TICKETBAI FITXATEGIEN SINADURA ELEKTRONIKOAREN ZEHAZTAPENAK

1. Helburua.

Eranskin honetan TicketBAI fitxategien sinadura elektronikoa egiteko zehaztapenak (aurrerantzean, sinaduraren zehaztapenak) ezartzen dira.
Sinadura elektronikoaren zehaztapenak identifikatzaile bakar honekin identifikatuko dira: https://ticketbai.araba.eus/tbai/sinadura/
Identifikazio hori nahitaez sartu behar da TicketBAI fitxategien sinadura elektronikoan.
Horretarako zehaztapenen esparru orokorra eta bertsioa adierazteko eremua erabili behar da, baliozkotzeko baldintza orokorrak eta bereziak aplikatuz.

2. Irismena.

2.1 Eragileak.

Sinadura elektronikoa sortzeko eta baliozkotzeko prozesuan honako eragile hauek aritzen dira:

- Sinatzailea: sinadura sortzeko gailua daukan pertsona fisikoa edo juridikoa edo nortasun juridikorik gabeko erakundea, TicketBAI fitxategi bat sinatzen duena.
- Egiaztatzailea: sinadurara zehaztapen jakin batzuetan eskatzen diren baldintzen arabera sinadura elektroniko bat baliozkotzen edo egiaztatzen duen erakundea (pertsona fisikoa zein juridikoa).
- Konfiantzazko zerbitzugilea: ziurtagiri elektronikoak ematen dituen edo sinadura elektronikoaren inguruko beste zerbitzuren bat egiten duen pertsona fisikoa edo juridikoa.
- Sinadura zehaztapenak ematen dituena: dokumentu hau, sinatzaileak eta egiaztatzaileak sinadura elektronikoak sortzeko eta baliozkotzeko prozeduretan erabili beharrekoa, sortzen eta kudeatzen duen erakundea.

2.2. Sinadura elektronikorako onartutako formatua.

TicketBAI fitxategien sinadura elektronikorako onartutako formatua honako hau da: XAdES (XML AdvancedElectronicSignatures), 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 hurrengo bertsioetarako, sintaxian egindako aldaketak aztertuko dira eta profila estandarren bertsio berrira egokitzea onartuko da eranskin hau aldatuz.
Zehaztapen hauetan ds: aurrizkia erabiliko da XMLDSig estandarrean zehaztutako elementuak aipatzeko eta xades: aurrezkia XAdES estandarrean zehaztutakoak aipatzeko.

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

2.3. Sinadura elektronikoa sortzea.

Sinadura elektronikoa sortzeko dagoeneko badauden liburutegi kriptografikoak edo produktuak erabili behar lirateke.

Ez da beharrezkoa sinatzean TSA zerbitzu batek emandako denbora-zigilua (TimeStamping) txertatzea sinaduran.

2.4. Sinadura elektronikoa egiaztatzea.
Egiaztatzaileak zeinahi metodo estandarizatu erabil dezake eranskin honekin bat etorriz sortzen diren sinadurak egiaztatzeko. Sinadura baliozkotzeko honako baldintza hauek bete behar dira gutxienez:

1. Sinaduraren osotasunaren baliozkotasuna bermatu behar da.
2. Ziurtagiriak baliozkoak izan behar dira fitxategia sinatzen denean.
3. Sinatzaile ziurtagiria gordailu publiko batean baliagarri dagoen ziurtapen praktiken berariazko adierazpen baten arabera egin behar da.
4. Sinatzaile ziurtagiria egin duena konfiantzako zerbitzugile kualifikatuen (QTSP) zerrendan egon behar da. Zerrenda hori hemen aztertu daiteke: https://webgate.ec.europa.eu/tl-browser/#/.

