DENBORA ZIGILATZEKO POLITIKA (TSA)

Erreferentzia:	IZENPE-TSAPD
Bertsio zkia.:	v 1.1
Data:	**2018ko otsailaren 16a**

Aurkibidea

Edukia

1 Sarrera

IZENPEk denbora zigilatzeko zerbitzu kualifikatua eskaintzen du Konfiantzako Zerbitzugile Kualifikatu den aldetik –1999/93/EE Zuzentaraua indargabetzen duen Europako Parlamentuaren eta Kontseiluaren identifikazio elektronikoari eta barne-merkatuko transakzio elektronikoetarako konfiantzako zerbitzuei buruzko uztailaren 23ko 910/2014 Araudiaren arabera–.

Zerbitzu horrek datu bat denbora-lerroaren une jakin batean egotearen ebidentzia digitalak sortzen eta erregistratzen ditu modu fidagarrian eta konfiantzazkoan, datu elektronikoen fidagarritasuna nabarmen hobetuta.

IZENPEk Denbora Zigilatzeko Agintaritza (TSA) sortu du denbora zigilatzeko zerbitzua egiteko.

Dokumentu honek Denbora Zigilatzeko Agintaritzaren (TSA) politika deskribatzen du. TSAren politika horrek zehazten ditu denbora-zigilua sortzeko Denbora Zigilatzeko Agintaritzaren politika eta prozesu orokorrak, baita haren zerbitzuak ere. Halaber, IZENPEren Ziurtapen Praktiken Deklarazioaren (ZPD) prozesu eta xehetasun tekniko gehigarriak zehaztuko dira.

Kanpo-entitate batek ikuskatuko ditu definitutako prozedurak eta horien ezarpen zuzena, betiere ETSIk EN 319 421 arauaren bidez definitutako zehaztapenen arabera.

2 Definizioak eta akronimoak

2.1 Definizioak

Dokumentu honen ondorioetarako, Ziurtapen Praktiken Deklarazioan erabiltzen diren definizioak eta akronimoak aplikatzen dira, honako hauez gain:

- **Denbora Zigilatzeko Agintaritza (TSA):** denbora-zigiluko tokenak jaulkitzen dituen agintaritza.
- **Hirugarren alde erabiltzailea:** IZENPEk eskaintzen duen denbora-zigilu batean konfiantza duen erabiltzailea.
- **Harpideduna:** TSAk eskaintzen dituen zerbitzuak erabiltzen dituen eta terminoak eta baldintzak modu esplizituan onartzen dituen pertsona.
- **Denbora zigilatzeko politika:** denbora-zigiluko token bat sortzen denean TSAri aplikatzen zaizkion arauak.
- **Denbora-zigiluko tokena:** datu digital batzuen existentzia eta une jakin bat lotzen dituen datu-objektua. Datu bat denbora-lerroko une jakin batean bazegoela jasotzen duen ebidentzia gisa da baliagarria.
- **Denbora zigilatzeko unitatea:** hardware- eta software-osagaiak, denbora-zigiluko tokenak denbora-iturri bakar batetik eskaintzen dituen unitate gisa kudeatzen direnak. Osagai klonatuak edo osatuak izan daitezke, eskuragarritasun handia lortzearren.
- **TSAren praktiken deklarazioa:** TSA baten politikak eta praktikak, batez ere harpidedunei eta hirugarren aldeei bideratuta.
- **Coordinated Universal Time:** Eguzki-denbora, meridiano nagusian (0º). Denbora-eskala segundoan oinarritzen da –ETSI TS 102.023 arauan eta ITU-R Recommendation TF.460-5 arauan definitzen denaren arabera–.
- **UTC(k):** "k" laborategi batek UTCaren arabera egindako denbora-eskala, betiere gehienez 100ns inguruko desbideratzea lortzearren.

2.2 Akronimoak

TSA: Time Stamp Authority
TSU: Time Stamp Unit
TST: Time Stamp Token
UTC: Coordinated Universal Time
eIDAS: 1999/93/EE Zuzentaraua indargabetzen duen Europako Parlamentuaren eta Kontseiluaren identifikazio elektronikoari eta barne-merkatuko transakzio elektronikoetarako konfiantzako zerbitzuei buruzko uztailaren 23ko 910/2014 Araudia
TSAPD: TSAren Praktiken Deklarazioa
ZPD: Ziurtapen Praktiken Deklarazioa

