

# Egoitzako ziurtagiriak eta SSL/TLS zerbitzari segurua

Izenperen ziurtagirien gida



# SSL

## Zer ziurtagiri aukeratu?

Zerbitzari seguruko hainbat ziurtagiri mota daude, beharraren eta behar den segurtasun-mailaren arabera.

Administrazio publikoen kasuan, gainera, egoitza elektronikorako ziurtagiri espezifiko bat hautatzeko aukera dago.

### SSLren eta egoitza elektronikoaren abantailak

- Zure webgunea **berme handienekin** segurtatzen dute.
- Erantzukizun zibileko aseguru baten babesa daukate.
- **SHA-2 eta 2048 biteko** algoritmoekin sinatuta daude.
- Maila handieneko estandar kriptografikoak eta CABForum-en eskakizunak betetzen dituzte.
- **Nabigatzaile eta sistema eragile** garrantzitsuenek ezagutzen dituzte.
- **Posizionamendua hobetzen dute** Googleko bilaketetan (posizionamendu altuagoa eskaintzen die SSLrekin segurtatuta dauden guneei).
- Googlek eskatzen duen **gardentasun-egiaztapenarekin** jaulkitzen dira.
- Bizirik, ezeztatuta eta iraungita dauden ziurtagiriak **kudeatzeko tresna**.



# SSL ziurtagiri motak



## DOMEINUKO SSL DV ZIURTAGIRIA

- Balidazio azkarra eta erraza
- Domeinua bakarrik egiaztatzen da
- Gehienez bi izen alternatibo oinarrizko prezioan
- Wildcard sartzeko aukera ematen du



## ERAKUNDEKO SSL OV ZIURTAGIRIA

- Domeinua eta erakundea egiaztatzen dira
- Gehienez bi izen alternatibo oinarrizko prezioan
- Wildcard sartzeko aukera ematen du



## SSL ZIURTAGIRI KUALIFIKATUA

- 910/2014 Europako Erregelamenduaren (eIDAS) arabera kualifikatua
- Gehienez bi izen alternatibo oinarrizko prezioan



## EGOITZAKO ZIURTAGIRI KUALIFIKATUA

- 910/2014 Europako Erregelamenduaren (eIDAS) arabera kualifikatua
- Administrazio publikoena bakarrik
- Egoitza elektronikoak aldizkari ofizialean argitaratuta egon behar du
- Gehienez bi izen alternatibo oinarrizko prezioan

# Behar diren profilak



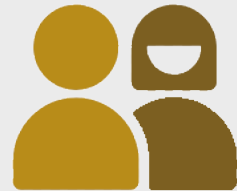
## ORDEZKARIA/BEZEROA

**DOMEINUAREN TITULAR** den erakundearen alta sinatuko du eta pertsona baimendunen gaikuntza baimenduko du.

**Pertsona baimendunen aldaketek** ordezkariak sinatutako eskaera berri bat dakarte.

**Ziurtagiri kualifikatuen eskaera guztiak sinatu** beharko ditu.

Izenpe edo eNAN ziurtagiri kualifikatua erabili behar duzu.



Acceso con certificado



Alta/Modificación Cliente

## PERTSONA BAIMENDUNAK

SSL erakunde baten izenean kudeatzeko baimena dutenak.

Denek bistaratuko dituzte baimenduta dauden erakunde guztien ziurtagiri guztien ekintzak.

TSLetan onartutako edozein ziurtagiri kualifikatu erabil dezakete.

# Alta eta baimena: Aplikazioa erabiltzeko betekizunak



## Alta

- Edonork egin dezake aplikazioan alta emateko eskabidea.



- Sortutako eskabidea (PDF) erakundean ahala/autoritatea duen pertsonak sinatu beharko du (adibidez, alkateak). Ziurtagiriak kudeatzeko baimena ematen zaien pertsonak hartuko ditu barnean.
- Izenpek eskabide-dokumentua egiaztatu eta gaikuntzaren berri emango du, pertsona baimendunek tramitatzen hasteko aukera izan dezaten.

