

## PKIren DIBULGAZIO AKORDIOA (PDS)

Bertsio zk.: v 1.0  
Data: 2017ko maiatzaren 29a

---

© IZENPE 2017

Dokumentu hau IZENPErena da. Osotasunean soilik erreproduzi daiteke.

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

[www.izenpe.com](http://www.izenpe.com)  
[info@izenpe.com](mailto:info@izenpe.com)  
Tel.: 945 017 490



## AURKIBIDEA

1	SARRERA	3
2	HARREMANETARAKO DATUAK	3
3	ZIURTAGIRI MOTAK, BALIOZKOTZEKO ETA ERABILTZEKO PROZEDURA	3
4	MUGAK KONFIANTZAN	6
5	HARPIDEDUNEN BETEBEHARRAK	7
6	KONFIANTZA DUTEN HIRUGARREN BATZUEN BETEBEHARRAK	7
7	ERANTZUKIZUNEN MUGA	8
8	APLIKATZEKOAK DIREN AKORDIOAK, ZIURTAPEN PRAKTIKEN DEKLARAZIOA ETA ZIURTAPEN POLITIKAK	9
9	DATU PERTSONALAK BABESTEKO POLITIKA	9
10	ITZULTZEKO POLITIKAK	9
11	APLIKATZEKO LEGERIA, AUZIAK KONPONTZEKO MEKANISMOAK	10
12	AUDITORIAK, ZIURTAPENAK ETA ZIURTAPEN AGINTARITZEN ETA BILTEGIEN KONFIANTZAKO ZIGILUAK	10
13	BERTSIOEN KONTROLA	11



## 1 SARRERA

Dokumentu hau *ETSI EN 319 411-1 B* eranskinaren eskakizun teknikoen arabera sortu da: *“Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements”*.

PKI dibulgatzeko akordio honek ez du Ziurtapen Praktiken Deklarazioa (ZPDA) edo dagozkion ziurtapen-politikak ordeztzeko xedea. *Ziurtapen eta Zerbitzu Enpresa-Enpresa de Certificación y Servicios, Izenpe, SAK* (aurrerantzean IZENPE) bere ziurtagiriak kudeatzeko erabiltzen ditu ZPDA edo dagozkion ziurtapen-politikak.

Bi horiek eskura daude eta kontsulta daitezke [www.izenpe.eus](http://www.izenpe.eus) web-gunean.

## 2 HARREMANETARAKO DATUAK

Zerbitzu-egilearen izena	Ziurtapen eta Zerbitzu Enpresa-Enpresa de Certificación y Servicios, IZENPE, SA
Posta-helbidea	Tomas Zumarraga Dohatsuaren kalea, 71-1. 01008 Vitoria-Gasteiz
Posta elektronikoko helbidea	<a href="mailto:info@izenpe.com">info@izenpe.com</a>
Telefonoa	902 542 542

Ziurtagiri bat ezeztatzea eskatzeko formularioa eta prozedura [www.izenpe.eus](http://www.izenpe.eus) web-gunean lor daitezke.

## 3 ZIURTAGIRI MOTAK, BALIOZKOTZEKO ETA ERABILTZEKO PROZEDURA

IZENPEk jaulkitako ziurtagiri mota bakoitzari dagozkion xehetasunak Ziurtagiri bakoitzerako berariazko politika dokumentuan arautzen dira. Dokumentu hori *Ziurtapen Praktiken Deklarazioa* dokumentuarekin batera dator.

DESKRIBAPEN LABURRA	EUSKARRIA	POLITIKAREN IDENTIFIKATZAILEA	OID, POLITIKA	Ziurtatze-maila eIDAS
HERRITARRA				
<b>B@K</b>	HSM	NCP	1.3.6.1.4.1.14777.5.2.5	Txikia
<b>B@KQ</b>	HSM	QCP-n	1.3.6.1.4.1.14777.2.18.3	Oinarrizkoa
<b>Herritarraren Ziurtagiria</b>	Txartela/Token USBa (txip kriptografikoa)	QCP-n-qscd	eIDAS profila	Handia
			1.3.6.1.4.1.14777.2.6	
			eIDAS aurreko profila	Handia



