornitzaile batzuen zerbitzuan ere.

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	**Egoitza**
SSL OV	**Egoitza EV**
SSL EV	

Ziurtagiri mota horrek web-zerbitzarietan datu-komunikazioak TLS/SSL bidez ezartzea du xede.

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

– *SSL MOTAKO ZIURTAGIRIAK*,

  Egindako balidazioaren arabera, ziurtagiria honelakoa izan daiteke:

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

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

    Ziurtagiri horiek 1, 2 edo 3 urtez izan daitezke baliozkoak.

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

Ziurtagiri hori, kualifikatu gabetzat jotzen dena, antolakundearen egiaztapenaren eta domeinuaren titulartasuna identifikatzeko erabiliko da, eta Interneteko erabiltzaile bati zentzuzko bermea eskainiko dio sartzen ari den webgune horren titulartasuna ziurtagirian identifikatutako antolakundearena dela.

Ziurtagiri horiek 1, 2 edo 3 urtez izan daitezke baliozkoak.

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

  Ziurtagiri hori, kualifikatu gabetzat jotzen dena, antolakundearen egiaztapenaren eta domeinuaren titulartasuna identifikatzeko erabiliko da, eta Interneteko erabiltzaile bati berme sendoa eskainiko dio sartzen ari den webgune horren titulartasuna ziurtagirian identifikatutako antolakundearena dela.

  Ziurtagiri horiek 1 edo 2 urtez izan daitezke baliozkoak.

– *EGOITZA ELEKTRONIKOA MOTAKO ZIURTAGIRIAK*

Zerbitzu Publikoetarako Hiritarren Sarrera Elektronikoari buruzko ekainaren 22ko 11/2007 Legearen esparruan, IZENPEk mota hauetako ziurtagiriak jaulkitzen ditu:

- ***EGOITZA ELEKTRONIKOA,***

  Ziurtagiri kualifikatu gabe honetan egoitzaren titularra den Herri Administrazioa edo administrazio-organo edo -entitatea identifikatzen da.

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

  Ziurtagiri horiek 1, 2 edo 3 urtez izan daitezke baliozkoak.

- ***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 1 edo 2 urtez izan daitezke baliozkoak.

1.2 Identifikazioa

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

ZIURTAGIRIA	OID
SSL DV	1.3.6.1.4.1.14777.1.2.4
SSL OV	1.3.6.1.4.1.14777.1.2.1
SSL EV	1.3.6.1.4.1.14777.6.1.1
Egoitza elektronikoa	1.3.6.1.4.1.14777.1.1.3
EV duen egoitza elektronikoa	1.3.6.1.4.1.14777.6.1.2

1.3 Komunitatea eta erabilera-esparrua

Erabiltzailetzat hartuko dira,

- Ziurtagiriaren eskatzailea, ziurtagiria antolakunde baten izenean eskatzen duen pertsona.
- Ziurtagiriaren harpideduna, ziurtagirian identifikatutako antolakundea.

Erabilera-esparrua. Ziurtagirien titulartasuna duen Herri Administrazioaren edo administrazio-organoaren edo -entitatearen eskumenen esparruan erabiliko dira ziurtagiriak.

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.

CA/Browser Forum-aren dokumentuetan adierazten dena betetzeko eskakizuna hartuko du barnean aldeen artean dagoen legezko tresnak.

Ziurtagiri-harpidedunaren betebeharrak

Harpidedunak Ziurtapen Praktiken Deklarazioan –*Harpidedunaren betebeharrei* buruzko atala– jasotzen diren betebeharrak bete beharko ditu.

2 Eskakizun operatiboak

2.1 Beharrezko dokumentazioaren zerrenda

- **Jaulkitzeko eskaera**, behar bezala beteta eta sinatuta:
  - Eskuzko sinadura bidez
  - Sinadura elektroniko bidez: IZENPEren ziurtagiri onartu bidez edo eskatzailea identifikatzen duen NAN bidez

Eskatzaileak horrela onartuko ditu eskaera sinatzeko datan aplikatzekoak diren *erabilera-baldintzak eta harpidedunaren kontratua*, www.izenpe.com web-orrian argitara emandakoak.

