

ZIURTAPEN ETA ZERBITZU ENPREA-EMPRESA DE CERTIFICACIÓN Y SERVICIOS, IZENPE,
S.A. ENPRESAK EMANDAKO DENBORA ZIGILATZEKO UNITATEEN ZIGILU-ZIURTAGIRIEI
BURUZKO DIBULGAZIO-TESTUA (PDS)

Izenpe 2025

 IZENPE
Beato Tomás de Zumarraga 71 - 1ª Planta
01008 Vitoria - Gasteiz
Tel.: 945 067 723
www.izenpe.com





ALDAKETEN KONTROLA

BERTSIOA	DATA	ALDAKETAK
1,0	2025/06/19	Dokumentua onartzea.



AURKIBIDEA

1	AKORDIO OSOA.....	4
2	TSAREN HARREMANETARAKO INFORMAZIOA.....	4
3	DENBORA- ETA ERABILERA-ZIGILUAREN MOTA	4
4	ZIURTAGIRIAREN ERABILERA-MUGAK	5
5	HARPIDEDUNEN BETEBEHARRA	5
6	TSU ZIURTAGIRIEN EGOERAZ FIDATZEN DIREN ALDERDIEN EGIAZTATZEKO BETEBEHARRAK	5
7	ERANTZUKIZUNAREN MUGAK	6
8	APLIKA DAITEZKEEN AKORDIOAK ETA ZIURTAPEN-PRAKTIKA ETA -POLITIKEN DEKLARAZIOA	6
9	PRIBATUTASUN POLITIKA.....	6
10	ITZULKETA-POLITIKA.....	7
11	LEGE APLIKAGARRIA, KEXAK ETA EZTABAIDAK EBAZTEA	7
12	LIZENTZIAK ETA BILTEGIA, MARKA FIDAGARRIAK ETA IKUSKARITZA	7



Dokumentu hau da PKI Disclosure Statement (aurrerantzean, PDS), Ziurtapen eta Zerbitzu Enpresa-Enpresa de Certificación y Servicios, Izenpe, S.A.k (aurrerantzean, Izenpe) emandako TSUren zigilu-ziurtagiriei dagokiena.

1 AKORDIO OSOA

1. Izenperen Denbora Zigilatzeko Agintaritzaren informazio-adierazpen honen helburua ez da erakunde horrek Denbora Zigilatzeko Zerbitzu Kualifikatua emateko baldintza osoak definitzea, baizik eta haien laburpen bat egitea.

2 TSAren HARREMANETARAKO INFORMAZIOA

2. Zerk bultzatzen du Izenperen Ziurtapen Agintaritza?
 - Ziurtapen eta Zerbitzu Enpresa - Empresa de Certificación y Servicios Izenpe S.A.
 - Tomas Zumarraga Dohatsuaren kalea, 71 – 01008 Vitoria-Gasteiz
 - Telefono: 900 840 123

3 DENBORA- ETA ERABILERA-ZIGILUAREN MOTA

3. Denbora zigilatzeko zerbitzu kualifikatua Izenperen denbora zigilatzeko agintaritzak eskaintzen du, konfiantzazko zerbitzuen emaille gisa eta eIDAS Erregelamenduarekin⁵ bat etorritz.
4. PDS horrek ezaugarri hauek ditu:
 - Denbora-zigiluaren protokolorako IETF RFC 3161 eta RFC 5816 araei jarraitzen zaie.
 - Zigilatze-profilerako eta politiketarako, 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) jarraitzen zaie.
 - TSAren politikaren betekizunak gako publikoaren kriptografian, gako publikoaren ziurtagirietan (X.509) eta denbora-iturri fidagarrietan oinarrituta daude.
 - IZENPEk jaulkitako denbora zigilatzeko token guztiek barnean hartzen dute politika identifikatzeko objektua: (OID) 1.3.6.1.4.1.14777.300.1.
 - IZENPEk jaulkitako denbora zigilatzeko token guztiek barnean hartzen dute tokena sinatzeko erabiltzen den Time-stamp ziurtagiria.
 - Sinatzeko erabiltzen den ziurtagiria sortzean SHA256WithRSAEncryption erabiltzen da, betiere 4096 bit-eko gako luzerarekin, eta TSA zerbitzuak soilik erabil dezake.

⁵ 910/2014 (EB) Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2014ko uztailaren 23koa, barne-merkatuko transakzio elektronikoetarako identifikazio elektronikoari eta konfiantzazko zerbitzuei buruzkoa, 1999/93/EE Zuzentaraua indargabetzen duena, Europako Parlamentuaren eta Kontseiluaren 2024ko apirilaren 11ko 2024/1183 (EB) Erregelamendua aldatua, zeinak (EB) 910/2014 Erregelamendua aldatzen baitu nortasun digitalaren esparru europarrari dagokionez.



