1. SARRERA

ZIURTAPEN ETA ZERBITZU ENPRESA-EMPRESA DE CERTIFICACION Y SERVICIOS IZENPE SA

Dokumentu honek Ziurtapen eta Zerbitzu Enpresa - Empresa de Certificación y Servicios, IZENPE, S.A.k (aurrerantzean, IZENPE) webguneetarako igorritako ziurtagiriei dagokien ziurtapen-politika ezartzen du, bere aldaera desberdinetan.

Helburua da ziurtagiri mota honetarako *IZENPEren Ziurtapen Praktiken Adierazpenean* modu orokorrean definitutakoa zehaztea eta osatzea, bai eta *CA/Browser Forum-aren Baseline Requirements (aurrerantzean, BR), EV gidalerroetan (aurrerantzean, EVBR)* eta ETSIren zehaztapenetan (www.etsi.org) jasotako dokumentu espezifikoetan ere. IZENPEk aipatutako arauen azken bertsio argitaratua onartzen du.

Horrela, IZENPEk ETSIk ezarritako honako ziurtapen-politika hauei jarraitzen die:

- DVCP (Domain Validation Certificate Policy): SSL DV ziurtagirietarako.
- OVCP (Organisational Validational Certification Policy): SSL OV ziurtagirietarako.
- QEVCP -(Erakundearen Baliozkotze Ziurtagirien Politika): SSL Cualificados EV ziurtagirietarako.

Dokumentu honetan jasotako Root CA eta Sub CA 1.3.1. atalean zehazten dira. Egindako

egiaztapen-motaren arabera, IZENPEk honako ziurtagiri hauek igortzen ditu:

- *DOMEINU BIDEZ BALIOZKOTUTAKO SSL (SSL DV),*

Ziurtagiri hau ez da kualifikatua kontsideratzen eta webgunea ostatatzen duen domeinuaren titulartasuna identifikatzeko erabiltzen da. Nabigatzailearen erabiltzaileari domeinuaren zilegitasunari buruzko berme arrazoizkoa eskaintzen dio.

Ziurtagiri horiek 195 eguneko baliozkotasuna dute.

- *ERAKUNDEAK BALIOZKOTUTAKO SSL (SSL OV),*

Ziurtagiri hau ere ez da kualifikatua kontsideratzen eta domeinua eta erakundea identifikatzeko erabiltzen da. Nabigatzailearen erabiltzaileari ziurtagiriaren bidez identifikatutako erakundearen jabetzakoa den webgune batera sartzen ari dela bermatzen dio.

Ziurtagiri horiek 195 eguneko baliozkotasuna dute.

- *BALIOZKOTZE HEDATU KUALIFIKATUKO SSL (SSL EV),*

Ziurtagiri hori kualifikatutzat jotzen da EUROPAKO PARLAMENTUAREN ETA KONTSEILUAREN 2014ko uztailaren 23ko 910/2014 (EB) Erregelamenduaren arabera. Erregelamendu hori 1183/2024 (EB) Erregelamenduak aldatu zuen, identifikazio elektronikoari eta barne-merkatuko transakzio elektronikoetarako konfiantzazko zerbitzuei buruzkoak, eta 1999/93/EE Zuzentaraua (EIDAS Erregelamendua) indargabetzen du. Domeinua eta erakundea identifikatzeko erabiltzen da eta nabigatzailearen erabiltzaileari erakunde identifikatuarena den webgune batera sartzen ari delako

berme sendoa eskaintzen dio.

Ziurtagiri horiek 195 eguneko baliozkotasuna dute.

1.1 Ikuspegi orokorra

Dokumentu honen helburua da IZENPEk igorritako webguneen autentifikazio-ziurtagirien erabiltzaileei aplikatzen zaizkien konfiantzazko zerbitzuen baldintzak eta ezaugarriak arautzea, bai eta IZENPEk bere gain hartzen dituen betebeharrak ezartzea ere, honako hauen harira:

- Ziurtagirien kudeaketa, eta haien eskaera, jaulkipen, erabilera eta baliotasunaren amaierari buruzko baldintza aplikagarriak.
- Ziurtagirien balio-egoeraren kontsulta-zerbitzua ematea, baita zerbitzu horren erabilerari eta eskaintzen diren bermeei dagozkien baldintzak ere.

Horrez gain, dokumentuak barne hartzen ditu, zuzenean edo erreferentzien bidez, honako hauei buruzko xehetasunak: Aurreko paragrafoan deskribatutako zerbitzuak erabiltzen edo horien mende dauden aldeei aplikatzen zaien erantzukizun-araubidea. Prozedura eta instalazioetan aplikatzen diren segurtasun-kontrolak (haien eraginkortasuna arriskuan jarri gabe publiko egin daitezkeen neurrian). Isilpekotasun eta sekretu profesionalaren arauak, baita jabetza, aktiboen titulartasuna, datu pertsonalen babesa eta publikoaren eskura jartzea egokitzat jotzen diren beste informazio-alderdi batzuk ere.

IZENPEk Publikoki fidagarriak diren zerbitzari TLS ziurtagirien igorpen eta kudeaketarako Oinarrizko Baldintzen indarreko bertsiora egokitzen du bere jarduera: https://www.cabforum.org. Dokumentu honen eta aipatutako Oinarrizko Baldintzen artean desadostasunik balego, Oinarrizko Baldintzek izango dute lehentasuna dokumentu honen gainetik.

2026ko apirilaren 15etik aurrera, Ziurtapen Agintaritza (KA) honek SSL/TLS ziurtagiri berriak emateari utzi dio, 2007ko AC ziurtagiriaren pean. Ziurtapeneko Praktiken Deklarazio (PZN) hau indarrean egongo da soilik etete-data baino lehen emandako ziurtagirien kudeaketa, ezeztapena eta egoeraren baliozkotzea arautzeko, epemuga naturalera arte.

1.2 Dokumentuaren izena eta identifikazioa

Dokumentu hau honela izendatzen da: «Ziurtapen Politika – Webguneen Autentifikazio Ziurtagirietarako Ziurtapen Praktiken Adierazpena»

- Bertsioa: 2.9
- Argitaratze-data: 2026/01/19
- Kokapena: http://www.izenpe.eus/s15-content/es/contenidos/informacion/doc_especifica/es_def/index.shtml

Ziurtagirien identifikaziorako, IZENPEk honako objektu-identifikatzaile hauek (OID) esleitu dizkie:

ROOT 2007:

ZIURTAGIRIA	POLITIKAREN OID
DV SSL	1.3.6.1.4.1.14777.1.2.4
OV SSL	1.3.6.1.4.1.14777.1.2.1
SSL kualifikatua	1.3.6.1.4.1.14777.6.1.3

ROOT 2024:

ZIURTAGIRIA	POLITIKAREN OID
DV SSL	1.3.6.1.4.1.14777.50.1.2
OV SSL	1.3.6.1.4.1.14777.50.2.2
SSL kualifikatua	1.3.6.1.4.1.14777.50.3.2

Bertsioen kontrola

VERSIÓN	CAMBIO
1.0	- Eskakizunak gehitu dira 2.2 atalean – 2.1 eta 2.2 ataletako eskakizunak eguneratu dira – 2.2 ataleko eskakizunak eguneratu dira – Aurkibidea gehitu da. – Oin-oharra gehitu da. – Eskakizunak ezabatu dira 2.1 eta 2.2 ataletan. – Urtea kendu da azaletik.
1.1	– Domeinua baliozkotzeko eskakizunak eguneratu dira (2.2 atala). – Irudiak ezabatu dira 2.3 eta 2.6 ataletan.
1.2	CCA baliozkotzeko eskakizunak eguneratu dira (2.2 atala).

1.3	- 1. Sarrera Google Certificate Transparency proiektuaren esparruan, IZENPEk igorritako EV SSL eta EV HQ ziurtagiriak IZENPEk hitzarmena duen Log Server (erregistro-zerbitzari) zerbitzuaren CT zerbitzuan argitaratuko dira. - 1.1. Ziurtagiriaren deskribapena. * Zigilu elektronikoaren ziurtagiriari buruzko araudia eguneratu da. * Ziurtagirien balio-epea eguneratu da: 1 edo 2 urte. - 1.2. Identifikazioa * CA/B FORUMeko OIDak gehitu dira * Ziurtagirien serie-zenbakiek gutxienez 64 bit-eko entropia izan beharko dute. - 1.3 atala eta ondorengoak. EV ziurtagiriak erakunde pribatuentzat igortzeko terminologia egokitu da. - 14. Xedapen orokorrak. * Identifikazio-betebeharrak. Kasu guztietan IZENPEk domeinuaren titulartasuna edo kontrola egiaztatzen duela adierazten da. Ziurtagiriaren sinatzailearen betebeharrak. Gako publikoaren zabalkunde akordioan (PDS) ezarritakoak jasotzen dira. 1, 2. eta 3. atalak. Oinarrizko Eskakizunak (BRak) betetzeari buruzko azalpenak gehitu dira.
1.4	– EV SSL eta EV HQ ziurtagirien politikaren OID eguneratu da. – “1.1. Ziurtagirien deskribapena” atalean adierazten da Qualified EV SSL eta Qualified EV HQ ziurtagiriak eIDAS Erregelamenduaren arabera kualifikatuak direla. – Sarreran zehazten da ziurtagiri GUZTIAK CTetan argitaratuko direla. – HQ ziurtagiriei buruzko erreferentzia guztiak ezabatu dira. –
1.5	- Profil kualifikatuak gehitu dira.
1.6	Domeinuaren titulartasuna egiaztatzeko honako metodo hauek gehitu dira: - Domeinuaren kontaktuari sortutako helbide elektronikoa. - DNS CAA kontaktuari sortutako helbide elektronikoa. - DNS TXT kontaktuari sortutako helbide elektronikoa. - DNS kontsulta (DNS Lookup). - Azken ziurtagirietarako zein Sub CAetarako baliogabetze-arrazoiak eta epeak zehaztu dira.
1.7	Honako elementu hauek gehitu dira: - Ziurtagirien proba-ibilbideak (indarrean dagoena, baliogabetua, iraungia).

	- RSA gakoaren parametroen egiaztapena. - “Aurreziurtagiriaren” definizioa gehitu da. - Bertsio-zenbakia handitzeko betebeharra, aldaketarik egin ez bada ere. Honako elementu hauek ezabatu dira: - IZENPEk gaur egun igortzen dituen profilen EV ziurtagiriak. - Baliogabetze-prozedura: orain Ziurtapen Praktiken Adierazpenera (CPS) bidaltzen da. - IZENPEren CA publikoek barne-domeinuetarako ziurtagiririk igortzen ez dutela zehazten da.
1.8	Dokumentua RFC 3647 egiturara egokitu da.
1.9	– Aldaketen kontrolaren atala bertsioen historiako taula honekin ordezkatu da. – Profil guztien indarraldia 395 egunera eguneratu da. – DNS CAA metodoa ezabatu da. – .eus domeinuetarako Whois metodoa gehitu da.
2.0	- SSL, HQ eta EV SSL ziurtagiri kualifikatuei buruzko erreferentziak ezabatu dira. – IZENPEren posta-helbidea eta helbide elektronikoa eguneratu dira. - Politikaren idazketa orokorra berrikusi da.
2.1	– 3.2.2.1 Identitatea: SSL ziurtagiri kualifikatuen inguruan. Erakundeen egiaztapen-iturrien zerrenda sartu da, CABFORUMen arabera. – Azala: Dokumentuaren tituluaren oin-oharra ezabatu da telefono-zenbakiaren akats bat dela eta.
2.2	– Azala: Dokumentuaren tituluaren oin-oharra ezabatu da telefono-zenbakiaren akats bat dela eta Atalak: -1 “Ziurtagirien Gardentasuna” paragrafoa zuzendu da. - 3.1 atalean, RFC 6962ari buruzko paragrafoa ezabatu da. - 3.2.2.1 Identitatea: egiaztapen-iturrien zerrenda zabaldu da. – 3.2.2.1 Identitatea: SSL ziurtagiri kualifikatuen inguruan. Erakundeen egiaztapen-iturrien zerrenda sartu da, CABFORUMen arabera - 3.2.2.2.4. Balioztapen-metodoak zuzenak dira, baina “c” deskribapena ez dator bat inongo kasurekin; falta da CABFORUM 3.2.2.4.4aren araberako metodoaren deskribapena - 4.1.2 Ezin egiaztatu daitekeen sorrerako informazioa duten erakundeei buruzko erreferentziak ezabatu dira.

	- 4.6 Itzulpenaren zuzenketa: “baliogabetzea” esaten zen, eta “berritzea” izan behar zuen. - 4.4.3 “Ziurtagirien Gardentasuna”ri buruzko zuzenketa - 4.9.6 Berridatzi egin da. - 6.3.2 Akats tipografikoa: 395 zioen tokian 398 esan behar zuen. 6.1.5 “≥” eragilea gehitu zaio 2048 balioari. - 9.1.3 Zuzenketa: “I” letrak IZENPEri egiten dio erreferentzia.
2.3	- Formatuaren homogeneizazioa. - 1., 1.2 eta 1.3.1 atalak aldatu egin dira ROOT berriari buruzko informazioa gehitzeko. - CABFORUMi egindako erreferentziak zuzendu dira. - 3.2.2.2. Gaizki etiketatuta zegoen, 3.2.2.2.2 gisa. - 3.2.2.4. Gaizki etiketatuta zegoen, 3.2.2.2.4 gisa. - 3.2.2.4. 3.2.2.4 atalean BR 3.2.2.4.1en aipamena ezabatu da. - 7.1.8. “UserNotice”-ri egindako aipamen zaharkitua. - 6.1.5 eta 7.1.3 atalak aldatu egin dira ROOT berriari buruzko informazioa gehitzeko.
2.4	- Atalen berridazketa: 1.6.1, 1.6.2, 2.1, 2.2, 4.4.2 - Atal berriak gehitu dira: 1.6.3, 1.6.4, 4.2.4, 5.4.1.1, 4.3.1.1, 4.3.1.2, 4.3.1.3, 7.1.2.1, 7.1.2.1.1, 7.1.2.2, 7.1.3.1,7.1.3.1.1, 7.1.3.1.2, 7.1.3.2, 7.1.3.2.1, 7.1.3.2.2, 7.1.4.1, 7.1.4.2,
2.5	- Ziurtapen Politika (CP) eta Ziurtapen Praktiken Adierazpena (CPS) bateratu egin dira – CP dokumentuan lehen “Ikus CPS dokumentuko dagokion atala” moduan markatuta zeuden atal guztiak CPS dokumentuko dagokion atalarekin ordezkatu dira.
2.6	- 3.2.2.4 atala aldatu da 3.2.2.4.2 metodoa ezabatzeko. – 3.2.2.1 atala aldatu da egiaztapen-iturri berriak gehitzeko.
2.7	– 7.2.2 atala aldatu da «Issuing Distribution Point» luzapena kritikotzat ezartzeko.
2.8	5.7.1.2 Errebokazio masiboko planaren atala.
2.9	195 eguneko iraupeneko SSL ziurtagiriak
3.0	1.1,4.3,5.8 TLS ziurtagiriak emateari uztea 2026ko apirilaren 15ean, 2007ko EAEn.

1.3 PKIko partaideak

Konfiantzazko zerbitzuen kudeaketan eta erabileran inplikatutako alderdiak:

1. Ziurtapen Agintaritza
2. Erregistro Agintaritza

3. Sinatzaileak edo ziurtagirien titularrak
4. Konfiantzazko hirugarren alderdiak
5. Beste partaide batzuk

1.3.1 Ziurtapen-agintaritzak

Politika honen esparruan, IZENPEk honako Ziurtapen Agintaritza hauek ditu:

RAÍZ 2007

Tipo	CN	SHA1 hatz-marka
Root	IZENPE.com	2F783D255218A74A653971B52CA29C45156FE919:
Sub	EAEko Herri Administrazioen CA - CA AAPP Vascas (2)	F79CDA11E7917419A0418DB84BA743C5313AD7F0:
Sub	Certificate CA EV SSL	C68BADE5F069778A003074E619DAB2E7928342D5:

ROOT 2007 ZIURTAPEN-AGINTARITZA

Eremua / Luzapena	Edukia
bertsioa	3. bertsioa
serialNumber	00B0B75A16485FBFE1CBF58BD719E67D:
Eremua / Luzapena	**Edukia**
signatura	sha256WithRSAEncryption:
issuer	
CN	IZENPE.com
EDO	IZENPE S.A.
C	ES
validity	2037/12/13
subject	
CN	IZENPE.com
EDO	IZENPE S.A.

C	ES
SubjectPublicKeyInfo	RSA 4096 bits
extensions	
subjectAltName	
rfc822Name:	info@izenpe.com
directoryName	
KALE	Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz
EDO	IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
subjectKeyIdentifier	1D1C650EA8F2257BB491CFE4B1B1E6BD55746C05:
keyUsage	Ziurtagirien sinadura, CRLen sinadura offline, ziurtagiriak baliogabetzeko zerrenden (CRL) sinadura (06)

SUB ZIURTAPEN-AGINTARITZA: «EAEko Herri Administrazioen CA - CA AAPP Vascas (2)»

Eremua / Luzapena	**Edukia**
bertsioa	3. bertsioa
serialNumber	24C5C8AA566F8EE84CBEA7055CE164A4:
signatura	sha256WithRSAEncryption:
Eremua / Luzapena	**Edukia**
issuer	
CN	IZENPE.com
EDO	IZENPE S.A.
C	ES
validity	2037/12/13
subject	
CN	EAEko Herri Administrazioen CA - CA AAPP Vascas (2)

OU	AZZ Ziurtagiri publikoa - Certificado publico SCA
EDO	IZENPE S.A.
C	ES
SubjectPublicKeyInfo	RSA 4096 bits
extensions	
subjectAltName	
rfc822Name:	info@izenpe.com
directoryName	
KALE	Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz
EDO	IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
subjectKeyIdentifier	C0A94AF7472587FFBCB5A689CE82D246A889EBA3:
authorityKeyIdentifier	1D1C650EA8F2257BB491CFE4B1B1E6BD55746C05:
certificatePolicies	
policyIdentifier	Jaulkipen-jarraibide guztiak
Directive certifier ID	CPS
cpsURI	http://www.izenpe.eus/cps
authorityInfoAccess	
Access method	Ziurtagiriaren online egoera-protokoloa (1.3.6.1.5.5.7.48.1)
Alternative name	
Eremua / Luzapena	**Edukia**
URL address	http://ocsp.izenpe.com:8094
cRLDistributionPoints	http://crl.izenpe.com/cgi-bin/arl2
keyUsage	Ziurtagirien sinadura, CRLen sinadura offline, ziurtagiriak baliogabetzeko zerrenden (CRL) sinadura (06)
Digital footprint	F79CDA11E7917419A0418DB84BA743C5313AD7F0:

SUB ZIURTAPEN-AGINTARITZA: «Certificate CA EV SSL»

Eremua / Luzapena	**Edukia**
bertsioa	3. bertsioa
serialNumber	687DB7171744DA235B3F625A7393F8A5:
signatura	sha256WithRSAEncryption:
issuer	
CN	IZENPE.com
EDO	IZENPE S.A.
C	ES
validity	2028/07/06
subject	
CN	Certificate CA EV SSL
OU	BZ Ziurtagiri publikoa - Certificado publico EV
EDO	IZENPE S.A.
C	ES
SubjectPublicKeyInfo	RSA 4096 bits
extensions	
subjectAltName	
rfc822Name:	info@izenpe.com
directoryName	
KALE	Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz
Eremua / Luzapena	**Edukia**
EDO	IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
subjectKeyIdentifier	C6EDFE77FB51564DFCABD5E3B10C13A3BF54E39B:
authorityKeyIdentifier	1D1C650EA8F2257BB491CFE4B1B1E6BD55746C05:
certificatePolicies	

policyIdentifier	Jaulkipen-jarraibide guztiak
Directive certifier ID	CPS
cpsURI	http://www.izenpe.eus/cps
authorityInfoAccess	
Access method	Ziurtagiriaren online egoera-protokoloa (1.3.6.1.5.5.7.48.1)
Alternative name	
URL address	http://ocsp.izenpe.com
cRLDistributionPoints	http://crl.izenpe.com/cgi-bin/arl2
keyUsage	Ziurtagirien sinadura, CRLen sinadura offline, ziurtagiriak baliogabetzeko zerrenden (CRL) sinadura (06)
Digital footprint	C68BADE5F069778A003074E619DAB2E7928342D5:

RAÍZ 2024

Tipo	CN	SHA1 hatz-marka
Root	ROOT CA SSL IZENPE 2024	68E93296DEEB4254C18C49C4E80F5D8FA3D38A93:
Sub	SUBCA SSL 2024	E3A0E57B82D88AE25E0A488C51C1E40E2AC0DB18:

ROOT 2024 ZIURTAPEN-AGINTARITZA

Eremua / Luzapena	**Edukia**
bertsioa	3. bertsioa
serialNumber	1BE568F081EDFEEE7776604E73FA081E:
signatura	sha384ECDSA:
issuer	
Eremua / Luzapena	**Edukia**
CN	ROOT CA SSL IZENPE 2024
EDO	IZENPE S.A.
C	ES

validity	2049/09/24
subject	
CN	ROOT CA SSL IZENPE 2024
EDO	IZENPE S.A.
C	ES
SubjectPublicKeyInfo	ECC(384 bits)
extensions	
subjectKeyIdentifier	EADC1AEECBD319D1B12B4FDB12CB56795DB2B0EA:
keyUsage	Ziurtagirien sinadura, CRLen sinadura offline, ziurtagiriak baliogabetzeko zerrenden (CRL) sinadura (06)

SUB ZIURTAPEN-AGINTARITZA: «SUBCA SSL 2024»

Eremua / Luzapena	**Edukia**
bertsioa	3. bertsioa
serialNumber	45C858662468EEA028BAEDB26E098D37:
signatura	sha384ECDSA:
issuer	
CN	ROOT CA SSL IZENPE 2024
EDO	IZENPE S.A.
C	ES
validity	2049/09/24
subject	
CN	SUBCA SSL 2024
ORGANIZATIONIDENTIFIER	VATES-A01337260:
Eremua / Luzapena	**Edukia**
EDO	IZENPE S.A.
C	ES

SubjectPublicKeyInfo	ECC(384 bits)
extensions	
subjectKeyIdentifier	5730599CA33DA068ECB3DBCFD555C8AACC5D00A9:
authorityKeyIdentifier	EADC1AEECBD319D1B12B4FDB12CB56795DB2B0EA:
certificatePolicies	
policyIdentifier	Jaulkipen-jarraibide guztiak
Directive certifier ID	CPS
cpsURI	http://www.izenpe.eus/cps
authorityInfoAccess	
Access method	calssuer
URL address	http://www.izenpe.eus/contenidos /informacion/cas_izenpe/es_cas/adjuntos/ izenpe_root_ssl_2024.crt
cRLDistributionPoints	http://crl.izenpe.eus/2024/izsslroot.crl
keyUsage	Ziurtagirien sinadura, CRLen sinadura offline, ziurtagiriak baliogabetzeko zerrenden (CRL) sinadura (06)
Digital footprint	E3A0E57B82D88AE25E0A488C51C1E40E2AC0DB18:

1.3.2 Erregistro-agintaritzak

IZENPE da ziurtagiri hauek igortzeko prozesuan parte hartzen duen Erregistro Agintaritza bakarra. Identifikazio- eta egiaztapen-lanak modu automatizatuan egiten ditu, ziurtagiria Sinatzaileari igorritakoa ziurtagirian agertzen den domeinu-izenaren gaineko benetako kontrolarekin bat datorrela bermatzeko helburuarekin. Kontrol esklusiboa

Ez da inolako egiaztapenik (ez identitateari buruzkoa, ez domeinuaren kontrolari buruzkoa) hirugarren alderdien esku utziko.

1.3.3 Sinatzaileak

Sinatzaileak dira ziurtagiriak jasotzen dituzten pertsona juridikoak, eta Termino eta Baldintzen

dokumentuan ezarritakoaren arabera lotuta geratzen dira.

1.3.4 Konfiantzazko hirugarren alderdiak

Konfiantzazko hirugarren alderdiak dira Interneteko erabiltzaileak, TLS/SSL protokoloen bidez ziurtagiri horiek dituzten webguneekin konexioak ezartzen dituztenak eta haiengan konfiantza izatea erabakitzen dutenak.

1.3.5 Beste partaide batzuk

Xedapenik gabe.

1.4 Ziurtagiriaren erabilera

1.4.1 Ziurtagiriaren erabilera baimenduak

Webguneen autentifikazioko ziurtagiriek webgune bat autentifikatzen dute eta hari igorri zaion pertsona juridikoarekin lotzen dute.

Politika honen arabera igorritako webguneen autentifikaziorako ziurtagiri kualifikatu guztiak ziurtagiri kualifikatuak dira, eIDAS Araudiaren eta honako arau europar hauetan ezarritako betekizunen arabera: ETSI EN 319 411-2 (EBko ziurtagiri kualifikatuak igortzen dituzten konfiantzazko zerbitzu-emaileentzako eskakizunak). ETSI EN 319 412-4 (Webgune ziurtagirien ziurtagiri-profila)

1.4.2 Ziurtagiriaren erabilera debekatuak

Ziurtagiriak igorri ziren funtzio eta helburuetarako soilik erabili behar dira, eta ezin dira beste funtzio edo xede batzuetarako erabili.

Era berean, indarrean dagoen legeria aplikagarriaren arabera erabili behar dira.