- Erakundearen **IFZ.**
- **Nortasunaren egiaztagiria eta entitate eskatzailearen indarraldia** (ikus 2.2 Eskaera-prozedura atala)
- **Eskatzaileak entitatearen izena erabiltzeko duen ahalmenaren egiaztagiria** (ikus 2.2 Eskaera-prozedura atala)

2.2 Eskaera-prozedura

- ESKATZAILEAK ziurtagiria jaulkitzeko eskaera eta beharrezko dokumentazioa bidali beharko du,
  - IZENPE, SAren helbidera –TOMAS ZUMARRAGA DOHATSUA k., 71 –1.a – 01008 VITORIA-GASTEIZ–.
  - Bitarteko telematiko bidez certservidor@izenpe.net helbide elektronikora.
  - Edo IZENPEren webgunean horretarako antolatutako aplikazioaren bidez.

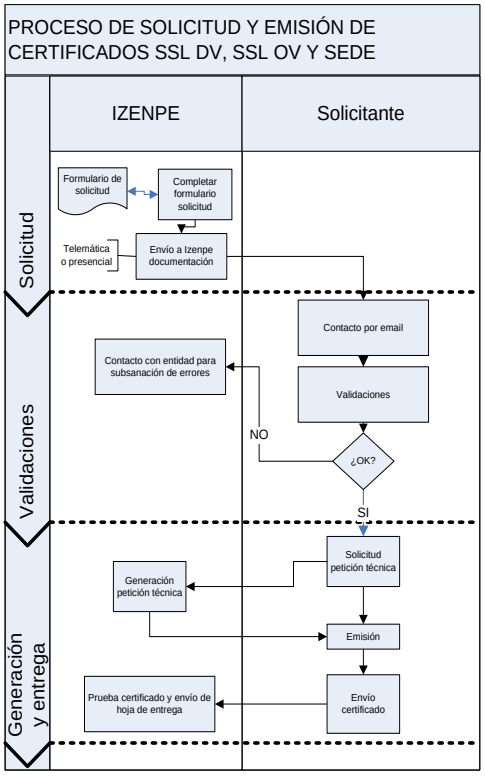
  Jaulkitzeko eskaera sinatuta, eskatzaileak harpidedunaren kontratua eta erabilera-baldintzak onartuko ditu.
- Dokumentazioaren balidazioa,