## Pertsona baimendunak

- Izenperen identifikazio elektronikorako bitarteko profesional edo pertsonal batekin (BakQ, herritarra, korporatiboa...) sartuko dira aplikazioan.
- Erakundekoak izan daitezke edo ez, ordezkariaren erabakia da hori.
- Pertsona berak hainbat erakundetarako baimena izan dezake.

Helbide elektronikohonetan jasoko dira DV edo OV ziurtagiriaren eskabideei buruzko jakinarazpen guztiak.

Bezero-erakunde horretarako pertsona baimendunak gehitzeko aukera ematen du.

**Bezeroaren datuak**

Nahitaezko datuak bete behar dira (\* batekin markatutariakoak)

Erakundearen datuak

Erakundearen IFK\*

Erakundearen izen ofiziala\*

Erakundearen izen komertziala

Kalea:  Zenbakia:  Solairua:  Atea:

Herria:  Probintzia:  Herrialdea:  Posta Kodea:

Emaila jakinarazpenak (DV, OV)\*

Ordezkarieren harreman datuak

Atzerritarra

Izena:\*  Lehen Abizena:\*  Bigarren Abizena:\*

NAN:\*  Email:\*  Telefonoa:\*

Erakundearen IFK\*  Ordezkaria kargua:\*

Erakundearen izen\*

Fakturazio Datuak

Bezeroaren datuak koptatu

Kalea:  Zenbakia:  Solairua:  Atea:

Herria:  Probintzia:  Herrialdea:  Posta Kodea:

Terminoak eta baldintzak

Kontratu izenpetzailearen erreferentzia

Baimendutako eskatzaileen zerrenda

Imprimir solicitud

Alta/Modificación Cliente

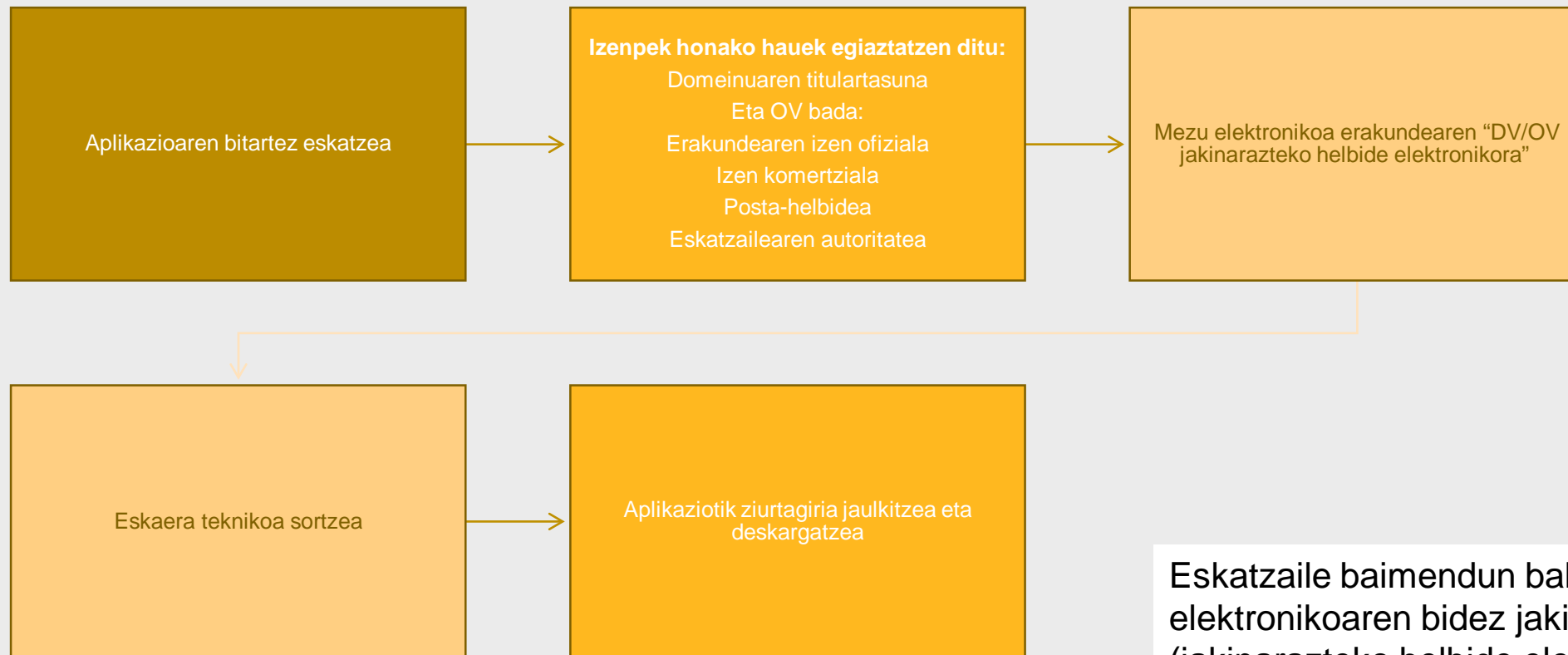
Cancelar

**Inprimatu eskabidea:** erakundearen ordezkariek sinatu beharreko PDFa sortzen du.

**Bezeroaren alta/aldaketa:** formularioan sartutako aldaketak gordetzen ditu.

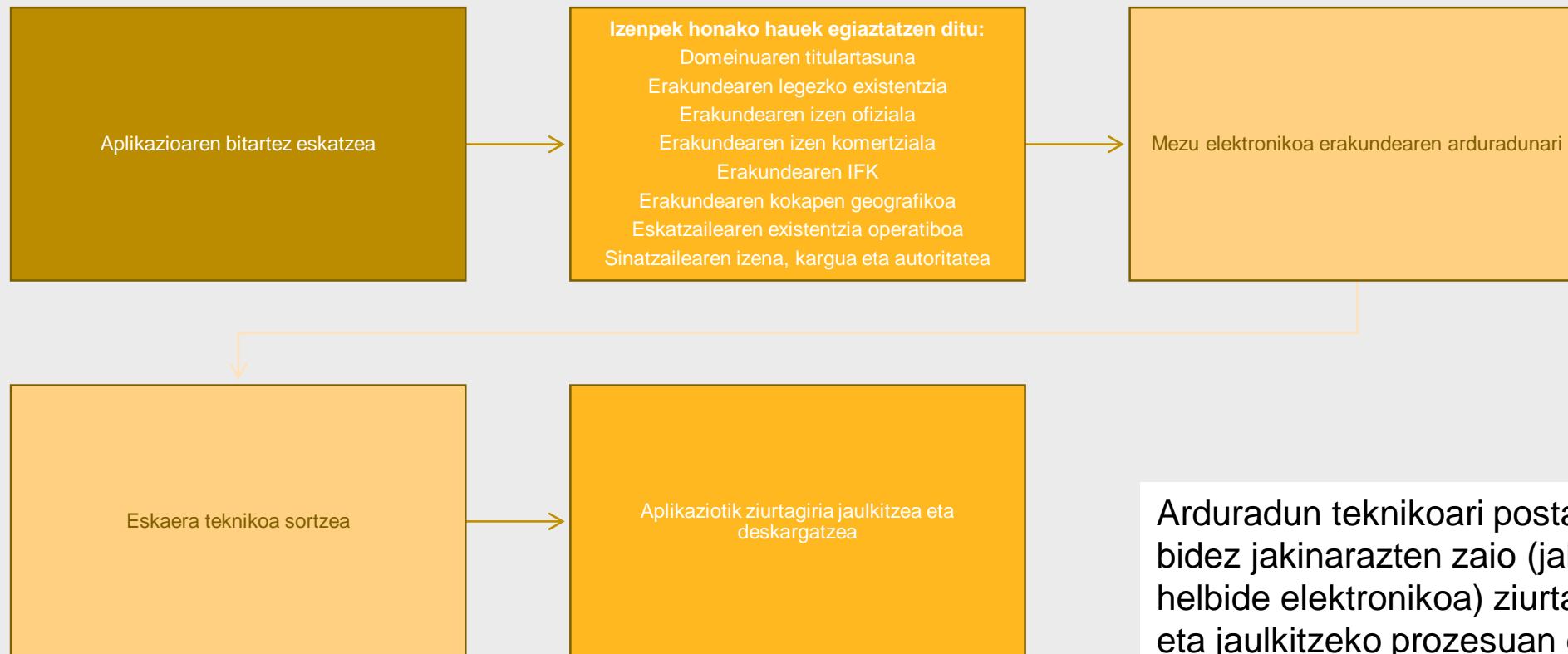
**Utzi:** sartu eta gorde ez diren aldaketak ezabatzen ditu.