2.5. Sinadura zehaztapenak kudeatzea.
Sinadura zehaztapenak mantentzeko, eguneratzeko, argitaratzeko eta hedatzeko ardura Arabako Foru Aldundiak dauka.
Zehaztapen hauen eguneratzeak Arabako Aldizkari Ofizialean eta hemen argitaratuko dira: https://ticketbai.araba.eus/tbai/sinadura/

3. Sinadura elektronikoa baliozkotzeko politika.
Atal honetan zehaztuko da zer hartu behar duen kontuan sinatzaileak sinadura elektronikoa sortzeko eta zer hartu behar duen kontuan egiaztatzaileak sinadura elektronikoa baliozkotzeko.

3.1. Indarraldia.
Sinadura zehaztapen hauek indarrean egongo dira argitaratzen direnetik eguneratutako bertsio berria argitaratu arte. Bertsio eguneratua argitaratuz gero, aldi batez bi bertsioak erabili ahal izango dira; horrela, jarduleek beren plataformak bertsio berriaren zehaztapenetara moldatu ahal izango dituzte. Trantsizioaldi horren iraupena bertsio berrian adierazi beharko da. Hori amaitutakoan bertsio eguneratua soilik erabili ahal izango da.

3.2. Arau orokorrak.
Sinadura elektronikoan aritzen diren eragileek (sinatzaileek eta egiaztatzaileek) bete beharreko arau orokorrak sinadura zehaztapen guztietan agertu beharreko nahitaezko eremu batean biltzen dira. Arau horien bidez sinadura sortzen duen pertsonak edo erakundeak eta hura egiaztatzen duen pertsonak edo erakundeak sinadura elektronikoaren inguruan dituzten erantzukizunak ezar daitezke. Hain zuzen ere, arauetan ezartzen da zer bete behar duten gutxienez batak eta besteak (sinatzailearenak sinatuta egon behar dira; egiaztatzailearenak ez).

3.3. Sinatzaileak bete beharreko arauak.
Sinatzaileak egiaztatu behar du sinatu beharreko TicketBAI fitxategian ez dagoela denbora pasatu ahala sinaduraren emaitza aldatu dezakeen eduki dinamikorik. Sinatu beharreko

TicketBAI fitxategia sinatzaileak berak sortu ez badu, egiaztatu behar du haren barruan ez dagoela inolako eduki dinamikorik (makroak, esate baterako).

XAdES formatua: XAdESenveloped sinadurak baino ez dira onartuko. XAdESenveloping eta XAdESdettached sinadurak ez dira onartuko.
Sinatzaileak gutxienez honako etiketa hauetako informazioa eman behar du SignedProperties eremuan (eremu honetako propietateak batera sinatzen dira XMLDsig sinadura sortzean; propietateak nahitaezkoak dira):

- SigningTime: sinatzaileak noiz egin duen sinadura.
- SigningCertificatev2 edo SigningCertificate[1]: ziurtagiriak eta haietan erabilitako segurtasun algoritmoak. Elementu hau sinatu egin behar da, ziurtagiria ordezteko modurik egon ez dadin.
- SignaturePolicyIdentifier: sinadura elektronikoa sortzeko oinarritzat hartzen diren sinadura zehaztapenak identifikatzen ditu. Honen elementuetan honako datu hauek adierazi behar dira:
    - Sinadura zehaztapenen dokumentu honen berariazko aipamena, xades:SigPolicyId elementuan. Horretarako, sinadura zehaztapenen bertsioa identifikatzen duen OID agertu behar da, edo haien URL helbidea.
    - Sinadura zehaztapenen dokumentuaren aztarna digitala eta erabili den algoritmoa, <xades:SigPolicyHash> elementuan. Horri esker egiaztatzaileak balio hau kalkulatu dezake eta ziurtatu dezake sinadura sortzeko aplikatutako zehaztapenak baliozkotzeko aplikatukoak berak direla.

