# ZIURTAPEN PRAKTIKEN DEKLARAZIOAREN EGUNERATZEA

Erreferentzia: IZENPE-ACTUALIZACIÓN DPC
Bertsio zkia.: v 5.03
Data: 2015eko martsoaren 10a



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

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

# Informazio orokorra

## Dokumentuen kontrola

| | |
|---|---|
| **Izenburua:** | Ziurtapen Praktiken Deklarazioa eguneratzea. |
| **Bertsioa:** | 5.03 |
| **Onartze-data:** | 2015/03/10 |
| **Erabilitako dokumentazioa:** | ZPD 5.02 |
| **Egilea(k)** | Izenpeko Aholkularitza Juridikoa<br>IZENPEko arlo teknikoa |
| **Aldaketak/Iruzkinak** | 5.03 bertsioa 5.02. bertsioaren eguneratzea da |

IZENPE, SAren Ziurtapen Praktiken Deklarazioren 9.11. epigrafearen arabera, aldaketak egin daitezke Ziurtapen Praktiken Deklarazioan. Aldaketa horiek dokumentu honetan jaso badira ere, IZENPE, SAk ematen dituen ziurtagiriak eskatzen edo erabiltzen badituzu, edo ziurtagiri horietaz fidatzen bazara, nahitaez ezagutu beharko duzu oso-osorik Ziurtapen Praktiken Deklarazio eguneratua.

## 1. SARRERA_Egokitzapena

**Zuzenketa:**

IZENPEk ETSI arauen arabera egindako ikuskapenaren ondorioz, eta beste zerbitzu batzuk txertatzearen eraginez, honako aldaketa hauek hartu dira barnean:

| EPIGRAFEA | ALDAKETA |
|---|---|
| **Dokumentu osoa** | **"Onartu" guztien ordez "kualifikatu" terminoa** |
| **1. Sarrera** | **Jatorrizkoa:**<br>IZENPEk ETSIren (Telekomunikazioetako Estandarren Europako Institutuaren) estandarren adierazpenak jarraitzen ditu, eta honako bi arau hauen zehaztapen teknikoen (TS) arabera lortu du ziurtapena: sinadura sortzeko gailu seguru batean (QCP Public + SSCD) sortutako ziurtagiri kualifikatuak jaulkitzeko 101 456 arauaren zehaztapen teknikoen arabera; eta gako publikoko azpiegitura-ziurtagiriak (PKI) jaulkitzeko 102 042 arauaren zehaztapen teknikoen arabera, betiere balidazio hedatuko ziurtagirien politikari, EVCP, eta CA/Browser Forum-ek onartutako gidei jarraituta.<br><br>**Ordeztua:**<br>IZENPEk ETSIren (Telekomunikazioetako Estandarren Europako Institutuaren) estandarren adierazpenak jarraitzen ditu, eta honako bi arau hauen zehaztapen teknikoen (TS) arabera lortu du ziurtapena: sinadura sortzeko gailu seguru batean (QCP Public + SSCD) sortutako ziurtagiri kualifikatuak jaulkitzeko 101 456 arauaren zehaztapen teknikoen arabera; eta ziurtagiri kualifikatuak eta ez kualifikatuak jaulkitzeko 102 042 arauaren arabera. Balidazio hedatuko ziurtagirien politikari (EVCP) jarraitzen dioten zerbitzari seguruko ziurtagirietarako, eta erakundearen balidazio-politikari (□VCP) jarraitzen dioten zerbitzari seguruko ziurtagirietarako, CA/Browser Forum-ek onartutako gidei ere jarraituko zaie.<br><br>**Jatorrizkoa:**<br>TS 101 456 eta TS 102 042 arauen ezartzen diren TS zehaztapen teknikoek ziurtapenen kudeaketa eta praktikari buruzko oinarrizko baldintzak zehazten dituzte, eta baldintza horiek bete behar dituzte ziurtagiri kualifikatuak eta kualifikatu gabeak jaulkitzen dituzten entitateek, baldin eta jaulkitzen dituzten ziurtagiriak Europako Parlamentuko 1999/93/EE zuzentarauaren lege-esparruaren araberakoak badira –zuzentarau hori Espainiako erregimen juridikoan sinadura elektronikoari buruzko 59/2003 |