3 Esparrua

Dokumentu honek definitzen ditu Denbora Zigilatzeko Agintaritzaren (TSA) eragiketa- eta kudeaketa-praktikak, betiere harpidedunek eta konfiantzazko hirugarrenek denbora zigilatzeko zerbitzuen fidagarritasuna ebaluatu ahal izan dezaten. TSAren politikaren betekizunak bat datoz Europako eIDAS araudiaren xedapenekin. IZENPEren denbora zigilatzeko zerbitzuak sinadura elektroniko bati aplika dakizkioke, edo denboraren puntu jakin batean datu digital batzuen existentziaren ebidentzia eskatzen duen edozein aplikaziori. Politikaren betekizun horiek gako publikoko kriptografian, gako publikoko ziurtagirietan (X.509) eta denbora-iturri fidagarrietan oinarritzen dira. Organismo independenteek dokumentu hau eta IZENPEren ZPDa erabil ditzakete TSA honen eta denbora zigilatzeko zerbitzuen fidagarritasuna ebaluatzeko.

4 Kontzeptu orokorrak

4.1 Denbora zigilatzeko zerbitzuak

Denbora zigilatzeko zerbitzuek bi osagai hartzen dituzte barnean:

- Denbora-zigiluen hornikuntza: denbora-zigiluaren tokenak sortzeaz arduratzen den osagai teknikoa.
- Denbora-zigiluen administrazioa: denbora zigilatzeko zerbitzuen eragiketa monitorizatzen eta kontrolatzen duen zerbitzuaren osagaia. Denbora zigilatzearen kudeaketak bermatzen du denbora-zigilatzean erabiltzen diren erlojuak behar bezala sinkronizatuta daudela UTCarekin.

4.2 Denbora Zigilatzeko Agintaritza

IZENPEren TSAk bere gain hartzen du “Denbora zigilatzeko zerbitzuak” atalean adierazten diren denbora zigilatzeko zerbitzuen hornikuntzaren gaineko erantzukizuna. IZENPEren TSAk denbora-zigiluko hainbat unitate identifikagarrirekin (TSU) jardun dezake, eta TSU bakoitzak gako desberdina izan dezake (ikus “6.8.4. Denbora-zigiluko tokenaren profila” atala).

TSU baten barruan, gakoak klona daitezke eta osagai erredundanteetan erabil daiteke eskuragarritasun handiko betekizunak betetzeko.

IZENPEren TSA identifikatuta dago denbora zigilatzeko zerbitzuek erabilitako ziurtagiri digitalean. Profila eskuragarri dago “6.8.3ren ziurtagiriaren profila” atalean.

4.3 Harpideduna

Erakunde bat edo partikular bat izan daiteke harpideduna. Harpideduna erakunde bat bada, erakunde horri aplikatzen zaizkion betebeharrak aplikatzen zaizkie haiekin lotzen diren azken erabiltzaileei ere bai. Edonola ere, erakundea izango da erantzulea azken erabiltzaileek ez badituzte betebeharrak zuzen betetzen. Horrenbestez, erakunde horrek behar bezala informatu beharko ditu azken erabiltzaileak. Harpideduna erabiltzaile partikular bat bada, azken erabiltzailea zuzenean izango da betebeharrak betetzearen erantzulea.

4.4 Denbora zigilatzeko politika eta TSAren praktiken deklarazioa

4.4.1 Xedea

Denbora zigilatzeko politika eta praktiken deklarazioa, honela defini daitezke:

- Harpidedunak zein denbora-zigiluen agintaritza jaulkitzaileak bete behar dituzten alderdiak definitzen ditu TSAren politikak. TSAk, denbora-zigiluko token bat sortzen duenean, aplikatzen dituen arauak eta prozesuak barnean hartzen dira.
- TSAren praktiken deklarazioaren bidez adierazten da denbora zigilatzeko zerbitzua nola osatuta dagoen politikaren betekizunak betetzeko.

- IZENPEren ZPDan deskribatutako prozesuen osagarri gisa, TSAren politika honek prozesu eta politika espezifikoak deskribatzen ditu.

4.4.2 Zehaztasun-maila.

TSAren politikak zehazten ditu zer prozesu erabiltzen den denbora zigilatzeko zerbitzuak egiteko, betiere ZPDan deskribatzen diren prozesuak zabalduta.

4.4.3 Ikuspegia

TSAren politika prozesu orokorretara bideratzen da. ZPDan edo barne dokumentuetan zehazten dira antolamendu-egituren, prozedura operatiboen eta komunikazio-azpiegituren gisako xehetasun teknikoak. Barne-dokumentuak ez daude jendearentzat eskuragarri.

5 TSAren politikarako sarrera eta betekizun orokorrak

5.1 Identifikazioa

IZENPEk honako politika-identifikatzaile (OID) hau jartzen die bere TSA bidez jaulkitako denbora-zigiluko token guztiei.