Ziurtagiri hauek ez dira diseinatuak, ez dira erabil daitezke, eta ez da baimenik ematen honako erabileretarako: egoera arriskutsuen monitorizaziorako ekipamendu gisa, erroreak onartzen ez dituen funtzionamendua eskatzen duten erabileretarako, hala nola: instalazio nuklearren funtzionamendua, nabigazio- edo aire-komunikazio-sistemak, armamentu-sistemen kontrola eta non akats batek heriotza, zauri larriak edo ingurumenari kalte larriak eragin ditzakeen.

Ziurtagiri baten egoera-baliozkotasunari buruzko informazio-zerbitzua kontsultatu gabe, politika honen arabera igorritako ziurtagirietan konfiantza jartzen duen erabiltzaile edo hirugarren batek ez du politika honen babesik izango, eta ez du erreklamatzeko edo ekintza legalik abiarazteko eskubiderik izango IZENPEren aurka, ziurtagiri horren erabileraren edo konfiantzaren ondoriozko kalte, galera edo gatazkengatik.

IZENPEk espresuki debekatzen du politika honen arabera igorritako ziurtagiriak honakoetarako erabiltzea: komunikazio zifratuei legez kontra eustea edo deszifratzeko (MITM), paketeen ikuskapen sakona (DPI) eta antzeko jarduerak.

1.5 Politikaren administrazioa

1.5.1 Dokumentuaren erakunde erantzulea

IZENPE, helbidea: Tomas Zumarraga Dohatsuaren kalea 71, 1. solairua, 01008 Vitoria-Gasteiz, eta NIF A-01337260, da politika honetan oinarrituta igorritako ziurtagirien Ziurtapen Agintaritza.

1.5.2 Harremanetarako pertsona

Hornitz ailearen izena	**Ziurtapen eta Zerbitzu Enpresa - Empresa de Certificación y Servicios IZENPE SA**
Zuzendaritza	Tomas Zumarraga Dohatsuaren kalea, 71, 1. solairua. 01008 Vitoria-Gasteiz
Helbide elektronika:	izenpe@izenpe.eus

Segurtasun-arazoak jakinarazteko —hala nola gakoaren urraketa susmoak, ziurtagirien erabilera desegokia, iruzurra, baliogabetze-eskaerak edo bestelako gorabeherak— jarri harremanetan: **incidencias@izenpe.eus**.

1.5.3 CPSaren egokitasuna CP honen aldean zehazteko organo erantzulea

IZENPEren Segurtasun Batzordea da CP hau onartzeko ardura duen organoa.

1.5.4 CPSaren onarpen-prozedurak

IZENPEk bere ziurtapen-zerbitzuak kudeatzen ditu eta ziurtagiriak igortzen ditu CA/Browser Forum-ek ezarritako Ziurtagiri Fidagarrien Emisio eta Kudeaketarako Oinarrizko Baldintzen indarreko bertsioaren arabera. Baldintza horiek helbide honetan kontsulta daitezke: https://cabforum.org/baseline-requirements-documents/

IZENPEk urtero berrikusten eta eguneratzen du CP hau, bertsio berriak identifikatu eta www.izenpe.eus webgunean argitaratuz.

1.6 Definizioak eta akronimoak

1.6.1 Definizioak

- ***Solicitante:*** Ziurtagiri bat eskatzen duen (edo berritzen saiatzen den) pertsona fisiko edo juridikoa. Behin ziurtagiria igorrita, eskatzailea Sinatzaile (Subscriber) izendatzen da. Gailuentzako igorritako ziurtagirien kasuan, eskatzailea da ziurtagirian aipatutako gailua kontrolatzen edo ustiatzen duen entitatea, nahiz eta ziurtagiri-eskaera gailuak berak bidali.
- ***CAA:*** RFC 8659aren arabera (http://tools.ietf.org/html/rfc8659): «DNSren Certification Authority Authorization (CAA) baliabide-erregistroak domeinu-izen baten titularrari aukera ematen dio domeinu horretarako ziurtagiriak igortzeko baimena duten Ziurtapen Agintaritza (CA) bat edo gehiago zehazteko. CAA erregistroek CA publiko bati aukera ematen diote kontrol osagarriak ezartzeko, ziurtagiri okerrik ez igortzeko arriskua murrizteko.»
- ***CAren gako-parea:*** Gako-pare bat, non gako publikoa Root CA eta/edo Sub CA ziurtagiri batean edo gehiagotan agertzen den Subject Public Key Info gisa.
- ***Ziurtagiria:*** Sinadura digital bat erabiltzen duen dokumentu elektronikoa, gako publiko bat identitate batekin lotzeko.
- ***Ziurtapen-politika:*** Ziurtagiri jakin baten aplikagarritasuna zehazten duen arau multzoa, komunitate jakin bati eta/edo segurtasun-eskakizun komunak dituen PKI inplementazio bati dagokiona.
- ***Ziurtagiri-gorabeheraren txostena:*** Gakoaren konpromisoa, ziurtagiri baten erabilera desegokia, edo ziurtagiriei lotutako iruzur, erabilera oker edo jokabide desegokiaren susmoari buruzko erreklamazio edo jakinarazpena.
- ***Ziurtagiri-profila*** Ziurtagiriaren edukia eta haren hedapenen eskakizunak zehazten dituzten dokumentu edo fitxategi multzoa, 7. atalean ezarritakoaren arabera; adibidez, CA baten CPS dokumentuko atal bat edo CA softwareak erabiltzen duen ziurtagiriaren txantiloia.
- ***Ziurtagiriak baliogabetzeko zerrenda (CRL):*** Aldian-aldian eguneratzen den eta denbora-zigilua duen zerrenda, bertan CA batek baliogabetutako ziurtagiriak jasotzen dira; zerrenda hori ziurtagiri horiek igorri dituen CAk sortu eta sinatzen du digitalki.
- ***Ziurtagirien gardentasuna (CT)***: Webguneen autentifikazio-ziurtagirien gainbegiratze-esparru irekia, non ziurtagiri horietako bat jaulkitzen denean, CT erregistroetan argitaratzen den. Horrela, domeinuaren titularrek euren domeinuetarako igorritako ziurtagiriak gainbegiratu eta oker igorritako ziurtagiriak detekta ditzakete.
- ***Ziurtapen-agintaritza (CA):*** Ziurtagiriak sortu, igorri, baliogabetu eta kudeatzeaz arduratzen den erakundea. Termino honek bai Root CAei, bai Sub CAei egiten die erreferentzia.
- ***Ziurtapen Praktiken Adierazpena (CPS):*** Ziurtagiriak sortu, igorri, kudeatu eta erabiltzeko gobernantza-esparrua osatzen duten dokumentuetako bat.
- ***Domeinuaren kontaktua:*** Domeinu-izenaren titular, kontaktu tekniko edo administratibo gisa erregistratutako pertsona edo entitatea. WHOIS erregistroan, DNS SOA erregistroan edo Domeinu-izenaren Erregistratzailearekin harreman zuzenaren bidez agertzen dena.
- ***Domeinu-etiketa:*** RFC 8499aren arabera (http://tools.ietf.org/html/rfc8499): «Domeinu-izen baten parte den zero edo gehiagoko oktetoen zerrenda ordenatua. Grafoen teoriaren arabera,

etiketa batek nodo bat identifikatzen du domeinu-izen posible guztien grafoko zati batean.»

- ***Domeinu-izena:*** Domeinu Etiketen zerrenda ordenatua, Domeinu Izenen Sistemako (DNS) nodo bati esleitua.
- ***eIDAS Erregelamendua:*** (EB) 910/2014 Erregelamenduari egiten dio erreferentzia, 1183/2024 (EB) Erregelamenduak aldatua.
- ***CA igorlea:*** Ziurtagiri jakin bati dagokionez, ziurtagiri hori igorri duen CA da. Root CA edo Sub CA izan daiteke.
- ***Gakoaren arriskua:*** Gako pribatu bat arriskuan dagoela esaten da haren balioa baimenik gabeko pertsona bati agerian utzi bazaio edo pertsona horrek hura atzitu badu.
- ***Gako-parea:*** Gako pribatu batek eta hari dagokion gako publiko batek osatzen duten multzoa.
- ***Objektu-identifikatzailea:*** Identifikatzaile alfanumeriko edo numeriko bakarra, Nazioarteko Normalizazio Erakundearen (ISO) estandar aplikagarriaren arabera erregistratua, objektu edo objektu-mota jakin bati esleitua.
- ***OCSP zerbitzaria:*** CAren autoritatearen pean jarduten duen lineako zerbitzaria, haren Errepositorioarekin konektatua, ziurtagirien egoerari buruzko eskaerak prozesatzeko ardura duena. Ikus ere: Online Certificate Status Protocol.
- ***Gako pribatua:*** Bere titularrak sekretupean gordetzen duen gako-parearen gakoa, sinadura digitalak sortzeko eta/edo gako publikoarekin zifratutako fitxategiak edo erregistro elektronikoak deszifratzeko erabiltzen dena.
- ***Gako publikoa:*** Gako pribatuaren titularrak publikoki zabal dezakeen gako-parearen gakoa, hirugarren konfiantzazko alderdiek sinadura digitalak egiaztatzeko eta/edo mezuak zifratzeko erabil dezaketen gakoa, mezu horiek gako pribatua erabiliz soilik deszifra daitezkeelarik.
- ***Gako publikoaren azpiegitura:*** Ziurtagiriak eta gakoak gako publikoan oinarritutako kriptografiaren bidez fidagarritasunez sortu, igorri, kudeatu eta erabiltzea ahalbidetzen duen hardware, software, pertsona, prozedura, arau, politika eta betebeharren multzoa.
- ***Ausazko balioa:*** CAk eskatzaileari zehazten dion balioa, gutxienez 112 bit-eko entropia duena.
- ***Erregistro-agintaritza (RA):*** Ziurtagirien subjektuen identifikazio eta autentifikazioaz arduratzen den erakunde juridikoa, CA ez dena eta, beraz, ez duena ziurtagiririk sinatzen edo igortzen. RA batek ziurtagiri-eskaera eta/edo baliogabetze-prozesuetan parte har dezake. RA terminoa rol edo funtzio bat deskribatzeko adjektibo gisa erabiltzen denean, ez du zertan entitate bereizi bat izan; CA beraren parte izan daiteke.
- ***Datu-iturri fidagarria:*** Subjektuaren identitatea egiaztatzeko erabiltzen den identifikazio-agiria edo datu-iturri bat, enpresa eta administrazio publikoek fidagarritzat jotzen dutena, eta ziurtagiri bat lortzeko helburuaz bestelako xede batekin hirugarren batek sortua.
- ***Konfiantzazko hirugarren alderdia:*** Ziurtagiri baliagarri batean konfiantza duen pertsona fisiko edo erakunde juridikoa. Aplikazio-softwarearen hornitzaile bat ez da hirugarren konfiantzazko alderditzat hartzen banatzen duen softwareak ziurtagiriarekin lotutako informazioa soilik bistaratzen badu.
- ***Biltegia:*** PKIren gobernantzako dokumentu publikoak (adibidez, CP, CPS) eta ziurtagirien egoera jasotzen dituen online datu-basea, CRL edo OCSP erantzun moduan.

- ***Root CA:*** Goiko mailako ziurtapen-agintaritza, bere Root ziurtagiria aplikazio-softwarearen hornitzaileek banatzen dutena eta Sub CAei ziurtagiriak igortzen dizkiena.
- ***Root ziurtagiria:*** Root CAk bere burua identifikatzeko eta Sub CAei igorritako ziurtagirien egiaztapena ahalbidetzeko auto-sinatutako ziurtagiria.
- ***Subjektua:*** Ziurtagiri batean subjektu gisa identifikatutako pertsona fisikoa, gailua, sistema, unitatea edo erakunde juridikoa. Subjektua izan daiteke Sinatzailea bera edo haren kontrolpean eta ustiapenean dagoen gailua.

- ***Subjektuaren identifikazio-informazioa:*** Ziurtagiriaren subjektua identifikatzen duen informazioa. Ez du barne hartzen subjectAltName hedapenean zerrendatutako domeinu-izena, ezta subjektuaren commonName eremua ere.
- ***Sub CA:*** Bere ziurtagiria Root CA batek edo beste Sub CA batek sinatutako ziurtapen-agintaritza.
- ***Harpideduna:*** Ziurtagiria jasotzen duen pertsona fisiko edo erakunde juridikoa, eta sinatzailearen akordio baten edo erabilera-baldintzen bidez legez lotuta geratzen dena.
- ***WHOIS:*** Domeinu-izenaren erregistratzailearengandik edo erregistroaren operadorearengandik zuzenean berreskuratutako informazioa, RFC 3912an definitutako protokoloaren bidez, RFC 7482an definitutako RDAP protokoloaren bidez, edo HTTPS bidezko webgune baten bidez.
- ***Wildcard ziurtagiria:*** Ziurtagiri bat, non gutxienez wildcard domeinu-izen bat jasotzen den ziurtagiriaren Subject Alternative Name eremuan.

1.6.2 Akronimoak

- **CA:** Ziurtapen Agintaritza
- **CAA:** Ziurtapen Agintaritzaren Baimena
- **CN:** Izen Arrunta
- **CP:** Ziurtapen Politika
- **CPS:** Ziurtapen Praktiken Deklarazioa
- **CRL:** Ziurtagiriak Baliogabetzeko Zerrenda
- **CT:** Ziurtagirien Gardentasuna
- **DNS:** Domeinu Izenen Sistema
- **DN:** Izen Bereizia
- **EIDAS:** eIDAS Erregelamendua
- **ETSI:** Telekomunikazio Arauen Europako Institutua
- **EV:** Balioztapen Hedatua
- **FQDN:** Domeinu Izen Kualifikatua
- **HSM:** Hardwarearen segurtasun-modulua: Gako kriptografikoak sortzeko eta babesteko gailua.
- **HTTP:** Hipertestuaren Transferentzia Protokoloa
- **ISO:** Normalizaziorako Nazioarteko Erakundea
- **OCSP:** Online Ziurtagirien Egoera Protokoloa

- **OID:** Objektu Identifikatzailea
- **OV:** Erakundearen Balioztapena
- **PDS:** PKIren Zabalkundearen Adierazpena
- **PKI Public Key:** Azpiegitura
- **PKCS:** Gako Publikoaren Kriptografia Arauak
- **RA:** Erregistro Agintaritza
- **TLS/SSL:** Garraio Geruzaren / Konexio Seguruko Geruzaren Segurtasun Protokoloa
- **UTC:** Denbora Unibertsal Koordinatua

1.6.3 Erreferentziak

Dokumentua	Izenburua
ETSI EN 319 401	Sinadurak eta Azpiegitura Elektronikoak (ESI); Konfiantzazko Zerbitzu-emaileentzako politika orokorren eskakizunak
ETSI EN 319 403	Sinadurak eta Azpiegitura Elektronikoak (ESI); Konfiantzazko Zerbitzu-emailearen bateragarritasunaren ebaluazioa – Ebaluazio-erakundeentzako eskakizunak
ETSI EN 319 411-1	Ziurtagiriak igortzen dituzten Konfiantzazko Zerbitzu-emaileentzako politika- eta segurtasun-eskakizunak; 1. zatia: Eskakizun orokorrak
ETSI EN 319 411-2	Ziurtagiriak igortzen dituzten Konfiantzazko Zerbitzu-emaileentzako politika- eta segurtasun-eskakizunak; 2. zatia: EBko ziurtagiri kualifikatuak
ETSI EN 319 421	Denbora-zigiluak igortzen dituzten Konfiantzazko Zerbitzu-emaileentzako politika- eta segurtasun-eskakizunak
RFC 2119	RFCetan derrigortasun-mailak adierazteko erabilitako gako-hitzak
RFC 3492	Punycode: Unicode Bootstring kodeketa, nazioartekotutako domeinu-izenetarako (IDNA)
RFC 3647	Interneteko X.509 Gako Publikoaren Azpiegitura: Ziurtapen-politika eta ziurtapen-praktiken esparrua
RFC 3986	Punycode: Baliabide Identifikatzaile Uniformea (URI): Sintaxi orokorra
RFC 5280	Interneteko X.509 PKI ziurtagiri eta baliogabetze-zerrenden (CRL) profila
RFC 6960	X.509 PKIrako OCSP protokoloa (Online Certificate Status Protocol)

RFC 6962	Ziurtagirien Gardentasuna
RFC 8737	Ziurtagiriak automatikoki kudeatzeko ingurunea (ACME): TLS Aplikazio Protokoloaren ALPN luzapena

1.6.4 Konbentzioak

Dokumentu honetan agertzen diren «behar du», «ez du behar», «derrigorrezkoa», «beharrezkoa da», «ez da beharrezkoa», «behar luke», «ez luke behar», «gomendatua», «daiteke» eta «aukerazkoa» bezalako gako-hitzak RFC 2119n deskribatzen den moduan interpretatuko dira.

2. BILTEGIAREN ARGITALPENA ETA ERANTZUKIZUNAK

2.1 Biltegiak

IZENPEk informazio publikoaren biltegi bat du www.izenpe.eus webgunean eskuragarri, eguneko 24 orduetan eta asteko 7 egunetan. Bertan, CP/CPS dokumentuak, Root ziurtagiriak eta Sub CA ziurtagiriak kontsulta daitezke.

2.2 Ziurtapen-informazioaren argitalpena

CP honek estaltzen dituen ziurtagiri elektronikoen igorpenari buruzko informazioa www.izenpe.eus webgunearen bidez dago eskuragarri, eta informazio hau barne hartzen du:

- Ziurtapen-politika eta ziurtapen-praktiken adierazpena.
- Ziurtagiri-profilak eta baliogabetze-zerrendak.
- PKI Informazioaren Adierazpenak (PDS).
- Ziurtagirien erabilera-baldintzak, legez loteslea den tresna gisa.
- IZENPEren Root ziurtagiriak eta Sub CAak deskargatzeko aukera, informazio osagarriarekin batera.

IZENPEk beharrezko neurri guztiak hartuko ditu biltegi hau etengabe erabilgarri egon dadin

bermatzeko. Aplikazio-softwarearen hornitzaileek beren garapenak probatu ditzakete honako helbide

hauek erabiliz:

ROOT 2007 |Egoera|URLa| |-|-| |Baliozkoa|https://test-ev-qualified.izenpe.eus/| |Iraungia|https://test-expired-ev.izenpe.eus/| |Baliogabetua|https://test-revoked-ev.izenpe.eus/|

ROOT CA SSL IZENPE 2024 |Egoera|URLa| |-|-| |Baliozkoa|https://test-valid-ev-2024.izenpe.eus| |Iraungia|https://test-expired-ev-2024.izenpe.eus| |Baliogabetua|https://test-revoked-ev-2024.izenpe.eus|

2.3 Argitalpenaren maiztasuna edo unea

IZENPEk urtero berrikusten ditu bere ziurtapen-politikak eta praktikak, eta dokumentu hau eguneratzen du, dokumentu honetako «1.5.4 Onarpen-prozedura» atalean ezarritako jarraibideen arabera.

CP/CPS dokumentuetan egindako edozein aldaketa berehala argitaratuko da.

CRLen argitalpen-maiztasuna dokumentu honetako 4.9.7 «CRLen sorkuntza-maiztasuna» atalean definituta dago.

2.4 Biltegirako sarbide-kontrolak

IZENPEk irakurketa-soileko sarbidea ematen dio bere biltegian argitaratutako informazioari, eta kontrolak ezartzen ditu honako hauetarako: Baimenik gabeko pertsonek zerbitzuko erregistroak gehitzea, aldatzea edo ezabatzea saihestea. Gordetako informazioaren osotasuna eta egiazkotasuna babestea. Horretarako, IZENPEk sistema fidagarriak erabiltzen ditu, honako hau ziurtatzeko:

- Soilik baimendutako pertsonek egin ditzaketela anotazioak edo aldaketak.
- Argitaratutako informazioaren egiazkotasuna egiaztatzeko.
- Ziurtagiriak jendaurreko kontsultarako eskuragarri egoteko.
- Segurtasun-eskakizunei eragiten dieten aldaketa teknikoak detektatzeko.

3. IDENTIFIKAZIOA ETA AUTENTIFIKAZIOA

3.1 Izenen esleipena

Ziurtagirien kodeketa RFC 5280 estandarraren arabera egiten da: "Interneteko Gako Publikoaren Azpiegiturako X.509 Ziurtagiriaren Profila eta Ziurtagiriak Baliogabetzeko Zerrenda (CRL)". CPS eta CP dokumentuetan ziurtagiri-profilean definitutako eremu guztiak, esplizituki bestelakorik adierazten ez bada, UTF8String kodeketa erabiliz idazten dira.

Gainera, SSL ziurtagiri kualifikatuen kasuan, IZENPEk Balioztapen Hedatuaren azken gidalerroetan ezarritako betekizunak beteko ditu, hemen eskuragarri: https://cabforum.org/working-

groups/server/extended-validation/guidelines/.

3.1.1 Izen-motak

CP honek estaltzen dituen azken entitateko ziurtagiri elektronikoek Subject Name eremuan izen bereizi bat (DN) dute, eta horren osaera ziurtagiri-profilean ezarritako informazioan oinarritzen da (dokumentu honetako 7.1 atala). IZENPEk betetzen ditu X.500, RFC 5280 eta CA/Browser Forum-ek (BR eta EVG) ezarritako eskakizunak.

Common Name eremuak ziurtagiriaren sinatzailea definitzen du.

3.1.2 Izenak esanguratsuak izateko beharra

Subject Name eremuan sartutako izen bereizi (DN) guztiak esanguratsuak dira. Ziurtagiriaren sinatzaileari lotutako atributuen deskribapena pertsonentzako irakurgarria da (ikus dokumentu honetako 7.1.4 atala: “Izenen formatua”).

Subject Distinguished Name eremua ere CA/Browser Foroak ezarritako 9.2 atalean jasotako betekizunen mende egongo da, balioztatze zabaldutako ziurtagirien jaulkipen eta kudeaketarako gidaren barruan, kontsulta daitekeena hemen: https://cabforum.org/extended-validation/.
IZENPEk ez du wildcard ziurtagiririk igortzen EV politiken pean.

3.1.3 Sinatzaileen anonimotasuna edo ezizenaren erabilera

Ziurtapen Politika honen arabera, IZENPEk ez du ezizenik onartzen.

3.1.4 Izenen forma desberdinak interpretatzeko arauak

ISO/IEC 9594 arauak ezarritako X.500 estandarrean definitutako eskakizunak aplikatzen dira.

3.1.5 Izenen bakartasuna

Ziurtagiriaren sinatzaileari emandako izen bereizia (DN), Konfiantzazko Zerbitzu-emailearen domeinuan, bakarra izan beharko da.

3.1.6 Marka komertzialen aintzatespena, autentifikazioa eta rola

Ziurtagiri-eskatzaileek ez dute izenik sartu behar ziurtagiri-eskaeretan, balizko sinatzaileak hirugarrenen eskubideak urratzeko arriskua izan dezakeenik.

IZENPEk ez du zehazten eskatzaileak ziurtagiri-eskaeran adierazitako izenaren gaineko eskubiderik duenik. Era berean, IZENPE ez da epaile, bitartekari edo arbitro gisa jarduten, ez eta pertsona, erakunde edo domeinu-izenen jabetzari buruzko auziak ebazten ere.

IZENPEk eskubidea gordetzen du ziurtagiri-eskaera baztertzeko, proposatutako izenarekin gatazka bat badago.

3.2 Hasierako identitate-balioztapena

IZENPEk webguneen autentifikazio ziurtagirietan jasotako informazioa balioztatzeko prozesua egiten du, CA/Browser Forum-ek ezarritako "Ziurtagiri fidagarrien jaulkipen eta kudeaketarako Oinarrizko Eskakizunak" dokumentuan oinarrituta. Eskura daitezke hemen: https://cabforum.org/working-groups/server/baseline-requirements/requirements/.

Horrez gain, SSL ziurtagiri kualifikatu bat igorri aurretik, IZENPEk bermatzen du ziurtagiri mota horietan sinatzaileari buruz jasotako informazio guztia: CA/Browser Forum-ek ezarritako «Balioztapen Hedatuko Ziurtagiriak igortzeko eta kudeatzeko Gida»ren 11. atalean definitutako eskakizunak betetzen dituela eta aipatutako eskakizunen arabera egiaztatu dela. Gida hori hemen kontsulta daiteke: https://cabforum.org/working-groups/server/extended-validation/guidelines/

IZENPEk atal honetan egindako baieztapen guztiak erregistratzen ditu, aldizkako barne-auditoriako eta auditoria independenteko prozesuen parte gisa.

3.2.1 Gako pribatua edukitzearen frogapena egiteko metodoa

IZENPEk PKCS#10 formatuan egindako ziurtagiri-eskaera bat jasotzen du, sinatzailearen ordezkariak bere ingurunean sortutako gako pribatuz sinatua eta gako pribatu horrekin lotutako gako publikoa barne hartzen duena.

3.2.2 Erakundearen identitatearen autentifikazioa

Ziurtagiri bat lehen aldiz eskatu aurretik, IZENPEk erakundea bere sisteman aurrez erregistratzea eskatzen du, ordezkari baten baimenarekin. Prozesu horretan, erakundearen eta ordezkariaren informazioa iturri fidagarri baten bidez balioztatuko da, 3.2.2.1 atalean ezarritakoaren arabera, eta informazio hori erabiliko da gero OV eta EV ziurtagiriak igortzeko.

3.2.2.1 Nortasuna

IZENPEk ez du webguneen autentifikaziorako ziurtagiririk igortzen sinatzailea pertsona fisiko bat denean.

- DV ziurtagirien kasuan, IZENPEk ez du erakunde sinatzailearen identitatea ezta bestelako informaziorik egiaztatzen.