| | |
|---|---|
| | legearen bitartez sartu zen-.<br><br>**Ordeztua:**<br>TS 101 456 eta TS 102 042 arauen ezartzen diren TS zehaztapen teknikoek ziurtapenen kudeaketa eta praktikari buruzko oinarrizko baldintzak zehazten dituzte, eta baldintza horiek bete behar dituzte ziurtagiri kualifikatuak eta kualifikatu gabeak jaulkitzen dituzten entitateek, baldin eta jaulkitzen dituzten ziurtagiriak Europako Parlamentuko eta Kontseiluko 1999/93/EE zuzentarauaren lege-esparruaren araberakoak –zuzentarau hori Espainiako erregimen juridikoan sinadura elektronikoari buruzko 1999/93 legearen bitartez sartu zen– eta, ondoren, identifikazio elektronikoari eta barne-merkatuko transakzio elektronikoetarako konfiantzako zerbitzuei buruzko 910/2104 araudiaren (eIDAS) araberakoak badira. |
| **1.1. Aurkezpena** | **Erantsia:**<br>• "Egiaztapen Zerbitzuak zerbitzua erabiltzen duen entitateari aukera ematen dio IZENPEk jaulkitako ziurtagiriak erabiltzeko. Horretarako, ziurtagirien egoera begiratzen du, CRL (Certificate Revocation List) protokoloaren bidez.<br>• ZAIN sinadura-zerbitzuen plataforma konfiantzako zerbitzuen plataforma bat da, segurtasun-zerbitzu global eta estandarizatuen multzoa hartzen duena barne (kautotzea, baimentzea, sinadura elektronikoa eta datuen babesa), web-zerbitzu gisa.<br>• IZENPEk dohainik eskaintzen du id@zki. Nabigatzaile baten barruan integratu ahal izateko applet itxura duen Java aplikazio bat, elektronikoki sinatzeko eta zifratzeko funtzionaltasuna duena.<br>• IZENPEren sinadura-euskarriko zerbitzua ohiko sinadura-euskarriaren bertsio digitala da. Pertsona batek sinatu behar dituen dokumentuak jasotzeko azpil batean datza.<br>• ZIURRA komunikazio ziurtatuko zerbitzuak konfiantzako hirugarren gisa ("notario digital" gisa) jarduten du, eta, hartara, mezu elektroniko edo SMS bat igorri dela eta hartzaileak mezu hori hartu duela fede ematen du.<br>• Argitalpena Jasota Uzteko eta Egiaztatzeko Zerbitzuak aukera ematen du kontratazio publiko batean barnean hartzen den informazioaren hedapen publikoaren hasierako unea fedez egiaztatzeko.<br>• EG ITZA hodeian ziurtagiriak gordetzeko zerbitzuak aukera ematen |

| | |
|---|---|
| | du azken erabiltzailearen ziurtagiriak modu seguruan gordetzeko. “<br><br>**Ezabatua:**<br>• “IZENPEk informatikako hainbat aplikazio ditu, baita sinadura elektronikoa erabiltzen duten aplikazioak garatzeko zehaztapen teknikoak ere. Aplikazio horiek lizentziapean eskaintzen dizkie entitate erabiltzaileei.”<br><br>**Pertsona fisikoaren, juridikoaren eta gailuaren sailkapena erantsita taulan** |
| **Ziurtapen-agintaritzak.** | **Ezabatua:**<br>“**2003ko mendeko** ziurtapen-agintaritzak.<br>CA horiek IZENPEren oinarrizko CA berrira migratu dira.”<br><br>**CA 2003ko mendeko CAen taulak ezabatua**<br><br>**subCA SSL EV taula zaharkitua ezabatua** |
| **1.3.3. Ziurtagirien erabiltzaile diren azken entitateak** | **Izenburua aldatua, “Azken entitate erabiltzaileak” ordez “Ziurtagirien erabiltzaile diren azken entitateak”** |
| **1.3.4. Denbora-zigiluen erabiltzaile diren azken entitateak** | **1.3.4. “Denbora-zigiluen erabiltzaile diren azken entitateak” puntua sortua** |
| **1.3.5. Konfiantzako hirugarren batzuk** | **Jatorrizkoa:**<br>“Ziurtapen Praktiken Deklarazio honen barruan, IZENPEk jaulkitako ziurtagiriak jasotzen dituzten pertsona fisiko edo juridikoak ziurtagirietan konfiantza duten hirugarren batzuk dira; beraz, ziurtagiri horietan konfiantza izatea erabakitzen dutenean, ziurtapen-praktiken deklarazio honetan jasotakoa aplikatuko zaie.”<br><br>**Ordeztua:**<br><br>“Ziurtapen Praktiken Deklarazio honen barruan, IZENPEk jaulkitako ziurtagiriak eta denbora-zigiluak jasotzen dituzten pertsona fisiko edo juridikoak ziurtagirietan eta denbora-zigiluetan konfiantza duten hirugarren batzuk dira; beraz, ziurtagiri eta denbora-zigilu horietan konfiantza izatea erabakitzen dutenean, ziurtapen-praktiken deklarazio honetan jasotakoa aplikatuko zaie”. |