Denbora-zigiluko tokena	**1.3.6.1.4.1.14777.3.3**

5.2 Erabiltzaile-erkidegoa eta aplikagarritasuna

Denbora zigilatzeko zerbitzuaren erabiltzaileak zerbitzu hori behar duten harpidedunak eta hirugarren aldeak izango dira. Hilean eskaera kopuru jakin bateko muga dago, muga horretatik aurrera zerbitzuak kostu gehigarria izango du. Baldintzak eta tarifak kontsultatzeko, jarri IZENPErekin harremanetan.

5.3 Adostasuna

Aldian behingo barne- eta kanpo-ikuskapenek ziurtatuko dute denbora zigilatzeko politika betetzen dela.
IZENPEk "**¡Error! No se encuentra el origen de la referencia.** Betebeharrak eta erantzukizunak" talean definitzen diren betebeharrak betetzen ditu, eta kontrol egokiak ezar daitezen ziurtatzen du, "**¡Error! No se encuentra el origen de la referencia.**. **¡Error! No se encuentra el origen de la referencia.** administrazioa eta eragiketa" atalean zehazten denaren arabera.

6 Politikak eta praktikak

6.1 Konfiantza-sistemak hedatzea eta mantentzea

TSAren gakoak eta haren zerbitzuak konfiantzako ingurune batean sortzen dira. IZENPEk erabiltzen dituen sistemek eta produktuek zerbitzu egokiak eskaintzen dituzte, eskatzen diren ziurtasun-mailen arabera. IZENPEk adierazten du segurtasun-betekizunen analisi egokia egiten duela eta aldaketak kontrolatzeko prozedurak dituela.

6.2 Konfiantzako zerbitzuaren praktiken deklarazioa

Politika honetan, ZPDan eta betekizun teknikoak, operatiboak eta prozedurazkoak definitzen dituzten barne-dokumentu osagarrietan ezarritako arauen arabera egiten ditu bere zerbitzuak TSAk. IZENPEk TSAko zerbitzu espezifikoak eskain diezazkioke modu pribatuan eskatzaile bati.

6.2.1 TSAren praktiken deklarazioa

TSAren praktiken deklarazioak definitzen du IZENPE nola atxikitzen zaien ZPDan eta beste barne-dokumentu batzuetan identifikatutako betekizunei.
Definitutako prozedurak eta horien ezarpen zuzena urtero ikuskatuko ditu kanpo-entitate independente batek.
TSAren praktiken deklarazioa eta garrantzizko bestelako dokumentazioa eskura dago www.izenpe.com web-gunean.
TSAren dibulgazio-deklarazioa "**¡Error! No se encuentra el origen de la referencia. ¡Error! No encuentra el origen de la referencia.**" puntuan barnean hartzen da. Barne-dokumentuak ez dira argitara ematen. TSAko praktiken gaineko aldaketak, edo beste edozein dokumentu argitaraturen gaineko aldaketak, ZPDaren zehaztapenen arabera egin beharko dira.

6.2.2 TSAren dibulgazio-praktiken deklarazioa

Dokumentu honetan ezartzen diren terminoak eta baldintzak lotesleak dira IZENPEren denbora zigilatzeko zerbitzuak erabiltzen dituzten harpidedun guztientzat eta hirugarren alde guztientzat. Politika hori osatzen duten beste dokumentu batzuk –hala nola ZPDa– aurki daitezke www.izenpe.com web-gunean.

- ✓ IZENPEren TSA zerbitzua denbora zigilatzeko zerbitzu kualifikatua da eIDAS araudiaren arabera.
- ✓ Harremanetan jartzeko informaziorako, kontsultatu ZPDaren "1.5.2 Harremanetarako datuak" atala.
- ✓ Denbora-zigiluak jaulkitzen dituen entitatearen betebeharrak dokumentu honen "**¡Error! No se encuentra el origen de la referencia.** Denbora-zigiluak jaulkitzen dituen ntitatearen betebeharrak" atalean definituta daude.
- ✓ Harpidedunaren betebeharrak dokumentu honen "**¡Error! No se encuentra el origen e la referencia.** Denbora-zigiluen harpidedunaren betebeharrak" puntuan definituta daude.