			1.3.6.1.4.1.14777.2.18.1	
<b>ENTITATEAREN ORDEZKARIA</b>				
<b>Entitatearen ordezkaria</b>	HSM	QCP-n	1.3.6.1.4.1.14777.2.14	Oinarrizkoa
	Txartela/Token USBa: txip kriptografikoa	QCP-n-qscd	1.3.6.1.4.1.14777.2.12	Handia
	Softwarea: IZENPEren ziurtagirien edukitzailea	QCP-n	1.3.6.1.4.1.14777.2.16	Oinarrizkoa
<b>NORTASUN JURIDIKORIK GABEKO ENTITATEAREN ORDEZKARIA</b>				
<b>Nortasun juridikorik gabeko entitatearen ordezkaria</b>	HSM	QCP-n	1.3.6.1.4.1.14777.2.15	Oinarrizkoa
	Txartela/Token USBa: txip kriptografikoa	QCP-n-qscd	1.3.6.1.4.1.14777.2.13	Handia
	Softwarea: IZENPEren ziurtagirien edukitzailea	QCP-n	1.3.6.1.4.1.14777.2.17	Oinarrizkoa
<b>PROFESIONALA</b>				
<b>Entitate publikoko langilea</b>	Txartela/Token USBa: txip kriptografikoa	QCP-n-qscd	1.3.6.1.4.1.14777.4.14.1	Handia
	Softwarea: IZENPEren ziurtagirien edukitzailea	QCP-n	1.3.6.1.4.1.14777.4.14.2	Oinarrizkoa
	HSM	QCP-n	1.3.6.1.4.1.14777.4.14.3	Oinarrizkoa
<b>Entitate publikoko langilea, goitizena duena</b>	Txartela/Token USBa: txip kriptografikoa	QCP-n-qscd	<b>Sinatzea</b> 1.3.6.1.4.1.14777.4.13.1.1	Handia
		NCP+	<b>Kautotzea</b> 1.3.6.1.4.1.14777.4.13.1.2	Handia
		Ez dago erabilgarri	<b>Zifratzea</b> 1.3.6.1.4.1.14777.4.13.1.3	Handia
<b>Korporatibo kualifikatua</b>	Txartela/Token USBa: txip kriptografikoa	QCP-n-qscd	1.3.6.1.4.1.14777.2.19.1	Handia
	Softwarea: IZENPEren ziurtagirien edukitzailea	QCP-n	1.3.6.1.4.1.14777.2.19.2	Handia



	HSM	QCP-n	1.3.6.1.4.1.14777.2.19.3	Oinarrizkoa
<b>Korporatibo kualifikatu gabea</b>	Txartela / token USBa	NCP+	1.3.6.1.4.1.14777.1.1.1	Ez dago erabilgarri (kualifikatu gabea)
<b>Entitate publikoetako langilea (eIDAS aurrekoa)</b>	Txartela / token USBa	QCP public + SSCD	1.3.6.1.4.1.14777.4.1	Ez dago erabilgarri
<b>Eusko Jaurlaritzako langilea (eIDAS aurrekoa)</b>	Txartela / token USBa	QCP public + SSCD	1.3.6.1.4.1.14777.7.1	Ez dago erabilgarri
<b>Korporatibo publiko onartua (eIDAS aurrekoa)</b>	Txartela / token USBa	QCP public + SSCD	1.3.6.1.4.1.14777.4.2	Ez dago erabilgarri
<b>Korporatibo publiko onartu gabea (eIDAS aurrekoa)</b>	Txartela / token USBa	NCP+	1.3.6.1.4.1.14777.1.1.1	Ez dago erabilgarri
<b>Korporatibo pribatu onartua (eIDAS aurrekoa)</b>	Txartela / token USBa	QCP public + SSCD	1.3.6.1.4.1.14777.2.2	Ez dago erabilgarri
<b>Korporatibo pribatu onartu gabea (eIDAS aurrekoa)</b>	Txartela / token USBa	NCP+	1.3.6.1.4.1.14777.5.2.2	Ez dago erabilgarri

#### ENTITATE ZIGILUA

Entitate-zigilua	Edukitzailera. IZENPEren ziurtagirien edukitzailera	QCP-I-qscd	1.3.6.1.4.1.14777.2.11	Oinarrizkoa
	HSM	QCP-I	1.3.6.1.4.1.14777.2.20	Oinarrizkoa