# Jaulkitze-zikloa: SSL DV eta OV



Eskatzaile baimendun bakoitzari posta elektronikoaren bidez jakinarazten zaio (jakinarazteko helbide elektronikoa) ziurtagiriak eskatzeko eta jaulkitzeko prozesuan egindako urrats bakoitza.

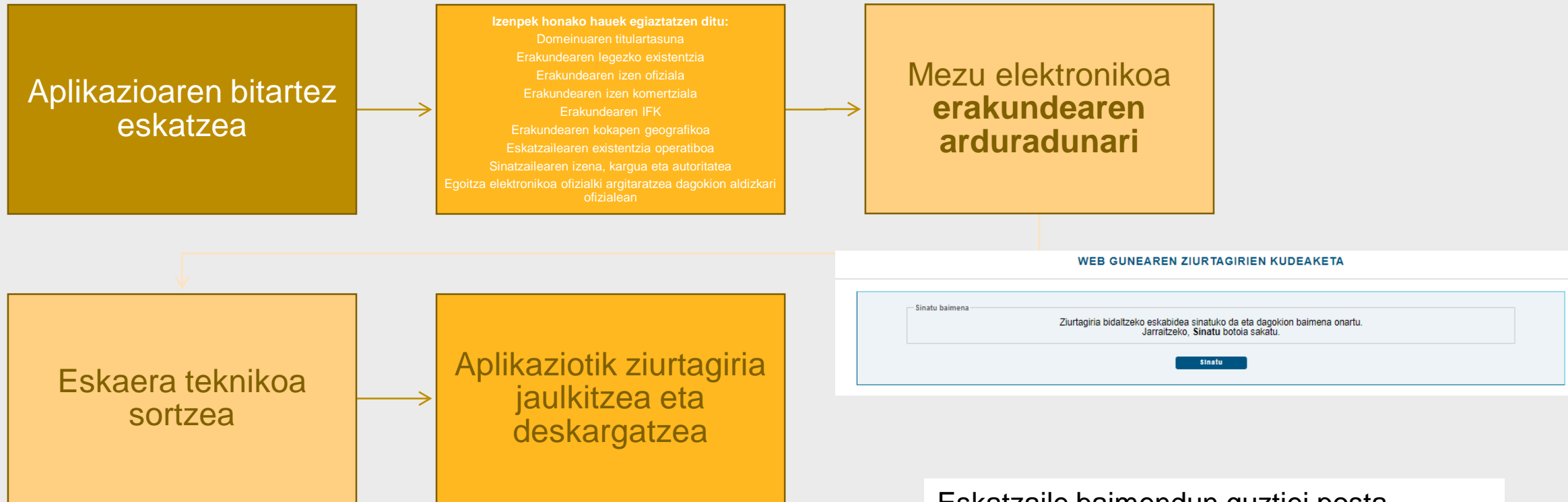
# Jaulkitze-zikloa: SSL kualifikatuak



Arduradun teknikoari posta elektronikoaren bidez jakinarazten zaio (jakinarazteko helbide elektronikoa) ziurtagiriak eskatzeko eta jaulkitzeko prozesuan egindako urrats bakoitza.



# Jaulkitze-zikloa: egoitza kualifikatuak



Eskatzaile baimendun guztiei posta elektronikoaren bidez jakinarazten zaie ziurtagiriak eskatzeko eta jaulkitzeko prozesuan egindako urrats bakoitza.

