III. ERANSKINA[1]

TICKETBAI SOFTWAREAREKIN EGINDAKO ERAGIKETAREN ALTA- ETA BALIOGABETZE- FITXATEGIEN SINADURA ELEKTRONIKOAREN ZEHAZTAPENAK

1. Xedea.

Dokumentu honek ezartzen ditu TicketBAI softwarearekin egindako eragiketaren alta- eta baliogabetze-fitxategien sinadura elektronikoaren zehaztapenak (aurrerantzean, sinatzeko zehaztapenak) TicketBAI betebeharra erregulatzen duen araudiak aipatzen duena.

Sinadura elektronikoaren zehaztapenak identifikatzaile bakar batekin identifikatuko dira: https://www.gipuzkoa.eus/ticketbai/sinadura.

Identifikazio hori nahitaez sartu beharko da TicketBAI softwarearekin egindako eragiketaren alta- eta baliogabetze-fitxategien sinadura elektronikoan, eta dagokion identifikazio-eremua erabiliko da espezifikazioen esparru orokorra zehazteko, bai eta hura baliozkotzeko aplikatu beharreko baldintza orokor eta espezifikoak dituen bertsioa ere.

2. Irismena.

2. 1. Jarduleak.

Sinadura elektronikoa sortzeko eta baliozkotzeko prozesuko jarduleak honako hauek dira:

– Sinatzailea: nortasun juridikorik gabeko pertsona fisikoa edo juridikoa, sinadura sortzeko gailu bat duena eta TicketBAI softwarearekin alta emateko edo eragiketa baliogabetzeko fitxategi bat sinatzen duena.

– Egiaztatzailea: sinadura elektroniko bat baliozkotzen edo egiaztatzen duen erakundea, pertsona fisikoa zein juridikoa izan, sinadura zehatzaren zehaztapen batzuek eskatzen dituzten baldintzetan oinarrituta.

– Konfiantzazko zerbitzuen emailea: ziurtagiri elektronikoak ematen dituen edo sinadura elektronikoarekin lotutako beste zerbitzu batzuk ematen dituen pertsona fisikoa edo juridikoa.

– Sinadura-zehaztapenen igorlea: dokumentu hau sortzeaz eta kudeatzeaz arduratzen den erakundea; horren bidez, sinatzaileak eta egiaztatzaileak hori bete dute sinadura elektronikoa sortzeko eta baliozkotzeko prozesuetan.

2. 2. Sinadura elektronikorako onartutako formatua

TicketBAI softwarearekin egindako eragiketaren altako eta baliogabetzeko fitxategien sinadura elektronikorako onartutako formatua FormatoXAdes (XML AdvancedElectronicSignatures) da, ETSI en 319 132-1 V1.1.1, ETSI TS 103 171 V2.1.1 eta ETSI TS 101 903 V1.4.2 zehaztapen teknikoen arabera. Estandarraren

[1] Eranskin hau urtarrilaren 18ko 16/2022 Foru Aginduaren azken xedapenetako lehenaren bi apartauak aldatu du. Aipatutako foru aginduak TicketBAI fitxategiak zuzentzeko zerbitzuen beharkizunak, prozedura eta zehaztapen tekniko eta funtzionalak arautzen ditu. Foru agindua Gipuzkoako Aldizkari Ofizialean argitaratu ondorengo egunean jartzen da indarrean (2022/01/24ko GAO), eta 2022ko urtarrilaren 1etik aurrera sortzen ditu ondorioak.

ondorengo bertsioetarako, sintaxiaren aldaketak aztertuko dira, eta profila estandarraren bertsio berrira egokitzea onartuko da, eranskin hau aldatuz.

Sinaduraren zehaztapen horietan, ds: eta xades: aurrizkiak erabiliko dira XMLDSig eta XAdES estandarretan definitutako elementuei erreferentzia egiteko, hurrenez hurren.

XAdES formatuan hainbat mota daude; sinadura oinarrizko mota sortzeko prestatu behar da gutxienez, sinadura-zehaztapenei buruzko informazioa gehituz (EPES mota).

2. 3. Sinadura elektronikoa sortzea.

Sinadura elektronikoa sortzeko dagoeneko badauden liburutegi kriptografikoak edo produktuak erabiltzea komeni da.

Ez da beharrezkoa sinaduran TSA zerbitzu batek emandako denbora-zigilua txertatzea sinatzen den unean.

2. 4. Sinadura elektronikoa egiaztatzea

Egiaztatzaileak edozein metodo estandarizatu erabil dezake eranskin honen arabera sortutako sinadura egiaztatzeko. Sinadura bat baliozkotzeko honako baldintza hauek bete behar dira gutxienez:

1. Sinaduraren osotasunaren baliozkotasuna bermatu behar da.

2. Sinadura egiten denean ziurtagiriak baliozkoak izan behar dira.

3. Sinatzaile-ziurtagiria gordailu publiko batean baliagarri dagoen ziurtapen-praktiken deklarazio jakin baten arabera egin behar da.

4. Ziurtagiri sinatzailearen jaulkitzaileak konfiantza- zerbitzu kualifikatuen emaileen zerrendan egon beharko du (QTSP). Zerrenda hori hemen dago eskuragarri: https://webgate.ec.europa.eu/tl- browser/#/

2. 5. Sinatzeko zehaztapenak kudeatzea

Gipuzkoako Foru Aldundiari dagokio sinatzeko zehaztapenak mantentzea, eguneratzea, argitaratzea eta zabaltzea.

Zehaztapen horien eguneratzeak Bizkaiko Aldizkari Ofizialean eta esteka honetan argitaratuko dira: https://www.gipuzkoa.eus/ticketbai/sinadura

3. Sinadura elektronikoa baliozkotzea.

Atal honetan, sinadura elektronikoa sortzeko prozesuan sinatzaileak eta sinadura elektronikoa baliozkotzeko prozesuan egiaztatzaileak kontuan hartu beharko dituzten baldintzak zehazten dira.

3. 1. Indarraldia.

Sinadura-zehaztapen horiek baliozkoak dira argitaratzen direnetik bertsio eguneratu berri bat argitaratzen den arte, eta aldi baterako epe bat eman daiteke, bi bertsioak elkarrekin bizi izan daitezen, tartean dauden eragileen plataformak bertsio berriaren zehaztapenetara egokitu ahal izateko. Bertsio berrian aldi horren iraupena zehaztu beharko da; amaitutakoan bertsio eguneratua baino ez da izango baliozkoa.

3. 2. Arau komunak.

Sinadura elektronikoan, sinatzailean eta egiaztatzailean parte hartzen duten eragileentzako arau komunak nahitaezko eremua dira, eta sinaduraren zehaztapen guztietan agertu behar dute. Arau horiei esker, sinadura elektronikoa sortzen duen

pertsona edo erakundearen eta sinadura hori egiaztatzen duen pertsona edo erakundearen gaineko erantzukizunak ezar daitezke, aurkeztu beharreko gutxieneko baldintzak zehaztuta, betiere izenpetuta sinatzailearentzako baldintzak badira, edo ez izenpetuta, egiaztatzailearentzako baldintzak badira.

3. 3. Sinatzaileak bete beharreko arauak.

Sinatzaileak bere gain hartuko du sinatu beharreko fitxategian sinaduraren emaitza denboran zehar alda dezakeen eduki dinamikorik ez egotearen ardura. Sinatu beharreko fitxategia sinatzaileak sortu ez badu, pertsona horrek ziurtatu beharko du fitxategiaren barruan ez dagoela eduki dinamikorik (makroak, adibidez).

XAdES formatua: XAdESenveloped sinadurak bakarrik onartuko dira. XAdESenveloping eta XAdESdettached sinadurak ez dira onartuko.

Sinatzaileak, gutxienez, SignedProperties eremuko etiketa hauetan jasotako informazioa eman beharko du (eremu horretan, XMLDsig sinadura sortzeko orduan batera sinatutako propietate batzuk daude); horiek nahitaezkoak dira:

– SigningTime: sinatzaileak sinadura-prozesua noiz egin zuen zehazten du.

– SigningCertificatev2 edo SigningCertificate[2]: ziurtagiri bakoitzean erabilitako segurtasun- algoritmoen eta ziurtagirien erreferentziak jasotzen ditu. Elementu hori sinatu egin beharko da, ziurtagiria ordezteko aukerarik egon ez dadin.

– SignaturePolicyIdentifier: sinadura elektronikoa sortzeko prozesuaren oinarri diren sinadura- zehaztapenak identifikatzen ditu, eta honako eduki hauek izan behar ditu azpibanatzen den elementuetan:

a) Sinadura-zehaztapenen dokumentu honen erreferentzia esplizitua, xades elementuan: SigPolicyId. Horretarako, sinaduraren zehaztapenen bertsio zehatza identifikatzen duen OIDa edo haren kokapenaren URLa agertuko da.

b) Dagokion sinadura-zehaztapenen dokumentuaren aztarna digitala eta erabilitako algoritmoa, <xades: SigPolicyHash> elementuan; horrela, egiaztatzaileak egiaztatu ahal izango du, balio hori kalkulatuz, sinadura hura baliozkotzeko erabiliko diren sinadura- zehaztapenen arabera sortu dela.

SignedProperties eremuan ezar daitezkeen gainerako eremuak aukerakoak dira:

– SignatureProductionPlacev2 edo SignatureProductionPlace[3]: dokumentua sinatu den leku geografikoa definitzen du.

– SignerRolev2 edo SignerRole[4]: pertsonak sinadura elektronikoan duen rola definitzen du. Erabiltzen bada, balio hauetako bat eduki beharko du ClaimedRoles eremuan:

a) "Supplier" edo "igorlea": jaulkitzaileak sinatzen duenean.

b) “customer” edo “hartzailea”: sinadura hartzaileak egiten duenean.

c) "Thirdparty" edo "hirugarrena": jaulkitzailea edo hartzailea ez den beste pertsona edo erakunde batek sinatzen duenean.

[2] SigningCertificateV2 - ETSI EN 319132 , SigningCertificate - ETSI TS 101 903, ETSI TS 103 171

[3] SignatureProductionPlaceV2 - ETSI EN 319 132 , SignatureProductionPlace - ETSI TS 101 903, ETSI TS 103 171

[4] SignerRoleV2 - ETSI EN 319 132 , SignerRole - ETSI TS 101 903, ETSI TS 103 171

– CommitmentTypeIndication: sinatzailearen ekintza definitzen du sinatutako dokumentuaren gainean (onartu, informatu, jaso, ziurtatu...).

– AllDataObjectsTimeStamp: denbora-zigilu bat du, sinadura sortu aurretik kalkulatua, ds:Reference-n dauden elementu guztien gainean.

– IndividualDataObjectsTimeStamp: denbora-zigilu bat du, sinadura sortu aurretik kalkulatua, ds:Reference delakoetan dauden elementu batzuen gainean.

CounterSignature etiketa, sinadura elektronikoaren berrespena, UnsignedProperties eremuan sar daitekeena, aukerakoa da. Hurrengo sinadurak, seriean edo paraleloan, XAdES estandarraren arabera gehituko dira (EN 319 102-1 dokumentua).

3. 4. Egiaztatzailearen arauak.

Sinadura elektroniko aurreratuaren oinarrizko formatuan ez dago baliozkotze-informaziorik, ziurtagiri sinatzaileaz gain. Egiaztatzaileak ezaugarri hauek erabili ahal izango ditu sinadura sortzeko erabili diren sinadura-zehaztapenen baldintzak betetzen direla egiaztatzeko:

– Signing Time: sinadura elektronikoak egiaztatzeko, adierazitako datan ziurtagirien egoera egiaztatzeko adierazpen gisa baino ez da erabiliko; izan ere, denbora-erreferentziak denbora-zigilu baten bidez baino ezin dira ziurtatu (batez ere bezero-gailuetako sinaduren kasuan).

– SigningCertificatev2 edo SigningCertificate: SigningCertificatev2 edo SigningCertificate: ziurtagiriaren (eta, hala badagokio, ziurtapen- katearen) egoera egiaztatzeko eta egiaztatzeko erabiliko da, sinadura sortzen den egunean, baldin eta ziurtagiria iraungi ez bada eta egiaztapen-datuak (CRL, OCSP) eskuratu badaitezke edo PSCk ziurtagiriaren egoera historikoki baliozkotzeko zerbitzu bat eskaintzen badu.

– SignaturePolicyIdentifier: egiaztatu beharko da sinadura sortzeko erabili diren sinadura- zehaztapenak bat datozela zerbitzu horretarako erabili behar denarekin.

Badago itxarote-aldi bat (zuhurtasun-aldia edo graziazko aldia esaten zaiona), ziurtagiria ezeztatu denez egiaztatzeko erabil daitekeena. Egiaztatzaileak denbora hori itxaron dezake sinadura baliozkotzeko edo une berean egin eta gero berriro baliozkotzeko. Izan ere, baliteke atzerapen txiki bat egotea sinatzaileak ziurtagiri bat baliogabetzen duenetik ziurtagiriaren baliogabetze-egoerari buruzko informazioa dagozkion informazio-puntuetara banatzen den arte. Gomendatzen da aldiaren iraupena, sinadura egiten denetik, CRLak erabat freskatu arte gehienez igaro daitekeen denbora izatea, gutxienez, edo OCSP zerbitzuan ziurtagiriaren egoera eguneratzeko behar den denbora, bestela. Aldi horiek ziurtapen-zerbitzua egiten duenaren araberakoak izaten dira.

3. 5. Algoritmoak erabiltzeko arauak.

ETSI TS 119 312 V1.3.1 zehaztapenean onartzen diren RSA sisteman oinarritutako algoritmo guztiak erabil daitezke. Gutxieneko ezaugarriak:

– Gakoaren tamaina 1024tik gorakoa izan behar da.

– SHA256 edo bertsio berriagoa.

4. TicketBAI softwarearen arkitekturatik eratorritako betekizunak

4. 1. Onartzen diren ziurtagiriak.

TicketBAI softwareak honako ziurtagiri hauetakoren bat erabili beharko du TicketBAI softwarearekin egindako eragiketaren alta- eta baliogabetze- fitxategiak elektronikoki sinatzeko:

– Gailuaren ziurtagiria, fakturazio-gailu bakoitzerako identitate bakarra ematen duena, instalatuta eta fakturak jaulkitzen diren gailuari lotuta.

– Pertsona fisikoaren edo erakundearen ordezkariaren ziurtagiria, pertsona fisikoaren edo juridikoaren nortasuna egiaztatzeko aukera ematen duena, hurrenez hurren.

– Enpresa-zigilua. Ziurtagiri teknikoa da, eta TicketBAI software batek edo sail edo lantalde bateko pertsona- talde batek erabil dezake. Ziurtagiri hau enpresek lanerako erabili ohi duten kautxuzko zigiluaren antzekoa da.

– Autonomoaren ziurtagiria: kualifikatu gabeko ziurtagiria, Pertsona Fisikoen errentaren gaineko zergari buruzko Foru Arauaren arabera ekonomia- jarduerak egiten dituzten pertsona fisikoentzat igortzen dena. Ziurtagiriaren igorpenerako pertsona fisikoak baldintza hori akreditatu beharko du.

4. 2. Sinaduraren murrizketak arkitekturaren arabera.

4. 2. 1. Bezero-sinaduradun arkitekturak.

Bezeroan sinadura duen arkitekturatzat hartzen da sinadura egiten duen TicketBAI softwarea fakturazio- gailuan bertan dagoenean, bertara sartzen denetik. Esaterako, aplikazioa idazmahaian.

Sinatzeko urruneko beste gailu batean sartu behar bada, arkitektura zerbitzari-sinaduraduna da.

Honelako arkitekturetan ziurtagiriek ez dute murrizketarik. Hauek erabil daitezke sinatzeko: gailuaren ziurtagiria, pertsona fisikoaren ziurtagiria, erakundearen ordezkariaren ziurtagiria, enpresa- zigilua edo autonomoaren ziurtagiria.

4. 2. 2. Zerbitzari-sinaduradun arkitekturak.

Zerbitzari-sinadura duen arkitekturatzat hartzen da sinadura egiten duen TicketBAI softwarea bertara sartzeko erabiltzen den fakturazio-gailuaz bestelako gailu batean kokatuta dagoenean. Beraz, bezeroa fakturatzeko gailua urrunetik sartzen da beste gailu batera sinadura egiteko.

Gainera, fakturak egiteko prozesua inoren ikuskapenik gabe egiten bada (batch), arkitektura zerbitzari-sinaduraduna da.

Hauek erabil daitezke sinatzeko: pertsona fisikoaren ziurtagiria, erakundearen ordezkariaren ziurtagiria, enpresa-zigilua, autonomoaren ziurtagiria edo gailuaren ziurtagiria.

Hirugarrenei edo hartzaileei fakturazioa egiten dieten enpresen kasuan ezin izango da zerbitzariko gailuaren ziurtagiria erabili.

4. 2. 3. Bezero-sinadura eta zerbitzari-sinadura erabil daitezkeen arkitekturak.

Arkitektura banatuetan sinadura bezeroan zein zerbitzarian egin daiteke, kasuan kasuko murrizketak kontuan edukiz.

Esaterako, web aplikazioetan:

– Aplikaziora sartzeko nabigatzaileak instalatuta duen gailuan egingo litzateke sinadura bezeroan, eta sinadura duten arkitekturen murrizketak aplikatuko lirateke.

– Zerbitzariko sinadura nabigatzailea sartzen den urrutiko zerbitzarian egingo litzateke, eta kasu horretan zerbitzariko sinadura duten arkitekturen murrizketak aplikatuko lirateke.

Arkitektura batek ezin du eman aukera aldi berean bezero-sinadurak eta zerbitzari-sinadurak egiteko. Baliagarri dauden arkitekturetako bat hautatu behar da.

5. Elkarrekikotasun-klausula.

Elkarrekikotasun gisa, eranskin honetan jasotako sinadura elektronikoko zehaztapenak betetzat joko dira zergadunek Arabako Foru Aldundiak edo Bizkaiako Foru Aldundiak ondorio horietarako ezarritako zehaztapenak betetzen dituztenean.