araba.eus

Bizkaia
foru aldundia
diputación foral

Gipuzkoako
Foru Aldundia

EUSKO JAURLARITZA
GOBIERNO VASCO

TicketBAI 1.0 sinadura-politika

Bertsioaren data: 2019/12/19

AURKIBIDEA

1 SARRERA

1.1 Dokumentuaren xedea

TicketBAI sinadura-politika (hemendik aurrera, politika) Araba, Gipuzkoa eta Bizkaiko Foru Aldundiek eta Eusko Jaurlaritzak fitxategien TicketBAI sinadura elektronikoaren inguruan beren gain hartu dituzten irizpideen multzoa da.

TicketBAI fitxategien definizioa, egitura eta ezaugarri teknikoak honako dokumentu honetan biltzen dira: "TicketBAI sistemaren ezaugarri funtzionalak eta teknikoak". Laburbilduta: TicketBAI fitxategi batean egindako faktura bakar baten datuak biltzen dira XML formatuan, bai fakturaren datuak berak, bai kontroleko datuak (fakturen kateamendua, zer gailuk egin duen faktura, zer entitatek garatu duen aplikazioa, eta abar).

Sinadura-politika hau erraz irakurtzeko moduko formatu batean egon beharko da eskuragarri, sinadura elektronikoa sortzeko eta baliozkotzeko errekerimendu guztiak bete behar direnean aplikatzeko prest, alegia.

1.2 Erreferentziak

Politika hau prestatzeko honako zehaztapen tekniko hauek eduki dira kontuan:

- ETSI EN 319 132-1 V1.1.1 (2016-04) XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures.

- ETSI EN 319 132-2 V1.1.1 (2016-04) XAdES digital signatures; Part 2: Extended XAdES signatures.

- EN 319 102-1 V1.1.1 (2016-05) Procedures for Creation and Validation of AdES Digital Signatures.

- ETSI TS 119 312 V1.3.1 (2019-02) Cryptographic Suites.

Gainera, aplikatu beharreko oinarrizko arautegi hau hartu da aintzat:

- 910/2014 (EE) Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2014ko uztailaren 23koa, barne-merkatuan transakzio elektronikoak egiteko identifikazio elektronikoari eta konfiantzako zerbitzuei buruzkoa dena eta 1999/93/EE Zuzentaraua indargabetzen duena.

- 59/2003 Legea, abenduaren 19koa, sinadura elektronikoari buruzkoa.

- 2016/679 (EB) ERREGELAMENDUA, EUROPAKO PARLAMENTUAREN ETA KONTSEILUARENA, 2016ko apirilaren 27koa, datu pertsonalen tratamenduari dagokionez pertsona fisikoen babesari eta datu horien zirkulazio askeari buruzko arauak ezartzen dituena eta 95/46/EE Zuzentaraua (Datuak babesteko Erregelamendu Orokorra) indargabetzen duena.

- 3/2018 Lege Organikoa, abenduaren 5ekoa, datuak babesteko eta eskubide digitalak bermatzeko dena.

- 40/2015 Legea, urriaren 1ekoa, sektore publikoaren araubide juridikoarena.

- 56/2007 Legea, informazioaren gizarteari bultzada emateko neurriei buruzkoa.

- 3/2010 Errege Dekretua, urtarrilaren 8koa, Administrazio Elektronikoaren esparruan Segurtasun Eskema Nazionala arautzen duena.

- 4/2010 Errege Dekretua, urtarrilaren 8koa, Administrazio Elektronikoaren esparruan Elkarreragingarritasun Eskema Nazionala arautzen duena.

2 TICKETBAI SINADURA-POLITIKAREN IRISMENA

Politika honetan XML fitxategiak TicketBAI sistemaren arabera sinatzeko baldintza orokorrak zehazten dira.

Argitaratzen denetik eguneratze bat argitaratu arte izango da baliozkoa.

Sinadura-politika honek identifikatzaile bat bakarrik edukiko du: http://ticketbai.eus/politicafirma. Identifikatzaile hori nahitaez txertatu behar da sinadura elektronikoan; horretarako, esparru-politika eta bertsioa (baliozkotzeko baldintza orokorrekin eta bereziekin) identifikatzeko eremua erabili behar da.

2.1 Jarduleak

Sinadura elektronikoa sortzeko eta baliozkotzeko prozesuko jarduleak honako hauek dira:

- Sinatzailea: sinadurak sortzeko gailua daukan pertsona fisikoa edo juridikoa, edo nortasun juridikorik gabeko entitatea, TicketBAI fitxategi bat sinatzen duena.

- Egiaztatzailea: sinadura-politika jakin bateko baldintzak aplikatuz sinadura elektroniko bat baliozkotzen edo egiaztatzen duen entitatea (pertsona fisikoa zein juridikoa).

- Konfiantzako zerbitzugilea: sinadura elektronikoari dagozkion ziurtagiri elektronikoak ematen edo horren inguruko beste zerbitzuren bat egiten duen pertsona fisikoa edo juridikoa.