SignedProperties eremuan ezar daitezkeen gainerako etiketak aukerakoak dira:

- SignatureProductionPlacev2 edo SignatureProductionPlace[2]: non sinatu den dokumentua.
- SignerRolev2 edo SignerRole[3]: pertsonak sinadura elektronikoan duen rola zehazten du. Erabiliz gero, balio hauetako bat ezarri behar da ClaimedRoles eremuan:
    - “Supplier” edo “igorlea”: sinadura igorleak eginez gero.
    - “Customer” edo “hartzailea”: sinadura hartzaileak eginez gero.
    - “Thirdparty” edo “hirugarrena”: sinadura egiten duena ez bada ez igorlea ez hartzailea.
- CommitmentTypeIndication: zer egin duen sinatzaileak dokumentuarekin (onartu, berri eman, jaso, ziurtatu...).
- AllDataObjectsTimeStamp: ds:Reference elementu guztietan denbora zigilua ezartzen du, sinadura sortu aurrekoa, hain zuzen.
- IndividualDataObjectsTimeStamp: ds:Reference elementu guztietan denbora zigilua ezartzen du, sinadura sortu aurrekoa, hain zuzen.

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.

CounterSignature etiketak sinadura elektronikoa berresten du; UnsignedProperties eremuan sar daiteke eta aukerakoa da. Hurrengo sinadurak, sailan edo paraleloan, XAdES estandarrarekin bat etorriz gehituko dira (EN 319 102-1 dokumentua).

3.4. Egiaztatzaileak bete beharreko arauak.

Sinadura elektroniko aurreratuaren oinarrizko formatuan dagoen baliozkotze informazio bakarra sinatzaile ziurtagiria da. Egiaztatzaileak honako atributu hauek erabil ditzake sinadura sortzeko aplikatutako sinadura zehaztapenak betetzen direnez egiaztatzeko:

- Signing Time: sinadura elektronikoak egiaztatzean, data jakin batean ziurtagiriak nola egon diren egiaztatzeko baino ez da erabiliko; izan ere, denbora erreferentziak ziurtatzeko modu bakarra denbora zigilua da (batez ere sinadura bezero gailu baten bidez eginez gero).
- SigningCertificatev2 edo SigningCertificate: sinadura sortu denean ziurtagiria (eta, behar den kasuetan, ziurtapen katea ere bai) nola egon den egiaztatzeko erabiliko da, baldin eta iraungita ez badago eta egiaztatzeko datuak (CRL, OCSP) eskuratu ahal badira edo, bestela, ziurtapen zerbitzua egiten duenak ziurtagiriaren egoeraren historia aztertzeko aukera ematen badu.
- SignaturePolicyIdentifier: egiaztatu behar da sinadura sortzeko aplikatutako sinadura zehaztapenak bat ote datozen zerbitzu jakin baterako erabili beharrekoekin.

Aldi batez (zuhurtasun aldia edo graziazko aldia) ziurtagiria ezeztatu den ala ez egiaztatu daiteke. Hain zuzen ere, egiaztatzaileak aldi hori igaro arte itxaron dezake sinadura baliozkotzeko; bestela, sinatu ahala baliozkotu dezake eta gero berriz baliozkotu. Izan ere, baliteke zenbait denbora pasatzea sinatzailea ziurtagiri bat ezeztatzen hasten denetik ziurtagiriaren ezeztapenaren egoeraren berri behar diren informazio puntuetara heldu arte. Gomendatzen da aldi horren iraupena, sinadura egiten denetik, gutxienez CRLak erabat freskatu arte gehienez igaro daitekeen denbora izatea edo, bestela, OCSP zerbitzuan ziurtagiriaren egoera eguneratzeko behar den denbora. Denbora horiek ziurtapen zerbitzua egiten duenaren araberakoak alda litezke.

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 arkitekturaren ondoriozko baldintzak.