- ✓ Hirugarren batzuen betebeharrak dokumentu honen “**¡Error! No se encuentra el rigen de la referencia.** Denbora-zigiluak egiaztatzen dituzten hirugarren aldeen betebeharrak” puntuan definituta daude.
- ✓ Denbora Zigilatzeko Agintaritzaren erantzukizunak dokumentu honen “**¡Error! No se ncuentra el origen de la referencia.** Erantzukizunak” puntuan definituta daude.
- ✓ Zerbitzuak IZENPEren prezio-katalogoko tarifen araberako kostua du.
- ✓ IZENPEk TSAren eragiketa guztien erregistroa gordetzen du, dokumentu honen “**¡Error! No se encuentra el origen de la referencia.** Ebidentziak jasotzea” puntuan ditzera ematen denaren arabera.
- ✓ Erreklamazioak eta auziak ebazteko, kontsultatu ZPDaren “9.12 Erreklamazioak eta auzien ebazpena” puntua.
- ✓ Harpidedunek eta hirugarren aldeek onartu egiten dituzte IZENPEk definitutako erabilera-baldintzak.
- ✓ Ziurtapen Agintaritza batek jaulkitzen du IZENPEren TSAren ziurtagiria, eta Agintaritza horren ziurtatze-politikak IZENPEren ZPDan adierazten diren jarraibideak betetzen ditu.
- ✓ IZENPEren TSA zerbitzuak jaulkitako denbora-zigiluko token bakoitzak barnean hartzen du “**¡Error! No se encuentra el origen de la referencia.** Denbora-zigiluko tokenaren rofila” atalean definitutako objektu-identifikatzailea.
- ✓ Onartzen diren hash-algoritmoak adierazten dira “**¡Error! No se encuentra el origen de a referencia.** Denbora-zigiluaren eskaeraren profila” atalean. TSA tokenaren sinadura-algoritmoa “**¡Error! No se encuentra el origen de la referencia.** Denbora-zigiluko okenaren profila” atalean definitzen da.
- ✓ TSAk +/- 1 segundoko UTC denbora-estandar minimoekin bateragarria den denbora-doitasuna ziurtatzen du. IZENPEren TSAk ez ditu denbora-zigiluko tokenak jaulkiko, ezin badu denbora-doitasun hori ziurtatu.
- ✓ Erantzukizun-mugak dokumentu honen “**¡Error! No se encuentra el origen de la eferencia.** Erantzukizunak” atalean, ZPDan eta erabiltzaileekin mantentzen diren beste zerbitzu-akordio batzuetan definitzen dira.

6.3 Betebeharrak eta erantzukizunak

IZENPEk honako betebehar hauek hartzen ditu bere gain, Denbora Zigilatzeko Praktiken Deklarazio honen arabera denbora-zigiluak jaulkitzen dituen entitatea den aldetik:

6.3.1 Denbora-zigiluak jaulkitzen dituen entitatearen betebeharrak

IZENPEren Denbora Zigilatzeko Agintaritzak denbora-zigiluko token seguruak (TST) jaulkitzen ditu denbora zigilatzeko zerbitzuen erabiltzaileentzat (harpidedunentzat zein hirugarren aldeentzat).

IZENPEren Denbora Zigilatzeko Agintaritzak bere gain hartzen du denbora zigilatzeko zerbitzuak egiteko erantzukizuna. IZENPEren Denbora Zigilatzeko Agintaritzak denbora zigilatzeko hainbat unitate identifikagarrirekin (TSU) lan egin dezake, eta horietako bakoitzak bere sinadura-gakoa izan dezake.

IZENPEren Denbora Zigilatzeko Agintaritza identifikatuta dago denbora zigilatzeko zerbitzuetarako erabiltzen den ziurtagiri digitalean.

IZENPEren Denbora Zigilatzeko Agintaritzak bere zerbitzuak eskaintzen dizkie harpidedun guztiei eta denbora-zigiluak egiaztatzen dituzten hirugarren aldeei, baldin eta haien betebeharrak “6.3. Betebeharrak eta erantzukizunak” atalean zehaztutakoaren arabera beteko dituztela hitz ematen badute.

6.3.2 Denbora-zigiluen harpidedunaren betebeharrak

Denbora-zigiluko harpidedunak denbora zigilatzeko zerbitzua erabil dezake soilik ETSI EN 319 422 arauaren zehaztapenen arabera.

Harpidedunak egiaztatu beharko du denbora zigilatzeko agintaritzak behar bezala sinatu duela denbora-zigiluko tokena, baita denbora-zigiluko tokena sinatzeko erabilitako gako pribatua ez dela ezeztatu.

Harpidedunak Izenperen Denbora Zigilatzeko politika honekin bete behar du, www.izenpe.eus-en eskuragarri.

6.3.3 Denbora-zigiluak egiaztatzen dituzten hirugarren aldeen betebeharrak

Denbora zigilatzeko token bat jasotzen denean, hirugarren aldeak egiaztatu beharko du behar bezala sinatuta dagoela eta denbora-zigilua sinatzeko erabilitako gako pribatua ez dela ezeztatu.

Denbora-zigiluak sortzeko erabiltzen den ziurtagiria iraungitzen ez den bitartean, posible izango da haren baliagarritasuna egiaztatzea dagokion CRLan.