| | |
|---|---|
| | **Jatorrizkoa:**<br>“Hirugarrenek ziurtagirietan jartzen duten konfiantza harpidedunekiko harremanetan ziurtagiri horietaz egiten duten erabilera objektiboaren araberakoa izaten dela jotzen da.”<br><br>**Ordeztua:**<br>“Hirugarrenek ziurtagirietan eta denbora-zigiluetan jartzen duten konfiantza harpidedunekiko harremanetan ziurtagiri horietaz egiten duten erabilera objektiboaren araberakoa izaten dela jotzen da.”<br><br>**Jatorrizkoa:**<br><br>“Hirugarrenek arduraz erabili behar dituzte ziurtagiri mota guztiak eta fede onez eta leialtasunez jardun behar dute. Halaber, ez dute izan behar ziurtagiriaren kategoriari dagokion konfiantza-esparruaren barruan bidalitako mezuei uko egitea helburu duten iruzur- edo zabarkeria-jarrerarik.”<br><br>**Ordeztua:**<br><br>“Hirugarrenek arduraz erabili behar dituzte ziurtagiri eta denbora-zigilu mota guztiak eta fede onez eta leialtasunez jardun behar dute. Halaber, ez dute izan behar ziurtagiriaren edo denbora-zigiluaren kategoriari dagokion konfiantza-esparruaren barruan bidalitako mezuei uko egitea helburu duten iruzur- edo zabarkeria-jarrerarik.” |
| **1.4.1. Ziurtagiriaren erabilera egokiak** | **“Ziurtagiri kualifikatua” ataletik “Ziurtagiri kualifikatu gabea” atalera eraman da:**<br>“Egoitzako eta EV Egoitzako ziurtagiriak webguneak modu fidagarrian identifikatzeko jaulkitzen dira.<br><br>Egoitza eta ziurtagiri elektronikoko ziurtagiriak egoitza elektronikoa eta dokumentuen zigilatze elektronikoa identifikatzeko jaulkitzen dira, betiere *Zerbitzu Publikoetarako Hiritarren Sarrera Elektronikoari buruzko 11/2007 Legean* aurreikusitakoaren arabera.”<br><br>**Jatorrizkoa “Gailu informatikoko ziurtagiria” atalean:**<br>“Gailu informatikoen eragiketaz arduratzen diren entitateei zerbitzari seguruko ziurtagiriak (SSL eta SSL EV) eta aplikazio-ziurtagiriak jaulkitzen zaizkie.”<br><br>**Ordeztua:**<br><br>“Gailu informatikoen eragiketaz arduratzen diren entitateei zerbitzari seguruko ziurtagiriak (SSL DV, SSL □V, SSL EV, Egoitza eta Egoitza EV) eta aplikazio-ziurtagiriak jaulkitzen zaizkie.” |

| | |
|---|---|
| **1.6.1. Definizioak** | **Erantsia:**<br>“Denbora zigilatzeko agintaritza (TSA): denbora-zigiluko tokenak jaulkitzen dituen agintaritza” |
| **2.2. Ziurtapen-informazioaren argitalpena** | **Jatorrizkoa:**<br>“Informazio hori http://www.izenpe.com web-orrian dago eskuragarri, 24 orduetan eta asteko 7 egunetan.”<br><br>**Ordeztua:**<br>“Informazio hori www.izenpe.com web-orrian dago eskuragarri, 24 orduetan eta asteko 7 egunetan.<br><br>**Jatorrizkoa:**<br>“Ezeztatutako Ziurtagirien Zerrendak argitaratzeari dagokionez, sarbide azkarra eta segurua bermatzen zaie erabiltzaileei eta ziurtagirien harpidedunei.”<br><br>**Ordeztua:**<br>“Ezeztatutako Ziurtagirien Zerrendak argitaratzeari dagokionez, sarbide azkarra, segurua eta doakoa bermatzen zaie erabiltzaileei eta ziurtagirien harpidedunei.” |
| **2.2.1. Argitalpen- eta jakinarazte-politika** | **Jatorrizkoa:**<br>"Zerbitzuaren zehaztapenetan edo baldintzetan egindako aldaketak IZENPEren web-orri nagusiaren (http://www.Izenpe.com) bidez jakinaraziko zaizkie erabiltzaileei."<br><br>**Ordeztua:**<br>Zerbitzuaren zehaztapenetan edo baldintzetan egindako aldaketak IZENPEren web-orri nagusiaren (www.izenpe.com) bidez jakinaraziko dizkie IZENPEk erabiltzaileei. |
| **3.2.1. Gako pribatuaren jabetza frogatzeko metodoak** | **Jatorrizkoa:**<br>Gako-parea<br>• Erregistro-entitate batek sortua bada, honela frogatzen da gako pribatuaren jabetza: gailu kriptografikoa entregatzeko eta onartzeko prozedura fidagarriaren indarrez, horri dagokion ziurtagiriaren bitartez, eta barruan duen gako-pareari esker.<br>• Ziurtagiriaren gakoen edukitzaileak sortua bada, honela frogatzen da gako pribatuaren jabetza: ziurtagiria behar bezala |