- OV ziurtagirien kasuan,
    - IZENPEk erakunde sinatzailearen helbide posta eta identitatea egiaztatzen ditu,

entitate mota (pribatua edo publikoa) kontuan hartuta:

- Sinatzailea sektore pribatuko erakunde bat bada, IZENPEk bere identitatea eta helbidea egiaztatzen ditu dagokion erregistro ofiziala kontsultatuz.

Erakunde publiko baten kasuan, egiaztapena dagokion Aldizkari Ofiziala eta erreferentzia gisa erabiltzen diren beste erregistro publiko batzuk kontsultatuz egiten da.

IZENPEk balioztatzen du ziurtagiria eskatzen duen erakundearen izena eta helbide postala ofizialki erregistratutako datuekin bat datozela, goian deskribatutakoaren arabera.

- SSL ziurtagiri kualifikatuen kasuan,

IZENPEk erakundearen existentzia, helbidea eta identitatea egiaztatzen ditu, entitate motaren arabera:

- Sinatzailea sektore pribatuko erakunde bat bada, IZENPEk bere identitatea eta helbidea egiaztatzen ditu dagokion erregistro ofiziala kontsultatuz.
- Erakunde publiko baten kasuan, egiaztapena dagokion Aldizkari Ofiziala eta erreferentzia gisa erabiltzen diren beste erregistro publiko batzuk kontsultatuz egiten da.

Kasuen hauetan IZENPEk erabiliko dituen egiaztapen-iturriak honako hauek dira:

BERTSIOA	DATA
3	2025/06/19

Deskribapena	URL	PAIS	PROVINCIA
EUSKAL HERRIKO ALDIZKARI OFIZIALA	https://www.euskadi.eus/y22-bopv/es/bopv2/datos/Ultimo.shtml	ES	EUSKADI
DIARI OFICIAL DE LA GENERALITAT DE CATALUNYA	https://dogc.gencat.cat/es/inici/index.html	ES	CATALUNYA
TOKI ERAKUNDEEN ERREGISTROA	https://www.euskadi.eus/registro-de-entidades-locales/web01-a2tokiad/es/	ES	EUSKADI
Justizia Ministerioa – Erakunde Erlijiosoen	https://maper.mjusticia.gob.es/Maper/buscarRER.action	ES	

Erregistroa			
ZERGA AGENTZIA	https://www10.agenciatributaria.gob.es/wlpl/BURT-JDIT/ws/VNifV2SOAP	ES	
MERKATARITZA ERREGISTROA	https://sede.registradores.org/site/invitado/mercantil/busqueda#/	ES	
SEKTORE PUBLIKOKO ERAKUNDEEN INBENTARIOA	https://www.pap.hacienda.gob.es/invente2/pagMenuPrincipalV2.aspx/	ES	
ESPAINIAKO BANKUA	www.bde.es	ES	
ESTATUKO ALDIZKARI OFIZIALA	https://www.boe.es/buscar/boe.php	ES	
BIZKAIKO ALDIZKARI OFIZIALA	https://apps.bizkaia.eus/BT00/	ES	BIZKAIA
GIPUZKOAKO ALDIZKARI OFIZIALA	https://egoitza.gipuzkoa.eus/es/bog	ES	GIPUZKOA
ARABAKO ALDIZKARI OFIZIALA	https://www.araba.eus/botha/	ES	ALAVA/ARABA
EUSKAL HERRIKO ALDIZKARI OFIZIALA	https://www.euskadi.eus/y22-bopv/es/p43aBOPVWebWar/	ES	EUSKADI
Deskribapena	**URL**	**PAIS**	**PROVINCIA**
PAIS	buscarAvanzada.do?idioma=es&tipoBusqueda=2		

EUSKADIKO ELKARTEEN ERREGISTROA	https://www.euskadi.eus/ registro-asociaciones-buscador/ web01-a2aderre/es/	ES	EUSKADI
SEKTORE PUBLIKOKO ERAKUNDEEN INBENTARIOA	https://www.pap.hacienda.gob.es/ invente2/pagMenuPrincipalV2.aspx/	ES	
NAFARROAKO TOKI ERAKUNDEAK	https://www.navarra.es/es/ buscador-de-entidades-locales	ES	NAVARRA
SINDIKATU- ETA ENPRESA-ERAKUNDEAK	https://expinterweb.mites.gob.es/ deose/publico/expedientes	ES	

IZENPEk ziurtatzen du ziurtagiriaren sinatzaile den erakundearen izena, helbidea eta identifikazio fiskaleko zenbakia eskaeran jasotakoa bat datozela aurrez azaldutako ataletan kontsultatutako erregistro ofizialetan ageri diren datuekin.

IZENPEk CA/Browser Foroak zehaztutako betekizunak beteko ditu, Balioztatze Hedatuko Ziurtagirien (EV) jaulkipen eta kudeaketarako Gidan jasotakoak; gida hori hemen kontsulta daiteke: https://cabforum.org/extended-validation/

3.2.2.2 Izen komertziala edo marka erregistratua

Subjektuaren identifikazio-informazioak izen komertzial bat edo marka erregistratu bat barne hartzen badu, IZENPEk 3.2.2.1 atalean deskribatutako egiaztapen-prozedura eta irizpide berdinak aplikatuko ditu eskatzaileak izen edo marka hori erabiltzeko duen eskubidea egiaztatzeko.

SSL ziurtagiri kualifikatuen kasuan, identitatearen egiaztapen sakona eskatzen da, CA/Browser Forum-eko Balioztapen Hedatuko Ziurtagiriak igortzeko eta kudeatzeko Gidaren 11.3 atalean definitutakoaren arabera.

3.2.2.3 Herrialdearen egiaztapena

Herrialdea 3.2.2.1 atalean zerrendatutako edozein metodo erabiliz egiaztatuko da.

3.2.2.4 Domeinuaren baimena eta kontrolaren balioztapena

Webguneen autentifikazioko ziurtagirietan domeinua balioztatzeko, IZENPEk CA/Browser Forum-en Oinarrizko Eskakizunetako dokumentuan deskribatutako honako metodo hauetako bat erabiltzen du:

- 3.2.2.4.4 Domeinuaren kontaktuari bidalitako mezu elektronikoa
- 3.2.2.4.7 DNSn egindako aldaketa
- 3.2.2.4.14 DNS TXT kontaktuari bidalitako mezu elektronikoa
- 3.2.2.4.18 Webguneko aldaketa adostua – 2. bertsioa
- 3.2.2.4.19 Webguneko aldaketa adostua ACME bidez

IZENPEk dokumentatutako prozedura bat jarraituko du erabilitako metodo bakoitzerako, eta ziurtagiri bakoitzaren igorpen-prozesuan erabilitako metodoa zehazten duten erregistroak gordeko ditu. CA/Browser Forum-en Oinarrizko Eskakizunetan deskribatutako gainerako metodoak ez dira domeinua balioztatzeko erabiltzen..

- Domeinuaren kontaktuari bidalitako mezu elektronikoa (BR 3.2.2.4.4)

  Ausazko balio bat duen mezu elektroniko bat bidaliko zaio eskatutako domeinuko helbide hauetako bati edo batzuei: «admin», «administrator», «webmaster», «hostmaster» edo «postmaster».

- DNSn egindako aldaketa adostua (BR 3.2.2.4.7). Eskatzaileak aldaketa bat egingo du ziurtagiria eskatzen duen domeinuaren DNS erregistroan. Aldaketa honek IZENPEk bidalitako ausazko eta bakarreko kode bat gehitzea dakar, CNAME, TXT edo CAA eremu batean. Behin eskatzaileak aldaketa hori egiten duenean, IZENPEk egiaztapena egingo du.

  IZENPEk ausazko eta bakarreko kode bat emango du ziurtagiri-eskaera bakoitzerako, eta ez du kode hori berrerabiliko 30 egun igaro ondoren.

  Helburu horretarako, CAA sarrera bat egon beharko da «contactemail» motakoa eta baliozko helbide elektroniko batekin, adibidez: CAA 0 contactemail contacto@example.com

  IZENPEk ausazko eta bakarreko kode bat emango du ziurtagiri-eskaera bakoitzerako, eta ez du kode hori berrerabiliko 30 egun igaro ondoren.

- DNS TXT kontaktuari bidalitako mezu elektronikoa (BR 3.2.2.4.14): IZENPEk eskatzaileari ausazko eta bakarreko kode bat bidaltzen dio mezu elektroniko bidez, DNSko TXT erregistroan agertzen den helbidera. «_validation-contactemail» azpidomeinuan TXT sarrera bat egon behar da baliozko helbide elektroniko batekin, adibidez:

  _validation-contactemail.izenpe.eus. 299 IN TXT ‘contacto@example.com’

  IZENPEk ausazko eta bakarreko kode bat emango du ziurtagiri-eskaera bakoitzerako, eta ez du kode hori berrerabiliko 30 egun igaro ondoren.

- DNSn egindako aldaketa adostua (BR 3.2.2.4.18): IZENPEk eskatzaileari eskatzen dio bere webguneko «/.well-known/pki-validation» bide-izenean fitxategi bat argitara dezala, eta bertan IZENPEk aurrez bidalitako ausazko kode bakarra jaso behar da. Behin eskatzaileak aldaketa hori egiten duenean, IZENPEk egiaztapena egingo du.

- Webgunean egindako aldaketa adostua ACME bidez:

Eskatzaileak FQDN baten gaineko kontrola duela egiaztatzen da domeinua balioztatuz, ACME HTTP Challenge metodoa erabiliz, RFC 8555eko 8.3 atalean definitzen den bezala. Ondoren, RFC 8555ean ezarritakoei gehitzen zaizkien eskakizun osagarriak zehazten dira: IZENPEk HTTP eskaerari erantzun arrakastatsua jaso behar du, hau da, HTTP 2xx egoera-kode bat jaso behar da. Tokena (RFC 8555eko 8.3 atalean definitua) ez da 30 egunez baino gehiagoz erabili behar sortu zenetik. CPS dokumentuak ausazko balioetarako iraupen laburragoa ezar dezake. Kasu horretan, CAk bere CPS dokumentuan zehaztutakoa bete behar du. IZENPEk ez du birbideratzerik jarraitzen.

IZENPEk egiaztatzen du sinatzailearen ordezkariak kontrola duela webguneen autentifikazio-ziurtagirietan sartzen diren domeinu-izen osoen (FQDN) gainean. Horretarako, ziurtagiri horien eskaerak erregistratzeko aplikazioaren bidez: IZENPEk egiaztatzen du sinatzailearen ordezkariaren identitatea eta FQDN izena. Ondoren, baieztatzen du eskaera domeinua kontrolatzen duen kontaktu batetik datorrela (aurreko atalean deskribatutako metodoen arabera), edo kontaktu horrek baimena eman diola. Halaber, egiaztatzen du ziurtagiri-eskaera dagokion entitatea erregistratu ondoren egin dela.

Gainera, webguneen autentifikazioko ziurtagiria igorri aurretik, IZENPEk egiaztatzen du: Sartu beharreko domeinua publikoa dela (hau da, ez dela barne-domeinua); eta Erregistro publikoak kontsultatzen dituela domeinua arrisku handikoa ez dela ziurtatzeko, hala nola Google Safe Browsing-ek identifikatutako domeinuak.

3.2.2.5 IP helbide bidezko autentifikazioa

IZENPEk ez du ziurtagiririk igortzen IP helbideen identifikaziorako.

3.2.2.6 Wildcard domeinuen balioztapena

RAk egiaztatu behar du sinatzaileak domeinuaren izen-espazio osoa legez kontrolatzen duela, OV motako wildcard ziurtagirietan.

Ziurtagiri wildcard batean izartxoa domeinu-sufixu publiko baten edo kontrolatutako erregistro baten ezkerreko etiketaren kokalekuan badago, IZENPEk ziurtagiriaren igorpena baztertuko du, eskatzaileak domeinuaren izen-espazio osoaren kontrol legitimoa frogatzen ez badu.

Horretarako, IZENPEk Atzizki Publikoen Zerrenda kontsultatuko du, hemen eskuragarri: https://publicsuffix.org/. IZENPEk zerrenda hau aldian-aldian deskargatuko du erreferentzia eguneratuta mantentzeko.

3.2.2.7 Datu-iturrien fidagarritasuna

Datu-iturri bat datu-iturri fidagarritzat hartu aurretik, IZENPEk haren fidagarritasuna, zehaztasuna eta manipulazio edo faltsutzeekiko erresistentzia ebaluatuko ditu. Ebaluazio horretan kontuan hartuko

diren irizpideak hauek dira:

1. Emandako informazioaren antzinatasuna.
2. Datu-iturria zenbat maiztasunez eguneratzen den.
3. Datuen hornitzailearen identitatea eta informazioa biltzeko helburua.
4. Informazio-iturriaren sarbide publikoa.
5. Datuak faltsutzeko edo aldatzeko zailtasun erlatiboa.

3.2.2.8 CAA erregistroa

Ziurtagiriak igortzeko prozesuaren barruan, IZENPEk CAA erregistroak kontsultatuko eta prozesatuko ditu RFC 8659 estandarraren arabera, subjectAltName hedapenean agertzen den dNSName sarrera bakoitzerako (Onion motako domeinuak izan ezik).

CAA erregistroak prozesatzean, IZENPEk honako jabetza-etiketa hauek prozesatuko ditu: issue, issuewild eta iodef, RFC 8659ean zehaztutako moduan. iodef etiketak ez du derrigorrezko ekintzarik eskatzen, baina IZENPEk errespetatu beharko du baldin eta presente badago. Beste jabetza-etiketa batzuk onar DAITEZKE, baina EZ dute RFCan ezarritako derrigorrezko etiketekin gatazkarik izan edo haiek ordezkatu behar. IZENPEk “critical” adierazlea ERRESPETATUKO du eta ez du ziurtagiririk igorriko adierazle hori aktibatuta daukan eta ezagutzen ez duen etiketa bat aurkitzen badu.

IZENPEk CAA erregistro bat prozesatu ondoren ziurtagiria igortzen badu, hori erregistroaren TTL barruan edo gehienez 8 orduren buruan egin beharko du (bi horietatik handiagoa den epean).

3.2.3 Banakako identitatearen autentifikazioa

IZENPEk egiaztatzen du sinatzailearen ordezkaria webgunearen autentifikazio-ziurtagiria eskatzen duen pertsona fisiko bera dela, eskaera-inprimakia sinadura elektroniko kualifikatu baten bidez sinatuz. Horrek bere identitatearen benetakotasuna bermatzen du.

DV edo OV ziurtagirien kasuan, sinatzailearen ordezkariak beste eskatzaile baimendu batzuei eskaera egiteko gaitasuna delega diezaieke. Delegazio hori sinadura elektronikoz sinatu beharko da SSL ziurtagiriak kudeatzeko aplikazioaren bidez.

3.2.4 Sinatzailearen balioztatu gabeko informazioa

Ziurtagiri elektroniko batean sartutako informazio guztia RAk egiaztatzen du. Beraz, ez da balioztatu gabeko informaziorik sartzen igorritako ziurtagirien ‘Subject’ eremuan.

3.2.5 Agintaritza-balioztapena

IZENPEk egiaztatzen du eskatzaileak ordezkaritza-gaitasun nahikoa duela bezeroaren alta-

inprimakia sinadura elektronikoz sinatuz, eta horretarako IZENPEren ordezkariaren ziurtagiria onartuz, politika honetako 3.2.3 atalean deskribatzen den bezala. Inprimaki hori politika honetako aurreko atalean aipatzen ez den ziurtagiri kualifikatu batekin sinatzen bada, IZENPEren RAk sinatzailearen ordezkaritza-gaitasuna egiaztatuko du erregistro ofizialetan kontsultatuz (Merkataritza Erregistroa, Aldizkari Ofizialak, etab., ordezkaritza motaren arabera). Kontsulta horiek ordezkaritza-gaitasuna egiaztatzeko aukera ematen ez badute, IZENPEk sinatzailearekin harremanetan jarriko da froga osagarriak jasotzeko.

SSL ziurtagiriak eskatzeko online aplikazioaren bidez, entitate baten ordezkariak erabiltzaile elkartuak sor ditzake DV eta OV ziurtagiriak entitatearen izenean eskatzeko.

SSL ziurtagiri kualifikatuen eskaeren kasuan, IZENPEk CA/Browser Forum-ek «Balioztapen Hedatuko Ziurtagiriak igortzeko eta kudeatzeko Gidan (EV)» ezarritako betekizunak beteko ditu.

3.2.6 Elkarreragingarritasun-irizpideak

Ez dago IZENPEtik kanpoko ziurtapen-agintariekin elkarreragingarritasun-harremanik.

3.3 Gakoa berriro igortzeko identifikazioa eta autentifikazioa

3.3.1 Gakoa berriro igortzeko ohiko prozesurako identifikazioa eta autentifikazioa

Sinatzaileek edozein ziurtagiriren gakoa berriro igortzea eska dezakete IZENPEren web-aplikazioaren bidez. Eskaera berriak balioztapen berriak behar izan ditzake, aurreko batzuk iraungita badaude.

Berritze-eskaeraren autentifikazio-baldintzak ziurtagirien berritze-prozesuari buruzko CP honetako atalean deskribatzen dira (ikusi dokumentu honetako 4.6. atala).

3.3.2 Baliogabetze-eskaerarako identifikazioa eta autentifikazioa

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

3.4 Baliogabetze-eskaerarako identifikazioa eta autentifikazioa

IZENPEk bere diskrezioz baliogabetu ahal izango du CP honek estaltzen duen edozein ziurtagiri.

Baliogabetze-eskaeraren autentifikazio-baldintzak dokumentu honetako 4.9 atalean zehazten dira.

4. ZIURTAGIRIEN BIZITZAREN ZIKLOAREN ERAGIKETA-BALDINTZAK

4.1 Ziurtagiri-eskaera

4.1.1 Nork aurkez dezake ziurtagiri-eskaera

Webguneen autentifikazio-ziurtagiriak eskatzea honako hauek baino ezingo dute egin: Sinatzailearen ordezkariek, edo Ziurtagiria sinatzailearen izenean eskatzeko behar bezala baimendutako pertsonek, eta domeinu-izenaren kontrola frogatu dutenek (ziurtagirian sartuko den domeinua). Domeinu-izenaren kontrol hori IZENPEk egiaztatuko du, politika honetako «3.2 Hasierako identitate-balioztapena» atalean deskribatutako moduan.

Gainera, ziurtagiri kualifikatuen kasuan, IZENPEk CA/Browser Forum-ek ezarritako «Balioztapen Hedatuko Ziurtagiriak igortzeko eta kudeatzeko Gida»ri jarraituko dio.

4.1.2 Alta-prozesua eta erantzukizunak

Ziurtagiria igorri aurretik, IZENPEk dokumentazio hau bildu beharko du Eskatzailearengandik:

- Ziurtagiria igortzeko eskaera eta aplikagarriak diren baldintza orokorrak onartzea. Onarpen honekin, sinatzaileek ziurtatzen dute ziurtagiri-eskaeran jasotako informazio guztia zuzena dela.
- Eskaera teknikoa aurkeztea (PKCS#10 formatuan).
- Aplikagarria bada, dagokion tasa ordaintzea.

IZENPEko RAk egiaztatuko ditu: Erakunde sinatzailea, eta Sinatzailearen ordezkaria. Ziurtagiri-eskaera zuzena, osatua eta behar bezala baimendua den, dokumentuko «3.2 Hasierako identitate-balioztapena» atalean ezarritako eskakizunen arabera. IZENPEk balioztapen-prozesuan ezarritakoaz gain beste egiaztapen osagarri batzuk egin ahal izango ditu.

Egindako egiaztapenen froga guztiak bildu eta gordeko ditu.

Prozesu honetan alderdi bakoitzak dituen erantzukizunak dokumentu honetako 9.6.2 atalean jasota daude: «Betebeharrak eta bermeak».

4.2 Ziurtagiri-eskaeraren izapidetzea

4.2.1 Identifikazio- eta autentifikazio-funtzioen gauzatzea

Sinatzailearen ordezkariak IZENPEren RAri sinadura elektroniko kualifikatuarekin sinatutako formulario bat bidaliko dio, eta bertan webguneen autentifikazio-ziurtagirian sartuko den informazio guztia jasoko da. Informazio hori oinarri hartuta, IZENPEren RAk politika honetako «3.2 Hasierako identitate-balioztapena» atalean deskribatutako egiaztapenak egingo ditu.

IZENPEk eskaeran jasotako datuen egiazkotasuna egiaztatuko du, eta, hala dagokionean, ordezkariaren gaitasuna ere egiaztatuko du dagokion moduan, eta egindako egiaztapenen frogak gordeko ditu.

Kontratua formalizatzeko sortutako sinadura elektronikoa IZENPEk egiaztatuko du.

3.2 atalean zehaztutako iturri batek emandako aurrebalidazioko datuak edo dokumentuak ezin izango dira erabili 12 hilabete baino gehiago igaro badira balioztatu zirenetik.

4.2.2 Ziurtagiri-eskaeren onarpena edo ukapena

Webguneen autentifikazio-ziurtagiriak igortzeko prozesuan parte hartzen duen RA beti da IZENPE, eta, beraz, ez dio domeinu-jabetzaren balioztapena beste RA bati esleitzen.

IZENPEren RAk honako egiaztapen hauek egingo ditu, «3.2 Hasierako identitate-balioztapena» atalean deskribatutakoaren arabera: Sinatzailearen ordezkariak gako pribatua duela egiaztatzeko froga Erakundearen eta ziurtagiria eskatzen duen pertsonaren identitatearen autentifikazioa, Domeinuaren balioztapena.

Egiaztapen horien emaitzek eskaera onartzea edo ukatzea ekarriko dute. IZENPEk barne-datu-base bat mantentzen du, bai baliogabetutako ziurtagirientzat, bai phishinga edo beste erabilera iruzurti batzuk susmatuta aurrez ukatutako eskaerentzat. Informazio hori erabiltzen da etorkizuneko eskaera susmagarriak identifikatzeko, ziurtagiria igortzeko baimena eman aurretik.

Gainera, IZENPEk prozedura dokumentatuak garatzen, mantentzen eta ezartzen ditu arrisku handikotzat jotzen diren ziurtagiri-eskaeretan egiaztapen gehigarriak eskatzeko eta identifikatzeko, eskaerak behar bezala egiaztatu direla ziurtatzeko.

Egiaztapen horietako bat egiaztatu ezin bada, IZENPEk ziurtagiri-eskaera ukatuko du, eta ez du zertan ukapenaren arrazoia azaldu. Eskaera ukatu zaion sinatzailearen ordezkariak eskaera berri bat aurkez dezake geroko data batean.

OV ziurtagiri- eta ziurtagiri kualifikatuen eskaerak IZENPEren konfiantzazko langileek kudeatuko dituzte. Ziurtagiri kualifikatuak igortzeko onarpen-sistemak gutxienez bi konfiantzazko langileren

parte-hartzea eskatzen du: batek eskaera balioztatzeko eta besteak onartzeko.

Halaber, IZENPEk egiaztatzen du domeinu-izen bakoitzerako CAA erregistro bat existitzen den, RFC 8659 arauan ezarritako prozedurari jarraituz, eta bertan adierazitako prozesatzeko jarraibideen arabera.

CAA erregistro hori existitzen bada, IZENPEk ez du Ziurtagiria igorriko, baldin eta eskaera aplikagarri diren CAA erregistroen multzoarekin koherentea dela zehazten ez badu.

4.2.3 Ziurtagiri-eskaeren izapidetze-epea

Ziurtagiri-eskaera baten izapidetze-epea neurri handi batean sinatzailearen ordezkariak IZENPEk onartutako prozeduren arabera beharrezko informazioa eta dokumentazioa ematen duen araberakoa da. Hala ere, IZENPEk ahal duen guztia egingo du balioztapen-prozesua —eskaera onartzea edo ukatzea dakarrena— gehienez bost lanegunetan amaitzeko.

Epe hori noizbehinka gainditu daiteke IZENPEren kontroletik kanpoko arrazoiengatik. Horrelako kasuetan, eskaera egin duen sinatzailearen ordezkariari atzerapenaren arrazoien berri ematen saiatuko da IZENPE.

4.2.4 Ziurtagiri-agintaritzaren baimena (CAA)

IZENPEk CAA erregistroak onartzen ditu TLS ziurtagiriak eta Marka Egiaztatuaren ziurtagiriak igortzeko, 3.2.2.8 atalean deskribatzen den bezala.

FQDN baterako TLS ziurtagiriak IZENPEk igortzea baimendu nahi duten sinatzaileek, beren DNS eremuan "issue" edo "issuewild" propietatea eta “izenpe.com” edo “izenpe.eus” balioa duten CAA erregistro bat gehitu behar dute.

4.3 Ziurtagiriak igortzea

4.3.1 CAren ekintzak ziurtagiria igortzean

RAk ziurtagiri-eskaera onartu ondoren, ziurtagiriak sortzeko sistemak RFC 5280 arauaren eta CA/Browser Forum (BRs eta EVGs) baldintzen betetzea egiaztatzen duten kontrol batzuk aplikatzen ditu, ziurtagiria igorri aurretik. Egindako egiaztapenen ondoren, ziurtagiria dagokion ziurtagiri-motaren profil onartuaren arabera igortzen da.

IZENPEk, halaber, aldian behin gainbegiratzen ditu igorritako ziurtagirietan gerta litezkeen desbideratzeak.

Ziurtagiri elektronikoen igorpenarekin lotutako prozesuek autentifikazio anitzeko sistemak erabiltzen dituztela bermatzen dute kontu guztietan.

