



TicketBAI softwarea garatzen duten enpresentzako ohar teknikoa

Arabako, Bizkaiko eta Gipuzkoako TicketBAI zerbitzuen SSL/TLS ziurtapen katearen aldaketa

Kanpoko probak edo aurreproduktzioa

Produktzioa

2026ko urriak 1

2026ko azarotik 2027ko urtarrilera bitartean aurreikusia. Egoitza elektronikoko bakoitzean aldeztu aurretik komunikatuko da

Garrantzitsua

Komunikazio hau TicketBAI zerbitzuetan zentratzen bada ere, jasotako gomendioak foru aldundien zerbitzu elektronikoen makinatutik makinara egiten diren beste integrazio batzuei ere aplikatu dakizkieke, zerbitzu horiek ziurtapen azpiegitura berriari lotutako ziurtagiriak erabiltzen dituztenean.

1. Komunikazioaren xedea

Arabako, Bizkaiko eta Gipuzkoako foru aldundiek berriro egingo dituzte beren TicketBAI zerbitzuekiko komunikazioak babesten dituzten SSL/TLS ziurtagiriak.

Berriro horren ondorioz, aldaketa bat izango da TicketBAIren HTTPS zerbitzariak hiru lurraldeetan duten ziurtapen katean. Ziurtagiri berriak Sectigoren ziurtapen hierarkia berri bati egongo dira lotuta, eta alde batera utziko dute gaur egun erabiltzen den katea.

HTTPS konexioa ezartzean helmugako zerbitzariak aurkezten duten ziurtagiriari eragiten dio aldaketak. Ez du eraginik aplikazioek erabiltzen dituzten gailu edo sinadura ziurtagirietan, eta ez ditu aldatzen ez TicketBAI mezuen formatua, ez zerbitzu funtzionalak eta ez fitxategiak identifikatu eta sinatzeko mekanismoak.

Aldaketa hori prestatzeko, beharrezkoa izango da konfiantzazko biltegian ohar tekniko honetan adierazten diren ziurtapen agintaritzak (CAk) sartzeari, baina egun dauden eta beste zerbitzu edo ziurtapen kate batzuk balidatzeko oraindik beharrezkoak diren konfiantzazko CAk ezabatu gabe.

Komunikazioak izaera bateratua du. Izan ere, software soluzio berak lurralde batean baino gehiagotan operatzeko balio dezake, hasieran zein aldunditan erregistratu den kontuan hartu gabe.

Foru aldundien beste zerbitzu batzuekin (BIHa, SILICIE, faktura elektronikoa edo antzekoak) makinaz makinako integrazioak garatzen dituzten edo horien ardura duten enpresek ere hartu beharko dute kontuan aldaketa hau. Zerbitzu horiek hierarkia berriari lotutako ziurtagiriak erabiltzen dituztenean, konfiantzazko biltegiak eguneratu eta probak egiteko jarraibideak ere aplikagarriak izango dira.

2. Aldaketaren deskribapena

Aplikazio bat HTTPS bidez konektatzen denean TicketBAI zerbitzu batera, zerbitzariak ziurtagiri elektronikoa bat aurkezten du identitatea egiaztatzeko eta komunikazio zifratua ezartzeko.

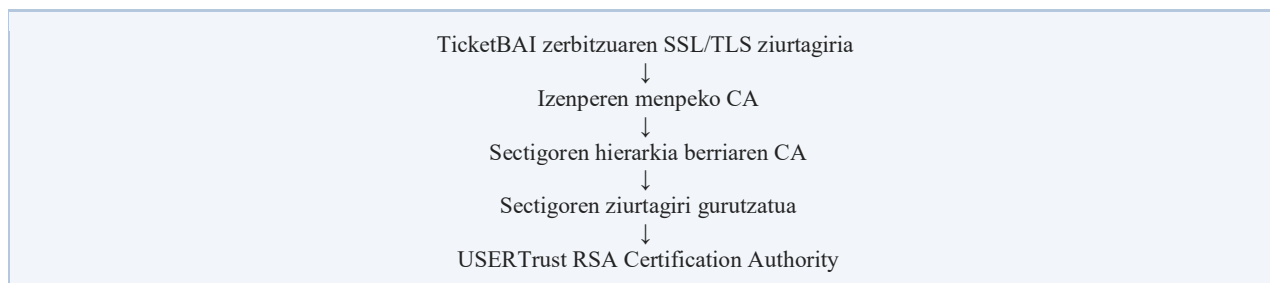
Sistema berriro ondoren, Arabako, Bizkaiko eta Gipuzkoako TicketBAI zerbitzariak Sectigoren ziurtapen hierarkia berriaren arabera jaulkiko dituzte ziurtagiriak.

Konexioak behar bezala balidatu daitezkeen, nahitaezkoa izango da aplikazioen konfiantzazko biltegian gordeta edukitzea ziurtapen bide baliodun bat eraikitzeko beharrezkoak diren ziurtapen agintaritzak (CAk).

3. Ziurtapen kate berria eta konfiantzazko biltegien eguneraketa

Hiru aldundiek erabiliko duten ziurtapen katearen konfiantzazko bidea USERTrust CA erroan amaituko da.

Modu sinplifikatuan, hau izango da katea:



Sectigoren hierarkia berriak bide zuzena du bere CA erro propioraino. Dena den, Arabako, Bizkaiko eta Gipuzkoako TicketBAI zerbitzariak kate bat izango dute USERTrustera iristea ahalbidetuko duen konfiantzazko bide bat eraikitzeko.

Konfigurazio horren helburua da aplikazio, gailu eta sistema zaharrekin dagoen bateragarritasuna handitzea haien konfiantzazko biltegien USERTrust CA erro bat eduki bai baina Sectigoren CA nagusi berria oraindik instalatu ez zaienean.

Sectigoren ziurtagiri gurutzatuari esker, sistema horiek bide baliodun bat eraiki dezakete TicketBAI zerbitzuaren ziurtagiritik dagoeneko instalatua duten USERTrust CA erroraino. Horrek murriztu egiten du ziurtapen hierarkia berrira aldatzeko prozesuan etenak gertatzeko arriskua.

Konfiantzazko biltegi propioa erabiltzen duten enpresa garatzaileek egiaztatu behar dute biltegi horrek ziurtapen kate berria balidatzeko aukera ematen duela. Horretarako, beharrezkoa izango da CA erro bezala Sectigo Public Server Authentication Root R46 erroa gehitzea.

Behin erro hori instalatuta, aplikazioak prest egongo dira Sectigoren ziurtapen hierarkia berria zuzenean balidatzeko, eta ez dira geratuko USERTrust-erako bateragarritasun bidearen mende soil-soilik. Aldaketa honek ez du beharrezko egiten USERTrust erroa instalatzea; izan ere, bateragarritasun bidea konfiantzazko biltegien erro hori baduten sistemetan erabiltzeko pentsatuta dago.

Foru aldundiek aurkeztutako zerbitzarien azken ziurtagiriak ez dira konfiantzazko biltegien sartu behar. Ziurtagiri horiek epe jakin baterako balio dute, eta aldian-aldian berrituko dira. Haietan konfiantza zuzena izateak berritze bakoitzean softwarea edo haren biltegia berriro eguneratzera behartuko luke.

Azken ziurtagiriak desberdinak izango dira zerbitzu eta ingurune bakoitzerako, kasuan kasuko DNS izenei lotuta egongo baitira. Hala ere, Arabako, Bizkaiko eta Gipuzkoako TicketBAI zerbitzuek hierarkia bera erabiliko dute, baita ziurtapen bide bera ere USERTrust-era iristeko.

4. Kurba eliptikoetan oinarritutako etorkizuneko ziurtagirietarako prestatzea

2026rako aurreikusitako aldaketan, RSAn oinarritutako ziurtagiriak eta ziurtapen kateak erabiliko dira. Aldaketa honetan, ez dago aurreikusita kurba eliptikoen kriptografian oinarritutako SSL/TLS ziurtagiriak erabiltzea.

Hala ere, segurtasun kriptografikoa indartzeko, etorkizunean beharrezkoa izan liteke kurba eliptikoetan edo ECCn oinarritutako SSL/TLS ziurtagiriak erabiltzea.

Sectigok badu hierarkia espezifiko bat mota horretako ziurtagirietarako. Dagokion CA erroa Sectigo Public Server Authentication Root E46 erroa da.

Horregatik, prebentzio neurri gisa, gomendatzen da konfiantzazko biltegien Sectigo Public Server Authentication Root E46 CA erroa ere sartzea.

Horrela, aplikazioak prestatu ahal izango dira etorkizunean kurba eliptikoetan oinarritutako SSL/TLS ziurtagirietara pasatzeko, eta konfiantzazko biltegiak berriro eguneratu beharra murriztuko da.



CA erro hori instalatzeak ez du esan nahi TicketBAI zerbitzuak berehala hasiko direnik kurba eliptikoen ziurtagiriak erabiltzen. Edozein aldaketa gertatuz gero, aldez aurretik komunikatuko da.

E46 erroa konfiantzazko biltegian sartzeak ere ez du berez bermatzen kurba eliptikoen ziurtagiriekin bateragarritasuna egongo denik. Aplikazioak, sistema eragileak eta erabilitako TLS liburutegiek bateragarriak izan beharko dute dagozkien algoritmo eta kurba kriptografikoekin.

5. Aldaketaren egutegia

5.1. Kanpoko proben edo aurreprodukzioaren inguruneak

Aurreikuspena da SSL/TLS ziurtagiri berriak 2026ko urriaren 1ean instalatzea Arabako, Bizkaiko eta Gipuzkoako TicketBALren kanpoko proben edo aurreprodukzioaren inguruneetan.

Egun horretatik aurrera, enpresa garatzaileek probatu beharko dute beren aplikazioak behar bezala konektatzen direla dagozkien inguruneetara, eta egokitzat jotzen dituzten bidalketak ere egin beharko dituzte proba moduan.

Eguneraketa egin beharko da behar diren CA ziurtagiriak txertatuta, baina oraindik beharrezkoak diren beste CA ziurtagiri batzuk konfiantzazko biltegitik ezabatu gabe.

Aurreprodukzio inguruneekin HTTPS konexio bat ezartzen bada ziurtagiriaren balidazioan errorerik izan gabe, argi geratuko da aplikazioa prest dagoela ziurtapen hierarkia berriakoa.

5.2. Produkzio inguruneak

Litekeena da ziurtagiri berriak data desberdinetan instalatzea foru aldundi bakoitzaren produkzio ingurunean, lan hori 2026ko azarotik 2027ko urtarila bitartean egitea aurreikusita baitago. Nolanahi ere, foru aldundi bakoitzaren egoitza elektronikoan horren berri emango da aldez aurretik.

6. CA ziurtagiriak deskargatzea

6.1. Aurreikusitako aldaketarako beharrezkoa den ziurtagiria

- **CA erroa → Sectigo Public Server Authentication Root R46:**
https://www.izenpe.eus/contenidos/informacion/descargas_tecnica/es_def/adjuntos/SECTIGO/SectigoPublicServerAuthenticationRootR46_ROOT.crt.cer

Aplikazioek konfiantza izan behar dute Sectigo Public Server Authentication Root R46 CA erroan. Dagokien ziurtapen bidea eraikitzeke, zerbitzuek mendeko, bitarteko eta gurutzatutako ziurtagiriak aurkeztu beharko dituzte.

6.2. Etorkizunean kurba eliptikoetara pasatzeko gomendatutako ziurtagiria

- **CA erroa →, Sectigo Public Server Authentication Root E46:**
https://www.izenpe.eus/contenidos/informacion/descargas_tecnica/es_def/adjuntos/SECTIGO/SectigoPublicServerAuthenticationRootE46_ROOT.crt.cer

CA erro hau instalatzea prebentzio neurri bat da, eta ez da TicketBAI zerbitzuek hasieran aurkeztuko duten RSA katearen parte.

7. Laguntza eta gorabeheren komunikazioa

Zalantzak edo gorabeherak agertuz gero, proba edo bidalketa zein zerbitzuekin egiten den eta hari dagokion aldundiari komunikatu beharko zaizkio.

Enpresa berak lurralde batean baino gehiagotan jardun dezake. Kasu horretan, gorabehera zein lurraldetako zerbitzuan gertatu den, eta lurralde horretako harremanetarako gunera jo beharko da.



	Araba	Bizkaia	Gipuzkoa
	945 18 15 30	946 083 566	943 113 000
	egoitza.sede@araba.eus	programak@bizkaia.eus	ticketbaikontsultak@gipuzkoa.eus

Gorabeheren berri ematean, informazio hau adierazi beharko da: software lizentzia eta bertsioa, eragindako ingurunea, zerbitzuaren URLa, probaren data eta ordua, eta errore mezu osoa.

8. Mantentze lanetarako gomendio orokorra

Segurtasun jardunbide egoki orokor gisa, gomendatzen da aplikazioek erabiltzen dituzten konfiantzazko biltegiak edo edukiontziak eguneratuta izatea. Biltegi propioak erabiltzen direnean, aldian-aldian berrikusi behar da beharrezkoak diren konfiantzazko CAk sartuta daudela, sistema eragile eta plataforma nagusiek mantentzen dituzten biltegiak erreferentzia hartuta.

Era berean, gomendatzen da konexio seguruak ezartzeko eta balidatzeko erabiltzen diren liburutegi kriptografikoak eta TLS osagaiak eguneratuta edukitzea.

Neurri hauek erraztu egiten dute konfiantzazko ziurtapen agintaritza berriak sartzeari, eta baliagarriak gertatzen dira gorabeheren arriskua murrizteko, zerbitzu elektronikoen erabiltzen dituzten ziurtapen hierarkietan aldaketak sartzen direnean.