| | |
|---|---|
| | erabiliz.<br><br>**Ordeztua:**<br><br>Gako-parea<br><br>• erregistro-entitate batek sortua bada eta gakoak txartel kriptografiko batean kokatuta daudenean, honela frogatzen da gako pribatuaren jabetza: gailu kriptografikoa entregatzeko eta onartzeko prozedura fidagarriaren indarrez, horri dagokion ziurtagiriaren bitartez, eta barruan duen gako-pareari esker.<br>• erregistro-entitate batek sortua bada eta gakoak HSM batean kokatuta daudenean, honela frogatzen da gako pribatuaren jabetza: HSMan zaintzeko prozedura fidagarriaren indarrez, eta gakoak harpidedunak soilik eskuratzeko prozedura fidagarriaren bitartez.<br>• Ziurtagiriaren gakoen edukitzaileak sortua bada, honela frogatzen da gako pribatuaren jabetza: ziurtagiria behar bezala erabiliz. |
| **3.3. Gakoak berriro jaulkitzeko eskaeretarako identifikatzea eta kautotzea** | **Jatorrizkoa:**<br>“Ziurtagiria ezeztatu eta beste bat jaulki ondoren, gakoak berritu egin behar dira beti.”<br><br>**Ordeztua:**<br>“IZENPEk gakoak sortzen dituen ziurtagirietan, ziurtagiria ezeztatu eta beste bat jaulki ondoren, gakoak berritu egin behar dira beti.” |
| **4.1. Ziurtagiri-eskaera.** | **Jatorrizkoa:**<br>“Horretarako, zehaztasunez idatzi behar dira identifikazio-dokumentuetan bildutako izen-abizenak, betiere ziurtagiriaren edukian finkatutako baldintza teknikoek eragiten dituzten leku-mugak kontuan izanik.”<br><br>**Ordeztua:**<br><br>“Horretarako, zehaztasunez idatzi behar dira identifikazio-dokumentuetan bildutako datu identifikatzaileak, betiere ziurtagiriaren edukian finkatutako baldintza teknikoek eragiten dituzten leku-mugak kontuan izanik.” |
| **4.2.2. Eskaerak onartzea edo baztertzea** | **Erantsia:**<br>“Eskaera hori zerbitzari bat kautotzeko domeinu-izen bat barnean hartzen duen ziurtagiri baterako denean, IZENPEk baimendutako CAen erregistroa (CAA erregistroa) aztertuko du, RFC 6844 arabera. CAA erregistro horiek badaude eta, erregistratuta ez dagoelako, IZENPEri ez badiote ziurtagiri horiek jaulkitzeko aukera ematen, IZENPEk ez du ziurtagiri hori jaulkiko, |

| | |
|---|---|
| | baina eskatzaileek eskaera egin ahal izango dute berriro, behin IZENPEk balizko gorabehera hori konpondu ahal izan duenean.” |
| **4.2.3. Gako pribatuaren zaintza** | **Erantsia:**<br>““Ziurtagiria hodeian” zerbitzuaren kasuan, ziurtagirien azken erabiltzaileko gako pribatuak gailu kriptografiko seguruetan gordeta daude –FIPS 140-2 3. maila arauarekin ziurtatuta daude gailu horiek–. “ |
| **4.3. Ziurtagiria jaulkitzea** | **Erantsia:**<br>**“**Ez dira desblokeatzeko kodeak (PIN edo PUK) emango IZENPEk gakoak sortu ez dituen ziurtagirien kasuan.” |
| **4.3.1. CAren jardunak ziurtagiriak jaulkitzean** | **Jatorrizkoa:**<br>“Ziurtagiriaren arabera, gailu kriptografikoan edota software-euskarrian jaulki daiteke.”<br>**Ordeztua:**<br>“Ziurtagiriaren arabera, smartcard-ean, HSMan edota software-euskarrian jaulki daiteke.”<br><br>**Jatorrizkoa:**<br>“Gailu kriptografikoan jaulkitzerakoan jarraitu beharreko prozedura:”<br>**Ordeztua:**<br>“Smartcard-ean jaulkitzerakoan jarraitu beharreko prozedura:”<br><br>**Erantsia:**<br><br>I. “HSMan jaulkitzerakoan jarraitu beharreko prozedura:”<br><br>• Erregistro Entitateak egiaztatu egiten du eskatzaileek aurkeztutako dokumentuaren baliozkotasuna.<br>• Kautotze-lana amaitu ondoren, ziurtagiri bat jaulkitzeko eskatzen dio IZENPEri erregistro-entitateak.<br>• Eskaera erregistro-entitate baimendu batek bidali duela egiaztatu ondoren, IZENPEk ziurtagiria jaulkitzen du –ezarritako prozedurari jarraiki– eta erregistro-entitateari igortzen dio.<br>• Eskaera IZENPEk bidali duela egiaztatu ondoren, erregistro-entitateak sinadura sortzeko gailuan kargatzen du ziurtagiria, gailu kriptografikoak kudeatzeko prozesu seguru bat erabiliz.<br>• Arrazoiren batengatik IZENPEk ziurtagiria ez jaulkitzea |