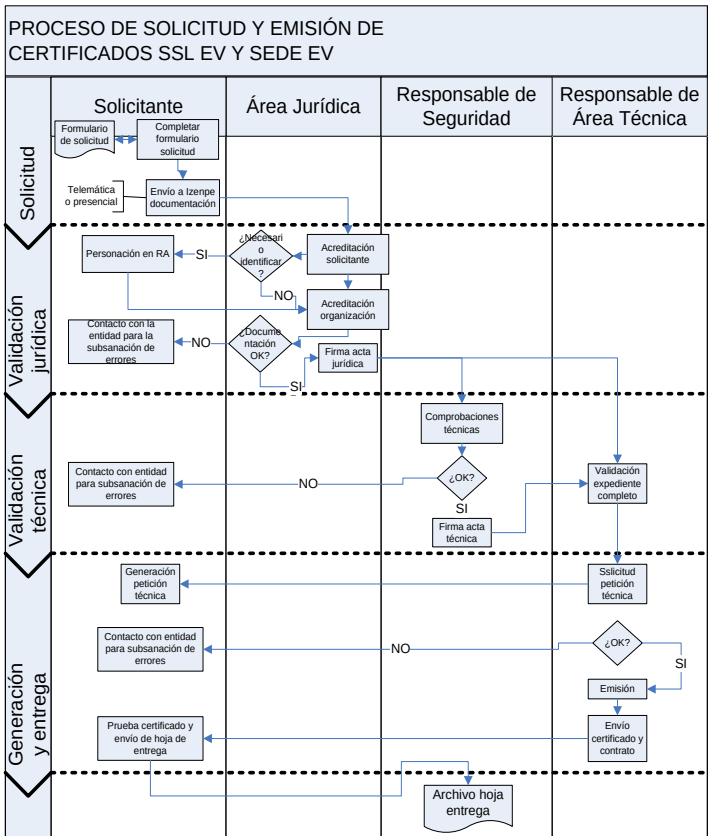
SSL DV **SSL OV** **SSL EV** **Egoitza** **Egoitza EV**	➢ Titularrak (registrant) antolakunde eskatzailearekin bat etorri beharko du. Hala izan ezean, harpidedunak erabiltzeko eskubidea duela egiaztatu beharko du eskatzaileak. Eskatzaileak domeinua edo azpidomeinua erabiltzeko eskubidea duela egiaztatzea. ▪ .es domeinuak: www.nic.es ▪ .eu domeinuak: www.eurid.eu ▪ .eus domeinua: whois.nic.eus ▪ Beste edozen domeinua: whois.icann.org ➢ CAA egiaztatzea, erregistratuta badaude, eta beti RFC 6844aren gidalerroei jarraituta. ➢ SSL DV, SSL OV eta Egoitza egiaztagirien kasuan, wildcard-ak onartuko dira host izenetan edo azpidomeinuetan, betiere entitate eskatzaileak domeinu osoaren legezko kontrola egiaztatzerik badu. Hala izan ezean, eskaera baztertuko da. Esate baterako, ezin izango dira jaulki "*.co.uk" edo "*.local", baina bai "*.adibide.com" Adibide, SA. enpresari.
	➢ Nortasunaren egiaztagiria eta entitate eskatzailearen indarraldia: ○ Entitate publikoan: ▪ Izena*: aldizkari ofiziala, idazkariaren ziurtagiria edo Merkataritza Erregistroa

SSL OV **SSL EV** **Egoitza** **Egoitza EV**	▪ IFK*: Datuak Babesteko Espainiako Agentzia, aldizkari ofiziala edo Merkataritza Erregistroa ○ Entitate pribatuan: ▪ Izena*: dagokion erregistroko jatorrizko ziurtagiria edo informazio-ohar sinplea ▪ IFK*: Datuak Babesteko Espainiako Agentzia, dagokion erregistroko jatorrizko ziurtagiria edo informazio-ohar sinplea ➢ Eskatzaileak entitatearen izena erabiltzeko ahalmenaren egiaztagiria: ○ Entitate publikoan*: idazkariak/letratuak egindako ziurtagiria, informazio-ohar sinplea edo aldizkari ofizialean jasotako erreferentzia, jaulkitzeko eskaeraren aurreko 13 hilabeteetan ○ Entitate pribatuan*: dagokion erregistroko jatorrizko ziurtagiria edo informazio-ohar sinplea * Ez da beharrezkoa, IZENPEk eskatzaileari jaulki dion eta indarrean dagoen ziurtagiri korporatibo onartuaren kasuan edo entitateko ziurtagiriaren kasuan, betiere ziurtagiria azken 39 hilabeteetan jaulki bada (13 hilabete EV ziurtagirien kasuan). ➢ Posta elektroniko bidez egiaztatzea eskatzaileak ziurtagiriaren tramitazioaren berri duela. ➢ Posta helbidea egiaztatzea, • Datuak Babesteko Agentzietan. • Telefono-operadoreen orrietan. • EUDELen, Euskadiko udalerrietarako. • Merkataritza Erregistroa Gaineratutako dokumentazioa eta egiaztatutakoa bat ez badatoz, eskabidean jasoarazi den helbidean erakunde eskatzaileak modu egonkorrean diharduela egiaztatuko du IZENPEk. ➢ Herrialdea egiaztatzea: ○ Datuak Babesteko Espainiako Agentzia, Eudel, Telefono-operadoreen orriak edo Merkataritza Erregistroa ➢ IZENPEren barneko datu-baseetan ukatuen zerrenda egiaztatzea. ➢ Mcafee TrustedSource-ean arrisku handiko eskaerak egiaztatzea
SSL EV **Egoitza EV**	➢ Entitate eskatzailearen telefono finkoaren (ez mugikorraren) zenbakia dela egiaztatzea. Egiaztatzeko iturriak: • Telefono-operadoreen orriak, datuak babesteko agentziak edo Eudel, Euskadiko udalerrietarako. • Ondoren dei bidez egiaztatzea. ➢ Dokumentazioa egiaztatzeko sinadura duala, • Aholkularitza juridikoak. • Eta Arlo Teknikoak. ➢ Arlo Teknikoko arduradunek egindako egiaztapenak balidatzea.