4.3.1.1 Root CAk ziurtagiriak igortzeko baimen eskuzkoa

Root CA batek ziurtagiri bat igortzeko, IZENPEk baimendutako pertsona batek (adibidez, CA sistemaren operadorea, sistemaren arduraduna edo PKIren administratzailea) komando zuzena exekutatu beharko du Root CAk sinadura eragiketa burutu dezan.

4.3.1.2 Ziurtagiriaren edukia sinatu aurretik linting prozesua

Ziurtagiri-profilak baldintza horien arabera inplementatzea konplexua denez, CA batek "Linting" prozesu bat ezartzea praktika ona dela jotzen da, sinadura egin aurretik ziurtagiri bakoitzaren egokitzapen teknikoa egiaztatzeko. Aurreziurtagiri bat Linting prozesutik igaro bada, ez da beharrezkoa azken ziurtagiriari Linting berriz aplikatzea, betiere CAk kontrol tekniko bat badu sinatuko den ziurtagiria Preziurtagiriari dagokiola egiaztatzeko, RFC 6962 dokumentuko 3.2 atalean deskribatutakoaren arabera.
2024ko irailaren 15etik aurrera, GOMENDATZEN da CAk Linting prozesu hori ezartzea. 2025eko martxoaren 15etik aurrera, IZENPEK DERRIGORREZ ezarri beharko du Linting prozesu hori.

IZENPEK sektorean zabalki onartutako Linting tresnak ERABILI BEHAR LITUZKE, honako helbide hauetan eskuragarri daudenak: https://cabforum.org/resources/tools/. Bereziki, zlint eta pkimetal tresnak erabiltzea gomendatzen da.

4.3.2 CAk ziurtagiria igorri izanaren berri ematea sinatzaileari

Behin ziurtagiria igorrita, IZENPEk jakinarazpen bat bidaltzen du sinatzailearen ordezkariak sinatutako bezeroaren alta-inprimakian adierazitako helbide elektronikora, ziurtagiria deskargatzeko prest dagoela adieraziz.

4.4 Ziurtagiriaren onarpena

4.4.1 Ziurtagiria onartutzat jotzeko egintza

Ziurtagiriaren eskaera-prozesuan, sinatzailearen ordezkariak erabilera-baldintzak onartzen ditu eta ziurtagiria eskuratzeko borondatea adierazten du, horiek baitira ziurtagiria sortzeko beharrezko baldintzak.

4.4.2 CAk ziurtagiria argitaratzea

Root eta Sub ziurtagiriak IZENPEren biltegi orokorrean argitaratzen dira (ikusi dokumentu honetako 2.2 atala).

IZENPEk aurreziurtagiri bat sortzen du igorritako ziurtagiri bakoitzeko, RFC 6962 (Ziurtagirien Gardentasuna) arauaren arabera. Aurreziurtagiri horrek igorri nahi den ziurtagiriaren informazio bera dauka eta igorri balitz bezala hartzen da (nahiz eta benetan ez den igorri). Ziurtagiri horiek eskuragarri egongo dira ziurtagirien gardentasuneko zerbitzariak kontsultatzen dituen edonorentzat.

4.4.3 CAk ziurtagiriaren igorpenari buruz beste entitate batzuei jakinaraztea

Webgunearen autentikaziorako ziurtagiriak igorri aurretik, aurreziurtagiri bat bidaltzen da IZENPEren Root ziurtagiria jasotzen duten ziurtagirien gardentasuneko zerbitzuaren erregistroetara.

4.5 Gako-parearen eta ziurtagiriaren erabilera

4.5.1 Gako pribatuaren eta ziurtagiriaren erabilera

IZENPEk ez ditu CP honen arabera igorritako ziurtagirien gako pribatuak sortzen edo gordetzen. Ziurtagiriaren gakoen zaintza eta kontrola, ziurtagirian sartuko den domeinu-izenaren kontrola egiaztatu duen sinatzailearen ordezkariari dagozkio. Beraz, gako publikoari lotutako gako pribatuaren ardura zaintzailea izango da.

4.5.2 Gako publikoaren eta ziurtagiriaren erabilera hirugarren fidagarrien aldetik

Erabiltzaile-erakundeek eta ziurtagiriaren fidagarritasunean konfiantza duten hirugarrenek ziurtagiri elektronikoen erabilerarako aplikagarriak diren estandarrekin bateragarriak diren softwareak erabili behar dituzte (X.509, IETF, RFC, eta abar). Webgunera konektatzeko segurtasun-neurri gehigarriak behar badira, erabiltzaile-erakundeek lortu beharko dituzte.

Webgunearen autentifikazio-ziurtagiri baten bidez bermatutako konexio segurua ezartzea espero duten hirugarrenek ziurtatu behar dute konexio hori sortu dela Ziurtagiriaren balio-epearen barruan, Ziurtagiria PK honen arabera eman zen helbururako erabiltzen ari dela, eta Ziurtagiria aktibo dagoela, eta baliogabetze-egoera egiaztatzen dela, dokumentu honen «4.10 Ziurtagirien egoerari buruzko informazio-zerbitzuak» atalean xedatutakoaren arabera.

4.6 Ziurtagiriak berritzea

4.6.1 Ziurtagiria berritzeko inguruabarrak

Ziurtagiri bat berritzeko, eskatzaileak dokumentu honetan deskribatutako ziurtagiriak igortzeko

prozesuari jarraitu beharko dio.

4.6.2 Nork eska dezake berritzea

Ziurtagiri bat berritzeko, eskatzaileak dokumentu honetan deskribatutako ziurtagiriak igortzeko prozesuari jarraitu beharko dio.

4.6.3 Ziurtagiriak berritzeko eskaeren izapidetzea

Ziurtagiri bat berritzeko, eskatzaileak dokumentu honetan deskribatutako ziurtagiriak igortzeko prozesuari jarraitu beharko dio.

4.6.4 Ziurtagiri berriaren jaulkipenaren jakinarazpena sinatzaileari

Ziurtagiri bat berritzeko, eskatzaileak dokumentu honetan deskribatutako ziurtagiriak igortzeko prozesuari jarraitu beharko dio.

4.6.5 Berritutako ziurtagiria onartutzat ematen duen jarduketa

Ziurtagiri bat berritzeko, eskatzaileak dokumentu honetan deskribatutako ziurtagiriak igortzeko prozesuari jarraitu beharko dio.

4.6.6 CAk berritutako ziurtagiriaren argitalpena

Ziurtagiri bat berritzeko, eskatzaileak dokumentu honetan deskribatutako ziurtagiriak igortzeko prozesuari jarraitu beharko dio.

4.6.7 CAk ziurtagiriaren igorpenari buruz beste entitate batzuei jakinaraztea

Ziurtagiri bat berritzeko, eskatzaileak dokumentu honetan deskribatutako ziurtagiriak igortzeko prozesuari jarraitu beharko dio.

4.7 Ziurtagiriaren gakoak berriz sortzea

Webguneen autentifikazioko ziurtagirien gakoak berritzea beti egingo da gako publiko eta pribatu berriak jaulkiz, ziurtagiri berri bat emateko prozesu berean oinarrituta.

4.7.1 Ziurtagiriaren gakoak berriz sortzeko inguruabarrak

Ziurtagiriaren gakoak kasu hauetan berrituko dira:

- Uneko gakoen iraungitze-epe hurbilarengatik, berritzeko eskatzaileak hala eskatuta.
- Gakoen segurtasun-haustea edo CP honetako «4.9 Ziurtagiriaren baliogabetzea eta etetea» atalean jasotako beste edozein egoera.

4.7.2 Nork eska dezake gako publiko berri baten ziurtapena

Ziurtagiri berri bat jaulkitzeko prozesu berari jarraituko zaio.

4.7.3 Gakoak berriz sortzeko eskaeren izapidetzea

Ziurtagiri berri bat jaulkitzeko prozesu berari jarraituko zaio.

4.7.4 Ziurtagiri berriaren jaulkipenaren jakinarazpena sinatzaileari

Ziurtagiri berri bat jaulkitzeko prozesu berari jarraituko zaio.

4.7.5 Berriz sortutako ziurtagiria onartutzat ematen duen jarduketa

Ziurtagiri berri bat jaulkitzeko prozesu berari jarraituko zaio.

4.7.6 CAk berriz sortutako ziurtagiriaren argitalpena

Ziurtagiri berri bat jaulkitzeko prozesu berari jarraituko zaio.

4.7.7 CAk ziurtagiriaren igorpenari buruz beste entitate batzuei jakinaraztea

Ziurtagiri berri bat jaulkitzeko prozesu berari jarraituko zaio.

4.8 Ziurtagiria aldatzea

Beraz, edozein aldaketa-behar ziurtagiri berri baten jaulkipena suposatzen du. Behin jaulkitako Ziurtagirietan ezin da aldaketarik egin.

4.8.1 Nork eska dezake ziurtagiriaren aldaketa

Aldaketa ez dago zehaztuta.

4.8.2 Nork eska dezake ziurtagiriaren aldaketa

Aldaketa ez dago zehaztuta.

4.8.3 Ziurtagirien aldaketa-eskaeren izapidetzea

Aldaketa ez dago zehaztuta.

4.8.4 Ziurtagiri berriaren jaulkipenaren jakinarazpena sinatzaileari

Aldaketa ez dago zehaztuta.

4.8.5 Aldatutako ziurtagiria onartutzat ematen duen jarduketa

Aldaketa ez dago zehaztuta.

4.8.6 CAk aldatutako ziurtagiriaren argitalpena

Aldaketa ez dago zehaztuta.

4.8.7 CAk ziurtagiriaren igorpenari buruz beste entitate batzuei jakinaraztea

Aldaketa ez dago zehaztuta.

4.9 Ziurtagiriaren baliogabetzea eta etetea

IZENPEk igorritako webguneen autentifikaziorako ziurtagiriak honako kasu hauetan baliogabetuko dira:

1. Ziurtagiriaren balio-epearen amaiera.
2. IZENPEk Fidagarritasun Zerbitzu Hornitzaile Kualifikatu gisa jarduera eteten duenean, baldin eta, ziurtagiriaren titularraren baimen espresarekin, IZENPEk igorritako ziurtagiriak beste fidagarritasun zerbitzu-hornitzaile batera transferitzen ez badira.
   a) eta b) kasuetan, ziurtagiriaren eraginkortasuna amaitutzat emango da aipatutako egoerak gertatzen direnean.
3. Dokumentu honetan adierazitako edozein arrazoi dela eta ziurtagiria baliogabetzea.

Ziurtagiriaren balio-epea iraungitzat joko da, IZENPEk gertaera erabakigarriren bat ezagutzen duenean eta hori bere Ziurtagirien Egoeraren Informazio eta Kontsulta Zerbitzuan jasotzen duenean.

IZENPEk komunikazio-kanal bat jartzen du eskuragarri honako hauentzat: sinatzaileak, hirugarren fidagarriak, software-hornitzaileak eta beste hirugarren batzuk.
Helbidea: incidencias@izenpe.eus Helbide horren bidez jakinarazi ahal izango dute ziurtagiri mota hauekin lotutako edozein gorabehera, hala nola: gako pribatuaren ustezko urraketa, ziurtagirien erabilera desegokia, iruzurra, urraketa edo jokabide desegokia.

IZENPEk, fidagarritasun-zerbitzu kualifikatuen hornitzaile gisa, eskubidea du ziurtagiri mota hau ez emateko edo baliogabetzeko, baldin eta ziurtagiriaren barruan agertzen den webgunearen domeinu-izenaren kontrola duen sinatzaileak ez badio erabilera egokia ematen, hirugarrenen jabetza industrial edo intelektualeko eskubideak urratuz, babestu nahi dituen aplikazio, webgune edo egoitza elektronikoen gainean; edo erabilera horrek nahasmena edo engainua sortzen badu aipatutako edukien, webgunearen edo aplikazioaren titularrari buruz.

IZENPE ez da erantzule izango atal honetan aurreikusitakoa betetzen ez duten ekipamendu, aplikazio, webgune edo egoitza elektronikoen titular edo arduradunen aurrean, eta ez da inolaz ere erantzule izango ziurtagiri horien erabilera desegokiaren ondoriozko erreklamazio edo auzi-eskarien aurrean.

4.9.1 Baliogabetzeko egoerak

4.9.1.1 Azken entitate baten ziurtagiri bat baliogabetzeko arrazoiak:

Aurreko atalean aurreikusitakoaz gain, webguneen autentifikaziorako ziurtagiri bat baliogabetzeko arrazoiak honako hauek izango dira:

1. Baimendutako pertsonen eskaera bidezko baliogabetzea. Eskaera hori IZENPEk ezarritako moduan egin behar da beti.
    - Ziurtagiriaren euskarriaren galera.
    - Ziurtagiriarekin lotutako gako pribatua hirugarren batek erabiltzea.
    - Gako pribatuaren konfidentzialtasuna urratu edo arriskuan jartzea.
    - Ziurtapen Praktiken Adierazpenen (CPS) bertsio berrien argitalpenaren ondoriozko baldintza berriak onartzen ez badira hilabeteko epean.
2. Epaile edo administrazio-agintaritzaren agindua.
3. Ziurtagiriak identifikatzen duen webgunearen amaiera, desegitea edo itxiera.
4. Sinatzailearen nortasun juridikoaren amaiera edo desegitea.
5. Sinatzailearen ordezkariaren ordezkaritza amaitzea.
6. Sinatzailearen ordezkariaren ezintasun osoa edo partziala.
7. Sinatzaileak ziurtagiria eskuratzeko emandako datuen zehaztasunik eza edo baldintzen aldaketa, ziurtagiria errealitatetik aldentzen den moduan.

8. CPS honetan jasotako betebehar garrantzitsu baten urraketa, baldin eta urraketa horrek eragina izan badezake igorpen-prozesuan.

9. Ziurtagiria erabiltzea erabiltzaileengan produktuen edo zerbitzuen jatorriari buruzko zalantzak sortzeko, haien jatorria beste bat dela irudikatuz. Kasu hauetan kontsumitzaileen eta erabiltzaileen, merkataritzaren, lehiaren eta publizitatearen araudi aplikagarria hartuko da kontuan.

10. Sinatzailearen edo bere ordezkariaren eta IZENPEren arteko kontratuaren amaiera, edo emandako zerbitzuen ordainketarik eza.

11. IZENPEk ziurtagiriak sinatzeko/zigilatzeko erabiltzen dituen sinadura/zigilua sortzeko datuen konfidentzialtasuna urratzea edo arriskuan jartzea.

12. Ziurtagiriak estaltzen dituen Politika honen menpe dauden ziurtagiri-igorle Ziurtapen Agintaritzari (CA) aplikatzen zaizkion ikuskaritza-eskemek ezarritako baldintzak ez betetzea, bereziki algoritmoei eta gakoen tamainari buruzkoak, hirugarrenentzat onartezina den arriskua suposatzen badute.

Ziurtagiriak estaltzen dituen Politika honen menpe dauden ziurtagiri-igorle Ziurtapen Agintaritzari (CA) aplikatzen zaizkion ikuskaritza-eskemek ezarritako baldintzak ez betetzea, bereziki algoritmoei eta gakoen tamainari buruzkoak, hirugarrenentzat onartezina den arriskua suposatzen badute.

IZENPEren erantzukizuna mugatzen da honako kasu hauetara, baldin eta ez badu ziurtagiri bat baliogabetu behar bezala:

- Sinatzailearen ordezkariak, ezarritako prozeduraren arabera, baliogabetzea eskatu badu.
- Ziurtagiria kontratua amaitzeagatik baliogabetu behar bada.
- Baliogabetze-eskaera edo horren arrazoia epaile edo administrazio-erabaki bidez jakinarazi bazaio Sinatzaileari.
- 3. puntutik 7.era arteko arrazoiak modu egiaztagarrian frogatu badira, baliogabetze-eskaera egin duen pertsona identifikatu ondoren.

Delitu edo arau-hauste penalak diren ekintzak, IZENPEk horien berri ez badu izan, edo datuen komunikazioan egondako akatsak edo arduragabekeriak —horien ondorioz egindako jardueren erantzukizunetik— IZENPE salbuetsita egongo da.

Azken entitate baten ziurtagirien baliogabetze-eskaerak gehienez 24 orduko epean izapidetu behar dira, eskaera jasotzen denetik.

4.9.1.2 Sub CA ziurtagiri baten baliogabetze-arrazoiak

Sub CA ziurtagiriak gehienez 7 eguneko epean baliogabetu beharko dira ondorengo kasuetan:

1. Sub CAk idatziz eskatzen badu.
2. Sub CAk jakinarazten badu jatorrizko eskaera ez zela behar bezala baimendua eta ezin dela atzeraeraginez baimendu.

3. CA igorleak frogak lortzen baditu gako pribatua arriskuan dagoela edo ez dituela betetzen BR dokumentuaren 6.1.5 eta 6.1.6 atalak.

4. CA igorleak frogak lortzen baditu ziurtagiria oker igorri dela.
5. CA igorleak hautematen badu ziurtagiria ez dela CP edo CPS dokumentuarekin bat etorriz igorri.
6. CA igorleak zehazten badu ziurtagiriaren informazioa okerra edo zehaztugabea dela.
7. CA igorlea edo Sub CA jarduera uzten badute eta ez badago ziurtagirien baliogabetze-zerbitzua mantentzeko hitzarmenik beste CA batekin.
8. CA igorle edo Sub CAren ziurtagiriak emateko eskubidea baliogabetzen bada BR eskakizunen arabera, salbu eta CRL/OCSP zerbitzua mantentzeko hitzarmena badago.
9. CA igorlearen politika edo CPS dokumentuak hala eskatzen badu.
10. Ziurtagiriaren edukiak edo formatu teknikoak arrisku onartezina eragiten badie software-hornitzaileei edo hirugarrenei.
11. Hornitzaileek edo hirugarrenek (adibidez, CA/Browser Forum) zehazten badute algoritmo kriptografiko bat, sinadura bat edo gakoaren tamaina arrisku onartezina dela, eta ziurtagiri horiek baliogabetu eta ordeztu egin behar direla epe jakin batean.

4.9.2 Nork eska dezake baliogabetzea

Ziurtagiria Sinatzaileak, Erregistro Agintaritzak (RA) edo CA igorleak eska dezake baliogabetzea. Horrez gain, Sinatzaileek, konfiantzazko hirugarrenek, aplikazio-software hornitzaileek edo beste hirugarren batzuek ziurtagirien inguruko arazoen txostenak bidal ditzakete, eta horren bidez, CA igorleari ziurtagiria baliogabetzeko arrazoi arrazoitua jakinarazi.

4.9.3 Baliogabetze-eskaeraren prozedura

Baliogabetzea eskatu nahi duenak eskaera IZENPEri aurkeztu beharko dio. Ziurtagiria baliogabetzeko eskaera eskatzaileaz gain beste norbaitek egiten badu (adibidez, Sinatzailea edo gakoaren titularra ez den norbaitek), IZENPEk jakinaraziko dio gakoaren titularrari eta ziurtagiriaren Sinatzaileari baliogabetzea egin dela eta zergatia, aurrez edo aldi berean.

Eskatzaileak ziurtagiria baliogabetu ahal izango du kanal hauen bidez:

- Aurrez aurre,
    - IZENPEren egoitzan, hitzordua eskatuta: www.izenpe.eus
    - Sinatzailearen erakundearen bidez, IZENPEk harekin sinatutako dagokion tresna juridikoa badu.
- Online, webgunearen bidez: www.izenpe.eus
- Posta elektronikoz, baliogabetze-formularioa NAN elektronikoarekin sinatuta edo IZENPEk emandako ziurtagiri kualifikatu bat bidalita.

Autentifikatutako baliogabetze-eskaera, eta baita justifikazio-dokumentazioa ere, erregistratu eta artxibatu egiten dira.

IZENPEk web autentifikazio-ziurtagiria baliogabetu ondoren, ziurtagiri baliogabetuaren serie-zenbakia, data eta ordua, eta baliogabetzearen arrazoia jasotzen dituen CRL bat argitaratzen da direktorio seguru batean. Sinatzailearen ordezkariari jakinarazpena bidaliko zaio ziurtagiriaren balio-egoeraren aldaketari buruz, eskabidean adierazitako helbide elektronikora.

4.9.4 Baliogabetze-eskaeraren barkamen-aldia

Ez dago barkamen-aldirik aurreikusita, izan ere, eskaera jaso eta egiaztatzen denean, ziurtagiria berehala baliogabetzen da.

4.9.5 Baliogabetze-eskaera izapidetzeko CAren gehieneko epea

Entitate amaierako ziurtagirien baliogabetze-eskaerak gehienez 24 ordu igaro aurretik izapidetzen dira, eskaera jasotzea egiaztatu ondoren.
IZENPEk ziurtagiria berehala baliogabetzen du, aurrez aipatutako egiaztapenak egin ostean edo, hala badagokio, epaile- edo administrazio-erabakiaren bidez eskaera egiaztatuta dagoenean.

4.9.6 Fidagarriek egiaztatu beharreko baliogabetze-baldintzak

IZENPEk emandako ziurtagirietan konfiantza duten hirugarrenek hau egiaztatu beharko dute:

- Ziurtagiria baliozkoa dela eta aktibo jarraitzen duela.
- Ziurtapen-katean dauden ziurtagirien egoera.

4.9.7 CRLen argitalpen-maiztasuna (hala badagokio)

IZENPEk berehala argitaratzen du CRL bat ziurtagiri bat baliogabetzen denean.

Hurrengo CRLren programazioa bertan adierazten da, baina aurretik ere atera daiteke beharrezkoa bada. Baliogabetzerik gertatzen ez bada, CRL eguneratu egiten da egunero.

Erakunde-amaierako ziurtagirien CRLa gutxienez 24 orduero edo baliogabetze bat gertatzen den bakoitzean sortzen da, eta 10 eguneko balioa izaten du.

CA ziurtagirien CRLa (ARL) 12 hilean behin edo baliogabetze bat gertatzen denean argitaratzen da.

Iraungitako ziurtagiri baliogabetuak CRLtik ezabatzen dira. Baliogabetzearen erregistroa IZENPEren barne-erregistroetan 15 urtez gordeko da.

4.9.8 CRLentzako gehieneko latentzia (hala badagokio)

CRLa sortu eta gehienez 30 segundora argitaratu behar da.

4.9.9 Baliogabetzearen/Egoeraren lineako egiaztapenaren erabilgarritasuna

IZENPEk ziurtagiriaren egoeraren egiaztapen-zerbitzua eskaintzen die Erabiltzaile Entitateei denbora errealean, OCSP protokoloa (Online Certificate Status Protocol) erabiliz, erabiltzaile-aplikazioek ziurtagiriaren egoera egiazta dezaten.

Zerbitzu hau 24 orduz egunero, astean 7 egunetan erabilgarri dago.

4.9.10 Baliogabetzea online egiaztatzeko baldintzak

CRL zerbitzuaren erabilerak, sarbide librekoa, honako hauek eskatzen ditu:

- Beti azken CRLa egiaztatzea, eta hori ziurtagirian bertan ageri den "CRL Distribution Point" luzapenean adierazitako URLetik deskargatu daiteke.
- Erabiltzaileak gainera ziurtagiri-katearen hierarkiari dagokion CRL edo CRLak ere egiaztatu beharko ditu.
- Erabiltzaileak ziurtagiria sinatu duen CAk (Ziurtapen Agintaritzak) erantzuna sinatu duela egiaztatu beharko du.
-

Iraungitako ziurtagiri baliogabetuak CRLetik ezabatuko dira. Hala ere, ziurtagiriaren egoerari buruzko informazioa online eskuragarri izaten jarraituko da, iraungita egon arren.

OCSP zerbitzuaren erabilerak (hau ere sarbide librekoa):

- Ziurtagirian bertan ageri den "Authority Info Access" luzapenean jasotako URL helbidea egiaztatzea eskatzen du.
- Erabiltzaileak ziurtagiria sinatu duen CAk (Ziurtapen Agintaritzak) erantzuna sinatu duela egiaztatu beharko du.

4.9.11 Beste baliabide batzuk ziurtagiria baliogabetu dela jakinarazteko

IZENPEk informaziozko posta elektroniko bat bidaltzen dio ziurtagiriaren sinatzaileari, ziurtagiria baliogabetu denean.

4.9.12 Gakoa urratzen denerako baldintza bereziak

Ez dago baldintza berezirik ziurtagiria gakoaren urraketagatik baliogabetzen denean.
Baliogabetzearen gainerako arrazoietarako ezarritako baldintza berberak aplikatzen dira.

4.9.13 Ziurtagiria eteteko inguruabarrak

Ez da aurreikusten ziurtagiriak etetea.

4.9.14 Nork eska dezake etetea

Ez da aurreikusten ziurtagiriak etetea.

4.9.15 Ziurtagiria eteteko prozedura

Ez da aurreikusten ziurtagiriak etetea.

4.9.16 Etete-epearen mugak

Ez da aurreikusten ziurtagiriak etetea.

4.10 Ziurtagirien egoerari buruzko informazio-zerbitzuak

4.10.1 Funtzionamendu-ezaugarriak

Ziurtagirien Egoerari Buruzko Informazio eta Kontsulta Zerbitzuaren funtzionamendua honako hau da: OCSP zerbitzariak bezero OCSP baten eskaera jasotzen du, eta eskaeran dauden ziurtagirien baliozkotasun-egoera egiaztatzen du. Eskaera baliozkoa bada, OCSP erantzun bat igortzen da, kontsultatutako ziurtagirien uneko egoeraren berri ematen duena. Erantzun hori IZENPEren sinadura/zigilatzeko datuekin sinatuta dago, eta horrek bermatzen du ziurtagirien baliogabetze-egoerari buruzko informazioaren osotasuna eta benetakotasuna.