| | |
|---|---|
| | erabakitzen badu (nahiz eta kautotze-prozedurak egokiak izan), erabaki horren arrazoiak jakinarazi egin behar zaizkio eskatzaileari."<br><br>**Jatorrizkoa:**<br>"Eskaera-formularioarekin batera, eskatzaileak gako-parea sortu beharko du zerbitzarian bertan, eta IZENPEri eman beharko dio gako publikoa."<br>**Ordeztua:**<br>"Eskaera-formularioarekin batera, eskatzaileak gako-parea sortu beharko du zerbitzarian bertan, eta IZENPEri eman beharko dio eskaera teknikoa." |
| **4.3.3. CAk beste entitate batzuei ziurtagiria jaulki izana jakinaraztea** | **Jatorrizkoa:**<br>"IZENPEk ez die beste entitate batzuei jakinaraziko ziurtagiriak jaulki izana."<br><br>**Ordeztua:**<br>"IZENPEk ez die beste entitate batzuei jakinaraziko ziurtagiriak jaulki dituela, IZENPEren Certificate Transparency Log Server zerbitzuan argitaratutako EV ziurtagiriak izan ezik." |
| **4.5.1. Harpidedunaren gako pribatua eta ziurtagiriaren erabilera** | **Jatorrizkoa:**<br>"Harpidedunak,"<br>**Ordeztua:**<br>"Bere gakoak zaintzen dituen harpidedunak,"<br><br>**Erantsia:**<br>Bere gakoak IZENPEn gordetzen dituen harpidedunak,<br>• Ziurtagiria egokiro erabiliko du, eta, zehazki, ziurtagirien erabilera-mugak aintzat hartuko ditu.<br>• Arretaz zainduko du aktibatzeko gakoa, baimendu gabeko erabilerak saihestearren, Ziurtapen Praktiken Deklarazioko 6.1, 6.2 eta 6.4 sailek agintzen dutenaren arabera.<br>• IZENPEri eta, harpidedunaren ustez, ziurtagirian konfiantza duen edonori hau jakinaraziko dio, justifikatzerik ez dagoen atzerapenik gabe:<br>o Gako pribatuaren kontrola galdu izana, aktibatze-datuak arriskuan jartzeagatik edo beste edozein arrazoirengatik.<br>o Ziurtagiriaren edukian dauden okerrak edo izandako aldaketak (harpidedunak dakizkienak edo jakin litzakeenak). Aldaketak ziurtagiria ezeztatzea badakar, horretarako eskaera egin behar du harpidedunak.<br>• Gako pribatua erabiltzeari utziko dio ziurtagiriaren balio-epea |

| | |
|---|---|
| | amaitu ondoren.<br>• Gakoen edukitzaileei jakinaraziko die zein betebehar dagozkien.<br>• Ez du ziurtagiri-zerbitzuen ezartze teknikoa kontrolatuko eta manipulatuko, ezta atzeranzko ingeniaritzako ekintzarik egingo ere, aurrez Ziurtapen Entitatearen idatzizko baimenik eduki gabe.<br>• Ez du ziurtagiri-zerbitzuen segurtasuna arriskuan nahita jarriko.<br>• Ez ditu ziurtagirietako gako publikoei dagozkien gako pribatuak erabiliko inongo ziurtagiri izenpetzeko, ziurtapen-entitatea balitz bezala.<br>• Ziurtagirian zerrendatutako gako publikoari dagokion gako pribatua erabiliz sinadura digitalak sortzen dituen ziurtagiri kualifikatuen harpidedunak aitortu egin behar du, dagokion bitarteko juridikoaz, sinadura elektroniko horiek eskuz idatzitako sinaduren baliokide direla, gailu kriptografikoa erabiltzen denean, betiere Sinadura Elektronikoari buruzko Legearen 3.4. artikuluak agintzen duenaren arabera. |
| **4.9.3 Ezeztatzeko eskaeren tratamendua** | **Ezabatua:**<br>"Identifikatzeko honako hau eskatuko da:<br>○ Telefono bidez identifikatzeko pasahitza (gakoen orrian igorritakoa).<br>○ NAN /AIZ.<br>○ Entitatearen IFZ, pertsona juridikoaren ziurtagiria bada."<br><br>**Erantsia:**<br>"Ziurtagiri motari dagokion berariazko dokumentazioa kontsultatu, identifikaziorako zer beharko den jakiteko". |
| **4.9.4. Ezeztatzea prozesatzeko CAren epea** | **Jatorrizkoa:**<br>"4.9.3 atalean adierazitakoa egin ostean, eta RAk ziurtagiria ezeztatzeko izapideak behar bezala egin ondoren, ezeztatzea berehala izango da indarrean, gaur egungo legeriaren arabera."<br><br>**Ordeztua:**<br><br>"4.9.3 atalean adierazitakoa egin ostean, eta RAk ziurtagiria ezeztatzeko izapideak behar bezala egin ondoren, ezeztatzea gaur egungo legeriaren arabera izango da indarrean." |
| | |