Egiaztapena ziurtagiriaren balio-aldiaren ondoren egiten bada, hirugarren aldeak egiaztatu beharko du ea oraindik ere segurutzat jo daitezkeen erabilitako hash-funtzioa, algoritmoak eta gako kriptografikoen luzera.

6.4 Erantzukizunak

IZENPEk bere TSA politikaren eta bere ZPDaren arabera jarduten du, baita IZENPEren eta denbora zigilatzeko zerbitzuaren erabiltzaileen arteko bestelako akordio lotesle baten baldintzen arabera ere. IZENPEk ahalegin berezia egiten du bere zerbitzuetan eskuragarritasun handia eskaintzeko, baina ez du eskuragarritasunaren arloko erabateko bermerik eskaintzen, ezta denbora-zigiluetan doitasuna ere. IZENPE ez da inola ere onura-galeraren, zeharkako edo ondoriozko kalteen edo datu-galeraren erantzule izango, indarrean dagoen legeriak hala ahalbidetzen duen heinean. IZENPE ez da harpidedunak edo hirugarren aldeak egindako arau-hausteen ondoriozko kalteen erantzule izango, aplikatzekoak diren terminoetan eta baldintzetan. IZENPE ez da inola ere ezinbesteko gorabeheren ondoriozko kalteen erantzule izango, hala nola hondamendi naturalen, elektrizitatea edo telekomunikazioak erortzearen, suteen, kanpo-eraso ez aurreikusgarrien –birusen edo hacker-en erasoen–, gobernu ekintzen, edo greben ondoriozko kalteen erantzule. Edonola ere, IZENPEk gorabehera horien ondorioak arintzeko zentzuzko neurri guztiak hartuko ditu. IZENPEk ez ditu estaliko ezinbesteko gorabehera batek eragindako atzerapenaren ondoriozko kalteak.

6.5 Denbora-zigilua jaulkitzeko prozedura

Denbora Zigilatzeko Zerbitzua egiteko helburuarekin, IZENPE gakoen kudeaketaz arduratzen da, betiere dokumentu honen "**¡Error! No se encuentra el origen de la referencia.** Kontrol riptografikoak" atalean deskribatzen denaren arabera.

Politika horren arabera jaulkitako denbora-zigiluak berariazko ziurtagiri batzuekin sinatzen dira, eta ziurtagiri horiek, halaber, CN = Izenpe.com duen erroko Ziurtapen Agintaritzaren Ziurtapen Katearen mende jaulki dira.

Erroko Ziurtapen Agintaritzaren Ziurtapen Kate horri buruzko informazio gehiago lortu nahi izanez gero, kontsultatu ZPDaren "1.3.1. Ziurtapen-agintaritzak" atala.

6.5.1 Denbora zigilatzeko zerbitzuaren hornidura eta eskuragarritasuna

Entitate erabiltzaileak eskatuta jaulkiko dira denbora-zigiluak. Entitate erabiltzaileak dokumentu elektroniko baterako denbora-zigilu bat lortu nahi duenean, dokumentu horretatik abiatuta hash-balio bat edo hash-balio multzo bat kalkulatuko du. Denbora-zigiluaren eskaeraren egituran barnean hartuko da, eta IZENPEri igorriko zaio dagokion denbora-zigilua sortzeari ekin diezaion.

Denbora-zigilu horrek, IZENPEren sinadura elektronikoaren bitartez, lotuko ditu jasotako datuak eta horiek zer data eta ordutan hartu zituen.

Onartzen diren algoritmoak dokumentu honen "**¡Error! No se encuentra el origen de la eferencia.** Denbora-zigiluaren eskaeraren profila" atalean deskribatzen dira.

IZENPEk ez du zigilatzeko jaso dituen datuen errepresentazioaren gaineko inolako egiaztapenik edo tratamendurik egingo, denbora-zigiluan eta erregistro-sistemetan barnean hartzeaz harantzago. IZENPEk ez du egiaztatuko edukia, ezta zigilatu beharreko datuen errepresentazioaren egiazkotasuna edo datuen jatorria ere.

Denbora Zigilatzeko Zerbitzua urteko egun guztietan eta eguneko hogeita lau (24) orduetan izango da eskuragarri, IZENPErena ez den gorabeheraren bat edo mantentze-lanen bat salbu. IZENPEk behar besteko aurrerapenez eman beharko du mantentze-lan horien berri, eta gehienez hogeita lau (24) ordutan konpontzen saiatuko da.

Denbora zigilatzeko eskaerak zein erantzunak IETF RFC 3161 gomendioan deskribatutakoaren arabera kudeatzen dira.