Erabiltzaile Entitatearen ardura da IZENPEk eskura jarritako OCSP zerbitzariarekin funtziona dezakeen OCSP Bezeroa izatea.

IZENPEk baliabide nahikoekin funtzionatzen eta mantentzen ditu bere CRL eta OCSP zerbitzuak, baldintza normaletan erantzun-denbora egokia bermatzeko.

4.10.2 Zerbitzuaren eskuragarritasuna

IZENPEk beharrezko neurri guztiak hartzen ditu bere OCSP zerbitzuaren etenik gabeko erabilgarritasuna, ahal den neurrian, bermatzeko. IZENPEK BERE GAIN hartu beharko du CRL eta OCSP gaitasunak baliabide nahikoekin operatzea eta mantentzea, eta baldintza normaletan hamar (10) segundoko edo gutxiagoko erantzun-denbora eskaintzea.

4.10.3 Aukerako funtzionalitateak

Ez da aurreikusten.

4.11 Harpidetzaren amaiera

Ziurtagiria baliogabetzen da bere balio-epea amaitzen denean edo baliogabetu denean.

Ziurtagiri bakoitzaren iraungitze-data dagokion Ziurtapen Politikan adierazten da.

4.12 Gakoen zaintza eta berreskurapena

4.12.1 Gakoen zaintza eta berreskuratze-politika eta -praktikak

IZENPEk ez ditu sortzen web-autentifikazioko ziurtagirien gako pribatuak, eta, ondorioz, ez ditu gordetzen, ezta berreskuratzen ere.

4.12.2 Saio-gakoen kapsulazioari eta berreskurapenari buruzko politika eta praktikak

Ez da aurreikusten.

5. INSTALAZIO-, KUDEAKETA- ETA FUNTZIONAMENDU-KONTROLAK

5.1 Kontrol fisikoak

5.1.1 Guneen kokapena eta azpiegiturak

Informazioa prozesatzeko erabiltzen diren instalazioek honako baldintza hauek betetzen dituzte:

- Informazio-prozesamendurako instalazioak kokatzen diren eraikina fisikoki sendoa da, kanpo-hormak indartuta daude, eta bideozaintzako kamerez etengabe zainduta dago. Sarrera soilik baimendutako langileei mugatuta dago.
- Ate eta leiho guztiak itxita eta babestuta daude baimenik gabeko sarbideak saihesteko.

5.1.2 Sarbide fisikoa

Datuen prozesamendurako zentroa

IZENPEren instalazioek sarbide fisikoa kontrolatzeko sistema oso bat dute, honako hauek barne:

- Lur teknikotik sabai errealeraino hedatzen den perimetro-segurtasuna, baimenik gabeko sarbideak saihesteko.
- Instalazioetarako sarbide fisikoaren kontrola:
  - Sarbidea soilik baimendutako langileei ematen zaie.
  - Segurtasun-guneko sarbide-eskubideak aldian behin berrikusten eta eguneratzen dira.
  - Langile guztiek identifikazio ikusgarria eraman behar dute. Langileak animatzen dira baldintza hori betetzen ez duen edozein pertsona identifikatzera.
  - IZENPEkoak ez diren langileak instalazioetan lan egiten badute, behar bezala gainbegiratuta egoten dira.
- Gune segururako sarbideen erregistroa mantentzen da.
- Eraikinaren perimetroko ateetan kontrol-mekanismoak ezarrita daude.
- Zirkuitu itxiko telebista-sistemak IZENPEk ziurtapen-zerbitzuetarako erabiltzen dituen osagaiak zaintzen ditu.

Erregistro-agintaritzak (RA)

RAek IZENPEren Segurtasun Politikak eta hornitzaileentzako Segurtasun Politikak ezarritako segurtasun-irizpideak betetzen dituzte.

5.1.3 Hornidura elektrikoa eta aire girotua

Datuen prozesamendurako zentroak hornidura elektriko eta klimatizazio egokia dauka, funtzionamendu-ingurune fidagarri bat bermatzeko.

IZENPEren instalazioek honako hauek dituzte: Elikadura etengabea bermatzen duen SAI sistema. Sorgailu elektriko bat, hornidura elektrikoan edo klimatizazioan huts eginez gero, ekipoen itxiera ordenatua ahalbidetzen duena.

5.1.4 Ureztatze-arriskuaren aurkako babesa

IZENPEk beharrezko neurriak hartu ditu urarekiko esposizioaren eragina minimizatzeko.

5.1.5 Suteen prebentzioa eta babesa

IZENPEren datu-zentroak hauek ditu: Lur teknikotik sabai errealeraino doazen hesi fisikoak. Suaren detekzio automatikoa duen sistema bat, honako hauek egiteko gai dena:

- Larrialdia zaintzari eta IZENPEko langileei jakinaraztea.
- Aireztapen-sistema deskonektatzea. Suaren aurkako ateak ixtea. Hornidura elektrikoa etetea. Sua itzaltzeko sistema automatikoa aktibatzea.

5.1.6 Euskarria gordetzea

Babeskopiak dituzten euskarriak modu seguruan eta babestuan gordetzen dira.

5.1.7 Hondakinak ezabatzea

Informazio-euskarriak suntsitzeko prozedurak arautzen dituen politika bat dago indarrean.

Informazio konfidentziala duten euskarriak suntsitzen dira, informazioa berreskuraezina izan dadin.

5.1.8 Kanpoko babeskopia

IZENPEk babeskopiak gordetzen ditu ingurune seguru batean, istripuen aurka babestuta eta jatorrizko gune nagusitik nahikoa distantziara, hondamendiren bat gertatuz gero informazioa gal ez dadin.

5.2 Prozedura-kontrolak

5.2.1 Konfiantzazko rolak

"Konfiantzazko rola" gisa ulertzen da segurtasunean arazoak sor ditzakeen ardura duen pertsona bat, zeregina behar bezala gauzatzen ez bada (nahita edo ustekabean).

Rol horien funtzionamendu egokia bermatzeko, honako neurri hauek hartzen dira:

- Teknologia diseinatu eta konfiguratu da erroreak edo jokabide okerrak saihesteko.
- Eginkizunak hainbat pertsonaren artean banatzen dira, eta horrela, ekintza oker batek konplizitatea eskatuko luke.

IZENPEk definizio osoak ditu erakundean betetzen diren rol guztientzat, eta rol bakoitzaren ardurak argi zehaztuta daude.

5.2.2 Zeregin bakoitzerako behar den pertsona kopurua

Segurtasuna indartzeko, rol bakoitzerako pertsona bat baino gehiago esleitzen da. Salbuespen bakarra da operadorearen rola, administratzaileak ere bete dezakeena.

Era berean, rol berean hainbat pertsona egon daitezke.

5.2.3 Rol bakoitzerako identifikazioa eta autentifikazioa

Konfiantzazko rolek identitatearen egiaztapena behar dute, modu seguruan. Konfiantzazko rol guztiak pertsona fisikoek betetzen dituzte.

IZENPEk dokumentazio espezifikoa du rol bakoitzaren xehetasunekin.

5.2.4 Funtzioen bereizketa behar duten rolak

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

5.3 Langileen kontrolak

5.3.1 Kualifikazioak, esperientzia eta gaitasun-baldintzak

IZENPEk beharrezko esperientzia eta kualifikazioak dituzten langileak enplegatzen ditu.

Konfiantzazko rolak dituzten langile guztiak interes-gatazkarik gabe daude, eta ez dute eraginik izango IZENPEren funtzionamenduarekiko inpartzialtasunean.

5.3.2 Atzeko planoaren egiaztapen-prozedurak

Giza Baliabideen prozeduren bidez, IZENPEk egokiak diren ikerketak egiten ditu langileak kontratatu aurretik. Legezko murrizketak direla eta, ez da aurrekari penalik egiaztatzen.

5.3.3 Prestakuntza-baldintzak

IZENPEk bere langileei beharrezko prestakuntza eskaintzen die, beren eginkizunak trebetasunez eta egoki betetzeko. Prestakuntza urtean behin egiten da gutxienez, eta honako eduki hauek biltzen ditu, gutxienez:

- Ziurtapen Praktiken Adierazpenaren kopia.
- Segurtasunari buruzko sentsibilizazioa.
- Softwarearen eta hardwarearen funtzionamendua rol bakoitzerako.
- Segurtasun-prozedurak rol bakoitzerako.
- Kudeaketa- eta ustiapen-prozedurak rol bakoitzerako.
- Hondamendien aurreko berreskurapen-prozedurak. • Gorabeherak kudeatzeko prozedurak.

RAko operadoreek sarrera-prestakuntza eta sentsibilizazio espezifikoa jasoko dute, eta IZENPEk ezarritako maiztasunarekin eguneratuko da.

5.3.4 Hobekuntza-ikastaroen maiztasuna eta eskakizunak

IZENPEren jardueran aldaketa garrantzitsurik gertatzen bada, prestakuntza-plan bat egingo da, eta haren gauzatzea dokumentatuko da. Konfiantzazko Rolak betetzen dituzten langileek gutxienez urtean behin jasoko dute prestakuntza, beren gaitasun-maila mantentzeko. Prestakuntza horrek beti jaso beharko du edukiak berrikusteko saio bat.

5.3.5 Lanpostuen txandakatze-maiztasuna eta -sekuentzia

Langileek lanpostua aldatzen dute rolaren beharrek hala eskatzen dutenean edo langileak berak eskatuta.

5.3.6 Baimendu gabeko jardueren zehapenak

Informazioaren segurtasun-gorabeherak

IZENPEk informazio-segurtasuneko gertakarientzako kudeaketa-plan bat du.

Zehapen-prozesua

Barneko diziplina-araubide bat dago, langileei ezar dakizkiekeen zehapenak zehazten dituena.

5.3.7 Kontratista independenteentzako eskakizunak

IZENPEk azpikontratatutako langile guztiek, haren zerbitzuen funtzionamenduarekin loturiko funtzioak betetzen badituzte, IZENPEren Hornitzaileen Segurtasun Politikan ezarritako eskakizun berberak bete behar dituzte.

5.3.8 Langileei ematen zaien dokumentazioa

Trusted Roles betetzen dituzten langile guztiek hau jasotzen dute:

- Ziurtapen Praktiken Adierazpenaren kopia.
- Rol bakoitzari dagozkion ardurak eta prozedurak zehazten dituen dokumentazioa.
- Sistema osatzen duten osagai desberdinen eragiketa-eskuliburuetara sartzeko aukera.

5.4 Auditoria-erregistroen prozedurak

Auditoria-erregistroek IZENPEren edo Erregistro Agintaritzaren (RA) softwarean jasotako gertaera esanguratsuak berreraikitzen laguntzen dute, baita erregistroa sortu duen erabiltzailea edo gertaera identifikatzen ere. Erregistro hauek arbitrajee{tan ere erabiltzen dira gatazkak konpontzeko eta sinadura baten baliozkotasuna une zehatz batean egiaztatzeko.

5.4.1 Erregistratzen diren gertaera motak

Gertaera hauek gordetzen dira:

- Ziurtagiri berrien eskaerak
- Ziurtagiri-eskaera ukatuak
- Kontuen sarbide-urraketak
- Ziurtagirien sinadurak
- Ziurtagirien iraungitzeak
- Kontuetako saio-hasierak

- CRL zerrenden sinadurak
- CAn egindako aldaketak
- Ziurtagirien iraungitzeak

Zerrenda hau ez da osoa eta ziurtagiri-kudeaketarekin edo administrazio-funtzioekin zuzenean lotutako gertaeretara soilik mugatzen da. Ez dira sartzen beste sistemetan erregistratutako gertaera teknikoak.

Gertaera bakoitza data eta ordu zehatzarekin jasotzen da, fidagarri den ordu-iturria erabiliz.

5.4.1.1 Bideratzaile eta suebakien jarduera-erregistroak

Xedapenik gabe.

5.4.2 Erregistroak prozesatzeko maiztasuna

Erregistroak etengabe prozesatzen dira, eta teknologia-arloak hiruhileko bakoitzean auditoria egiten du. Auditoriaren txostenean honako hauek jasotzen dira:

- Baimenik gabeko sarbide-saiakeren zerrenda.
- CA bakoitzean sortutako erroreak.

5.4.3 Auditoria-erregistroen kontserbazio-epea

Erregistro-fitxategiaren informazioa online mantentzen da artxibatu arte. Artxibatuta daudenean, erregistro-fitxategiak 7 urtez gordetzen dira.

5.4.4 Auditoria-erregistroaren babesa

Erregistroaren informaziorako sarbidea soilik dagokion langileari ematen zaio, bere funtzioetarako. Auditore-rolak informazio hori kontsulta dezake. Erregistroa datu-base batean gordetzen da, eta sarbidea maila desberdinetan babestuta dago.

Auditoria-erregistroak baimenik gabe ezabatzea edo aldatzea blokeatuta dago. Datu-galera saihesteko kontingentzia-metodoak daude.

5.4.5 Auditoria-erregistroaren babeskopiak

Erregistroak datu-basean daude, eta beraz, datu-basearen eguneko babeskopiaren parte dira, babeskopien politikaren arabera.

5.4.6 Auditoria biltzeko sistema (barnekoa vs kanpokoa)

CA eta RA erregistro-fitxategiak IZENPEren barne-sistemetakoak dira.

5.4.7 Gertaeraren sortzaileari jakinaraztea

Ez da aurreikusten gertaera erregistratuaren jabeari jakinaraztea.

5.4.8 Ahulezien ebaluazioak

IZENPEren barne-sistemetako ahuleziak, kanpokoak eta barnekoak, hiruhilekoan behin ebaluatzen dira. Gainera, urteko sarrera-proba bat egiten da.

5.5 Erregistro-fitxategiak artxibatzea

5.5.1 Artxibatutako erregistro-motak

Datu edo fitxategi hauek artxibatzen dira, besteak beste:

- Ziurtagiri-eskaera eta erregistro-prozedurarekin lotutako datuak.
- Aurreko atalean deskribatutako auditoria-erregistroak.
- Gakoen erregistroa.

5.5.2 Datuak kontserbatzeko aldia

Ziurtagiri kualifikatuekin lotutako informazio eta dokumentazioa 15 urtez gordetzen da (jaulkipen-datarekin hasita). Beste ziurtagiri-mota batzuekin lotutako dokumentuak 7 urtez gordetzen dira (ziurtagiriaren iraungitze-datarekin hasita).

5.5.3 Artxiboaren babesa

Artxiboaren kudeaketa-prozedurak neurri hauek ezartzen ditu, bai paper formatuan, bai elektronikoan dauden erregistroak manipulatu edo suntsitu ez daitezen.

5.5.4 Artxiboaren babeskopien prozedurak

Babeskopien politika eta kontingentzia-plan bat dago, gertaera larrien aurrean nola jokatu zehazten dutenak. Gertaerak kudeatzeko estrategiaren diseinua aktiboen inbentarioan eta arrisku-analisian oinarritzen da.

5.5.5 Erregistroak denboraz zigilatzeko eskakizunak

IZENPEk erabiltzen dituen informazio-sistemek gertakari bakoitzaren erregistroaren ordu zehatza bermatzen dute. Erabilitako ordua iturri fidagarri batetik dator, eta sistema guztiak iturri horrekin sinkronizatuta daude.

5.5.6 Artxiboak biltzeko sistema (barnekoa vs kanpokoa)

Artxiboak biltzeko sistema IZENPEren instalazioetan eta zerbitzuak ematen dituzten entitateetako instalazioetan kokatzen da.

5.5.7 Artxibatuta dagoen informazioa lortzeko eta egiaztatzeko prozedurak

Informazio horretara sarbidea baimendutako langileetara mugatuta dago eta babestuta dago sarbide fisiko eta logikoaren aurrean, Ziurtapen Praktiken Adierazpen honen (CPS) 5. eta 6. atalen arabera.

5.6 Gako-aldaketa

CAren gako pribatuaren urraketaren arriskua minimizatzeko, gakoa aldatu egin behar da erabiltzen den algoritmoaren segurtasun-mailaren arabera. Gako berria aldatu ondoren, sinadura egiteko bakarrik erabili behar da. Gako zaharra, oraindik baliozkoa bada ere, sinadura zaharrak egiaztatzeko eskuragarri mantendu behar da, gako horrekin sinatutako ziurtagiri guztiak iraungi arte. Gako pribatu zaharra bakarrik mantendu behar da, gako horrekin sinatutako ziurtagirien CRLak sinatzeko erabiltzen bada, eta segurtasun-maila berdina izan behar du gako berriarekin. CAren gako berria sortzeko prozedura CA berrientzako eta aurreko CAetatik migratzeko Sortze Zeremonia Dokumentuan zehazten da. 6.1.5 atalak definitzen ditu erabiltzen diren gako-tamainak eta algoritmoak.

5.7 Konpromisoa eta hondamendietarako berreskurapena

5.7.1 Gorabeherak eta urraketa kudeatzeko prozedurak

5.7.1.1

Kontingentzia-plan bat dago, non egin beharreko ekintza guztiak, baliabideak eta langileak zehazten diren, baita nahita edo kasualitatez gertatutako gertaerek IZENPEren ziurtapen baliabide edo zerbitzuak kaltetu edo erabilezin bihurtzen dituztenean ere. Helburu nagusiak honako hauek dira:

- Berreskurapen-operazioen eraginkortasuna maximizatzea, hiru fasetan banatuta:
  - Jakinarazpen-/Ebaluazio-/Aktibazio-fasea, kalteak detektatzeko eta baloratzeko, eta plana abiarazteko.
  - Berreskurapen-fasea, zerbitzuak denbora batez eta partzialki berrezartzeko, sistema originaleko kaltea konpontzen den arte.
  - Berrekite-fasea, ohiko operazioak eta prozesuak berriro martxan jartzeko.

- Beharrezko ekintza, baliabide eta prozedurak identifikatzea, zerbitzuak partekatu moduan emateko CPD alternatibo batean, jarduera normalak luzaro eten direnean.
- IZENPEk izendatutako langileei ardurak esleitzea, eta jarraibideak ematea operazioak luzaro eten direnean berreskuratzeko.
- Parte hartzen duten alderdien arteko koordinazioa bermatzea (entitateko sailak, kanpoko kontaktuak eta hornitzaileak) kontingentzia-estrategian.

IZENPEren Kontingentzia Planak ziurtapen-zerbitzuak ematean beharrezko funtzio, operazio eta baliabide guztiei aplikatzen zaie. Planak IZENPEko zerbitzu-ematearekin lotutako langileei ere eragiten die.

Planak talde jakin batzuk sartzea aurreikusten du, IZENPEren operazioen berreskurapenean.

Kalteen ebaluazioak eta ekintza-plana Kontingentzia Plan berean zehazten dira.

Algoritmoak, erabilitako gako-tamainen konbinazioak edo beste inguruabar teknikoren batek sistemaren segurtasun teknikoa nabarmen murrizten badu, Kontingentzia Plana aktibatuko da. Ekonomia-eraginaren analisia egingo da, eta hauek barne hartuko ditu: Analisiak segurtasun-arazoaren izaera kritikoa, irismena eta gertakaria kudeatzeko berreskuratze-estrategia aztertuko ditu. Ekonomia-eraginaren txostenean puntu hauek zehaztu beharko dira:

- Kontingentziaren deskribapen zehatza, epeak eta bestelako xehetasunak.
- Gertakariaren izaera kritikoa, eremua
- Proposatutako konponbidea edo konponbideak.
- Aukeratutako konponbidearen ezarpen-plana, eta gutxienez honako hauek jasoko ditu:
  - Erabiltzaileei jakinaraztea modu eraginkorren bidez. Ziurtagirien eskatzaileak, sinatzaileak eta egiaztatzaileak (konfiantzazko hirugarrenak) sartzea.
  - Kontingentziaren argitalpena webgunean.
  - Kaltetutako ziurtagirien baliogabetzea.
  - Berritze-estrategia.

5.7.1.2 Konbokazio masiboko plana

2025eko irailaren 1etik, Izenpek plan integral eta praktiko bat mantentzen du ezeztapen masiboko ekitaldietarako

eskala handiko ziurtagirien ezeztapenen aurrean erantzun azkarra, koherentea eta fidagarria bermatzeko.

Plan hori urtero probatu, berrikusi eta eguneratuko da. Izenperen auditoreentzat ere eskuragarri egongo da.

5.7.2 Baliabide informatikoak, softwarea eta/edo kaltetutako datuak

Arazo horiek kudeatzeko estrategia IZENPEren Kontingentzia Planaren barruan dago.

5.7.3 Entitatearen gako pribatuaren urraketaren aurreko prozedurak

Baliogabetze-arrazoiak konpondu ondoren, Root Ziurtapen Agintaritzak honako hauek egin ditzake:

- CA igorlearentzat ziurtagiri berri bat sortzea.
- CAk igorritako ziurtagiri eta CRL berriak gako berriarekin sinatuta egon daitezen bermatzea.

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

Kontingentzia hori IZENPEren Negozio Jarraipen Planean sartuko da, eta honako ekintza hauek hartuko dira besteak beste:

1. Zerbitzu kaltetua emateari utzi.
2. Ustez arriskuan jarritako ziurtagiriak baliogabetu.
3. Sinatzaileei, erabiltzaileei eta hirugarrenei jakinarazi. Halaber, TSP konfiantza-hitzarmenak dituztenei, nabigatzaile fabrikatzaileei eta oro har, IZENPEk zerbitzu-hitzarmenak dituen beste entitate guztiei jakinarazpena bidaliko zaie.
4. TSPren jarduera etenaren plana martxan jartzeko beharra aztertzea, CPS eta indarreko araudia jarraituz.

5.7.4 Hondamendi baten ondoren negozioarekin jarraitzeko gaitasunak

Ziurtapen Agintaritzaren (CA) jarduera eten egingo da, hondamendiaren aurreko berreskurapen-prozedura amaitu eta kokaleku nagusian edo beste instalazio batean segurtasunez berreskuratu arte.

IZENPEren Kontingentzia eta Negozio Jarraipen Plana aktibatuko da.

5.8 CA edo RAren jarduera-etenaldia

IZENPEk Amaiera Plana du, egoera hori gertatzen denean jarraitu beharreko prozedura zehazten duena.

Jarduera eteten bada, IZENPEk sinatzaileei jakinarazi beharko die eragiketak amaitu baino gutxienez bi hilabete lehenago, komunikazio eraginkorra eta ziurtapen-zerbitzuen emaile gisa jarduera uzteko asmoa jasotzea bermatzen duen edozein bitartekoren bidez. Jakinarazpen horretan adieraziko da indarrean dauden ziurtagiri guztiak bi hilabeteko epean baliogabetuko direla.

CA batek iraungitzeagatik edo baliogabetzeagatik amaitzen badu, ziurtagiriaren egoerari buruzko kontsultak OCSP zerbitzuaren bitartez jasoko dira. CA amaitu ondoren, CA horrek igorritako ziurtagirien OCSP erantzunak IZENPEko beste CA batek sinatuko ditu, eta CA hori indarrean egongo da.

IZENPEko CRLek ez dituzte iraungitako ziurtagiriak sartzen, 4.9.7 atalean adierazitako CRLen argitalpen-maiztasunaren arabera.

IZENPEk jarduera etenaldia badu, ziurtagiriak baliogabetzeari buruzko informazioa azken CRL baten bidez emango da, non nextUpdate balioa "99991231235959Z" izango den, ETSI EN 319 411-1 araudiaren 6.3.9 atalaren arabera.

Era berean, jakinarazpena egingo zaie TSPei, nabigatzaileen fabrikatzaileei eta IZENPEk zerbitzuak emateko kontratuak dituen beste edozein entitateri.

CP/CPS honetan zehaztutakoaren arabera, IZENPEk beharrezko den bitartean gordeko ditu erregistro, baliogabetze-egoera eta erregistro-fitxategi guztiak. Zerbitzua beste entitate bati transferitzen bazaio, beharrezko neurriak hartuko dira transferentzia guztiak bermatuta burutzeko.

Jakinarazpen hau egiteko ardura izango dute IZENPEren Zuzendaritza Nagusiak edo Administrazio Kontseiluak izendatutako pertsonek, eta erabakiko dute mekanismo egokiena.

IZENPEk jarduera-etenaldia Agintaritza Gainbegiratzaileari jakinaraziko dio, bai eta iraungiko diren ziurtagirien inguruko informazioa ere. Jakinarazpen hori egingo da Konfiantzazko Zerbitzuen arloan ardura duen Ministerioaren egoitza elektronikoaren jakinarazpen-plataformaren bidez, jarduera-etenaldia baino gutxienez 3 hilabeteko aurrerapenez.

IZENPEk edo zerbitzua transferitu zaion entitateak, kontratua duten hirugarrenekin (identifikazioa, igorpena, ostatu ematea, etab.) dituzten baimenak amaitutzat joko dira.

IZENPEk edo zerbitzuaren transferentzia jasotzen duen entitateak bere ziurtagiri kualifikatu guztien baliozkotasun-informazioa eman beharko du, baita iraungita daudenak ere (ziurtagiri hori igorri zuen azpiko CAren iraungitze-data arte).

Izenpek ROOT CA 2007 ziurtagiriarekin SSL/TLS ziurtagiriak emateko zerbitzuak deuseztatzeko prozesu formala hasi du. Honako xedapen hauek aplikatuko dira:

Jaulkipenaren amaiera: Ziurtagiri berrien jaulkipena 2026/04/15ean eten zen.