| | |
|---|---|
| **4.9.10. Ezeztatzeak ohartarazteko eskura dauden beste modu batzuk** | **Jatorrizkoa:**<br>"IZENPEk ez du norberaren ziurtagirien egoera egiaztatzea ohartarazteko beste modurik."<br>**Ordeztua:**<br>"Ziurtagiri kualifikatu bat ezeztatzen denean, IZENPEk informaziorako mezu elektronikoa bidaltzen dio ziurtagiriaren harpidedunari" |
| **6.1.1. Gako-parea sortzea** | **Jatorrizkoa:**<br>• "Hardware-gailu kriptografikoan jaulkitako ziurtagiriak: gakoak gailu kriptografikoak sortzen ditu."<br>**Ordeztua:**<br>• Txartel kriptografikoan edo HSMan jaulkitako ziurtagiriak: gakoak gailu kriptografikoak sortzen ditu. |
| **6.1.2. Gako pribatua harpidedunari banatzea** | **Jatorrizkoa:**<br>• "Hardware-gailu kriptografikoan jaulkitako ziurtagiriak: kautotze eta sinadura elektroniko aurreratuko gako pribatuak gailu kriptografikoarekin batera ematen dira."<br>**Ordeztua:**<br>• "Txartel kriptografikoan jaulkitako ziurtagiriak: kautotzeko eta sinadurako gako pribatuak gailu kriptografikoarekin batera ematen dira."<br>**Erantsia:**<br>• HSMan jaulkitako ziurtagiriak: kautotzeko eta sinadurako gako pribatuak gailu kriptografikoan gordetzen dira." |
| **6.1.5. Gakoen tamainak eta erabilitako algoritmoak** | **Jatorrizkoa:**<br>• Gutxienez 2048 bit pertsona fisikoen gakoetarako, CSP zerbitzarietarako, TSA zerbitzarietarako eta ziurtagiri teknikoetarako.<br>**Ordeztua:**<br>• Gutxienez 2048 bit pertsona fisikoen, juridikoen eta gailuen gakoetarako, CSP zerbitzarietarako, TSA zerbitzarietarako eta ziurtagiri teknikoetarako. |
| **6.1.6. Ziurtapen-sinaduretako** | **Jatorrizkoa:**<br>"IZENPEk ziurtagiriak sinatzeko erabiltzen duen algoritmo-identifikatzailea (AlgorithmIdentifier) SHA-1 da (hash algoritmoa), RSArekin batera |