4.1. Onartzen diren ziurtagiriak.

TicketBAI softwareak honako ziurtagiri hauetako bat erabili behar du TicketBAI fitxategiei sinadura elektronikoa txertatzeko:

- Gailuaren ziurtagiria: gailu bakoitzari nortasun berezia ematen dio; fakturak edo ordainagiriak egiteko erabiltzen den gailuan instalatuta eta berarekin lotuta dago.
- Pertsona fisikoaren edo erakundearen ordezkariaren ziurtagiria: pertsona fisikoa edo pertsona juridikoa nor den frogatzen du.
- Enpresaren zigilua: ziurtagiri teknikoa da, TicketBAI softwareak bere kabuz erabil dezakeena, inor aurrean ez dagoela; gainera, sail edo lantalde bateko pertsona

batzuek ere erabil dezakete. Ziurtagiri hau enpresek lanerako erabili ohi duten kautxuzko zigiluaren antzekoa da.

- Autonomoaren ziurtagiria: kualifikatu gabeko ziurtagiria da. Jarduera ekonomiko bat autonomo modura egiten duten pertsona fisikoentzat egiten da, Pertsona fisikoen errentaren gaineko zergaren Foru Arauan ezartzen denarekin bat etorriz. Ziurtagiria egiteko, ezinbestekoa da pertsona fisikoak frogatzea hala ari dela lanean.

4.2 Sinaduraren murrizketak arkitekturaren arabera.

4.2.1. Bezero sinaduradun arkitekturak.

Bezero sinaduradun arkitekturetan, sinadura egiten duen TicketBAI softwarea fakturazioa egiteko erabiltzen den gailuan bertan dago. Esaterako, idazmahaiko aplikazio batean. Sinatzeko urruneko gailu batean sartu behar bada, horren arkitektura zerbitzari sinaduraduna da.
Honelako arkitekturetan ziurtagiriek ez dute murrizketarik. Honako hauek erabil daitezke sinatzeko: gailuaren ziurtagiria, pertsona fisikoaren ziurtagiria, erakundearen ordezkariaren ziurtagiria, enpresa zigilua edo autonomoaren ziurtagiria.

4.2.2. Zerbitzari sinaduradun arkitekturak.

Zerbitzari sinaduradun arkitekturetan, sinadura egiten duen TicketBAI softwarea fakturazioa egiteko erabiltzen den gailuan gabe beste batean dago. Beraz, fakturaziorako erabiltzen den bezero gailutik urruneko beste gailu batean sartzen da sinadura sortzeko.
Gainera, fakturak edo ordainagiriak egiteko prozesua inoren ikuskapenik gabe egiten bada (batch), arkitektura zerbitzari sinaduraduna da.
Honako hauek erabil daitezke sinatzeko: pertsona fisikoaren ziurtagiria, erakundearen ordezkariaren ziurtagiria, enpresa zigilua edo autonomoaren ziurtagiria.
Arkitektura hauetan ezin da erabili gailuaren ziurtagiria sinatzeko.

4.2.3. Bezero sinadura eta zerbitzari sinadura erabil daitezkeen arkitekturak.

Arkitektura banatuetan, bezero sinadura zein zerbitzari sinadura hauta daiteke, bakoitzaren murrizketak kontuan edukiz.
Esaterako, web aplikazioetan:

- Bezero sinadura aplikazioan sartzeko erabiltzen den nabigatzailea instalatuta dagoen gailuan egiten da; bezero sinaduradun arkitekturen murrizketak aplikatzen dira.
- Zerbitzari sinadura nabigatzailearen bidez sartzen den urruneko zerbitzarian egiten da; zerbitzari sinaduradun arkitekturen murrizketak aplikatzen dira.

Arkitektura batean ezin dira aldi berean egin bezero sinadurak eta zerbitzari sinadurak. Baliagarri dauden arkitekturetako bat hautatu behar da.

5. Elkarrekikotasuna.

Elkarrekikotasuna aplikatuta, eranskin honetan bildutako sinadura elektronikoari buruzko zehaztapenak betetzat joko dira zergadunek betetzen badituzte horretaz Arabako Foru Aldundiak edo Bizkaiko Foru Aldundiak ezarritako zehaztapenak.