Fitxa bakoitzak aukera ematen du ziurtagiriak egoeraren arabera kudeatzeko:

- **Bezeroaren datuak:** harremanetarako eta fakturaziorako datuak aldatzeko.
- **Jaulkitzeko dauden** ziurtagirien kudeaketa: eskabide berriak egiteko edo tramitatzen ari direnak osatzeko.
- **Jaulkitako** ziurtagirien kudeaketa
- **Iraungitako** ziurtagirien kudeaketa
- **Ezeztatutako** ziurtagirien kudeaketa

Ziurtagiriaren bizi-zikloa



## WEB GUNEAREN ZIURTAGIRIEN KUDEAKETA

Irten

es | eu | en

AINHOA ANITUA GIL

Bezeroaren datuak

Egiteke dauden Ziurtagirien kudeaketa

Emandako Ziurtagirien kudeaketa

Iraungitako Ziurtagirien kudeaketa

Ezeztatutako ziurtagirien kudeaketa

Nahitaezko datuak bete behar dira (\* batekin markatutakoak)

Erakundearen datuak

<b>Erakundearen IFK:</b>	C99395279	<b>Erakundearen izen ofiziala:</b>	AYTO DE MASSACHUSSETS	<b>Erakundearen izen komertziala:</b>	MASSACHUSS
<b>Kalea:</b>	HIGH ROAD	<b>Zenbakia:</b>	5	<b>Solairua:</b>	2
<b>Herria:</b>	DENVER	<b>Probintzia:</b>	COLORADO	<b>Herrialdea:</b>	
<b>Posta Kodea:</b>		<b>Posta Kodea:</b>	54587		
<b>Emaila jakinarazpenak (DV, OV)</b>	seroscar2@gmail.com				

# Ziurtagiri bat eskatzea

“Jaulkitzeko dauden ziurtagirien kudeaketa” fitxan “Ziurtagiri berriaren eskabidea” hautatzean, erakundearen eta eskatzailearen datuak partzialki beteta izango dituen formularioa zabalduko da. Egoitzako ziurtagirietan, gainera, egoitza zein arautan argitaratuta dagoen adierazi beharko dugu.

Lehenik ziurtagiri mota hautatu behar dugu:

Datos cliente | Gestión Certificados pendientes | Gestión Certificados emitidos | Gestión Certificados caducados

Debe rellenar todos los datos obligatorios (marcados con \*)

Solicitud nuevo certificado

Tipo de certificado

Tipo Certificado:\*  Precio Certificado:

Datos solicitante

Extranjero

DNI:\* 72734342Q Nombre: ANTONIA  
Primer Apellido:\* ANTONIA Segundo Apellido:\* GIL  
Email:\* a-anton@izenpe.eus Teléfono:\* 666888444

Datos organización

CIF:\* C99395279 Empresa:\* AYTO DE MASSACHUSETTS  
Email notificaciones (DV, OV):\* seroccar2@gmail.com

Datos representante

Extranjero

DNI:\* 44674471F Nombre:\* JOHN  
Primer Apellido:\* DOE Segundo Apellido:\* MEMPHIS  
Teléfono:\* 555444777 Email:\* O-GARCIA@IZENPE.EUS

Bezeroaren datuak | **Egiteke dauden Ziurtagirien kudeaketa** | Emandako Ziurtagirien kudeaketa | Iraungitako Ziurtagirien kudeaketa | Ezetzatutako ziurtagirien kudeaketa

Nahitaezko datuak bete behar dira (\* batekin markatutakoak)

Eskaera ziurtagiri berria

Ziurtagiri mota

Ziurtagiri Mota:\*

Ziurtagiriaren Prezioa:

Egoitzaren datuak

Araua:\*

# Ziurtagiri bat eskatzea

Formularioaren amaieran domeinuaren datuak osatuko ditugu eta titulartasuna egiaztatzeko modua hautatu beharko dugu, baita ziurtagiriaren eskabide teknikoa —CSR— erantsi ere.

Mezu elektronikoa bidaliko da eskaera balidatzeko: DV eta OV ziurtagirien kasuan baimendunari, eta ziurtagiri KUALIFIKATUEN kasuan erakundearen ordezkariari.