Errebokazio jarraituko zerbitzuak: CAk gordailu, CRL eta OCSP erantzuneko zerbitzuak mantenduko ditu, CA/B Foroaren Oinarrizko Betekizunetan zehaztutako epeen arabera, emandako azken ziurtagiria amaitu edo ezeztatu arte.

Erregistroen kontserbazioa: Auditoretza-erregistro guztiak eta ziurtagiriak baliozkotu izanaren ebidentzia gutxienez zazpi (7) urtez artxibatu eta gordeko dira, autonomia-erkidego honek emandako azken ziurtagiria amaitzen denetik aurrera.

6. SEGURTASUN TEKNIKOKO KONTROLAK

6.1 Gako-pareak sortzea eta instalatzea

6.1.1 Gako-pareak sortzea

6.1.1.1 TSAren gakoak sortzea

Root CA eta Sub gako kriptografikoak FIPS 140-2 maila 3 (edo gehiago) betetzen duen hardware kriptografikoaren moduluan (HSM) sortu behar dira, eta baita Common Criteria EAL 4+ profil babestuarentzat ere. Gako kriptografiko guztiak ETSI TS 119 312an ezarritako algoritmoen eta gako-luzeren gutxieneko gomendioekin sortu behar dira.

6.1.1.2 RAren gako-pareak sortzea

Ez da aplikagarria.

6.1.1.3 Sinatzailearen gako-pareak sortzea

Webguneen autentifikazio-ziurtagirien gako pribatuak ziurtagiriaren sinatzaileak sortu eta gordetzen ditu.

6.1.2 Gako pribatua sinatzaileari entregatzea

CAk ez dio gako pribatua sortzen edo entregatzen sinatzaileari.

6.1.3 Gako publikoa ziurtagiriaren igorleari entregatzea

Gako publikoa, gako pribatuarekin batera gakoen sortze- eta zaintza-gailuan sortua, Ziurtapen Agintaritzari bidaltzen zaio PKCS#10 formatuko ziurtagiri-eskaera baten bidez.

6.1.4 CAren gako publikoa konfiantzazko hirugarrenei entregatzea

IZENPEko CAen gako publikoak hainbat bideren bidez banatzen dira, besteak beste IZENPEren webgunean: www.izenpe.eus. CP/CPSaren 1.3.1 atalean ere argitaratzen dira Root CA eta CA igorleen hatz-marka digitalak.

6.1.5 Gako-tamainak

Erabilitako algoritmoak honako hauek dira:

ROOT 2007 HIERARKIA

Erabilitako algoritmoak honako hauek dira:

IZEN MOTAK	GAKO MOTA
Root CA	RSA 4096 bits
Sub CA	RSA 4096 bits
IZEN MOTAK	**GAKO MOTA**
Webgunearen autentifikazio-ziurtagiria	RSA >=3072 bits

ROOT 2024 HIERARKIA

Erabilitako algoritmoak honako hauek dira:

IZEN MOTAK	GAKO MOTA
Root CA	ECC 384 bits
Sub CA	ECC 384 bits
Webgunearen autentifikazio-ziurtagiria	ECC 256384 bits

6.1.6 Gako publikoaren parametroak sortzea eta kalitatea egiaztatzea

Webguneen autentifikazio-ziurtagirien gako publikoak RFC 5280 eta PKCS#1 arauen arabera kodetzen dira.

6.1.7 Gakoak erabiltzearen helburuak (X.509 v3-ren «key usage» eremuan oinarrituta)

Ziurtagiri guztiek Key Usage eta Extended Key Usage luzapenak dituzte, gakoen erabilera baimenduen adierazle gisa.

Root CAren gakoak erabiltzen dira Sub CAren ziurtagirien, ARLen eta TSA ziurtagiriaren sinadurak egiteko. Sub CAren edo igorlearen gakoak erabiltzen dira soilik azken erabiltzaileen ziurtagirien eta CRLen sinadurak egiteko.

Azken erabiltzaileen ziurtagirientzako baimendutako gako erabilerak www.izenpe.eus webguneko ziurtagiri profil dokumentuan zehazten dira.

6.2 Gako pribatuaren babesa eta modulu kriptografikoaren ingeniaritza-kontrolak

6.2.1 Modulu kriptografikoaren estandarrak eta kontrolak

Segurtasun-hardwareko modulu bat (HSM) gako kriptografikoak sortu eta babesten dituen segurtasun-gailu bat da. HSM horrek gutxienez FIPS 140-2 (3. maila) edo Common Criteria EAL 4+ babesteko profilaren irizpideak bete behar ditu.

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

Sinadura elektroniko kualifikatuko ziurtagiriak dituen gailu kriptografikoek, sinadura sortzeko gailu kualifikatu egokiak (DSCF) direnez, CC EAL4+ segurtasun-maila betetzen dute. Hala ere, gutxieneko ITSEC E3 edo FIPS 140-2 (2. maila) edo baliokideko segurtasun-irizpideak betetzen dituzten ziurtagiriak ere onartzen dira.

Gailu hauek gailu seguruaren ziurtagiria galdu eta sinadura kualifikatua galtzea ekarriko balu, IZENPEk ziurtagiria baliogabetzeko prozedurari jarraituko dio, betiere gainbegiratze-organoak edo araudiak hala aginduta.

Sinatzaile-gailuentzako Europako araudi erreferentea da 2016ko apirilaren 25eko Batzordearen 2016/650 (EB) Erabaki Exekutiboa.

Dena den, IZENPEk kontrola mantentzen du sinatzaile-gailuak prestatu, biltegiratu eta banatzean gakoak sortzean.

6.2.2 Gako pribatuaren erabilerarako pertsona anitzeko kontrola (n/m)

CAren gako pribatuaren erabilerak gutxienez bi pertsonaren onespena eskatzen du.

6.2.3 Gako pribatuaren zaintza

Root CAren gako pribatuak FIPS 140-2 (3. maila) eta/edo CC EAL4+ ziurtagiridun gailu kriptografikoetan gordetzen dira, eta horrek bermatzen du gakoa inoiz ez dela gailutik kanpora ateratzen. Gako pribatua aktibatzeko eta erabiltzeko, pertsona anitzeko kontrola behar da, aurreko puntuan adierazi bezala.

Sub CAen gako pribatuak FIPS 140-2 (3. maila) ziurtagiridun gailu seguruetan gordetzen dira.

Sinatzaileek beren gako pribatuaren zaintza egiten badute, beraien erantzukizuna izango da beren kontrol osopean mantentzea.

6.2.4 Gako pribatuaren babeskopia

CAren modulu kriptografikoko gakoak berreskuratzeko prozedura bat dago (Root edo Sub izan), kontingentziaren kasuan aplikagarria.

Halaber, IZENPEren zaintzan dagoen sinatzailearen modulu kriptografikoko gakoak berreskuratzeko

prozedura bat ere badago, dagokion politiketan zehaztutako kasuetan aplikagarria.

Bi kasuetan, 6.2.2 puntuan adierazitako kontrol berberak aplikatzen dira.

6.2.5 Gako pribatua artxibatzea

IZENPEk gako pribatuen babeskopia bat egin dezake, eta ziurtatu behar du bikoiztutako datuen segurtasuna jatorrizko datuen maila berekoa dela, eta bikoiztutako datuen kopuruak ez duela gainditzen zerbitzuaren jarraitutasuna bermatzeko behar den gutxieneko kopurua. Sinadura sortzeko datuak ez dira inongo helburuarekin bikoizten.

6.2.6 Gako pribatuaren transferentzia modulu kriptografiko baten barruan edo kanpoan

Root CAren, Sub CAen, VA eta TSAren gako pribatuak HSM batean sortzen dira 6.2.1 puntuan adierazitakoaren arabera, eta ezin dira esportatu.

Kontingentziaren kasuan, gako pribatuak berreskuratzeko aukera dago 6.2.4 atalean adierazitakoaren arabera.

6.2.7 Gako pribatuaren biltegiratzea modulu kriptografiko batean

Root CAren eta Sub CAen gakoak sortzeko eta hardware kriptografikoan erabiltzeko prozedurak deskribatzen dituen Zeremonia Dokumentu bat dago.

CAren gakoak sortzerakoan, IZENPEk ETSI EN 319 411-1 eta CA/B Forumeko Gutxieneko Eskakizunen Gidei jarraitzen die.

Sinatzailearen gakoak sortzeko, txartel kriptografikoan, IZENPEk Europako Batzordearen (eIDAS) gomendioak eta EN 319 411-1 araua jarraitzen ditu.

Gako pribatuak modulu kriptografikoetatik kanpo gordetzen badira, fisikoki moduluaren barruan egongo balira bezala segurtasun-maila berarekin babestu behar dira.

6.2.8 Gako pribatuaren aktibazio-metodoa

Ziurtapen Agintaritzaren gako pribatuak FIPS 140-2 (3. maila) segurtasun-irizpideak betetzen dituen gailu kriptografiko batean sortu eta gordetzen dira.

Azken erabiltzailearen ziurtagirien gako pribatuen aktibazio- eta erabilera-mekanismoak ziurtagirien Politika Espezifikoan deskribatzen dira.

6.2.9 Gako pribatuaren desaktibazio-metodoa

Administratzaile-rola duen pertsona batek CAren gakoa desaktiba dezake sistema gelditua. Gako

hori berriro aktibatzeko, «6.2.8 Gako pribatuaren aktibazio-metodoa» atalean deskribatutakoari jarraitu behar zaio.

Azken erabiltzailearen ziurtagirien gako pribatuen desaktibazioa ziurtagirien Politika Espezifikoan dago jasota.

6.2.10 Gako pribatuaren suntsiketa-metodoa

CAen gakoak suntsitzeko prozedura bat dago.
CAren gakoak gordetzen dituen HSMa kendu behar bada, ezarritako prozedurari jarraituko zaio.

Prozedura hau ez da aplikatzen txartel kriptografiko edo edukiontzi seguruan erabiltzailearen sinadura- edo autentikazio-gakoetarako, gakoa berritzeko kasuan izan ezik, gailu kriptografiko beraren barruan.

6.2.11 Modulu kriptografikoaren ziurtapen-maila

Dokumentu honen 6.2.1 atalean zehaztuta dago.

6.3 Gako-pareak kudeatzearen beste alderdi batzuk

6.3.1 Gako publikoa artxibatzea

Webguneen autentifikazio-ziurtagiriak eta haiekin lotutako gako publikoak IZENPEk legeak eskatzen duen denbora-tartean gordetzen ditu, gaur egun 15 urtez.

6.3.2 Ziurtagirien tarte operatiboak eta gako pareak erabiltzekoaktarteak

Ziurtagirien eta horien gakoen baliozkotasun-epeak hauek dira:

- Root CAren ziurtagiria eta haren gako parea: ikusi CP honen «1.3.1 Ziurtapen Agintaritza» atala.
- Sub CAren ziurtagiria (webguneen autentifikazio-ziurtagiriak igortzen dituena) eta haren gako parea: ikusi CP honen «1.3.1 Ziurtapen Agintaritza» atala.
- Webguneen autentifikazio-ziurtagirien eta haien gako pareen epeak: gehienez 398 egun.

6.4 Aktibazio-datuak

6.4.1 Aktibazio-datuak sortzea eta instalatzea

Aktibazio-datuak, bai jatorrizko CAren gakoenak, bai azken entitatearen ziurtagiriek jaulkitako

mendeko CAenak, Ziurtapen Agintaritza horien gakoak sortzeko ekitaldian sortzen dira.

Azken erabiltzailearen ziurtagirien gakoen aktibazio-datuak, dagokienez, ziurtagiri bakoitzaren Politika Espezifikoan deskribatzen dira.

6.4.2 Aktibazio-datuen beste alderdi batzuk

Root CAren gakoaren aktibazio-datuak txartel fisiko desberdinetan banatzen dira, eta gutxienez bi pertsonaren parte-hartzea behar da edozein operazio egiteko. Gakoak dituzten txartelak kutxa sendo desberdinetan gordetzen dira.

Sub CAren gakoaren aktibazio-datuak ere txartel fisiko desberdinetan banatzen dira, eta bi pertsonaren esku-hartzea eskatzen du. Gakoak dituzten txartelak kutxa sendo desberdinetan gordetzen dira.

TSA eta VAren gakoak Sub CAen gakoekin sortu eta kudeatzen dira HSM berean, eta arau berberak aplikatzen zaizkie.

Harpidedunek beren aktibazio-datuak isilpean mantentzeko betebeharra dute.

6.4.3 Aktibazio-datuen beste alderdi batzuk

Dagokion ziurtagiri motaren Politika Espezifikoa kontsultatu behar da.

6.5 Segurtasun-informatikoko kontrolak

6.5.1 Segurtasun informatikoaren eskakizun tekniko espezifikoak

IZENPEren ziurtapen-zerbitzuetako sistema osatzen duten osagai desberdinetan hainbat kontrol aplikatzen dira (CA, IZENPEko datu-baseak, IZENPEko Internet zerbitzuak, CAren operazioa eta sarearen kudeaketa):

- Kontrol operatiboak
  - Operazio-prozedura guztiak behar bezala dokumentatuta daude dagokion eskuliburuetan.
  - Kontingentzia Plan bat dago.
  - Birus eta kode kaltegarrien aurkako babes-tresnak ezarri dira.
  - Ekipamendua etengabe mantentzen da eskuragarritasuna eta osotasuna etenik gabe bermatzeko.
  - Informazio-gordailuen, kanpoko gailuen eta baliabide zaharkituak biltegiratzeko eta segurtasunez ezabatzeko prozedura bat dago.
- Datuak trukatzea. Datu-truke hauek zifratuta daude konfidentzialtasuna bermatzeko:
  - Erregistro-datuen transmisioa ERen (Erregistro Agintaritzak) eta erregistroaren datu-basearen artean.

    - Aurre-erregistroko datuen transmisioa.
    - RAen eta CAen arteko komunikazioa.
- Baliogabetzeak argitaratzeko zerbitzuak behar diren funtzioak ditu 24/7 eskuragarri egoteko.
- Sarbide-kontrola
    - Erabiltzaile-identifikatzaile bakarrak erabiltzen dira, erabiltzaile bakoitza bere ekintzekin lotuta egon dadin eta erantzule izan dadin.
    - Eskubideak erabiltzaileari bere lanak egiteko behar duen gutxieneko pribilegioa emateko printzipioaren arabera esleitzen dira.
    - Erabiltzaileak postua aldatzen edo erakundea uzten dutenean, sarbide-eskubideak berehala kentzen dira.
    - Erabiltzaileen sarbide-maila hiru hilean behin berrikusten da.
    - Sistemako pribilegioak kasu bakoitzean esleitzen dira eta arrazoirik gabe kentzen dira.
    - Pasahitzen kalitate-jarraibideak daude.
    - Ziurtagiriak igortzeko gaitasuna duten operadore-kontu guztiek bi faktoreko sarbide-kontrola dute.

IZENPEk sistemaren mailan guztietan segurtasuna bermatzen duten politika eta prozedura espezifikoak ditu.

6.5.2 Segurtasun informatikoaren sailkapena

Ziurtapen-zerbitzuak eskaintzeko erabiltzen diren produktuek ISO/IEC 15408 estandarraren arabera nazioarteko ziurtagiria dute.

6.6 Bizitzaren zikloko kontrol teknikoak

6.6.1 Sistemaren garapen-kontrolak

Ekoizpen-sistemetan softwarearen inplementazioa kontrolatuta dago.

Sistemetan arazoak saihesteko, honako kontrol hauek aplikatzen dira:

- IZENPEren politikak aplikazio eta sistemak modu seguruan garatzeko arauak barne hartzen ditu.
- Aldaketen jarraipena egiteko prozedura formal bat dago. Aldaketak beharrezkoenetara mugatzen dira eta kontrol zorrotza jasaten dute.
- Sistema eragileetan aldaketak egitean, negozio-aplikazio kritikoak berrikusten dira, negozioaren jarraipen-planaren arabera.
- Sistema seguruak garatzeko ingeniaritza-printzipioak aplikatzen dira.
- Garapen-ingurunea behar bezala babestuta dago.
- Azpikontratatutako garapena IZENPEk gainbegiratzen eta kontrolatzen du.
- Garapenean segurtasun operatiboaren probak egiten dira.
- Informazio-sistema berrien, eguneratzeen eta bertsioen onarpen-probak ezartzen dira.
- Proba-datuak hautatu, babestu eta kontrolatzen dira.

6.6.2 Segurtasuna kudeatzeko kontrolak

IZENPEk jarraipen etengabea egiten du sistemak eta komunikazioak IZENPEren Segurtasun Politikari jarraitzen diotela bermatzeko. Prozesu guztiak indarreko lege eta araudien arabera erregistratu eta auditatzen dira.

6.6.3 Bizitza-ziKloaren segurtasun-kontrolak

Probak egiteko, ekoizpeneko datuekin ahalik eta bolumen handi antzekoena behar da. Ekoizpeneko datu-baseak saihesten dira, batez ere datu pertsonalak dituztenak.

6.7 Sareko segurtasun-kontrolak

Sareko segurtasuna maila askotako zonifikazioaren kontzeptuan oinarritzen da, suebaki erredundante ugari erabilita. Sare ez-seguruetan transferitutako informazio konfidentziala SSL/TLS protokoloak erabiliz zifratuta dago. Barruko eta kanpoko trafikorako IPS sistemak daude ezarrita.

6.8 Denbora zigilatzea

IZENPEk bere sistemetako ordua Armadako Errege Behatokiarekin konektatuta lortzen du, NTP protokoloari jarraituz. . NTP protokoloaren deskribapena IETF RFC 5905 estandarrean aurki daiteke.

Barne-zerbitzu honetatik abiatuta, IZENPEk denbora zigilatzeko zerbitzua (TSA) eskaintzen du, dokumentu arbitrarioetan denbora-zigiluak sortzea ahalbidetzen duena, IETF RFC 3161 eta ETSI EN 319 421 arauekin bat etorriz. Informazio gehiago IZENPEren Denbora Zigilatzeko Praktiken Adierazpenean aurkituko duzu.

7. ZIURTAGIRIAREN, CRLaren ETA OCSPren PROFILAK

7.1 Ziurtagiri-profila

Webguneen autentifikazio-ziurtagiriak ETSIk argitaratutako ETSI EN 319 412-4 estandar europarrekin bat datozen ziurtagiri-profila dira, “Webguneen ziurtagirietarako ziurtagiri-profila» izenekoa.

CA/B Forumeko politika-identifikatzaile hauek dituzte:

ZIURTAGIRIA	OID CA/B FORUM

DV SSL	2.23.140.1.2.1
OV SSL	2.23.140.1.2.2
EV SSL	2.23.140.1.1
SSL kualifikatua	2.23.140.1.1

7.1.1 Bertsio-zenbakiak

Ziurtagiriek X.509 3. bertsiokoak izan BEHAR DUTE.

7.1.2 Ziurtagiriaren luzapenak

Webgune honetan argitaratzen da webgunearen autentifikazioko ziurtagirien profila xehetasunez deskribatzen duen dokumentua, eta bertan sartzen dira luzapen guztiak: https://www.izenpe.eus/contenidos/informacion/doc_juridica/es_def/adjuntos/Perfiles_de_Certificados.pdf

7.1.2.1 Root Ziurtapen Agintaritzaren Ziurtagiria

- basicConstraints
  - Luzapen hau kritiko izan BEHAR DA. CA eremua true gisa ezarri BEHAR DA. pathLenConstraint eremuak EZ DU EGON BEHAR.
- keyUsage
  - Luzapen hau egon BEHAR DA eta kritiko gisa markatu BEHAR DA. keyCertSign eta cRLSign bitak aktibatuta egon BEHAR DIRA. Root CAren gako pribatuak OCSP erantzunak sinatzeko baldin badu, orduan
- certificatePolicies
  - Luzapen honek EZ LUKE EGON BEHAR.
- extKeyUsage
  - Luzapen honek EZ DU EGON BEHAR.

7.1.2.1.1 Root CA ziurtagiriaren balioa

EREMUA	MINIMOA	MAXIMOA
notBefore	Sinatu baino egun bat lehenago	Sinatzeko orduan
notAfter	2.922 egun (gutxi gorabehera 8 urte)	9132 egun (gutxi gorabehera 25 urte)

7.1.2.2 Erdiko Ziurtapen Agintaritzaren Ziurtagiria

1. ***basicConstraints***

Luzapen hau egon BEHAR DA eta kritiko gisa markatu BEHAR DA. CA eremua true gisa ezarri BEHAR DA. pathLenConstraint eremua egon daiteke.

2. ***authorityKeyIdentifier***
   Luzapen honek EGON BEHAR DU, baina EZ DA kritiko gisa markatu BEHAR. keyIdentifier eremu bat izan BEHAR DU, eta EZIN DITU EDUKI authorityCertIssuer eta authorityCertSerialNumber eremuak.
3. ***subjectKeyIdentifier***
   Luzapen honek EGON BEHAR DU, baina EZ DA kritiko gisa markatu BEHAR. CA jakin baten gako bat modu berezian identifikatzen du. CAren Ziurtagiriaren Gakoaren IDa dauka.
4. ***keyUsage***
   Luzapen hau egon BEHAR DA eta kritiko gisa markatu BEHAR DA. keyCertSign eta cRLSign bitak aktibatuta egon BEHAR DIRA. Sub CAren gako pribatuak OCSP erantzunak sinatzeko baldin badu, digitalSignature bitak aktibatuta egon BEHAR DU.
5. ***certificatePolicies***
   Luzapen honek EGON BEHAR DU, baina EZ DA kritiko gisa markatu BEHAR. Gutxienez PolicyInformation bat izan BEHAR DU.
6. ***extKeyUsage***
   Luzapen honek EGON BEHAR DU, baina EZ DA kritiko gisa markatu BEHAR.
   TLS zerbitzari ziurtagiriak emateko erabiltzen diren Sub CA ziurtagirientzat, id-kp-serverAuth balioa egon BEHAR DA. id-kp-clientAuth balioa egon DAITEKE. Balio hauek EZ DUTE EGON BEHAR: id-kp-emailProtection [RFC5280], id-kp-codeSigning [RFC5280], id-kp- timeStamping [RFC5280], id-kp-OCSPSigning [RFC5280] eta anyExtendedKeyUsage [RFC5280]. Ez LIRATEKE beste balio batzuk sartu behar.
7. ***authorityInformationAccess***
   Luzapen honek EGON BEHAR DU, baina EZ DA kritiko gisa markatu BEHAR. keyIdentifier eremu bat izan BEHAR DU, eta EZIN DITU EDUKI authorityCertIssuer eta authorityCertSerialNumber eremuak.
8. ***cRLDistributionPoints***
   Luzapen honek EGON BEHAR DU, baina EZ DA kritiko gisa markatu BEHAR. CAren CRL zerbitzuaren HTTP URLa eduki BEHAR DU.

7.1.3 Algoritmo-identifikatzaileak

IZENPEk sinatze- eta kodetze-algoritmo hauetako bat erabili BEHAR DU:

Root CN	Algoritmoaren identifikatzailea	Kodetzea
IZENPE.com (2007)	RSASSA-PKCS1-v1_5 con SHA-256	300D06092A864886F70D01010B0500:
ROOT CA SSL IZENPE 2024	ecdsaWithSHA384:	300A06082A8648CE3D040303:

7.1.3.1 SubjectPublicKeyInfo

Eskakizun hauek ***subjectPublicKeyInfo*** eremuari aplikatzen zaizkio, Ziurtagiri edo Aurreziurtagiri baten barnean. Beste kodetze motak ez dira onartzen.

7.1.3.1.1 RSA

IZENPEk RSA gako bat adierazi BEHAR DU rsaEncryption algoritmoaren identifikatzailearekin (OID: 1.2.840.113549.1.1.1). Parametroen eremuak EGON BEHAR DU, eta NULL esplizitu bat izan BEHAR DU. IZENPEk EZ DU beste algoritmo bat erabili behar RSA-PSS (OID: 1.2.840.113549.1.1.10) RSA gako bat adierazteko.

Kodetutako RSA gakoen ***AlgorithmIdentifier*** eremuak byte bidezko byte berdina izan behar du balio hamaseitar honekin: ***300d06092a864886f70d0101010500:***

7.1.3.1.2 ECDSA

CAk ECDSA gako bat adierazi behar du id-ecPublicKey algoritmo-identifikatzailea erabiliz (OID: 1.2.840.10045.2.1). Parametroek ***namedCurve*** formatua erabili BEHAR dute.

- P-256 gakoen kasuan, ***namedCurve***-k secp256r1 IZAN BEHAR DU (OID: 1.2.840.10045.3.1.7).
- P-384 gakoen kasuan, ***namedCurve***-k secp384r1 IZAN BEHAR DU (OID: 1.3.132.0.34).
- P-521 gakoen kasuan, ***namedCurve***-k secp521r1 IZAN BEHAR DU (OID: 1.3.132.0.35).

Kodetutako ECDSA gakoen ***AlgorithmIdentifier*** eremuak byte bidezko byte berdina izan behar du balio hamaseitar honekin:

- P-256 gakoetarako, 301306072a8648ce3d020106082a8648ce3d030107
- P-384 gakoetarako, 301006072a8648ce3d020106052b81040022
- P-521 gakoetarako, 301006072a8648ce3d020106052b81040023

7.1.3.2 Sinadura-algoritmoaren identifikatzailea

CA baten gako pribatuarekin sinatutako objektu guztiek baldintza horiek bete behar dituzte ***AlgorithmIdentifier*** eremua edo ***AlgorithmIdentifier-derived*** motakoa sinaduren testuinguruetan erabiltzeari dagokionez.