OHARRA:

- IZENPEk egiaztapen gehigarriak egin ahal izango ditu, hala nola: antolakundeak eskaera berrestea, edo eskatzaileari ziurtagiria antolakundearen izenean bideratzeko baimentzea, eta hori betetzen dela urtero berraztertzea, 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, balidazioa duala da.
- Aurreko egiaztapenak egitea ez da beharrezkoa izango informazioa gehienez 13 hilabeteko epean balidatua izan bada, EVetarako, eta 39 hilabeteko epean gainerako ziurtagirietarako.
- IZENPEk EZ du IP helbideak jaulkitzea aintzat hartzen (adib.: 1.2.3.4)





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.

Eskatzaileak Entrega eta Onarpen Orria sinatuta itzuli beharko dio IZENPEri.

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.

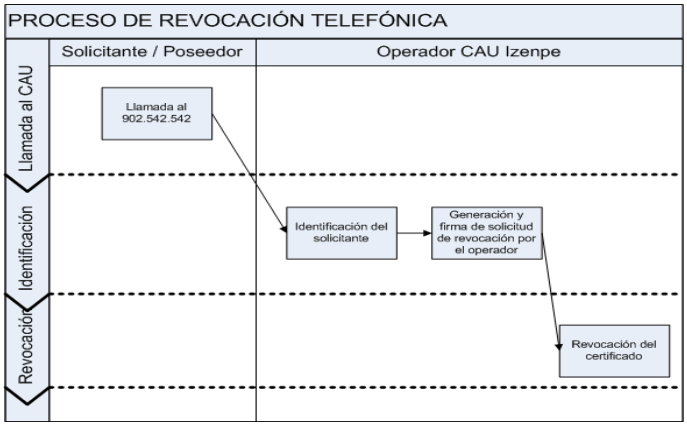
Honako hauek eska dezakete ziurtagiria ezeztatzea:

- Harpidedunak.
  Hauek dute ziurtagiria ezeztatzea eskatzeko baimena: entitate harpidedunaren legezko ordezkariak, langileen arduradunak edo aurreko bietako edozeinek baimendutako hirugarren batek.
- Eskatzaileak.
- IZENPE baimenduta dago azken entitateko harpidedunaren ziurtagiriak ezeztatzea eskatzeko, ZPDan aintzat hartutako kausa teknikoen kasuetan.