#### ADMINISTRAZIO ZIGILUA

Administrazio-zigilua	Softwarea: IZENPEren ziurtagirien edukitzailera	QCP-I	1.3.6.1.4.1.14777.4.11.2	Oinarrizkoa
-----------------------	---	-------	--------------------------	-------------



	HSM	QCP-I	1.3.6.1.4.1.14777.4.11.3	Oinarrizkoa
Erdi-mailako administrazio-zigilua (eIDAS aurrekoa)	HSM	NCP+	1.3.6.1.4.1.14777.4.4	Ez dago erabilgarri

**ZERBITZARI SEGURUA (SSL)**

<b>SSL DV</b>	Softwarea	DVCP	1.3.6.1.4.1.14777.1.2.4	Ez dago erabilgarri
<b>SSL OV</b>	Softwarea	OVCP	1.3.6.1.4.1.14777.1.2.1	Ez dago erabilgarri
<b>SSL EV</b>	Softwarea	EVCP	1.3.6.1.4.1.14777.6.1.1	Ez dago erabilgarri
<b>EGOITZA</b>	Softwarea	OVCP	1.3.6.1.4.1.14777.1.1.3	Ez dago erabilgarri
<b>EGOITZA EV</b>	Softwarea	EVCP	1.3.6.1.4.1.14777.6.1.2	Ez dago erabilgarri

**APLIKAZIOA**

Aplikazioa	Softwarea: IZENPEren ziurtagirien edukitzailea	NCP	1.3.6.1.4.1.14777.1.2.2	Ez dago erabilgarri
------------	--	-----	-------------------------	---------------------

**KODE SINADURA**

<b>Kode-sinadura</b>	Txartela	NCP+	1.3.6.1.4.1.14777.1.3.1	Ez dago erabilgarri
----------------------	----------	------	-------------------------	---------------------

#### 4 MUGAK KONFIANTZAN

IZENPEK ez du bere ziurtagirien konfiantza-muga espezifikorik aplikatzen politika horretan. Aurreko atalean kontsulta daitezke ziurtagiri mota bakoitzaren mugak (sinadura, zigilua, web-gunea).

IZENPEK, konfiantzako zerbitzu-egilea den aldetik, honako elementu hauen barne-erregistroak gordetzen ditu edo elementu horien artxibatze segurua ziurtatzen du:

- ✓ Kualifikatutako ziurtagiri guztiak 15 urtez, eta kualifikatu gabeak 7 urtez.
- ✓ Ziurtagiriak jaulkitzearen auditoria-ebidentziak, iraungitze-dataren ondoren 7 urtez.
- ✓ Ziurtagiriak ezeztatzearen auditoria-ebidentziak, iraungitze-dataren ondoren 7 urtez.

Honako log hauek biltegitratzen dira:



- ✓ Ziurtagiri-eskaera berriak
- ✓ Baztertutako ziurtagiri-eskaerak
- ✓ Kontuetarako sarbideen urraketak
- ✓ Ziurtagirien sinadura
- ✓ Ziurtagiriak ezeztatzea
- ✓ Kontuen logon-a
- ✓ CRLen sinadura
- ✓ CAetako aldaketak
- ✓ Ziurtagirien iraungipena