7.1.3.2.1 RSA

IZENPEk sinatze- eta kodetze-algoritmo hauetako bat erabili BEHAR DU: AlgorithmIdentifier kodetutako eremuak byte bakoitza berdina izan BEHAR DU zehaztutako balio hamaseitarrarekin:

- RSASSA-PKCS1-v1_5 con SHA-256:
  Kodetzea: 300d06092a864886f70d01010b0500:
- RSASSA-PKCS1-v1_5 con SHA-384:
  Kodetzea: 300d06092a864886f70d01010c0500:

- RSASSA-PKCS1-v1_5 con SHA-512:
  Kodetzea: 300d06092a864886f70d01010d0500:
- RSASSA-PSS SHA-256arekin, MGF-1 SHA-256arekin eta 32 byte-ko salt luzerarekin:
  Kodetzea: 304106092a864886f70d01010a3034a00f300d060960864801650304020 1
  0500a11c301a06092a864886f70d010108300d060960864801650304020 1
  0500a203020120
- RSASSA-PSS SHA-384arekin, MGF-1 SHA-384arekin eta 48 byte-ko salt luzerarekin:
  Kodetzea: 304106092a864886f70d01010a3034a00f300d060960864801650304020 2:
  0500a11c301a06092a864886f70d010108300d060960864801650304020 2 0500a203020130
- RSASSA-PSS SHA-512arekin, MGF-1 SHA-512arekin eta 64 byte-ko salt luzerarekin:
  Kodetzea: 304106092a864886f70d01010a3034a00f300d060960864801650304020 3:
  0500a11c301a06092a864886f70d010108300d060960864801650304020 3 0500a203020140

7.1.3.2.2 ECDSA

IZENPEk erabilitako gakoari dagokion sinadura algoritmoa erabili BEHAR DU:

Sinadura egiteko gakoa P-256 bada, sinadura ECDSA SHA-256ekin egin BEHAR DA. AlgorithmIdentifier kodetutako eremuak byte bakoitza berdina izan BEHAR DU hurrengo balio hamaseitarrarekin: ***300a06082a8648ce3d040302***.

Sinadura egiteko gakoa P-384 bada, sinadura ECDSA SHA-384ekin egin BEHAR DA. AlgorithmIdentifier kodetutako eremuak byte bakoitza berdina izan BEHAR DU hurrengo balio hamaseitarrarekin: ***300a06082a8648ce3d040303***.

Sinadura egiteko gakoa P-521 bada, sinadura ECDSA SHA-512ekin egin BEHAR DA. AlgorithmIdentifier kodetutako eremuak byte bakoitza berdina izan BEHAR DU hurrengo balio hamaseitarrarekin: ***300a06082a8648ce3d040304***.

7.1.4 Izen-formak

Webguneen autentifikazio-ziurtagirien kodetzea RFC 5280ren gomendioaren arabera egiten da, zehazki «Interneteko Gako Publikoaren Azpiegituraren X.509 Ziurtagirien Profila eta Ziurtagirien Bazterketa Zerrenda (CRL)». Ziurtagiri hauen profilaren barruan definitutako eremu guztiek, salbu eta beste modu batean adierazi ez badute, UTF8String kodetzea erabiltzen dute.

7.1.4.1 Izena kodetzea

Ziurtapen Bide baliagarri bakoitzeko (RFC 5280ko 6. atalaren arabera):

- Ziurtapen Bideko ziurtagiri bakoitzean, Issuer Distinguished Name eremuaren edukia bytez byte berdina izan behar da, CA emisorearen ziurtagiriaren Subject Distinguished Name eremuaren edukiarekin.
- Ziurtapen Bideko CA ziurtagiri guztietan, Subject Distinguished Name eremuaren edukia bytez byte berdina izan behar da, RFC 5280ko 7.1 atalean berdinak diren kontsideratzen diren DN guztien artean, baita iraungitako edo baliogabetutako ziurtagiriak barne.

7.1.4.2 Subjektuaren atributuak kodetzea

Xedapenik gabe.

7.1.4.3 Sinatzailearen ziurtagiriaren izen arrunta atributua

Xedapenik gabe.

7.1.4.4 Subjektuaren beste atributu batzuk

Xedapenik gabe.

7.1.5 Izen-murrizketak

CP/CPS honen pean ziurtagirien emisiorako Sub CAk ez daude teknikoki murriztuta.

7.1.6 Ziurtagirien politika-objektuaren identifikatzailea

Ziurtapen Politikarako Objektu Identifikatzailea (OID) dokumentu honen «1.2 Izena eta dokumentuaren identifikazioa» atalean zehaztutakoa da.

7.1.7 Politika-murrizketak luzapena erabiltzea

Ez dira politika-murrizketak erabiltzen.

7.1.8 Politika-kalifikatzaileen sintaxia eta semantika

Certificate Policies luzapenak politika-kualifikatzaile hauek jasotzen ditu:

- CPS Pointer: IZENPEren Certification Practice Statement-erako (CPS) lotura dauka: http://www.izenpe.com/cps.
- Politika-identifikatzailea: Ziurtagiriari lotutako politikaren OID adierazten du.

7.1.9 Ziurtapen-politika luzapen kritikoa prozesatzeko semantika:

CP luzapenak ziurtagiriarekin lotutako politika identifikatzen du, baita politika hori non kontsultatu daitekeen ere.

7.2 CRLaren profila

IZENPEk emandako ziurtagiriek honako estandar hauek betetzen dituzte:

- RFC 5280 – Internet X.509 Public Key Infrastructure Certificate and CRL Profile (2002ko apirila)
- RFC 4325 – Internet X.509 Public Key Infrastructure Authority Information Access Certificate Revocation List (CRL) Extension (2005eko abendua)
- RFC 4630 – Update to DirectoryString Processing in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (2006ko abuztua)

7.2.1 Bertsio-zenbakiak

2. bertsioa (Bertsio-eremuak 1 osoa izan behar du).

7.2.2 CRL luzapenak eta CRL sarrerak:

Luzapen hauek erabiltzen dira:

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

7.3 CRLaren profila

IZENPEren OCSP erantzunak RFC 6960 betetzen dute (Interneteko X.509 Gako Publikoen Azpiegiturako Ziurtagirien Egoeraren Online Protokoloa - OCSP), eta erantzunok OCSP Erantzuleak sinatzen ditu, eta haren ziurtagiria ziurtagiri kontsultatua sinatu zuen CA berak eman du.

7.3.1 Bertsio-zenbakiak

2,0. bertsioa

7.3.2 OCSP luzapenak

Eremua	Nahitaezkoa	Kritikoa
1. Issuer Alternative Name	EZ	EZ

2. Authority/Subject key Identifier	EZ	EZ
3. CRL Distribution Point	EZ	EZ
4. Key usage	Bai	Bai
5. Enhanced Key usage	Bai	Bai

8. ADOSTASUN-AUDITORIA ETA BESTE EBALUAZIO BATZUK

Webguneen autentifikazio-ziurtagiriak emateko sistema urtean behin adostasun-auditoria bat jasotzen du hauen arabera:

- Europako ETSI EN 319 401 arauak «Konfiantzazko zerbitzu-hornitzaileentzako politika orokorraren eskakizunak» eta ETSI EN 319 411-1 «Ziurtagiriak ematen dituzten konfiantzazko zerbitzu-hornitzaileentzako politika- eta segurtasun-eskakizunak».
- ETSI EN 319 411-2 «EBko ziurtagiri kualifikatuak ematen dituzten konfiantzazko zerbitzu-hornitzaileentzako eskakizunak».

Gainera, ziurtagiriak emateko sistema honako auditoria hauei lotuta dago:

- Informazioaren Segurtasunaren Kudeaketa Sistemaren (SGSI) auditoria UNE-ISO/IEC 27001 arauaren arabera «Informazioaren segurtasunaren kudeaketa-sistemetarako eskakizunak».
- Segurtasun Nazionaleko Eskema (ENS) egokitzapena, 2010eko urtarrilaren 8ko 3/2010 Errege Dekretuaren arabera, Administrazio Elektronikoaren esparruan ENS arautzen duena.
- Auditoria, Europako Parlamentuaren eta Kontseiluaren 2016ko apirilaren 27ko 2016/679 (EB) Erregelamenduaren (datu pertsonalen tratamenduari eta datu horien zirkulazio askeari dagokienez pertsona fisikoak babesteari buruzkoa) eta Datu Pertsonalak Babesteko eta Eskubide Digitalak Bermatzeko abenduaren 5eko 3/2018 Lege Organikoaren (DBEO/LOPD-GDD) arabera.

Era berean, arrisku-analisiak egiten dira Informazioaren Segurtasunaren Kudeaketa Sisteman ezarritako moduan.

8.1 Ebaluazioaren maiztasuna edo egoerak

Kualifikatutako ziurtagiriak diren kasuetan, auditoriak Europako arau hauetan ezarritako eskakizunak beteko direla ere bermatuko du: ETSI EN 319 411-2: «EBko kualifikatutako ziurtagiriak ematen dituzten konfiantzazko zerbitzu-hornitzaileentzako eskakizunak» eta ETSI EN 319 412-4: «Webguneen ziurtagirietarako ziurtagiri-profila».

Gainerako auditoria gehigarriaren maiztasuna egokituko da indarrean dauden arauen arabera.

8.2 Auditorearen nortasuna/kualifikazioak

Auditoreek gaitasuna dute eta konpetentzia frogatua dute segurtasun-sistema produktiboen auditorian, batez ere ziurtagiri digitaleko sistemekin lotutakoetan. Auditoreak ETSI EN 319 403 arauaren arabera akreditatuta egon behar du.

8.3 Auditorearen harremana ebaluatutako erakundeari

Barruko zein kanpoko auditoreak erabiltzen dira, baina kasu guztietan, independenteak dira auditatu beharreko produkzio-zerbitzutik.

8.4 Ebaluazioak estalitako gaiak

Adostasun-auditoriak honako gai hauek hartzen ditu barne:

- PKI prozesuak.
- Informazio-sistemak.
- Datuen prozesamendurako zentroaren babesa.
- Dokumentuak.

Gai hauek auditatzeko moduari buruzko xehetasunak IZENPEren Auditoria Planean zehazten dira.

8.5 Defizientzien ondorioz hartutako ekintzak

Segurtasun-istripuak IZENPEren Segurtasun Batzordeak kudeatzen ditu.

IZENPEk ikerketa bat irekiko du gehienez 24 ordutan istripua jasotzen duenetik, eta 4.9.5 atalean BRetan (Business Requirements - Negozio Eskakizunak) definitutako irizpideak kontuan hartuta, hartu beharreko ekintzak erabakiko ditu.

Gainera, IZENPEk gorabeheratzat jotzen dituen kasuen berri ematen du (iruzurrak, phishing-a, etab.). Anti-Phishing Working Group-en webgunean (www.apwg.org, eta emisioa baino lehen egiaztatzen du eskatzailea edo haren ordezkariak ez daudela IZENPEren segurtasun-gorabeheren barneko datu-basean.

Kasurik guztietan, IZENPEk eskubidea du ziurtagiriak ez emateko egoera susmagarrietan.

8.6 Emaitzen komunikazioa

Auditorien emaitzen txostenak Segurtasun Batzordeari entregatuko zaizkio azterketa egiteko.

8.7 Autoebaluazioak

IZENPEk ikuskatuko du CP/CPS hori betetzen dela, eta bere zerbitzuaren kalitatea kontrolatuko du. Horretarako, autoebaluazioak egingo ditu hiru hilean behin, gutxienez, ziurtagiri baten edo, gutxienez, SSL/TLSrako jaulkitako konfiantza publikoko ziurtagirien (EV ziurtagiriak barne) ehuneko hiruaren (% 3) artean balio handiena duen ausazko lagin bati buruz.

IZENPEk urteko autoebaluazio bat osatu eta bidali behar dio BKTEri, gutxienez politika hauen baldintzak bete ditzan:

- CCADBren politika.
- Chrome-ren root programaren politika.
- Mozilla-ren root biltegiaren politika.
- Ziurtagiri-sareen eta -sistemen segurtasun-baldintzak.
- Konfiantza publikoko TLS ziurtagirietarako oinarrizko baldintzak.
- Baliozkotze hedatuko gidak konfiantza publikoko TLS ziurtagirietarako.

9. BESTE GAI KOMERTZIAL ETA LEGAL BATZUK

9.1 Tarifak

IZENPEk dagokion ordainsaria jasoko du, Administrazio Kontseiluak onartutako tarifen arabera.

9.1.1 Ziurtagiriak egin edo berritzeko tarifak

Ziurtagiriak jaulkitzeari edo berritzeari aplikatu beharreko tarifak zehazteko, dokumentu honetako «9.1 Tarifak» atalean xedatutakoa beteko da.

9.1.2 Ziurtagirietara sartzeagatiko tarifak

Ez da aurreikusten.

9.1.3 Errebalidazio edo egoeraren informaziorako sarbide-tasak

IZENPEk doan eskaintzen ditu ziurtagirien egoerari buruzko informazio-zerbitzuak CRL eta OCSP protokoloen bidez.

9.1.4 Beste zerbitzu batzuetarako tasak

Beste zerbitzu batzuetarako aplikatzen diren tasak urtero onartzen ditu IZENPEren Zuzendaritza Kontseiluak.

9.1.5 Itzulketa-politika

IZENPEk ez du itzulketa-politika berezirik.

9.2 Finantza-erantzukizuna

IZENPEk, Erregistro Agintariek (RA) eta Erabiltzaile Erakundeek finantza-baliabide nahikoak izango dituzte euren operazioak mantentzeko eta funtzioak betetzeko.

9.2.1 Aseguru-estaldura

IZENPEk errenta-ardurako aseguru-poliza bat du ziurtagiriak sortzetik eratorritako akats eta hutsuneak estaltzeko, eta poliza honek soilik estaltzen ditu IZENPEk egiten dituen jarduerak. IZENPEren eta Erregistro Agintaritzen (esku hartzen dutenean) eta sinatzaileen eta ziurtagirien erabiltzaileen arteko harremana ez da nahitaezkoa, ezta fiduziarioa ere. Ziurtagirien sinatzaileek eta erabiltzaileek ezin diete eskatu IZENPEri edo Erregistro Agintaritzei zerbitzurik emateko, ez kontratu bidez, ez beste edozein bitartekoren bidez.

9.2.2 Beste aktibo batzuk

Ez da aurreikusten.

9.2.3 Azken erakundeentzako aseguruen estaldura edo bermeak

Ez da aurreikusten.

9.3 Enpresa-informazioaren konfidentzialtasuna

9.3.1 Informazio konfidentzialaren esparrua

Bere zerbitzuak emateko, IZENPEk eta Erregistro Agintariek datu mota batzuk biltzea eta gordetzea behar dute, tartean informazio pertsonala. Informazio hori zuzeneko interesdunek ematen dute, beren baimen adierazgarriaren bidez, edo baimenik gabe legediak aurreikusten dituen kasuetan, datu pertsonalen babesari buruzko araudian.

IZENPEk eta Erregistro Agintariek ziurtagirien emisio eta kudeaketarako eta beste sinadura

elektroniko zerbitzuetarako beharrezko datuak soilik biltzen dituzte; datuak ezin dira beste helburuetarako erabili sinatzailearen baimen adierazgarri eta idatzirik gabe.

IZENPEren pribatutasun-politika datu pertsonalen babesari buruzko indarrean dagoen legediaren arabera prestatu da.

IZENPEk eta Erregistro Agintariek ez dute informazio pertsonalik zabaltzen edo partekatzen, salbu eta Ziurtapen Praktiken Adierazpenean (CPS) eta IZENPEk eta Erregistro Agintariek emandako zerbitzuen amaierari buruzko ataletan azaltzen diren salbuespenetan.

IZENPEk eta Erregistro Agintariek sekretuan gordeko dute informazio hau:

- Ziurtagiri-eskaerak, onartuak edo ukatuak izan, eta ziurtagirien emisio eta mantentzean lortutako bestelako informazio pertsonal guztia, dagokion atalean zehaztutakoa izan ezik.
- IZENPEk sortu edo gorde dituen gako pribatuak.
- Transakzioen erregistroak, transakzio osoen erregistroak eta auditoria-arrastoak barne.
- IZENPEk edo Erregistro Agintariek eta haien auditoriek sortu edo gorde dituzten barne- eta kanpo-auditorien erregistroak.
- Negozioarekin jarraitzeko eta hondamendietatik berreskuratzeko planak.
- Segurtasun-politikak eta -planak.
- Operazio-erregistroak eta bestelako plan operatiboak, artxibo-planak, jarraipena eta antzeko beste plan batzuk barne.

9.3.2 Informazio konfidentzialaren esparrutik kanpo dagoen informazioa

Informazio hau ez da konfidentziala eta beraz, IZENPErekin sinatutako instrumentu legaleko interesdunek onartzen dute:

- Emandako edo emateko prozesuan dauden ziurtagiriak.
- Pertsona fisiko sinatzailea IZENPEk emandako ziurtagiri batekin lotzen duen informazioa.
- Ziurtagiriaren titularraren izen-abizenak, sinatzailea eta sinatzailea pertsona fisikoa denean, edo sinatzaileen izenak, sinatzailea pertsona juridikoa edo administrazio-erakundea denean, baita titularraren beste edozein inguruabar edo datu pertsonal ere, ziurtagiriaren xedearen arabera esanguratsua bada.
- Sartuta egonez gero, ziurtagiriaren titularraren helbide elektronikoa, sinatzailea eta sinatzailea pertsona fisikoa bada, edo gakoaren jabearen helbide elektronikoa, sinatzailea pertsona juridikoa edo erakunde publikoa bada, edo sinatzaileak gailu-ziurtagirietarako emandako helbide elektronikoa.
- Ziurtagirietan adierazitako erabilera eta muga ekonomikoak.
- Ziurtagirien baliozkotze-epea, jaulkipen-data eta iraungitze-data.
- Ziurtagiriaren serie-zenbakia.
- Ziurtagiriaren egoera edo baldintza desberdinak eta bakoitzaren hasiera-data, zehazki: sortzeko

eta/edo emateko zain, balioduna, baliogabetua, etenda edo iraungitakoa, baita egoeraren aldaketaren arrazoia ere.

- Ziurtagiriak Baliogabetzeko Zerrendak (CRLak) eta baliogabetze-egoerarekin lotutako bestelako informazioa.
- IZENPEren biltegian gordetako informazioa.
- Ziurtapen Praktiken Adierazpen honetako (CPS) informazio konfidentzialari buruzko atalean adierazi ez den beste edozein informazio.

9.3.3 Informazio konfidentziala babesteko ardura

IZENPEk edo Erregistro Agintariek eskubidea izango dute informazio konfidentziala argitaratzeko, legeak hala eskatzen duen neurrian.

Zehazki, ziurtagiriaren edukia egiaztatzen duten erregistroak agerian jar daitezke, ziurtagiriaren frogak behar diren epaiketa-prozesuetan, titularraren baimenik gabe ere.

Ziurtagiriak eIDAS1 eta eIDAS2 Erregelamenduen arabera eta 2020ko azaroaren 11ko 6/2020 Legearen arabera argitaratuko dira, non fidagarritasun-zerbitzu elektroniko jakin batzuk arautzen diren.

9.4 Informazio pertsonalaren pribatutasuna

IZENPEk bere Tratamendu Ekintzen Erregistroa eta datu pertsonalei buruzko bestelako informazioa argitaratzen du, interesatuek kontsulta dezaten honako webgune honen bitartez: www.izenpe.eus/datos.

9.4.1 Pribatutasun-plana

IZENPEren datu pertsonalen tratamendua bat dator Europako Parlamentuaren eta Kontseiluaren 2016ko apirilaren 27ko 2016/679 (EB) Erregelamenduan ezarritakoarekin, datu pertsonalen tratamenduari eta datu horien zirkulazio askeari dagokienez pertsona fisikoak babesteari buruzkoa, eta 95/46/EE Zuzentaraua (Datuak Babesteko Erregelamendu Orokorra, aurrerantzean DBEO) indargabetzen duena, bai eta gai horretan aplikatu beharreko berariazko araudia ere.

9.4.2 Pribatutzat jotzen ez den informazioa

IZENPEk pribatutzat jotzen du fidagarritasun-zerbitzuen erabiltzaile diren pertsona fisikoen informazio pertsonala, zeina ez den ziurtagirietan sartu behar, baita ziurtagiriaren egoerari eta baliozkotasunari buruzko informazio-kontsultako zerbitzu-mekanismoetan erabiltzen dena ere.

Nolanahi ere, informazio pribatutzat hartzen da ziurtagiri elektronikoak eskatzeko, berritzeko eta baliogabetzeko prozesuetan bildutako informazio guztia (hurrengo atalean adierazitakoa izan ezik), konfiantzazko zerbitzuen emailearen esku dauden gako pribatuak eta pribatutzat argi eta garbi identifikatutako beste edozein informazio.

IZENPEk neurri egokiak aplikatzen ditu informazio pribatua babesteko.

9.4.3 Pribatutzat jotzen ez den informazioa

Ez da informazio pribatutzat hartzen ziurtagiri elektronikoetan jasotako informazioa, ezta ziurtagirien baliozkotasun-egoerari buruzko informazioa eta egoera horren hasiera-data ere (aktiboa, baliogabetua, iraungia, etab.). eta egoera-aldaketaren kausa. Beraz, ziurtagiri elektronikoak, baliogabetutako ziurtagirien zerrendak eta horien eduki osoa ez dira informazio pribatutzat hartzen.

9.4.4 Informazio pribatua babesteko erantzukizuna

IZENPEk DBEOk eskatzen dituen segurtasun-neurriak hartzen ditu, ziurtagirien eskatzaileen eta sinatzaileen datu pertsonaletarako sarbideari eta tratamenduari dagokienez.

Neurri teknikoak eta antolaketa-neurriak ezartzeko orduan, honako alderdi hauek hartuko dira kontuan: teknikaren egoera, aplikatzeko kostuak, tratamenduaren izaera, irismena, testuingurua eta helburuak, eta interesdunen eskubide eta askatasunetarako arriskuak.

9.4.5 Informazio pribatua erabiltzeko jakinarazpena eta baimena

Pertsona fisikoen informazio pribatua lortzea ziurtagirien bizi-zikloko prozesuetan (eskaera, nortasunaren egiaztapena, berritzea, baliogabetzea, etab.) pertsona horien baimena beharko da beti, eta interesdunak adierazpen bat egin duela edo baiezko adierazpen argi bat egin duela ulertuko da.

9.4.6 Dibulgazioa, epaileak edo administrazioak hala eskatuta

IZENPEk ez ditu datu pertsonalak partekatuko, agintari administratibo edo judizialek hala eskatzen dutenean izan ezik.

9.4.7 Informazioa hedatzeko beste inguruabar batzuk

Ez da aurreikusten.

9.5 Jabetza intelektualeko eskubideak

Ziurtagirien gaineko eskubideak

IZENPE da egiten dituen ziurtagirien gaineko jabetza intelektualaren eskubideak dituen erakunde bakarra.

Kanpoan geratzen dira ziurtapen digitaleko sisteman erabilitako softwarearen ondoriozko jabetza intelektual eta industrialeko eskubideak, hirugarrenenak direnean.

Hau bera aplikatzen zaio baita ziurtagiriak baliogabetzeko datuen sistemari ere.

Ziurtapen-praktikaren gaineko eskubideak

IZENPEk guztizko jabetza-eskubideak ditu Ziurtapen Praktiken Adierazpen honen gainean.

Izenen gaineko jabetza-eskubideak

Sinatzaileak, eta hala badagokio gakoaren titularrak, kontserbatuko ditu eskubide guztiak (baldin badaude) ziurtagirian jasotako edozein markari, produktuen izenari edo merkataritza-izenari dagokionez.

Sinatzaileak, eta hala badagokio gakoaren titularrak, dira ziurtagirian agertzen den izen bereziaren jabeak, Ziurtapen Praktiken Adierazpen honen 3. atalean zehaztutako informazioz osatua.

Gakoen eta material kriptografikoen gaineko jabetza-eskubideak

Gako-pareak ziurtagirien harpidedunen jabetzakoak dira.

9.6 Adierazpenak eta bermeak

9.6.1 CAren adierazpenak eta bermeak

IZENPEren betebehar eta ardura, fidagarritasun zerbitzu hornitzaile gisa, ziurtagirien sinatzailearen aurrean eta kasu batzuetan erabiltzaile eta hirugarrenengan, ziurtagiriarekiko konfiantza dutenengan, zehaztuko dira erabilera baldintzen dokumentuan edo ziurtagiriaren emate kontratuan, eta bigarren mailan, Ziurtapen Praktiken eta Politiken Adierazpen honetan.

IZENPEk adierazten du ETSI EN 319 411 arauan ezarritako eskakizun teknikoak betetzen dituela ziurtagirien emisiorako, eta konpromisoa hartzen du arau hori edo ordezko arau batzuk betetzeko.
IZENPEk webguneen autentifikazio-ziurtagirien emisioa egiten du CA/Browser Forumak ezarritako «Ziurtagiri fidagarriak emateko eta kudeatzeko oinarrizko eskakizunak» betez, hau eskuragarri dagoen bezala: https://cabforum.org/. Era berean, IZENPEk ziurtagiriak emateko praktikak egokitu egingo ditu eskakizun horien indarreko bertsioari.

Baldintza horien eta politika honen artean inkoherentziarik egonez gero, baldintza horiek nagusituko dira.

Gainera, IZENPEk konpromisoa hartzen du kualifikatutako ziurtagirien emisioari dagokionez, CA/Browser Forum erakundeak mota horretarako ezarritako eskakizunak betetzeko (EV SSL ziurtagirietarako gida), eta eskakizun hauek honako helbide honetan kontsulta daitezke: https://cabforum.org/extended-validation/. Era berean, politika honekin desadostasunik izanez gero, CA/Browser Forum-eko eskakizunek lehentasuna izango dute.