- Tokenaren hash-algoritmoa SHA-256 da.
- 5. Izenpek denbora-zigilatzearen zerbitzu kualifikatua eskaintzeko erabiltzen duen TSU ziurtagiriaren indarraldia 5 urte artekoa da.
- 6. IZENPEren TSAk bere gain hartzen du “Denbora zigilatzeako zerbitzuak” atalean adierazten diren denbora zigilatzeako zerbitzuen hornikuntzaren gaineko erantzukizuna.
- 7. PDS honetan adierazitako ziurtagiriak denbora elektronikoko zigiluak sortzeko bakarrik erabil daitezke.
- 8. Ziurtagirien egoera egiaztatzea nahitaezkoa da ziurtagiriak erabiltzen diren bakoitzean, balio gabeteeen zerrenda (CRL) kontsultatuz. CRLa nola eta non aurkitu jakiteko informazioa ziurtagirian bertan dago.
- 9. Zigilu elektronikoaren baliozkotzeari eta Izenpek zigilu elektronikoak sortzeko erabiltzen duen ziurtagiriaren indarraldiaren egoerari buruzko egiaztapenak egin gabe, ez da haietaz fidatu behar. Kasu horretan, ez da inolako zilegitasunik izango Izenperen aurkako lege-ekintzak erreklamatzeko edo abiarazteko, zerbitzu horren erabileratik edo konfiantzatik datozen kalte, galera edo gatazkengatik.

4 ZIURTAGIRIAREN ERABILERA-MUGAK

- 10. Izenperen TSAk +/- 1 segundoko UTC gutxieneko denbora-estandarrekin bateragarria den denbora-zehaztasuna bermatzen du. IZENPEren TSAk ez ditu denbora-zigiluko tokenak jaulkiko, ezin badu denbora-doitasun hori ziurtatu.
- 11. 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.
- 12. Ziurtagiria iraungitzen denetik edo emandako zerbitzua amaitzen denetik, Izenpek 15 urtez gordeko ditu konfiantza-zerbitzu horri buruzko informazio eta dokumentazio guztia.

5 HARPIDEDUNEN BETEBEHARRA

- 13. Izenperen Denbora Zigilatzeako Zerbitzuaren Praktiken Deklarazioan, zerbitzu horren erabilerarekin lotuta jarduten duten alderdi guztien betebeharrak zehazten dira. Hemen eskuragarri: www.izenpe.eus.

6 TSU ZIURTAGIRIEN EGOERAZ FIDATZEN DIREN ALDERDIEN EGIAZTATZEKO BETEBEHARRAK

- 14. Denbora zigilatzeako token bat jasotzen denean, hirugarren aldeak egiaztatu beharko du behar bezala sinatuta dagoela eta denbora-zigilua sinatzeko erabilitako gako pribatua ez dela ezeztatu.
- 15. Denbora-zigiluak sortzeko erabilitako ziurtagiria iraungita ez dagoen bitartean, baliozkotasuna egiazta daiteke dagokion CRLan. Ziurtagiri horretan zehaztutako kokapenean dago eskuragarri CRL.



16. 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.

7 ERANTZUKIZUNAREN MUGAK

17. Izenpek Denbora Zigilatzeako Zerbitzuaren Praktiken Deklarazioaren arabera, bere DPCGren arabera eta Izenperen eta denbora zigilatzeako zerbitzuaren erabiltzaileen arteko beste edozein akordio lotesleren baldintzen arabera jarduten du bere TSA.
18. Izenpek ahaleginak egiten ditu bere zerbitzuetan erabilgarritasun handia emateko, baina ez du erabateko bermerik eskaintzen erabilgarritasunari dagokionez. IZENPE ez da inola ere onura-galeraren, zeharkako edo ondoriozklo kalteen edo datu-galeraren erantzule izango, indarrean dagoen legeriak hala ahalbidetzen duen heinean.
19. IZENPE ez da harpidedunak edo hirugarren aldeak egindako arau-hausteen ondoriozko kalteen erantzule izango, aplikatzeakoak diren terminoetan eta baldintzetan. Hala, Izenpek ez die erantzungo denbora-zigilu elektronikoak erabiltzean zabarkeriaz jokatu duten pertsoneri. Ondorio horietarako, eta nolana ere, zabarkeriatzat hartuko da Denbora Zigilatzeako Zerbitzuaren Konfiantzazko Praktiken Deklarazioan xedatutakoa ez betetzea, eta, bereziki, aldean betebeharrei eta erantzukizunari buruzko ataletan xedatutakoa ez betetzea.
20. Izenpe ez da, inola ere, ezinbesteko gertaerek eragindako kalteen erantzule izango; esaterako, hondamendi naturalek, elektrizitate- edo telekomunikazio-erorketek, suak, aurreikusi ezin diren kanpo-interakzioek (birusek, hackerren erasoek, gobernu-ekintzek edo grebek eragindakoak). Edonola ere, IZENPEk gorabehera horien ondorioak arintzeko zentzuzko neurri guztiak hartuko ditu. IZENPEk ez ditu estaliko ezinbesteko gorabehera batek eragindako atzerapenaren ondoriozko kalteak.