6.5.2 Denbora zigilatzeko eskaera

Denbora zigilatzeko eskaerak http://tsa.izenpe.com helbidera bidaliko dira, Content-Type: application/timestamp-query gisa kapsulatuta eta DERean kodetuta eta ASN.1ean deskribatuta (ikus IETF RFC 3161 gomendioa).

6.5.3 Denbora zigilatzeko eskaera bati erantzutea

Datatze digitalaren eskaera bati ematen zaizkion erantzunak http://tsa.izenpe.com helbidean jasotzen dira, Content-Type: application/timestamp-reply gisa kapsulatuta eta DERean kodetuta eta ASN.1ean deskribatuta.

Erantzunaren edukia da ASN.1 egitura bat –non barnean hartzen den eragiketaren emaitza (status), hau da, eragiketa behar bezala egin den edo ez– eta CMSSignedData

(timeStampToken) egitura bat –non barnean hartzen den Datatze Digitaleko Agintaritzak sinatutako datatze digitala (TSTInfo)–.

Datatze Digitaleko Agintaritzaren ziurtagiria CAk jaulkitako ziurtagiri bat da, id-kp-timestamping luzapena duena, eta adierazten du ziurtagiri hori soilik erabiliko dela dokumentu digitalak datatzeko helburuarekin.

7 TSAren administrazioa eta eragiketa

7.1 Segurtasunaren kudeaketa

IZENPEren TSAren segurtasunaren kudeaketa ZPDaren “5. Segurtasun fisikoaren, prozeduren eta langileen kontrolak” atalean deskribatzen da.

7.2 Aktiboen sailkapena eta kudeaketa

IZENPEren TSAk ziurtatzen du informazioak eta beste aktibo batzuek segurtasunaren arloan tratamendu egokia jasotzen dutela, ZPDaren “5.7. Larrialdietarako plana” atalean definitzen denaren arabera.

7.3 Langileen segurtasuna

Langileen segurtasun-kontrolak ZPDaren “5. Segurtasun fisikoaren, prozeduren eta langileen kontrola” atalean definitzen dira.

7.4 Kontrol kriptografikoak

7.4.1 TSAren gakoa sortzea

Konfiantza-rolak dituzten langileek egindako ingurune fisiko segurtatuan sortzen ditu IZENPEk gako kriptografikoak. Hash-algoritmoak, gakoaren luzera eta sinadura-algoritmoak dokumentu honen “7.5 Denbora zigilatzea” atalean deskribatzen dira. IZENPEren TSAren gakoak berariazko prozedura bati jarraituta sortzen dira. TSAren ziurtagiriak gehienez 5 urteko iraupena izango du.

7.4.2 TSUaren gako pribatua babestea

IZENPEren TSAk ziurtatzen du gakoen konfidentzialtasuna eta integritatea mantentzen dela. Zehazki, HSMak FIPS 140-2 3. mailako betekizunak betetzen ditu, baita dagokion profileko EAL4+ ziurtatze-maila ere. Ildo horretan, ZPDan IZENPEren mendeko CAetarako deskribatutakoaren pareko segurtasun-mailarekin mantentzen dira TSAren gakoak.

7.4.3 TSUaren gako publikoaren banaketa

IZENPEren TSAren ziurtagiria www.izenpe.com web-gunean eman da argitara.

7.4.4 Ziurtagiria berritzea, TSUaren gakoa birsortuta

Industriak algoritmoa, gakoaren luzera edo beste edozein segurtasun-neurri fidagarritzat jotzeari uzten badio, ziurtagiria iraungi aurretik ordezkatu beharko dira IZENPEren TSAren gakoak. Edonola ere, gakoak bi urtero berrituko dira eta jaulkiko da ziurtagiri berria.

7.4.5 TSUaren gakoaren bizi-zikloaren amaiera

IZENPEren TSAk ez du uzten ziurtagiri iraungi edo ezeztatu batekin timestamp erantzunak sinatzen. IZENPEren TSAren zerbitzuei amaiera ematen zaienean, TSAren ziurtagirien gako pribatu guztiak suntsituko dira, babeskopiak barne, gako pribatu horiek berreskuraezinak izateko moduan.

7.4.6 Denbora-zigiluak sinatzeko erabilitako modulu kriptografikoaren bizi-zikloaren kudeaketa

Hardwareko segurtasun-moduluen (HSM) ez-ukatzeko zerbitzuak manipulatzen ez direla –ez bidalketan, ez biltegiratzean– bermatzeko prozedurak ezartzen ditu IZENPEk.
Konfiantza-rolak dituzten langileek soilik instalatu eta aktibatuko dituzte hardware kriptografikoan biltzen diren sinadura-gakoak. IZENPEren barne-dokumentazioan deskribatzen dira HSMaren eragiketak, prozedurak eta bizi-zikloko kudeaketa.