## 5 HARPIDEDUNEN BETEBEHARRAK

---

- ✓ Informazio osoa eta egokia ematea IZENPERi, Ziurtapen Praktiken Deklarazioko eskakizunen arabera, erregistro-prozedurari dagokionez batez ere.
- ✓ Ziurtagirietan jasoarazi beharreko informazioaren egiazkotasuna, osotasuna eta gaurkotasuna bermatzea.
- ✓ Ziurtagiriak erabiltzeko baldintzak jakitea eta onartzea, baita haiei egiten zaizkien aldaketak ere.
- ✓ Ziurtagiriren bat jaulki eta eman aurretik, horretarako onarpena ematea.
- ✓ Ziurtagirien euskarriak ongi erabili eta gordeko direla bermatzea.
- ✓ Ziurtagiria egokiro erabiltzea, eta, zehazki, ziurtagirien erabilera-mugak aintzat hartzea.
- ✓ Arretaz zaintzea kredentzialak, baimendu gabeko erabilerak saihestearren, Ziurtapen Praktiken Deklarazioak agintzen duenaren arabera.
- ✓ IZENPERi eta harpidedunaren ustez ziurtagirian konfiantza duen edonori honako hau jakinaraztea, justifikatzerik ez dagoen atzerapenik gabe:
- ✓ Kredentzialak galdu, norbaitek ostu edo arriskuan jarri izana.
- ✓ Ziurtagiriaren edukian dauden okerrak edo izandako aldaketak (harpidedunak dakizkienak edo jakin litzakeenak). Aldaketak ziurtagiria ezeztatzea badakar, horretarako eskaera egin behar du harpidedunak.
- ✓ Baliozkotasun-aldia amaitu ondoren, identifikazio-baliabidea erabiltzeari uztea.
- ✓ Gakoen edukitzaileei jakinaraztea zein betebeharrak dagozkien.
- ✓ Ziurtagiri-zerbitzuen ezartze teknikoak ez kontrolatzea, manipulatzeko edo atzerantzko ingeniartzeko ekintzarik ez egitea, aurretik Ziurtapen Entitatearen idatzizko baimenik eduki gabe.
- ✓ Ziurtagiri-zerbitzuen segurtasuna arriskuan nahita ez jartzea.
- ✓ Ziurtagirietako gako publikoei dagozkien gako pribatuak ez erabiltzea inongo ziurtagiri izenpetzeko, ziurtapen-entitatea balitz bezala.

## 6 KONFIANTZA DUTEN HIRUGARREN BATZUEN BETEBEHARRAK

---

- ✓ Eman nahi zaion erabilerarako ziurtagiria egokia den ala ez jakiteko, informazioa iturri independenteetatik jasotzea.
- ✓ Ziurtagiriak erabiltzeko baldintzak ezagutzea, Ziurtapen Praktiken Deklarazioan aurreikusitakoaren arabera.
- ✓ Emandako ziurtagirien baliozkotasuna edo ezeztapena egiaztatzea. Horretarako, ziurtagirien egoerari buruzko informazioa erabiliko da.



- ✓ Ziurtagirien hierarkiako ziurtagiri guztiak egiaztatzea, sinadura digitalean edo hierarkiako ziurtagiriren batean konfiantza jarri baino lehen.
- ✓ Kontuan izatea ziurtagiria erabiltzeko dauden mugak, nonahi daudelarik ere: ziurtagirian bertan nahiz egiaztatzailearen kontratuan.
- ✓ Kontuan izatea kontratuan edo beste nonbait finkatutako badaezpadako neurri guztiak, edozein delarik ere haren izaera juridikoa.
- ✓ Jakinaraztea ziurtagiriari buruzko gertaera edo egoera irregular guztiak, ziurtagiria ezeztatzeko arrazoia izan daitezkeenak.
- ✓ Ziurtagiri-zerbitzuen ezartze teknikoak ez kontrolatzea, manipulatzeko edo atzeranzko ingeniartzeko ekintzarik ez egitea, aurrez IZENPEren idatzizko baimenik gabe.
- ✓ Ziurtagiri-zerbitzuen segurtasuna arriskuan nahita ez jartzea.
- ✓ Ziurtagiri kualifikatuen erabiltzailea behartuta dago aitortzera —dagokion tresna juridikoan— sinadura elektronikoko horiek eskuz idatzitako sinaduren baliokideak direla, eIDAS arauaren arabera.

## 7 ERANTZUKIZUNEN MUGA

---

IZENPEk bere gain hartuko ditu,

- ✓ Ziurtagirien indarraldiari buruzko edota ziurtagirien indarraldia iraungitzeari buruzko kontsulta-zerbitzuan ez sartzeak edo atzerapenez sartzeak pertsona edo erakunde bati sortzen zaizkion kalteak eta galerak.
- ✓ Identifikazio-bitartekoaren baliozkotasuna egiaztatzeko zerbitzuan barnean hartu ez izateagatik edo atzerapenez barnean hartzeagatik edonori eragiten zaizkion kalteak eta galerak.
- ✓ Era berean, ziurtagiri-zerbitzuak egiteko beharrezko funtzioak hirugarren batzuen esku uzten dituzenean, bere gain hartuko du pertsona horien jardunaren ondorioz hirugarren pertsonen aurrean sor daitezkeen edozein erantzukizun. Ildo horretan, 3.500.000 euroko zenbatekoa duen erantzukizun zibileko aseguruia eratu da, ziurtagirien erabilerak eragin ditzakeen kalteen eta galeren erantzukizun-arriskuari aurre egiteko.