Arau aplikagarrietan eta CPS honen dagokion atalean jasotako betebeharretan eragin gabe, Fidagarritasun Zerbitzu Hornitzaileak konpromisoa hartzen du, ziurtagiria ematerakoan honako hauek egiteko:

- Ziurtagiria eskaintzen duenaren eta sinatzailearen eta/edo haren ordezkariaren nortasuna eta egoera pertsonalak egiaztatzea, eta eskaera egiten duenak sinatzailearen baimena duela adierazteko adierazpena jasotzea.
- Erregistro-prozesuan, sinatzailearen pertsona juridikoari buruzko datuak eta ordezkariaren gaitasuna egiaztatzea. Egiaztapen horiek guztiak dokumentu honetan eta IZENPEren erregistro-protokolo eta -prozeduretan jasotakoaren arabera egitea.
- Egiaztapen-prozesuetan, IZENPEk hirugarrenen bidez egiaztapenak egin ditzake, notario-gaitasunekin edo erregistro espezializatuen bidez.
- Ziurtagiri-eskaerako informazio guztia eskaintzailearen eskutik datorrela egiaztatzea.
- Eskaintzaileak gako pribatuaren jabetza duela egiaztatzea, zeina gako publikoarekin lotuta baitago eta ziurtagiriaren parte izango baita.
- Ziurtagirien autentifikaziorako gako pribatuak sortzeko jarraitu diren prozedurak ziurtatzea, eta IZENPEk ez duela inongo kopiarik gordetzen edo mantentzen.
- Informazioa sinatzaileari, ordezkariari eta eskaintzaileari modu konfidentzialean jakinaraztea.
- Eskaintzaileari, sinatzaileari, ordezkariari eta beste interesdunei IZENPEren Ziurtapen Praktiken Adierazpena eta beste informazio garrantzitsu guztiak eskuratzea bermatzea, ziurtagirien bizitza zikloarekin lotutako prozeduren garapena arautzen duen Ziurtapen Politikaren arabera eta aplikagarri den legediaren arabera.

9.6.2 RAren adierazpenak eta bermeak

RArekin lotutako jarduerak soilik IZENPEk egingo ditu, webguneen autentifikazioko ziurtagirietarako guztientzat.

RAk betebehar hauek ditu:

- Oro har, IZENPEk ezarritako prozedurei jarraitzea, Ziurtapen Politikan eta Praktiken Adierazpenean jasotakoak, bere kudeaketa-, jaulkipen- eta baliogabetze-funtzioak betetzerakoan, eta esparru hori ez aldatzea.

- Bereziki, ziurtagiri-eskatzaile, sinatzaile eta haien ordezkari baten nortasuna eta helburu zehatzaren arabera garrantzitsuak diren egoera pertsonalak egiaztatzea, legeak onartzen dituen edozein bide erabiliz eta Politika honen xedapen orokorrei jarraituz.

- Domeinu-izenaren jabetza sinatzailearen nortasunean dagoela egiaztatzea edo, hala ez bada, sinatzailearen baimena jasotzea, eta hori webguneen autentifikazioko ziurtagirian lotzea, eskuragarri dagoen eta egoera teknologikoaren arabera jabetza hori egiaztatzeko balio duen edozein bide erabiliz.

-

- Sinatzailearen erabaki-gaitasuna argi eta garbi adieraztea domeinuaren jabetzari dagokionez, ziurtagiri-autentifikazioaren objektua den domeinuari dagokionez.
- Ziurtagirien eskaera, berritze edo baliogabetzeak kudeatzen dituen informazio eta dokumentazio guztia 15 urtez gordetzea.
- Eskaerak jasotzea eta kudeatzea www.izenpe.eus webguneko eskaerak kudeatzeko aplikazioaren bitartez.
- Ziurtagirien baliogarritasunari eragiten dioten baliogabetze-arrazoien azterketa zorrotza egitea.

9.6.3 Sinatzailearen adierazpenak eta bermeak

Webguneen autentifikazioko ziurtagiriei dagokienez, sinatzaileek kontrol osoa izan behar dute ziurtagirian jasotako domeinu-izenaren gainean, eta gako pribatuak beren erabilera esklusiboan mantendu behar dituzte. Politika honen arabera emandako ziurtagirien eskaintzaileak eta sinatzaileak betebehar hauek dituzte:

- Ziurtagiria ez erabiltzea Ziurtapen Politika eta Praktika honetan zehaztutako mugetatik kanpo.
- Ziurtagiria ez erabiltzea, baldin eta konfiantzazko zerbitzuen emaileak hura ematen duen ziurtapen-agintaritzaren jarduera utzi badu, batez ere, zigilua sortzeko datuak arriskuan jarri ahal izan badira eta horren berri eman bada.
- Ziurtagiriak eskatzeko informazioa egiaztatuta ematea eta eguneratuta mantentzea, horretarako gaitasun nahikoa duen pertsona batek sinatuz kontratuak.
- Ez eskatzea, ziurtagiriaren titular gisa, beste baten marka komertzialak, produktu-izenak edo jabetza industrial edo intelektualeko eskubideak, ez badu jabetza, lizentzia edo erabilera-baimen frogagarria.
- Jabetzako datuak, sinadura edo zigilua sortzeko datuak edo beste informazio sentikorra (gakoak, ziurtagiria aktibatzeko kodeak, pasahitzak, identifikazio pertsonaleko zenbakiak, etab.) arduraz zaintzea eta babestea, eta inola ere publiko ez egitea.
- Ziurtagirien erabilerari buruzko baldintzak ezagutzea eta betetzea, erabileraren mugak barne, erabilera-baldintzetan eta Ziurtapen Praktiken Adierazpenean jasotakoak.
- Ziurtapen Praktiken Adierazpenaren aldaketak ezagutzea eta betetzea.
- Ziurtagiria baliogabetzeko eskatzea, dokumentu honetan azaltzen den prozedurari jarraituz, eta IZENPEri jakinaraztea azkar baliogabetze hori edo gako pribatuen erabilera okerra, galera, zabalkundea edo aldaketarik izan dela susmatzen bada.
- Ziurtagirian dagoen informazioa berrikustea eta IZENPEri jakinaraztea akats edo desegokitasunik badago.
- Ziurtagirietan konfiantza jarri aurretik, egiaztatzea konfiantzazko zerbitzu-hornitzailearen sinadura elektroniko aurreratua edo zigilua.
- IZENPEri jakinaraztea azkar eskaeran emandako datuen aldaketa oro, eta, hala badagokio, ziurtagiria baliogabetzeko eskatzea.

Sinatzailea arduratuko da ziurtagiriaren erabilera egokia eta zaintza arduratsua bermatzeaz, ziurtagiria zein helburu eta funtziotarako eman den kontuan hartuta, baita IZENPEri jakinarazteaz ziurtagirian agertzen den egoera edo informazioa aldatu den bakoitzean, baliogabetu eta berriz emateko prozesuak burutu daitezen.

Era berean, sinatzailea arduratuko da IZENPEren, Erabiltzaile Erakundearen eta, behar izanez gero, hirugarrenen aurrean, ziurtagiria oker erabiltzen bada, egiazkoak ez diren adierazpenak egoten badira edo akatsak badaude, edo IZENPEri edo hirugarrenei kalte edo galerak eragiten dizkieten ekintzak edo hutsak badaude.

Sinatzailearen ardura eta betebeharra izango da ez erabiltzea ziurtagiria, konfiantzazko zerbitzu-hornitzaileak emisio-ardura utzi badu eta ez badago legeak aurreikusitako ordezkapenik egon. Edonola ere, sinatzaileak ez du ziurtagiria erabili behar hornitzailearen zigilua sortzeko datuak mehatxatuta eta/edo konprometituta egon badaitezke eta hornitzaileak edo sinatzaileak horren berri izan badu.

IZENPEren eta sinatzailearen arteko harremana, Ziurtagirien erabilera-erregimenari dagokionez, erabilera-baldintzei buruzko agiriaren bidez zehaztuko da, edo, hala badagokio, Ziurtagiria emateko kontratuaren bidez, eta IZENPEren eta dagokion Erakundearen arteko hitzarmen, akordio edo harreman-agiriekin bat etorriz.

9.6.4 Konfiantzazko alderdien adierazpenak eta bermeak

Ziurtagiriaren erabiltzaile egiaztatzaileak honako konpromiso hauek hartzen ditu:

- Modu independentean ziurtatzea ziurtagiria aurreikusitako erabilerarako egokia dela.
- Ziurtagiriak erabiltzeko modua eta baldintzak ulertzea, Ziurtapen Praktiken Adierazpenean eta IZENPErekin sinatutako ziurtapen-zerbitzua emateko kontratuan ezarritakoaren arabera.
- Emandako ziurtagirien baliozkotasuna edo baliogabetzea egiaztatzea. Horretarako, erabiltzaileak ziurtagirien egoerari buruzko informazioa kontsultatu beharko du.
- Ziurtapen-hierarkiako ziurtagiri guztiak egiaztatzea, sinadura digitalean edo hierarkia horretako edozein ziurtagiritan konfiantza izan aurretik.
- Ziurtagiria erabiltzeko mugak kontuan hartzea, ziurtagirian bertan agertu ala egiaztapen-kontratuan jaso.
- Kontratu edo beste tresna batean ezarritako edozein ohartarazpen edo arretari kasu egitea, edozein dela ere haien izaera juridikoa.
- Ziurtagiriari dagokionez, ezeztatzeko arrazoitzat har daitekeen edozein gorabehera edo egoera anomaloren berri ematea.
- IZENPEren aldez aurreko eta idatzizko baimenik gabe, ziurtapen-zerbitzuen inplementazio teknikoa monitorizatu, interferitu edo atzeranzko ingeniaritzarik ez egitea.
- Ziurtapen-zerbitzuen segurtasuna nahita arriskuan ez jartzea.

9.6.5 Beste parte hartzaile batzuen adierazpenak eta bermeak

Ez da aurreikusten.

9.7 Bermeak baztertzea

Ez da aurreikusten.

9.8 Arduraren mugak

Ziurtapen Agintaritzaren ardura

IZENPE arduratuko da Ziurtapen Praktiken Adierazpenean deskribatutako ziurtapen-zerbitzuak ematean jarrera negligentea edo arduragabea izateagatik, baita sinadura elektronikoari dagokion araudian jasotako betebehar legalak ez betetzeagatik ere, honako kasu hauek salbu:

- Inola ere ez da IZENPE arduratuko ziurtagirietan jasotako informazioak eragindako kalteengatik, baldin eta edukiak Ziurtapen Praktiken Adierazpenean zehaztutakoa aski betetzen badu.
- Inola ere ez da arduratuko ziurtagiri baten iraungitzearen ondorioz sortzen diren kalteengatik, betiere dokumentu honetan aurreikusitako argitalpen-betebeharrak neurri handi batean betetzen badira.
- IZENPEk ez ditu bere gain hartuko Ziurtagiriak, sinadura digitalak edo Adierazpen honetan jasotako beste zerbitzu edo transakzio batzuk erabiltzetik, entregatzetik, lizentziatik, eragiketatik edo eragiketarik ezetik eratorritako kalte zuzenak, zeharkakoak, bereziak, intzidentalak, ondoriozkoak, lortu gabeko irabaziak, datu-galerak eta zigor-kalteak, aurreikus daitezkeenak edo ez.
- IZENPEk ez du bere gain hartuko sinatzaileei edo fede oneko hirugarrenei egindako kalteen erantzukizunik, baldin eta ziurtagirian jasotako informazioaren zehaztasun-ezak agiri ofizial, notario edo baimenduen bidez ziurtatu badira, salbu eta dokumentu horiek Erregistro Agintaritzak eman baditu.
- Ez da erantzule izango sinatzaileei edo konfiantzazko alderdiei dagozkien betebeharrak ez betetzeagatik sortutako kalteengatik.

IZENPE izango da ziurtagirien baliozkotasuna kontsultatzeko zerbitzua eskura ez izateagatik edo berandu eguneratzeagatik edo ziurtagiriak iraungitzeagatik edozein pertsonari eragindako kalteen erantzulea.

Hirugarrenen aurrean erantzun beharko du, halaber, ziurtapen-zerbitzuak emateko beharrezkoak diren funtzioak eskuordetu dizkien pertsonen ekintzengatik. Ildo horretan, erantzukizun zibileko aseguru poliza bat sinatu da, ziurtagirien erabilerak sor ditzakeen kalte-galerak estaltzeko.

Erregistro Agintaritzaren erantzukizuna

Erregistro Agintaritza gisa jarduten duen eta IZENPE ez den edozein erakunde izango da bere gain hartutako eginkizunak betetzean sortutako kalteen erantzule IZENPEren aurrean, dagokion lege-

akordioan ezarritakoaren arabera.

Identifikatze-eginkizunak ziurtagiriak sinatzen dituzten administrazio publikoek egiten dituztenean, administrazio publikoen ondare-erantzukizunaren araubidea aplikatuko da, Sektore Publikoaren Araubide Juridikoari eta Administrazio Prozedura Erkideari buruzko Legean ezarritakoaren arabera.

Sinatzailearen erantzukizuna

Sinatzailea bere gako pribatuarekin sortutako sinadura digital baten bidez kautotutako transakzio elektroniko guztien erantzule izango da, baldin eta ziurtagiria IZENPEk emandako egiaztapen-zerbitzuen bidez balidatu bada.

Ziurtagiria galdu edo lapurtu izanaren jakinarazpenik jaso ez bada, Ziurtapen Praktiken Adierazpen honetan ezarritakoaren arabera, ziurtagiriak baimenik gabe eta/edo behar ez bezala erabiltzearen ondoriozko erantzukizun oro sinatzaileari egotziko zaio.

Ziurtagiriak onartzean, sinatzaileak konpromisoa hartzen du IZENPE, Erregistro Agintaritzak eta Erakunde Erabiltzaileei babesa emateko eta, behar izanez gero, kalte-ordaina ordaintzeko, ekintza edo hutsaren ondorioz sortutako kalte, galera, zor, gastu legal edo bestelako kostuak, profesionalen tasak barne, IZENPEk, Erregistro Agintaritzek edo Erakunde Erabiltzaileek jasandakoak, ziurtagirien erabilera edo argitalpenaren ondorioz, eta honako hauetatik eratorritakoak:

- Ziurtapen Agintaritzarekin lotzen duen instrumentu legalaren termino eta baldintzak ez betetzea,
- Ziurtagirien erabilera baimenik gabeko pertsona batzuekin egindako transakzio elektronikoetan,
- Sinatzailearen aldetik egindako egiaztapen faltsuak edo gezurrak,
- Sinatzaileak ziurtagirietan dagozkion datu materialak ezkutatzea, eta hori arduragabeki edo IZENPE, Erakunde Publiko Erabiltzaileei edo ziurtagirian konfiantza duten hirugarrenei engainatzeko asmoz egitea,
- Gako pribatuaren babesa ez betetzea edo galtzea, zabalkundea, aldaketa edo baimenik gabeko erabilera saihesteko neurri arrazoizkoak ez hartzea.

Horrekin lotuta, IZENPEk ez du arduratuko sinatzaileei edo onargarri diren hirugarrenei eragindako kalteengatik, sinatzaileak betebehar hauek ez betetzeagatik:

- IZENPEri edo Erregistro Agintaritzari eskaeretan edo emisio- eta baliogabetze-prozesuetan beharrezko informazio guztia osatu, egia eta zehatza ematea, zerbitzu-hornitzaileak akatsak detektatu ez baditu.
- Ziurtagiriari buruz emandako informazioan egindako aldaketa IZENPEri edo Erregistro Agintaritzari berehala jakinaraztea.
- Sinadura sortzeko datuak arduraz zaintzea, haien konfidentzialtasuna bermatzea eta baimenik gabeko sarbide edo argitalpenetatik babestea.
- Sinadura sortzeko datuen konfidentzialtasuna galdu den susmoa badago, ziurtagiria baliogabetzeko eskaera egitea.
- Ziurtagiriaren baliozkotze-epea amaitzean edo zerbitzu-hornitzaileak balioztatzen ez duenean, sinadura sortzeko datuak erabiltzetik uko egitea.

- Ziurtagirien erabilerari buruzko murrizketak errespetatzea eta zerbitzu hornitzaileak ezarritako erabilera baldintzak betetzea.

Konfiantzazko hirugarrenen ardura

Ziurtagiri baten gaineko konfiantza egiaztatu gabe duten hirugarrenek erantzukizun osoa dute konfiantza horrekin lotutako arrisku guztiengatik, eta inolaz ere ezin dute IZENPE, Erregistro Agintariak, Erakunde Erabiltzaileak edo Sinatzaileak errudun utzi ziurtagirietan edo sinaduretan konfiantza jarri izanagatik.

Horrekin lotuta, IZENPEk ez du arduratuko sinatzaileei edo hirugarrenei eragindako kalteengatik, elektronikoki sinatutako dokumentuen jasotzaileek honako betebehar hauek bete ez badituzte:

- Ziurtagiriaren erabilera-murrizketak eta transakzioen gehieneko kopuruak egiaztatzea eta kontuan hartzea.
- Ziurtagiriaren baliozkotasuna egiaztatzea.
- Ziurtagirien zerbitzu fidagarrietako zerrendan (TSL) ziurtagiri kualifikatuko identifikatzailea egiaztatzea.

9.9 Kalteen ordainketak

IZENPEk bere betebeharrak ez betetzeagatik edo araudi legalak urratzeagatik, kalteen ordainketarako klausulak sartuko dira IZENPE eta sinatzaileen eta egiaztatzaileren arteko instrumentu legaletan.

9.9.1 CAri kalte-ordaina

Ez da aurreikusten.

9.9.2 Sinatzaileei kalte-ordaina

Ez da aurreikusten.

9.9.3 Konfiantzazko hirugarrenei kalte-ordaina

Ez da aurreikusten.

9.10 Indarraldia eta amaiera

9.10.1 Indarraldia

Ziurtapen-politika hau indarrean jarriko da argitaratu den unean.

9.10.2 Amaiera

Politika hau baliogabetuko da dokumentuaren bertsio berri bat argitaratzen denean.

Bertsio berriak aurrekoa osorik ordezkatuko du. IZENPEk konpromisoa hartzen du politika hau urteroko berrikuntza-prozesu baten menpe jartzeko.

9.10.3 Amaieraren eta iraunkortasunaren ondorioak

Politika honen arabera emandako eta indarrean dauden ziurtagirientzat, bertsio berriak lehentasuna izango du aurrekoarekin talka egiten ez duen guztian.

9.11 Jakinarazpen banatuak eta parte-hartzaileen arteko komunikazioa

IZENPEk ezarriko ditu jakinarazpenak egiteko bide eta epeak instrumentu legal loteslearen bidez.

Orokorrean, IZENPEren webgunea (www.izenpe.eus) erabiliko da edozein motatako jakinarazpen eta komunikazioak egiteko.

9.12 Aldaketak

9.12.1 Aldaketa-prozedura

Ziurtapen Politikaren aldaketak IZENPEren Segurtasun Batzordeak onartuko ditu, eta horren berri emango da dagokion aktan, onartutako barne-prozeduraren arabera.

9.12.2 Jakinarazteko mekanismoa eta epea

Politika honen edozein aldaketa berehala argitaratuko da bere sarbide URLean.

Aldaketek ez badute eragin nabarmenik alderdi guztien betebehar eta arduren sisteman, ez eta zerbitzuen politika-aldaketetan ere, IZENPEk ez die erabiltzaileei aurretik jakinaraziko; besterik gabe, bertsio berria bere webgunean argitaratuko du.

9.12.3 OID aldatzeko egoerak

Zerbitzuaren baldintzak, betebehar eta arduren erregimena edo erabilera-mugak modu esanguratsuan aldatzen badira, zerbitzuaren politika eta haren identifikatzailea (OID) ere aldatu ahal izango dira, eta politika berriaren lotura ere sortu. Kasuan kasu, IZENPEk mekanismo bat ezarri ahal izango du proposatutako aldaketak jakinarazteko eta, dagokionez, interesdunen iritziak jasotzeko.

9.13 Gatazken ebazpenerako xedapenak

IZENPE kontsumoko artekaritza-sistemaren menpe dago, aplikagarri den legediaren arabera, eta hori erabiltzaileek eta sinatzaileek jartzen dituzten kexak edo gatazkak konpontzeko bide bezala. Sistema honen ebazpenak behin betikoak eta bi aldeentzat lotesleak dira.

Horretarako, ulertzen da eskatzailea edo sinatzailea sistema onartzen duela erreklamazioa dagokion kontsumoko artekaritza-batzordeari aurkeztu dion unean.

Ziurtagirien erabiltzaile edo sinatzaileek jartzen dituzten bestelako gatazka legalak, kontsumoko artekaritza-sistemak ez dituenak arautzen, dagokion jurisdikzioaren mende gelditukо dira.

9.14 Aplikagarri den legeria

Ziurtapen Praktiken Adierazpen honen exekuzioa, idazketa, interpretazioa eta baliagarritasuna Espainiako sinadura elektronikoari buruzko legearen arabera arautuko dira.

Dokumentu honi eta bertatik sortzen diren jarduerei aplikatzen zaizkien arauak honako hauek dira:

- 6/2020 Legea, azaroaren 11koa, Konfiantzazko zerbitzu elektronikoen zenbait alderdi arautzekoa.
- 910/2014 (EB) Erregelamendua (eIDAS 1), barne-merkatuko transakzio elektronikoetarako identifikazio elektronikoari eta konfiantzazko zerbitzuei buruzkoa, 1999/93/EE Zuzentaraua indargabetzen duena.
- 2024/1183 (EB) Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2024ko apirilaren 11koa, 910/2014 (EB) Erregelamendua aldatzen duena nortasun digital europarraren esparrua ezartzeari dagokionez (eIDAS 2).
- 39/2015 Legea, Administrazio Publikoen Administrazio Prozedura Erkidearena.
- 40/2015 Legea, Sektore Publikoaren Araubide Juridikoarena.
- 3/2018 Lege Organikoa, abenduaren 5ekoa, Datu Pertsonalak Babestekoa eta Eskubide Digitalak Bermatzekoa.
- (EB) 2016/679 Erregelamendua (DBEO), datu pertsonalen tratamenduari eta datu horien zirkulazio askeari dagokienez pertsona fisikoak babesteari buruzkoa.

IZENPEren konfiantzazko zerbitzuak emateko, honako arau tekniko hauek bete behar dira:

- ETSI EN 319 401: Konfiantzazko zerbitzuen emaileentzako politikaren baldintza orokorrak.
- Konfiantzako Zerbitzuen Praktiken eta Ziurtapen Elektronikoaren Adierazpen Orokorra, 5.7 bertsioa.
- ETSI EN 319 421: Konfiantzazko Zerbitzu Hornitzaileentzako politika- eta segurtasun-eskakizunak, denbora-zigiluak ematen dituztenentzat.
- ETSI EN 319 411-2: EBko ziurtagiri kualifikatuak ematen dituzten hornitzaileentzako eskakizunak.
- ETSI EN 319 412: Ziurtagiri elektronikoen profilak.
- ETSI EN 319 421: Konfiantzazko Zerbitzu Hornitzaileentzako politika- eta segurtasun-eskakizunak, denbora-zigiluak ematen dituztenentzat.

- ETSI EN 319 422: Denbora-zigiluen protokoloa eta denbora-zigiluen tokenen profilak.
- CABForum-en Oinarrizko Eskakizunak.
- CABForum-en EV Ziurtagiri Gidak.

9.15 Legea betetzeko konpromisoa

IZENPEk konpromisoa hartzen du webguneen autentifikazio-ziurtagiri mota bakoitzari aplika dakizkiokeen araudiak eta baldintzak betetzeko, «1.5.4. BZO onartzeko prozedura» dokumentu honetan.

9.16 Xedapen anitzak

9.16.1 Akordio osoa

Ziurtapen Praktiken Adierazpen honetako klausula bakoitza baliozkoa da berez, eta ez du eraginik gainerako klausulen baliozkotasunean. Klausula baliogabea edo osatugabea bada, haren ordez beste klausula baliokide bat ezar daiteke.

IZENPEren eskubide eta betebeharrei zuzenean eragiten dieten eta gainerako alderdiei eragiten ez dieten Ziurtapen Praktiken Adierazpen honetako termino eta xedapenak ezingo dira zuzendu, uko egin, osatu, aldatu edo ezabatu IZENPEren berariazko eta idatzizko baimenik gabe. Aldaketa horrek ez du beste alde guztien eskubide eta betebeharretan eragingo, eta ez da berrikuntza juridikoa, baizik eta aldaketa bat izango da.

9.16.2 Lagatzea

IZENPEk ez du erantzukizunik izango zerbitzurik ez dagoelako edo anomaliak daudelako, ez eta zuzenean edo zeharka eragin daitezkeen kalte-galerengatik ere, baldin eta etenaldi edo hondamendi hori halabeharrak, atentatu terroristek, sabotajeek edo greba basatiek eragin badute; hori guztia zerbitzua ahalik eta azkarren konpontzeko eta/edo berrezartzeko beharrezkoak diren jarduerei kalterik egin gabe.

9.16.3 Banakortasuna

Ez da aurreikusten.

9.16.4 Exekuzioa (abokatuen tasak eta eskubideei uko egitea)

Ez da aurreikusten.

9.16.5 Ezinbestea

Ez da aurreikusten.

9.17 Beste xedapen batzuk

Xedapenik gabe.