7.4.7 TSA ziurtagiriaren gako pribatua arriskuan egotea

IZENPEren TSA zerbitzuaren gako pribatua arriskuan badago, ZPDaren “5.7.3. Gako pribatuaren konpromisoaren aurreko prozedura” puntuan adierazitako prozedura aplikatuko da.
IZENPEren TSA zerbitzuaren gako pribatua arriskuan badago, ez dira token timestamp-ak jaulkiko.
Definitutako +/- 1 segundoko doitasun minimoa arriskuan badago, ez da denbora-zigilurik jaulkiko kalibrazioa zuzendu arte.
IZENPEren TSA zerbitzuaren gako pribatua arriskuan badago, IZENPEren web-orrian harpidedunentzako eta hirugarren aldeentzako garrantzizko informazioa argitaratuko da. Horrez gain, harpidedunei lehenbailehen jakinaraziko zaie.

7.4.8 TSAren amaiera

IZENPEren TSAren amaiera ZPDaren “5.8 CAren amaiera” atalean definitutako prozeduren arabera egingo da.

7.5 Denbora zigilatzea

7.5.1 Zerbitzua egiteko erabilitako denbora-iturria

IZENPEk Armadaren Errege Behategirako konexio baten bidez lortzen du bere sistemen denbora, NTP protokoloari jarraituta, betiere Eusko Jaurlaritzarekin ezarritako konexioaren bitartez. NTP protokoloaren deskribapena IETF RFC 5905 estandarrean aurki daiteke.

Barne-zerbitzu horretan oinarrituta, denbora zigilatzeko zerbitzua (TSA) eskaintzen du IZENPEk, eta zerbitzu hori erabili ahal izango da dokumentu arbitrarioetan denbora-zigiluak sortzeko, betiere IETF RFC 3161 estandarraren arabera.

7.5.2 Denbora-zigiluaren eskaeraren profila

- Denbora-zigiluaren eskaerak IETF RFC 3161ean definitutako egiturari jarraitu beharko dio.

- Eskaerak ETSI TS 101 861aren jarraibideei jarraitu beharko die.
- ETSI TS 119 312an zehazten da zer hash-algoritmo onartzen den. Edonola ere, IZENPEk industriaren gomendioei jarraitzen die suite kriptografikoei dagokienez.

7.5.3 TSAren ziurtagiriaren profila

TSUaren sinadura sortzeko datuak honako ziurtagiri hauekin lotuta daude:

Extension attribute	Value	Comment
Subject	CN = tsa.izenpe.com O = IZENPE S.A. C = ES	
Issuer Name	CN = Izenpe.com O = IZENPE S.A. C = ES	
Key Usage	Sinadura digitala (80)	
Extended Key Usage	Data inprimatzea (1.3.6.1.5.5.7.3.8)	
Subject key Identifier	<key identifier of this CA's public key>	
Authority key identifier	<key identifier of the issuing CA's public key>	
CRL Distribution Point	http://crl.izenpe.com/cgi-bin/arl2	URLs of the CRL Distribution points
Certificate Policy	[1]Ziurtagirien zuzentaraua: Zuzentarau-identifikatzailea=1.3.6.1.4.1.14777.3.3 [1,1]Zuzentarau-ziurtatzailearen informazioa: Zuzentarau-ziurtatzailearen IDa=CPS Ziurtatzailea: http://www.izenpe.com/cps [1,2]Zuzentarau-ziurtatzailearen informazioa: Zuzentarau-ziurtatzailearen IDa=Erabiltzaile oharra Ziurtatzailea: Ohar-testua: bermeen mugak ezagutzeko www.izenpe.com Ziurtagirian konfiantza izan aurretik kontratua irakurri Limitaciones de garantias en www.izenpe.com Consulte el contrato antes de confiar en el HYPERLINK http://www.izenpe.com	
Subject Information Access	[1]Agintaritza-informaziorako sarbidea Sartzeko metodoa=Sartzeko metodo ezezaguna (1.3.6.1.5.5.7.48.3) Ordezko izena: Helbidea URL=http://tsa.izenpe.com:8093/	

7.5.4 Denbora zigiluko tokenaren profila

- Denbora-zigiluaren protokolorako IETF RFC 3161 eta RFC 5816 arauei jarraitzen zaie.