IZENPEk egindako ziurtagiri-zerbitzuetan arduragabekeriarengatik edo behar adinako ardurarik izan ez delako erantzukizun du, baita sinadura elektronikokoari buruzko legerian ezartzen diren betebeharrak betetzen ez direnean ere. Hauek eragindako kalteetan izan eziz:

- ✓ Ziurtagirietako informazioek eragindakoak, betiere haien edukiak funtsean Ziurtagiri Praktiken Deklarazioa betetzen badu.
- ✓ Ziurtagirien eraginkortasuna agortzearen ondoriozkoak, betiere Ziurtagiri Praktiken Deklarazioan aurreikusitako argitalpen-betebeharrak betetzen baditu.
- ✓ Identifikazio-baliabideak desegoki erabiltzearen edo gero ezeztatzearen ondoriozkoak.
- ✓ IZENPE ez da sor daitezkeen kalte zuzen edo zeharkakoen, berezien, intzidentziakoen eta emergenteen erantzule izango, ezta eskuratu gabeko irabazien, datu-galeren eta zigorkalteen erantzule ere —aurreikusteko modukoak izan edo ez—, baldin eta horiek ziurtagirien, sinadura digitalen edo Ziurtagiri Praktiken Deklarazioan eskaintzen edo aurreikusten den bestelako edozein transakzio edo zerbitzuren erabilera, entrega, baimen, funtzionamendu edo funtzionamendu ezarekin lotuta badaude eta behar ez bezalako erabilerak eragin baditu.
- ✓ Ziurtagirian ageri diren datuen zehaztapen-ezagatik harpidedunari edo fede oneko hirugarren pertsonari eragindakoak, baldin eta datu horiek dokumentu publiko baten bidez





(notaritzakoa, judiziala edo administratiboa) ziurtatu badira, Erregistro Entitateak eman duen dokumentu bidez denean izan ezik.

IZENPE ez da ziurtagiriez fidatzen diren harpidedunek edo hirugarren pertsonak dituzten betebeharrak ez betetzeagatik harpidedunari edo fede oneko hirugarren pertsonari eragindako kalteen erantzule izango.

IZENPE ez den eta erregistro-entitate gisara aritzen den erakunde oro bere gain hartutako eginkizunek eragiten dituzten kalteen erantzule izango da IZENPEren aurrean, dagokion legetresnak finkatzen duenaren arabera.

## 8 APLIKATZEKOAK DIREN AKORDIOAK, ZIURTAPEN PRAKTIKEN DEKLARAZIOA ETA ZIURTAPEN POLITIKAK

Aplikatzekoak diren akordio, Ziurtapen Praktiken Deklarazio eta politika guztiak [www.izenpe.eus](http://www.izenpe.eus) web-gunean daude.

## 9 DATU PERTSONALAK BABESTEKO POLITIKA

<i>Datuak babesteari buruzko oinarritzko informazioa</i>	
<i>Arduraduna</i>	Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, SA
<i>Xedea</i>	Ziurtagiri elektronikoarekin lotzen diren zerbitzuak egitea eta kudeatzea.
<i>Eskubideak</i>	Sartzeko, zuzentzeko eta ezeztatzeko eskubidea —Tomas Zumarraga Dohatsuaren kalea, 71, 1. 01008 Vitoria-Gasteiz—.
<i>Informazio osagarria</i>	<a href="#">IZENPEren Ziurtapen Praktiken Deklarazioa.</a>

Ziurtagiri kualifikatuen kasuan, ziurtagiriak jaulkitzeko edo ezeztatzeko erregistro-datuak 15 urtez gordetzen dira IZENPEN, eta ziurtagiri kualifikatu gabeen kasuan 7 urtez.