| | |
|---|---|
| **algoritmoak** | (sinadura-algoritmoa). Algoritmo-identifikatzaile hori "Identifier for SHA-1 checksum with RSA encryption for use with Public Key Cryptosystem ne defined by RSA Inc." da. 2007. urtetik aurrera SHA-256 algoritmoa ezartzen hasi zen urratsez urrats, inguru teknologiko bakoitzaren arabera. Erabilitako padding-eskema emsa-pkcs1-v2.1 da (RFC 3447, 9.2 sekzioaren arabera)".<br>Azken erabiltzaileen ziurtagiriak SHA-1 duen RSArekin daude sinatuta. Ziurtagiriarekin sinatzeko, SHA-1 duen RSA edo altuagoa erabiltzeko gomendatzen die azken erabiltzaileei IZENPEk (SHA-224 edo SHA-256)."<br>**Ordeztua:**<br>"IZENPEk ziurtagiriak sinatzeko erabiltzen duen algoritmo-identifikatzailea (AlgorithmIdentifier) SHA-2 da (hash algoritmoa), RSArekin batera (sinadura-algoritmoa). Algoritmo-identifikatzaile hori "Identifier for SHA-2 checksum with RSA encryption for use with Public Key Cryptosystem ne defined by RSA Inc." da. Erabilitako padding-eskema emsa-pkcs1-v2.1 da (RFC 3447, 9.2 sekzioaren arabera)".<br>Azken erabiltzaileen ziurtagiriak SHA-2 duen RSArekin daude sinatuta. Ziurtagiriarekin sinatzeko, SHA-2 duen RSA edo altuagoa erabiltzeko gomendatzen die azken erabiltzaileei IZENPEk." |
| **6.2.1. Modulu kriptografikoen estandarrak** | **Jatorrizkoa:**<br>**"**Sinadura elektroniko aurreraturako ziurtagiriak dituzten gailu kriptografikoei dagokienez, sinadura sortzeko gailu seguru gisa onartuak (DSCF)…"<br>**Ordeztua:**<br>"Sinadura elektroniko kualifikatuko ziurtagiriak dituzten gailu kriptografikoei dagokienez, sinadura sortzeko gailu seguru gisa onartuak (DSCF)" |
| **6.2.3. Gako pribatuaren zaintza** | **Jatorrizkoa:**<br>"Harpidedunaren erantzukizuna izango da soilik bere kontrolpean mantentzea gako pribatua."<br>**Ordeztua:**<br>"Harpidedunak gako pribatua zaintzen duen kasuetan, hura arduratuko da bere kontrolpean soilik mantentzeaz." |
| **6.2.5. Gako pribatua artxibatzea** | **Ezabatua:**<br>"CAk ez ditu inoiz artxibatuko harpidedunen ziurtagiri onartuen gako pribatuak." |
| **6.2.6. Gako pribatuaren** | **Jatorrizkoa:** |

| | |
|---|---|
| **transferentzia, modulu kriptografikora edo modulu kriptografikotik** | “Gako pribatuak modulu kriptografikoetan sartzerakoan larrialdietan bakarrik erabiliko da 6.2.4. atalean adierazitako prozedura.”<br>**Ordeztua:**<br>“Gako pribatuak modulu kriptografikoetan berreskuratzeko larrialdietan soilik erabiliko da 6.2.4. atalean adierazitako prozedura.” |
| **6.2.7. Gako pribatua modulu kriptografikoan biltegiratzea** | **Erantsia:**<br>“IZENPEk, “hodeian” biltegiratutako azken erabiltzailearen ziurtagirien gakoak sortzeko, Europako Batzordearen gomendioak (eIDAS) eta CEN/TS 419241 gomendioak jarraitzen ditu.” |
| **6.2.8. Gako pribatua aktibatzeko metodoa** | **Erantsia:**<br>““Hodeian" dagoen ziurtagiriaren kasuan, harpidedunaren gako pribatura sartzeko bigarren kautotze-faktorea gaituko da, eta hori aldatu ahal izango da ziurtagiri motaren arabera.” |
| **6.2.9. Gako pribatua desaktibatzeko metodoa** | **Jatorrizkoa:**<br>“Gailu kriptografikoa irakurgailutik ateratzean, aribideko edozein eragiketa bukatzen da.”<br>**Ordeztua:**<br>“Txartel kriptografikoa irakurgailutik ateratzean, aribideko edozein eragiketa bukatzen da.” |
| **6.2.10. Gako pribatua deuseztatzeko metodoa** | **Erantsia:**<br>““Hodeian” dauden ziurtagirien gako pribatuen kasuan, IZENPErekiko erlazioa amaitzen denean edo iraungitzen direnean ezabatuko dira gakoak. “<br><br>**Jatorrizkoa:**<br>“Prozedura hori ez zaie aplikatzen erabiltzailea kautotzeko gakoari edo sinadura-gakoari, ez baitira CAk eratutakoak, gakoa berritzeko gailu kriptografiko bera berriro erabiltzen denean izan ezik. Horretan, aurreko gakoa suntsituko da eta euskarri berean beste gako batzuk sortuko dira.”<br>**Ordeztua:**<br>“Prozedura hori ez zaie aplikatzen txartel kriptografikoan jaulkitako erabiltzailea kautotzeko gakoari edo sinadura-gakoari, gakoa berritzeko gailu kriptografiko bera berriro erabiltzen denean izan ezik. Horretan, aurreko gakoa suntsituko da eta euskarri berean beste gako batzuk sortuko dira.” |
| **6.4.1. Aktibatzeko datuak sortzea eta** | **Erantsia:** |