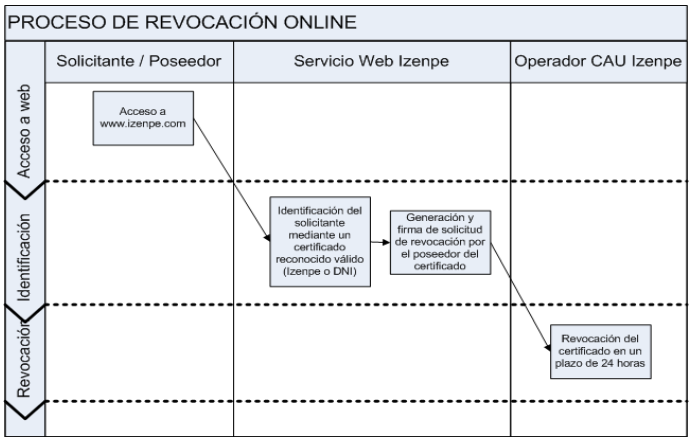
Prozedura

Ezeztatzea eskatzen duenak IZENPEren aurrean bideratuko du ziurtagiria *ezeztatzeko eskaera*.
Ziurtagiria edozein unetan ezeztatu ahal izango 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
  - Webgunearen izen osoa (FQDN)



- On line, www.izenpe.com helbidean.



- Edo posta bidez, Ezeztatzeko Eskaera sinatuta eta notario aurrean legitimatuta bidalita.

Ezeztatzeko arrazoiak

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

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 irizpideak 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 gertakariak

Ikuskapenei eta gertakarien analisiei dagozkien irizpideak,

- ☐ Kexak edo iradokizunak aurkezteko bideak,

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

☐ Izandako gertakarien barne-erregistroa.

Segurtasun-gertakariak IZENPEren Segurtasun Batzordeak kudeatzen ditu.

☐ Ikuskapenen urteko plangintza ETSIk ezarritako irizpideen arabera egingo da.

☐ IZENPEk gertakaritzat jotzen dituen kausak (iruzurrak, phising, eta abar) Anti-Phising Work Group-aren webgunera bideratzen ditu (www.apwg.org). Edonola ere, eta ziurtagiria jaulki aurretik, eskatzailea edo ordezkaria IZENPEren segurtasun-gertakarien barneko datu-basean ez daudela egiaztatzen du IZENPEK. Haatik, egoera susmagarrietan ziurtagiriak jaulkitzeko eskubidea du.

3 Aldaketaren kudeaketa

Dokumentu honetan egiten diren aldaketak IZENPEren Segurtasun Batzordeak onetsiko ditu.

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.com helbidean kontsultatu ahal izango dira.

4 Ziurtagirien profilak eta ezeztatutako ziurtagirien zerrendaren profilak

4.1 SSL DV ziurtagiria

Campo / extensión	Opcional / Crítica	Contenido
version		Versión 3
serialNumber		Número secuencial único
signature		sha256WithRSAEncryption
issuer		Igual al campo subject del certificado de la CA emisora
validity		1, 2 o 3 años
subject		
CN	Opcional	Dominio DNS o dirección IP
OU	Opcional	Departamento
C	Opcional	País
subjectPublicKeyInfo		RSA 2048 bits mínimo
extensions		
issuerAltName		Igual a la extensión subjectAltName del certificado de la CA emisora
subjectAltName		
dNSName		Dominios DNS adicionales
extendedKeyUsage		serverAuth, clientAuth, emailProtection
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.1.2.4 (1.3.6.1.4.1.14777.101.2.4 en Desarrollo), 2.23.140.1.2.1
cpsURI		http://www.izenpe.com/rpaservidor
userNotice		Bermeen mugak ezagutzeko www.izenpe.com Ziurtagirian konfiantza izan aurretik kontratua irakurri. Limitaciones de garantias en www.izenpe.com Consulte el contrato antes de confiar en el certificado
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crlinterna2
authorityInfoAccess		
ocsp		http://ocsp.izenpe.com
CA emisora		http://www.izenpe.com/contenidos/informacion/cas_izenpe/es_cas/adjuntos/AAPPNR_cert_sha256.crt
keyUsage	Opcional	digitalSignature, keyEncipherment