## 10 ITZULTZEKO POLITIKAK

IZENPEk ez du itzultzeko politikarik, eta arlo horretan indarrean dagoen legeriari lotuko zaio.



## 11 APLIKATZEKO LEGERIA, AUZIAK KONPONTZEKO MEKANISMOAK

---

### 11.1. Aplikatzeko den araudia

Ziurtapen Praktiken Deklarazio hau gauzatzeari, egiteari, interpretatzeari eta baliozkotasunari dagozkien alor guztietan aplikatu behar da sinadura elektronikoari buruzko Espainiako legeria. Honako hau da dokumentu honi eta ondoriozko eragiketei aplikatu dakiekeen araudia:

- ✓ Sinadura elektronikoari buruzko abenduaren 19ko 59/2003 Legea.
- ✓ Administrazio Publikoen Administrazio Prozedura Erkideari buruzko 39/2015 Legea.
- ✓ Sektore Publikoaren Erregimen Juridikoari buruzko 40/2015 Legea.
- ✓ Datuak babesteari buruzko 15/1999 Lege Organikoa.
- ✓ Identifikazio elektronikoari eta barne-merkatuko transakzio elektronikoetarako konfiantzako zerbitzuei buruzko 910/2104 Europako araudia (eIDAS).

### 11.2. Erreklamazioak eta auzien ebazpena

IZENPEk kontsumoko artekaritza-sistemaren kontrolpean dihardu, aplikagarri zaion legeriak aurreikusten duenaren arabera. Hala, eskatzaileen edo harpidedunen kexuak edo erreklamazioak artatu eta ebazteko dituzte, eta hartzen duen erabakia loteslea eta betearazlea izango da alde bientzat, herritarren ziurtagiriei dagokienez betiere.

Xede horretarako, eskatzaileak edo harpidedunak sistema hori onartzen duela joko da dagokion Kontsumoko Artekaritza Batzordean artekaritza-eskaera formalizatzen duen une beretik.

Kontsumoko artekaritza-sistematik at dauden herritarren ziurtagirien esparruan eskatzaileengandik edo harpidedunengandik sor daitezkeen beste edozein auzi dagokion jurisdikzioaren esku geratuko da.

## 12 AUDITORIAK, ZIURTAPENAK ETA ZIURTAPEN AGINTARITZEN ETA BILTEGIEN KONFIANTZAKO ZIGILUAK

---

Zerbitzuak eraginkortasunez garatzeko eta ezartzeko helburuarekin, IZENPEk informazioaren segurtasuna kudeatzeko sistema ezarri du konfiantza-zerbitzuekin lotzen diren prozesuetarako, betiere ISO27001 estandarren arabera.

IZENPEk ETSIaren (Telekomunikazioetako Estandarren Europako Institutuaren) estandarren adierazpenak jarraitzen ditu, eta honako hiru arau hauen zehaztapen teknikoaren arabera lortu du ziurtapena: ziurtagiri kualifikatuak jaulkitzeko EN 319 411-2 arauaren zehaztapen teknikoaren arabera; gako publikoko ziurtagiriak jaulkitzeko EN 319 411-1 arauaren zehaztapen teknikoaren arabera; eta denbora-zigiluak jaulkitzeko EN 319 422 arauaren arabera. Identifikazio elektronikoari eta barne-merkatuko transakzio elektronikoetarako konfiantzako zerbitzuei buruzko 910/2104 Europako araudiak (eIDAS) eskatzen dituen arauak dira.

Balidazio hedatuko ziurtagirien politikari (EVCP) jarraitzen dioten zerbitzari seguruko ziurtagirietarako, erakundearen balidazio-politikari (OVCP) jarraitzen dioten zerbitzari seguruko ziurtagirietarako eta domeinuaren balidazio-politikari (DVCP) jarraitzen dioten zerbitzari seguruko ziurtagirietarako, CA/Browser Forum-ek onartutako gidei ere jarraituko zaie ([www.cabforum.org](http://www.cabforum.org) web-gunean daude eskuragarri).

Ziurtapen guztiak kontsulta daitezke [www.izenpe.eus](http://www.izenpe.eus) web-gunean.



## 13 BERTSIOEN KONTROLA

---

Hasierako bertsioa.