| | |
|---|---|
| **instalatzea** | • "Hodeian" jaulkitako ziurtagiriak: ziurtagiri bakoitzari lotzen zaion gako pribatuaren erabilerak kautotzeko bigarren faktorea eskatzen du. |
| **6.8. Denbora-iturria** | **Jatorrizkoa:**<br>"NTP protokoloaren deskribapena IETF PKIX, RFC 1305 estandarrean aurki daiteke."<br>**Ordeztua:**<br>"NTP protokoloaren deskribapena IETF RFC 5905 estandarrean aurki daiteke." |
| **7.3. OCSP profila** | **Jatorrizkoa:**<br>Internet X.509 Public Key Infrastructure □nline Certificate Status Protocol-□CSP (RFC 2560) June 1999<br>**Ordeztua:**<br>Internet X.509 Public Key Infrastructure □nline Certificate Status Protocol-□CSP (RFC 6960) June 2013 |
| **8. Denbora Zigilatzeko Zerbitzuaren praktiken deklarazioa (TSA)** | **"8. Denbora Zigilatzeko Zerbitzuaren praktiken deklarazioa (TSA)" puntua sortua.** |
| **10.4.6. Datu pertsonalak dituzten fitxategien egitura** | **Jatorrizkoa:**<br>• Giza baliabideak: tarteko segurtasun-maila.<br>• Curriculum Vitaea: tarteko segurtasun-maila.<br>**Ordeztua:**<br>• Giza baliabideak: oinarrizko segurtasun-maila.<br>• Curriculum Vitaea: oinarrizko segurtasun-maila. |
| **10.6.1. Zerbitzua egiteko betebeharrak** | **Jatorrizkoa:**<br>"Zerbitzuak egin zaizkion pertsonaren sinadura sortzeko datuak ez gordetzea eta ez kopiatzea".<br>**Ordeztua:**<br>"Zerbitzuak egin zaizkion pertsonaren sinadura sortzeko datuak ez kopiatzea". |
| **10.6.2. Jardun fidagarriko betebeharrak** | **Jatorrizkoa:**<br>"ziurtagirien eraginkortasuna modu seguruan eta berehala iraungi edo bertan behera utziko bada, horren berri emango duela bermatzen du" |

| | |
|---|---|
| | **Ordeztua:**<br>"ziurtagirien eraginkortasuna modu seguruan eta berehala iraungiko bada, horren berri emango duela bermatzen du"<br><br>**Jatorrizkoa:**<br>"Ziurtagiri bat jaulki edo indargabetzen den edo bere indarraldia amaitu den eguna eta ordua zehaztasunez adierazi ahal izan dadin bermatzea"<br>**Ordeztua:**<br>"Ziurtagiri bat jaulki edo bere indarraldia amaitu den eguna eta ordua zehaztasunez adierazi ahal izan dadin bermatzea" |
| **10.6.7. Erregistro-entitatearen betebeharrak** | **Ezabatua:**<br>• "IZENPEri eskatzea behar den denboraz etetea ziurtagiriaren balioa, hori ezeztatzea eragin duen zergatia egiaztatzen duen dokumentazioa begiratzeko."<br>**Jatorrizkoa:**<br>• Ziurtagiriak jaulki, berritu, ezeztatu eta berraktibatzeko IZENPEk ezarritako prozedurak eta gai horretaz indarrean dagoen legeriak agindutakoa betetzea.<br>**Ordeztua:**<br>• Ziurtagiriak jaulki, berritu eta ezeztatzeko IZENPEk ezarritako prozedurak eta gai horretaz indarrean dagoen legeriak agindutakoa betetzea. |
| **10.6.10. Ziurtagirien erabiltzaile egiaztatzailearen betebeharrak** | **Jatorrizkoa:**<br>• Emandako ziurtagirien baliozkotasuna, etena edo ezeztapena egiaztatzea. Horretarako, ziurtagirien egoerari buruzko informazioa erabiliko da.<br>**Ordeztua:**<br>• Emandako ziurtagirien baliozkotasuna edo ezeztapena egiaztatzea. Horretarako, ziurtagirien egoerari buruzko informazioa erabiliko da. |
| **10.6.11. Denbora-zigiluak jaulkitzen dituen entitatearen betebeharrak** | **"10.6.11. Denbora-zigiluak jaulkitzen dituen entitatearen betebeharrak" puntua sortua.** |
| **10.6.12. Denbora-zigiluen harpidedunaren betebeharrak** | **"10.6.12. Denbora-zigiluen harpidedunaren betebeharrak" puntua sortua** |
| **10.6.13. Denbora-** | **"10.6.13. Denbora-zigiluak egiaztatzen dituzten hirugarren aldeen** |

| | |
|---|---|
| **zigiluak egiaztatzen dituzten hirugarren aldeen betebeharrak** | **betebeharrak" puntua sortua.** |
| **10.7.2. Denbora zigilatzeko agintaritzaren erantzukizuna** | **"10.7.2. Denbora zigilatzeko agintaritzaren erantzukizuna" puntua sortua.** |
| **10.13. Aplikatzeko den araudia** | **Erantsia:**<br>• Identifikazio elektronikoari eta barne-merkatuko transakzio elektronikoetarako konfiantzako zerbitzuei buruzko 910/2104 Europako araudia (eIDAS). |