4.2 SSL OV ziurtagiria

Campo / extensión	Opcional / Crítica	Contenido
version		Versión 3
serialNumber		Número secuencial único
signature		sha-256WithRSAEncryption
issuer		Igual al campo subject del certificado de la CA emisora
validity		1, 2 o 3 años
subject		
CN		Dominio DNS o dirección IP
OU	Opcional	Departamento
O		Nombre de la organización
L		Localidad
ST		Provincia
C		País
subjectPublicKeyInfo		RSA 2048 bits mínimo
extensions		
issuerAltName		Igual a la extensión subjectAltName del certificado de la CA emisora
subjectAltName		
dNSName		Dominios DNS adicionales
extendedKeyUsage		serverAuth, clientAuth, emailProtection
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.1.2.1 (1.3.6.1.4.1.14777.101.2.1 en Desarrollo), 2.23.140.1.2.2
cpsURI		http://www.izenpe.com/rpaservidor
userNotice		Bermeen mugak ezagutzeko www.izenpe.com Ziurtagirian konfiantza izan aurretik kontratua irakurri. Limitaciones de garantias en www.izenpe.com Consulte el contrato antes de confiar en el certificado
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crlinterna2
authorityInfoAccess		ocsp http://ocsp.izenpe.com:8094
keyUsage	Opcional	digitalSignature, keyEncipherment

4.3 Egoitza ziurtagiria

Campo / extensión	Opcional / Crítica	Contenido
version		Versión 3
serialNumber		Número secuencial único
signature		sha256WithRSAEncryption
issuer		Igual al campo subject del certificado de la CA emisora
validity		1, 2 o 3 años
subject		
CN		Dominio DNS o dirección IP
serialNumber		CIF
OU		Nombre de la sede
OU		"sede electrónica"
O		Entidad suscriptora
C		ES
subjectPublicKeyInfo		RSA 2048 bits mínimo
extensions		
issuerAltName		Igual a la extensión subjectAltName del certificado de la CA emisora
subjectAltName		
rfc822Name		Email de contacto de la sede
dNSName		Dominio DNS o dirección IP
directoryName		
2.16.724.1.3.5.1.2.1		"sede electrónica"
2.16.724.1.3.5.1.2.2		Entidad suscriptora
2.16.724.1.3.5.1.2.3		CIF
2.16.724.1.3.5.1.2.4		Nombre de la sede
2.16.724.1.3.5.1.2.5		Dominio DNS o dirección IP
extendedKeyUsage		serverAuth
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.1.1.3 (1.3.6.1.4.1.14777.101.1.3 en Desarrollo)
cpsURI		http://www.izenpe.com/cps
userNotice		Bermeen mugak ezagutzeko www.izenpe.com Ziurtagirian konfiantza izan aurretik kontratua irakurri. Limitaciones de garantias en www.izenpe.com Consulte el contrato antes de confiar en el certificado
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crlinterna2
authorityInfoAccess		ocsp http://ocsp.izenpe.com:8094
qcStatements		
QcCompliance		Presente
QcRetentionPeriod		15 años
keyUsage	Crítica	digitalSignature, keyEncipherment