- Politikaren egilea: dokumentu hau, sinatzaileak eta egiaztatzaileak sinadura elektronikoak sortzeko eta baliozkotzeko prozeduretan erabili beharrekoa, sortzen eta kudeatzen duen entitatea.

2.2 Sinadurarako onartzen diren formatuak

XAdES (XML AdvancedElectronicSignatures) formatua, ETSI EN 319 132-1 V1.1.1 zehaztapen teknikoaren arabera. Estandarraz geroztiko bertsioei dagokienez, sintaxian egindako aldaketak aztertuko dira eta politikaren eranskin baten bidez profila estandar berrira moldatzea onartuko da.

Dokumentu honetan ds: aurrizkia erabiliko da XMLDSig estandarrean zehaztutako elementuak aipatzeko eta xades: aurrezkia XAdES estandarrean zehaztutakoak aipatzeko.

XAdES formatuan hainbat mota daude; sinadura oinarrizko mota sortzeko prestatu behar da gutxienez, sinadura-politikari 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 zeinahi metodo estandarizatu erabil dezake politika honekin bat etorriz sortzen diren sinadurak 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. Sinatzaile-ziurtagiria egin duena konfiantzako zerbitzugile kualifikatuen (QTSP) zerrendan egon behar da. Zerrenda hemen azter daiteke: https://webgate.ec.europa.eu/tl-browser/#/.

2.5 Sinadura-politika kudeatzea

Dokumentu hau mantentzeko, eguneratzeko, argitaratzeko eta hedatzeko ardura Araba, Gipuzkoa eta Bizkaiko Foru Aldundiek eta Eusko Jaurlaritzak daukate.

Politika honen eguneratzeak hemen argitaratuko dira: http://ticketbai.eus/politicafirma.

3 SINADURA ELEKTRONIKOA BALIOZKOTZEKO POLITIKA

Atal honetan zehaztuko da zer hartu behar duen kontuan sinatzaileak sinadura elektronikoa sortzean eta zer hartu behar duen kontuan egiaztatzaileak sinadura elektronikoa baliozkotzean.

3.1 Indarraldia

Politika hau argitaratzen denetik bertsio eguneratu berria argitaratu arte egongo da indarrean. Bertsio eguneratua argitaratu ondoren, aldi batez bi bertsioak, berria eta zaharra, onartu ahal izango dira, TicketBAI proiektuan ari diren jarduleek astia eduki dezaten plataforma guztiak bertsio berrira moldatzeko. Bertsio berrian aldi horren iraupena zehaztu beharko da; amaitutakoan bertsio eguneratua baino ez da izango baliozkoa.

3.2 Arau orokorrak

Sinadura elektronikoan esku duten jarduleek (sinatzaileek eta egiaztatzaileek) bete beharreko arau orokorrak ezinbestean agertu behar dira sinadura-politiketan. Arau horiei esker sinadura elektronikoaren inguruko erantzukizunak ezar daitezke, hau da, sinadura sortu duen pertsona edo entitatearenak eta egiaztatzen duen pertsona edo entitatearenak. Hain zuzen ere, arauek bataren eta bestearen gutxieneko betekizunak ezartzen dituzte; sinatzailearenak sinatuta egon behar dira eta egiaztatzailearenak ez.

3.3 Sinatzaileak bete beharreko arauak

Sinatzailearen ardura izango da sinatu nahi duen fitxategian ez egotea eduki dinamikorik, denbora pasatu ahala sinaduraren emaitza alda dezakeenik. Sinatu nahi duen fitxategia ez badu sinatzaileak berak sortu, aztertu egin behar du, inolako eduki dinamikorik egon ez dadin (makroak, esaterako).

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

Sinatzaileak gutxienez honako etiketa hauetako informazioa eman behar du SignedProperties eremuan (eremu honetako propietate batzuk batera sinatzen dira XMLDsig sinadura sortzean; propietateak nahitaezkoak dira):

- SigningTime: sinatzaileak noiz egin duen sinatzeko prozesua.

- SigningCertificatev2: ziurtagiriak eta beren segurtasun-algoritmoak. Elementu hau sinatu egin behar da, ziurtagiria ordezteko aukerarik ez egoteko.

- SignaturePolicyIdentifier: sinadura elektronikoa sortzeko oinarritzat hartu den sinadura-politika zehazten du; honen osagai diren elementuetan honako datu hauek adierazi behar dira:

- Sinadura-politikaren dokumentu honen aipamen zehatza, xades:SigPolicyId elementuan. Horretarako, sinadura-politikaren bertsioaren OID identifikatzailea edo hura eskuragarri dagoen orriaren URL helbidea agertu behar da.

- Sinadura-politikaren dokumentuaren aztarna digitala eta erabili den algoritmoa, <xades:SigPolicyHash> elementuan; horrela, egiaztatzaileak balio hau bere aldetik kalkulatu eta jakin dezake sinadura sortzeko aplikatutako politika baliozkotzeko aplikatuko den bera den edo ez.

SignedProperties eremuan ezar daitezkeen gainerako eremuak aukerakoak dira:

- SignatureProductionPlacev2: non sinatu den dokumentua.

- SignerRolev2: zein den pertsonaren rola sinadura elektronikoan. