III. ERANSKINA

TICKETBAI FITXATEGIEN SINADURA ELEKTRONIKOA EGITEKO ZEHAZTAPENAK.

1. Helburua

Eranskin honetan TicketBAI fitxategien sinadura elektronikoa egiteko zehaztapenak (aurrerantzean, sinaduraren zehaztapenak) ezartzen dira, foru arau honetako 5. Artikuluan aipatua.

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

Identifikazio hori TicketBAI fitxategietako sinadura elektronikoan barneratu beharko da derrigorrez, zehaztapenen esparru orokorra eta bertsioa zehazteko identifikazioko dagokion eremua erabiliz baliozkotzeko aplikazioaren baldintza orokor eta espezifikoekin.

2. Irismena.

2.1. Nahasitako aktoreak.

Sinadura elektroniko bat sortu eta baliozkotzeko prozesuan nahasitako agenteak dira:

- Sinatzailea: sinadura sortzeko gailu bat duen eta TicketBAI fitxategi bat sinatzen duen pertsona fisiko edo juridikoa edo izaera juridikorik gabeko erakundea.

- Egiaztatzailea: Sinadurarako zehaztapen jakin batzuetan eskatzen diren baldintzei jarraiki sinadura elektroniko bat baliozkotu edo egiaztatzen duen erakundea, izan pertsona fisikoa zein juridikoa.

- Konfiantzazko zerbitzuen mailegatzailea: ziurtagiri elektronikoak igorri edo sinadura elektronikoarekin lotuta bestelako zerbitzuak ematen dituen pertsona fisiko edo juridikoa.

- Sinaduraren zehaztapenen jaulkitzailea: Sinadura elektronikoa sortu eta baliozkotzeko prozesuetan sinatzailea eta egiaztatzaileak jarraitu behar duen dokumentu hau sortu eta kudeatzeaz arduratzen den erakundea.

2.2. Sinadura elektronikorako onartutako formatua.

TicketBAI fitxategietako sinadura elektronikoetarako onartutako formatua XAdES (XML AdvancedElectronicSignatures) Formatua 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 osteko bertsioetarako sintaxiko aldaketak aztertuko dira eta profila estandarren bertsio berrirako egokitzea onartuko da eranskin hau aldatuz.

Sinaduraren zehaztapen hauetan zehar ds: eta xades: aurrizkiak erabiliko dira, hurrenez hurren, XMLDSig eta XAdES estandarretan zehaztutako elementuak aipatzeko.

Formatu mota ezberdinen barnean XAdES egokitu egin beharko da, gutxienez, oinarrizko klasea sortzeko, sinaduraren zehaztapenari buruzko informazioa gaineratuz, EPES klasea.

2.3. Sinadura elektronikoa sortzea

Sinadura elektronikoa sortzerakoan liburutegi kriptografikoak edo aurretiaz dauden produktuak erabiltzea komeni da.

Ez da ezinbestekoa sinatzen den unean TSA-ren zerbitzuek emandako Denbora Zigilua edo TimeStamping delakoa barneratzea sinaduran.

2.4. Sinadura elektronikoa egiaztatzea.

Egiaztatzaileak edozein metodo estandarizatu erabil dezake eranskin honen arabera sortutako sinadura egiaztatzeko. Hauek izango dira sinadura baliozkotzeko bete beharko diren gutxieneko baldintzak:

1. Sinadura osoaren baliozkotasunaren bermea.

2. Sinadura egin zen uneko ziurtagiriak baliozkotzea.

3. Ziurtapen espezifikoko Jardunaren Deklarazio baren arabera igorritako ziurtagiri sinatzailea, gordailu publiko batean eskuragarri.

4. Ziurtagiri sinatzailearen jaulkitzailea Konfiantzazko Zerbitzu Emaile Kualifikatuen (QTSP) zerrendan egon beharko da. Zerrenda hori eskuragarri dago hemen: https://webgate.ec.europa.eu/tl-browser/#/.

2.5. Sinadurarako zehaztapenak kudeatzea

Sinaduraren zehaztapenak mantendu, eguneratu, argitaratu eta dibulgatzearen ardura Gipuzkoako Foru Aldundiarena izango da.

Zehaztapen hauen eguneraketak Gipuzkoako Aldizkari Ofizialean eta hurrengo estekan argitaratuko dira: https://www.gipuzkoa.eus/ticketbai/sinadura.

3. Sinadura elektronikoa baliozkotzeko politika.

Atal honetan sinatzaileak sinadura elektronikoa sortzeko prozesuan eta egiaztatzaileak sinadura elektronikoa baliozkotzeko prozesuan aintzat hartzeko baldintzak zehaztuko dira.

3.1. Balio-epea.

Sinaduraren zehaztapen hauek baliozkoak dira argitaratzen direnetik eguneratutako bertsio berri bat argitaratu bitartean. Bitarteko denbora bat eman daiteke nahasitako aktoreen plataforma ezberdinak bertsio berriaren zehaztapenetara egokitzeko, eta denbora horretan bi bertsioak izango dira baliozkoak. Bitarteko denbora hori bertsio berrian hasi beharko da eta denbora hori igaro ostean eguneratutako bertsioa izango da soilik baliozkoa.

3.2. Ohiko arauak.

Sinadura elektronikoan nahasitako aktoreentzako, sinatzaileentzako eta egiaztatzailearentzako, ohiko arauak derrigorrez betetzeko eremua dira, sinaduraren zehaztapen guztietan agertu behar dena. Arau hauei esker sinadura sortzen duen pertsona edo erakundeari eta egiaztatzen duen pertsona edo erakundeari buruz sinadura elektronikoaren inguruko erantzukizunak ezar daitezke, bete behar diren gutxienezko betekizunak zehaztuz, sinatuta egon beharko direlarik, sinatzailearentzako betekizunak baldin badira, edo sinatu gabe, egiaztatzailearentzako betekizunak baldin badira.

3.3. Sinatzailearen arauak.

Sinatzailea arduratuko da sinatzeko TicketBAI fitxategian denboran zehar sinaduraren emaitza alda dezakeen eduki dinamikorik barnera ez dadin. Sinatzeko TicketBAI fitxategia ez baldin badu sinatzaileak sortu, pertsona horrek TicketBAI fitxategiaren barnean eduki dinamikorik ez dagoela ziurtatu beharko du (makroak esate baterako).

XAdES formatua: XAdESenveloped sinadurak onartuko dira esklusiboki. Ez da XAdESenveloping onartuko, ezta XAdESdettached ere.

Sinatzaileak, gutxienez, SignedProperties eremuaren barnean etiketa hauetan jasotzen den informazioa eman beharko du (eremu horretan XMLDsig sinadura sortzean elkarrekin sinatutako zenbait propietate barneratzen dira), derrigorrezkoak direnak:

- SigningTime: sinatzaileak sinaduraren prozesuan egin zuen unea zehazten du.

- SigningCertificatev2 edo SigningCertificate[1]: ziurtagiri bakoitzean erabilitako segurtasunezko ziurtagiri eta algoritmoen erreferentziak barneratzen dira. Elementu hori sinatu egin beharko da, ziurtagiria aldatzeko aukera ekidite aldera.

- SignaturePolicyIdentifier: sinadura elektroniko sortzeko prozesuak oinarritzat dituen sinaduraren zehaztapenak identifikatzen ditu, eta hura azpi banatzen den elementuetan eduki hauek barneratu behar dira:

a) Sinaduraren zehaztapeneko dokumentu honen erreferentzia esplizitua, xades:SigPolicyId elementuan. Horretarako, OID agertuko da, sinaduraren zehaztapenen bertsio zehatza identifikatzekoa, edo haren lokalizaziorako URL kodea.

b) Dagokion sinaduraren zehaztapenen dokumentuaren aztarna digitala eta erabilitako algoritmoa, <xades:SigPolicyHash> elementuan. Horrela, egiaztatzaileak aukera izan dezan, aldi berean, balio hori kalkulatuz, sinadura hura baliozkotzeko erabiliko diren sinaduraren zehaztapen berdinen arabera sortua dagoela egiaztatzeko.

SignedProperties eremuan gainera daitezkeen gainerako etiketak aukerakotzat hartuko dira:

- SignatureProductionPlacev2 edo SignatureProductionPlace[2]: dokumentuaren sinadura zein leku geografikotan egin den zehaztekoa.

- SignerRolev2 o SignerRole[3]: sinadura elektronikoan pertsonaren rola zehaztekoa. Hura erabiliz gero, balio hauetakoren bat adierazi beharko da ClaimedRoles eremuan:

a) “Supplier” edo “jaulkitzaile”: sinadura jaulkitzaileak egiten duenean.

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

d) “Thirdparty” edo “hirugarrena”: sinadura jaulkitzailea edo hartzailea ez den pertsona edo erakunde batek egiten duenean.

- CommitmentTypeIndication: sinatzaileak sinatutako dokumentuaren gainean egindako ekintza zehaztekoa (onartu egiten du, informatu, jaso, ziurtatu…).

- AllDataObjectsTimeStamp: denboraren zigilu bat barneratzen du, sinadura sortu aurretik kalkulatua, ds:Reference barneko elementu guztiei buruz.

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

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

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

- IndividualDataObjectsTimeStamp: denboraren zigilu bat barneratzen du, sinadura sortu aurretik kalkulatua, ds:Reference barneko elementu batzuei buruz.

CounterSignature etiketa, sinadura elektronikoaren berrespena eta UnsignedProperties eremuan sar daitekeena, aukerakotzat joko da. Hurrengo sinadurak, seriean edo paraleloan, XAdES estandarrean adierazten denari jarraiki gaineratuko dira, EN 319 102-1 dokumentuaren arabera.

3.4. Egiaztatzailearen arauak.

Sinadura elektroniko aurreratuaren oinarrizko formatuak ez du baliozkotze-informaziorik gaineratzen, ziurtagiri sinatzailetik harago. Hauek dira egiaztatzaileak sinadura sortzeko baliatutako sinaduraren zehaztapenaren betekizunak betetzen direla egiaztatzeko erabili ahalko dituen atributuak:

- Signing Time: soilik sinadura elektronikoak egiaztatzeko erabiliko da ziurtagiriek adierazitako datan zein egoeran dauden egiaztatzeko adierazle modura, izan ere, denboraren erreferentziak denboraren zigilu batekin soilik ziurta daitezke (bezero gailuetan egindako sinaduren kasuan bereziki).

- SigningCertificatev2 edo SigningCertificate:ziurtagiriak (eta, hala badagokio, ziurtagiri kateak) sinadura sortutako datan zein egoera zuen egiaztatu eta berresteko erabiliko da, baldin eta ziurtagiria iraungi ez baldin bada eta egiaztapen-datuak eskura badaitezke (CRL, OCSP) edo, bestela, PSC delakoan ziurtagiriaren egoeraren baliozkotze zerbitzu historiko bat eskaintzen baldin badu.

- SignaturePolicyIdentifier: sinadura sortzeko erabilitako sinaduraren zehaztapenak aipagai den zerbitzurako erabili behar denarekin bat datozen egiaztatu beharko da.

Itxarote-denbora bat dago, zuhurtzia edo grazia epe izenez ezaguna, ziurtagiri baten ezeztatze-egoera egiaztatzeko. Egiaztatzailea denbora horretan zehar zain egon daiteke sinadura baliozkotzeko edo une berean egin eta ondoren berriro baliozkotzeko. Hori horrela da sinatzaileak ziurtagiri baten ezeztapena hasten duenetik ziurtagiriaren ezeztatze-egoerari buruzko informazioa dagozkion informazio-puntuetara hedatzen den arte atzerapen labur bat egon daitekeelako. Denbora hori, sinadura egiten den unetik, CRL-ak osorik eguneratzeko baimendutako gehienezko denbora izatea edo ziurtagiriaren egoera OCSP zerbitzuan eguneratzeko gehienezko denborarekin bat etortzea gomendatzen da, gutxienez. Denbora horiek aldatu egin daitezke Ziurtagiri Zerbitzuaren Emailearen arabera.

3.5. Algoritmoak erabiltzeko arauak.

ETSI TS 119 312 V1.3.1. Zehaztapen teknikoan onartutako eta RSA izenekoan oinarritutako edozein algoritmo erabili ahalko da. Gutxienez eskatzen dena:

- Gakoaren tamaina 1024 baino handiagoa izango da derrigor.

- SHA256 edo ondorengoko bertsioak.

4. TicketBAI softwarearen arkitekturatik eratorritako betekizunak.

4.1. Baimendutako ziurtagiriak.

TicketBAI softwareak ziurtagiri hauetakoren bat erabili beharko du TicketBAI fitxategietako sinadura elektronikoetarako:

- Gailuaren ziurtagiria, fakturaziorako gailu bakoitzerako identitate bakarra ematen duena, instalatuta eta faktura edo egiaztagiriak igortzeko baliatzen den gailura lotua egonik.

- Pertsona fisikoaren edo erakundeko ordezkariaren ziurtagiria, pertsona fisikoa edo juridikoaren identitatea egiaztatzeko aukera ematen dutenak hurrenez hurren.

- Enpresaren zigilua, TicketBAI software batek laguntzarik gabe, edo laneko sail edo talde bateko kide diren pertsona multzo batek, erabil dezakeen ziurtagiri tekniko bat dena. Mundu fisikoan enpresa batek egunero erabiltzen duen kautxuzko zigilu baten ohiko erabilerarekin aldera daitekeen ziurtagiri bat da.

- Autonomoaren ziurtagiria: ziurtagiri ez kualifikatua, Pertsona Fisikoen Errentari buruzko Zergaren Foru Arauan aurreikusitakoarekin bat etorriz ekonomia jarduera bat garatzen duten pertsona fisikoentzat jaulkia. Igorri ahal izateko pertsona fisikoak inguruabar hori betetzen duela egiaztatzea eskatuko da.

4.2. Sinadura arloko murriztapenak arkitekturaren arabera

4.2.1. Bezero-sinaduradun arkitekturak.

Bezero-sinaduradun arkitekturatzat hartzen da, sinadura egiten duen TicketBAI softwarea hartara sartzeko baliatzen den fakturazioko gailuan bertan lekututa dagoenean. Esate baterako, mahaigaineko aplikazio bat

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, entitatearen ordezkariaren ziurtagiria, enpresa-zigilua edo autonomoaren ziurtagiria.

4.2.2. Zerbitzari-sinaduradun arkitekturak.

Arkitektura zerbitzari-sinaduraduntzat hartzen da, sinadura egiten duen TicketBAI softwarea hartara sartzeko baliatzen den fakturazioko gailua ez den gailu batean lekututa dagoenean. Beraz, bezeroaren fakturazio gailutik urruneko beste gailu batean sartzen da sinadura sortzeko.

Gainera, fakturak edo egiaztagiriak inolako ikuskapenik gabe igortzen baldin badira (batch), “arkitektura zerbitzari-sinaduraduna da”.

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

Kasu honetan, ezin da erabili gailuaren ziurtagiria sinatzeko.

4.2.3. Bezero-sinadura eta zerbitzari-sinadura erabiltzeko aukera ematen duten arkitekturak.

Arkitektura banatuetan sinadura bezeroan edo zerbitzarian egin daiteke, kasuan kasuko murrizketak kontuan izanik.

Esaterako, web aplikazio batean:

- Bezero-sinadura egiteko, aplikazioan sartzeko erabiltzen den nabigatzailea instalatuta duen gailua erabiltzen da. Bezero-sinaduradun arkitekturen murrizketa berak aplikatzen dira.

- Zerbitzari-sinadura nabigatzailea sartzen den urruneko zerbitzarian egingo litzateke. Kasu honetan, zerbitzari-sinaduraren arkitekturen murrizketa berak aplikatzen dira.

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

5. Elkarrekikotasun-klausula.

Elkarrekikotasunari begira, eranskin honetan barneratzen diren sinadura elektronikoko zehaztapenak bete direla ulertuko da zergadunek horri dagokionez Arabako Foru Aldundiak edo Bizkaiko Foru Aldundiak ezarrita dituzten zehaztapenak betetzen dituztenean.