8 APLIKA DAITEZKEEN AKORDIOAK ETA ZIURTAPEN-PRAKTIKA ETA -POLITIKEN DEKLARAZIOA

21. Denbora zigilatzeako zerbitzuaren konfiantza-praktika partikularren deklarazioaren dokumentuak, www.izenpe.eus helbidean argitaratuak, jasotzen du Izenpek konfiantza-zerbitzuen emaile gisa eskaintzen duen konfiantza-zerbitzu horren baldintzei eta ezaugarriei buruzko informazio publikoa, eta jasotzen ditu inplikaturako aldean betebeharrak eta TSAk denbora-zigiluko token bat emateari dagokionez aplikatzen dituen arauak eta prozesuak. Hemen eskuragarri: <https://www.izenpe.eus/politica-tsa/webize01-cndocjuridica/es/>

9 PRIBATUTASUN POLITIKA

22. Izenpek egiten duen datu pertsonalen tratamendua bat dator Europako Parlamentuaren eta Kontseiluaren 2016ko apirilaren 27ko 2016/679 (EB) Erregelamenduan xedatutakoarekin, datu pertsonalen tratamenduari eta datu horien zirkulazio askeari dagokienez pertsona fisikoak babesteari buruzkoa eta 95/46/EE Zuzentaraua indargabetzen duena, bai eta gai horri buruzko araudi nazional espezifikoen arabera aplikatzeakoak diren baldintzekin ere.



23. Izenpek interesdunei jakinarazten die ziurtagiriaren serie-zenbakia ezeztatutako ziurtagiriaren zerrendan (CRL) sartzen duela, edozein erabiltzailek ikus dezan, nahiz eta ziurtagiri elektronikorik ez izan, bai eremu publikoan, bai pribatuan.

10 ITZULKETA-POLITIKA

24. Izenpek ez dauka itzulketarako politikarik ezarrita.

11 LEGE APLIKAGARRIA, KEXAK ETA EZTABAIDAK EBAZTEA

25. Izenperen konfiantzazko zerbitzuen hornidura Espainiako legerian xedatutakoaren arabera arautuko da.
26. Oro har, Izenperen konfiantzazko zerbitzuen erabiltzaileek onartzen dute DPCGak eta/edo zuzenean edo zeharka lotutako praktika partikularren eta PDSen deklarazioak gauzatzearen edo interpretatzearen ondoriozko auzi, desadostasun, arazo edo erreklamazio oro dagozkien kontratuetan, baldintza orokorretan eta/edo gomendio edo hitzarmenetan ezarritakoaren arabera ebatziko dela.
27. Aldeek erabaki dute haien artean sortzen den edozein gatazka Zuzenbide Kolaboratiboko prozesu baten bidez ebatziko dutela, eta, ados jarri ezean, Vitoria-Gasteizko epaitegi eta auzietara jo ahal izango da.

12 LIZENTZIAK ETA BILTEGIA, MARKA FIDAGARRIAK ETA IKUSKARITZA

28. Izenpek, Konfiantzazko Zerbitzuen Emaila gisa, bere gako publikoko azpiegituraren hainbat akreditazio eta ziurtagiri ditu, eta, horietatik, honako hauek aplikatzen ditu bereziki ziurtagiri-mota horietan:
- ISO/IEC 27001 ziurtagiria, informazioaren segurtasunerako estandarra.
 - ISO/IEC 27701 ziurtagiria, ISO/IEC 27001en pribatutasuna kudeatzeko luzapena. Horren helburua da pribatutasunaren babesari buruzko orientazioa ematea, erakundeek informazio pertsonala kudeatzeko modua barne, eta pribatutasunari buruzko araudia betetzen dela erakusten laguntzea, hala nola Datuak Babesteko Erregelamendu Orokorra.
 - Denbora zigilatze zerbitzu elektronikoa: Denbora-zigilu elektronikoak ematea eta administratzea, Europako estandarren arabera:
 - ETSI EN 319 421-“Policy and Security Requirements for Trust Service Providers issuing Time-Stamps)
 - ETSI EN 319 422 “Timestamping protocol and time-stamp token profiles”.
29. IZENPEren TSA zerbitzua denbora zigilatze zerbitzu kualifikatua da eIDAS araudiaren arabera. Espainiako konfiantzazko zerbitzu-emailen konfiantzazko zerrendan (TSL, ingelesezko sigletan) sartuta dagoela egiazta daiteke, <https://sede.minetur.gob.es/esES/datosabiertos/catalogo/lista-prestadores-tsl> estekaren bidez.
30. IZENPEri egiten zaizkion ikuskapenak eskatutako aldizkakotasunarekin egiten dira, eta horretarako akreditatutako Adostasuna Ebaluatze Erakunde batek egiten ditu.