4.4 Egoitza EV ziurtagiria

Campo / extensión	Opcional / Crítica	Contenido
version		Versión 3
serialNumber		Número secuencial único
signature		sha256WithRSAEncryption
issuer		Igual al campo subject del certificado de la CA emisora
validity		1 o 2 años
subject		
CN		Dominio DNS o dirección IP
serialNumber		CIF
OU		Nombre de la sede
OU		"sede electrónica"
O		Entidad suscriptora
C		ES
businessCategory		[OID.2.5.4.15] Valor fijo "Government Entity"
jurisdictionOfIncorporationCountryName		[OID: 1.3.6.1.4.1.311.60.2.1.3] Valor fijo "ES"
subjectPublicKeyInfo		RSA 2048 bits mínimo
extensions		
issuerAltName		Igual a la extensión subjectAltName del certificado de la CA emisora
subjectAltName		
rfc822Name		Email de contacto de la sede
dNSName		Dominio DNS o dirección IP
directoryName		
2.16.724.1.3.5.1.2.1		"sede electrónica"
2.16.724.1.3.5.1.2.2		Entidad suscriptora
2.16.724.1.3.5.1.2.3		CIF
2.16.724.1.3.5.1.2.4		Nombre de la sede
2.16.724.1.3.5.1.2.5		Dominio DNS o dirección IP
extendedKeyUsage		serverAuth
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.6.1.2 (1.3.6.1.4.1.14777.106.1.2 en Desarrollo)
cpsURI		http://www.izenpe.com/cps
userNotice		Bermeen mugak ezagutzeko www.izenpe.com Ziurtagirian konfiantza izan aurretik kontratua irakurri. Limitaciones de garantías en www.izenpe.com Consulte el contrato antes de confiar en el certificado
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crlssiev2
authorityInfoAccess		ocsp http://ocsp.izenpe.com
qcStatements		
QcCompliance		Presente
QcRetentionPeriod		15 años
keyUsage	Crítica	digitalSignature, keyEncipherment

4.5 SSL EV ziurtagiria

Campo / extensión	Opcional / Crítica	Contenido
version		Versión 3
serialNumber		Número secuencial único
signature		sha-1WithRSAEncryption
issuer		Igual al campo subject del certificado de la CA emisora
validity		2 años
subject		
CN		Dominio DNS
OU	Opcional	Departamento
O		Organización
street	Opcional	Calle
L		Localidad
ST		Provincia
C		ES
postalCode	Opcional	Código postal
serialNumber		CIF
businessCategory		[OID.2.5.4.15] Valores posibles: - "Private Organization" para Organización privada - "Government Entity" para Entidad pública - "Business Entity" para Empresa - "Non-comercial Entity" para Entidad no comercial
jurisdictionOfIncorporationLocalityName	Opcional	[OID: 1.3.6.1.4.1.311.60.2.1.1] Localidad en la que está registrada la empresa
jurisdictionOfIncorporationStateOrProvinceName	Opcional	[OID: 1.3.6.1.4.1.311.60.2.1.2] Provincia en la que está registrada la empresa
jurisdictionOfIncorporationCountryName		[OID: 1.3.6.1.4.1.311.60.2.1.3] País en el que está registrada la empresa
subjectPublicKeyInfo		RSA 2048 bits mínimo
extensions		
issuerAltName		Igual a la extensión subjectAltName del certificado de la CA emisora
subjectAltName		
dNSName		Dominios DNS adicionales
basicConstraints		Entidad final
extendedKeyUsage		serverAuth
subjectKeyIdentifier		Identificador de la clave pública
authorityKeyIdentifier		Incluir sólo campo keyIdentifier
certificatePolicies		
policyIdentifier		1.3.6.1.4.1.14777.6.1.1 (1.3.6.1.4.1.14777.106.1.1 en Desarrollo)
cpsURI		http://www.izenpe.com/rpasslev
authorityInfoAccess		ocsp http://ocsp.izenpe.com
cRLDistributionPoints		http://crl.izenpe.com/cgi-bin/crlsslev
keyUsage	Crítica	digitalSignature, keyEncipherment

5 Aldaketen kontrola

5.1 0 bertsiotik 1.0 bertsiora

Eskakizun osagarriak

Eskakizunak 2.2. atalean txertatu dira.

Eskakizun eguneratuak

Eskakizunak 2.1. eta 2.2. ataletan eguneratu dira.

Argibideak

Eskakizunak 2.2. atalean eguneratu dira

Editoriala

Aurkibidea gehitu da.

Orri-oina gehitu da.

Ezabatutako eskakizunak

Eskakizunak ezabatu dira 2.1. eta 2.2. ataletan.

Urtea ezabatu da azalean.