- Zigilu-profilerako eta politiketarako arau hauei jarraitzen zaie: ETSI EN 319 421 arauari (Policy and Security Requirements for Trust Service Providers issuing Time-Stamps) eta ETSI EN 319 422 arauari (Time-stamping protocol and time-stamp token profiles).
- IZENPEk jaulkitako denbora zigilatzeko token guztiek barnean hartzen dute politika identifikatzeko objektua: (OID) 1.3.6.1.4.1.14777.3.3
- IZENPEk jaulkitako denbora zigilatzeko token guztiek barnean hartzen dute tokena sinatzeko erabiltzen den Timestamp ziurtagiria.
- Sinatzeko erabiltzen den ziurtagiria sortzean sha256WithRSAEncryption erabiltzen da, betiere 4096 bit-eko gako luzerarekin. TSAren zerbitzurako soilik erabiltzen da.
- Tokenaren hash-algoritmoa SHA-256 da.

7.5.5 Erlojua UTCarekin sinkronizatzea

- IZENPEren TSAk bere denbora-zerbitzaria du, eta zerbitzari hori ROArekin (Real Observatorio de la Armada, Armadaren Errege Behategia) sinkronizatuta dago.
- Kontrolak daude definitutako doitasuna arriskuan jar dezaketen sinkronizazio-arazoak hautemateko eta/edo kalibrazioan aldaketak hautemateko.
- TSAk UTC denbora-doitasuneko arauekin bateragarria den denbora-doitasuna ziurtatzen du, betiere +/- 1 segundoko doitasun minimoarekin. IZENPEren TSAk ez ditu denbora-zigiluko tokenak jaulkiko, baldin eta ez bada denbora-doitasuna ziurtatzen.
- IZENPEren TSAk eguneko azken minutuan –doikuntza planifikatuta dagoen minutuan– segundo gehigarrien tratamendu zuzena ziurtatzen du.

7.6 Segurtasun fisikoa eta ingurumenekoa

IZENPEk bere TSAren segurtasun fisikoa eta ingurumenekoa ziurtatzen du, ZPDaren “5. Segurtasun fisikoaren, prozeduraren eta langileen kontrolak” atalean definitzen denaren arabera.

7.7 Eragiketen kudeaketa

IZENPEren TSAk eragiketa-kontrol egokiak mantentzen ditu, ETSI EN 319 421 arauaren jarraibideen arabera. Dokumentu eta politika horiek barnekoak dira, eta ez daude jendearentzat eskuragarri; gainera, aldian behin barne- eta kanpo-berrikuspenen bidez egiaztatzen dira, kontrol horiek betetzen direla eta eraginkorrak direla ziurtatzeko.

7.8 Sareko segurtasuna

Sareko segurtasuna maila askotariko zonifikazioaren kontzeptuan oinarritzen da, firewall erredundante ugari erabilita. Sare ez-seguruen bitartez transferitzen den informazio konfidentziala modu zifratuan transferitzen da, SSL/TLS protokoloak erabilita.

7.9 Gertakarien kudeaketa

ZPDaren “5.7.1 Gertakariak kudeatzeko prozedurak” atalean definitutakoak.

7.10 Ebidentziak jasotzea

ZPDaren “5.4 Audit ” atalean adierazitakoak.

7.11 Denbora zigilatzeko zerbitzuen eragiketarekin lotzen den informazioa artxibatzea

Ziurtapen Agintaritzaren eragiketarekin lotzen diren erregistroak bezalaxe sortu eta biltegiratuko dira denbora zigilatzeko zerbitzuaren eragiketarekin lotzen diren erregistroak. Hurrenez hurreneko kontrolek erregistro guztien beharrezko integritatea, konfidentzialtasuna eta artxibatzea ziurtatzen dute, ZPDaren “5.5 Erregistroak artxibatzea” atalean zehazten den moduan.

IZENPEk ziurtatuko du neurri egokiak daudela bere erregistroak modu desegokian prozesa daitezen saihesteko.

7.12 Sistemetarako sarbideen kudeaketa

IZENPEren TSAk sarbide-kontrol egokiak ditu, ZPDaren “5. Segurtasun fisikoaren, prozeduraren eta langileen kontrolak” atalean definitzen denaren arabera.

7.13 Lege-betekizunak betetzea

IZENPEren TSA zerbitzuek eIDAS araudiaren betekizunak betetzen dituzte. IZENPEk ziurtatzen du neurri egokiak ezartzen direla datu pertsonalak baimenik gabe prozesa daitezen saihesteko. IZENPEk, halaber, erabiltzaileek TSAri emandako datu pertsonalen eta bestelako informazioaren konfidentzialtasuna ziurtatzen du.

7.14 Antolamendua

IZENPEren TSA mantentzen duen erakundea mendeko CAak antolatzen dituen erakunde bera da. ZPDan definituta daude antolamendu-segurtasuna, segurtasun teknikoa eta langileen segurtasuna, eta beste lege eta politika batzuen araberakoak dira, betiere politika honetan definitzen denari jarraituta.