Ziurtagiriaren datuak

Domeinua:\*

Izen alternatiboa 1:

Izen alternatiboa 2:

Izen alternatiboa 3:

Titulartasun lehenetsia egiaztatzeko modua:\*

Eskaera Teknikoa (Gehienez: 10KB):  [i](#)

Gainontzeko SAN-ak

Gainontzeko SAN-ak

+ -

# Domeinuaren titulartasuna egiaztatzeko moduak

Nahi den modua hauta daiteke

## DNS ALDAKETA

Izenpek mezu elektronikoa bidaltzen du ausazko balio batekin, eta eskatzaileak domeinuaren DNSan TXT erregistro bat gehitzeko erabili behar du. Eskatzaileak mezu elektronikoa jarraibideak bete behar ditu.

## DNS CAA [aukera lehenetsia]

Izenpek mezu elektronikoa bidaltzen du ausazko kode batekin DNS CAA erregistro batean agertzen den helbide elektronikora. Aldez aurretik CAA motako "contactemail" sarrera bat egon behar da, helbide elektronikoa batekin. Adibidez: CAA 0 contactemail [contacto@example.com](mailto:contacto@example.com). Kontaktuak mezu elektronikoa jarraibideak bete behar ditu.

## DNS TXT [aukera lehenetsia]

Izenpek mezu elektronikoa bidaltzen du ausazko kode batekin DNS TXT erregistro batean agertzen den helbide elektronikora. Aldez aurretik TXT motako sarrera bat egon behar da "\_validation-contactemail" azpidomeinuan, helbide elektronikoa batekin. Adibidez: \_validation-contactemail.izenpe.eus. 299 IN TXT [contacto@example.com](mailto:contacto@example.com). Kontaktuak mezu elektronikoa jarraibideak bete behar ditu.

## WEBGUNEA

Izenpek mezu elektronikoa bidaltzen du fitxategi batekin, eta eskatzaileak dominio/.well-known/pki-validation/ bide-izenean argitaratu behar du. Eskatzaileak mezu elektronikoa jarraibideak bete behar ditu.

## WHOIS

Izenpek mezu elektronikoa bidaltzen du ausazko balio batekin, WHOIS kontaktuan (Registrant, administraria edo teknikaria) agertzen den helbidera. Kontaktuak mezu elektronikoa jarraibideak bete behar ditu.



# Eskaera baten egoerak eta ekintzak

“Jaulki gabe” egoera mantenduko da 4 markak (*flag*) OK izan arte.

Gainera, marken egoeraren arabera, eskaera kudeatzeko hainbat ekintza gauzatu ahal izango da.

Egoerak / Markak	Ekintzak
Ordezkarria berrestea	<b>Kontsulta:</b> eskaera-formularioa zabaltzen du.
Domeinuaren titulartasuna egiaztatzea	<b>PDF deskarga:</b> eskaera-formularioa deskargatzen du.
CSR igota	<b>Editatu:</b> oraindik tramitatu EZ den eskaera batean aldaketak egiteko aukera ematen du.
Izenpek igortzea	<b>Ziurtagiria deskargatu</b>

# Ziurtagiri baten egoerak

Ziurtagiri bat jaulki ondoren, haren bizi-zikloaren egoerak eta horietako bakoitzean egin daitezkeen ekintzak honako hauek dira:

Egoerak / Markak	Ekintzak
<b>Jaulkita</b>	Deskargatu
<b>Bizirik</b>	Berritu
<b>Iraungita</b>	Ezeztatu
<b>Ezeztatuta</b>	

# Erakunde anitzeko baimendunak

## Hainbat erakunde profil beretik kudeatzea

Pertsona baimendun berak hainbat erakunderen ziurtagiriak kudeatzen dituzenean, zein bezeroren ziurtagiriak kudeatu nahi dituen hautatu beharko du autentifikatzen denean.



The screenshot shows a web interface for managing certificates. At the top left is the 'ee' logo. The title is 'WEB GUNEAREN ZIURTAGIRIEN KUDEAKETA'. Below the title, there are two radio buttons for selecting a company profile: 'Erakunde berria' (selected) and 'Erakunde berria, baimendunak'. Below these, there is a dropdown menu with 'KK-PAGA' selected. At the bottom right, there are two buttons: 'Berritu' and 'Ezartu'.



**Mila esker**

**Gracias**

---

[www.izenpe.eus](http://www.izenpe.eus)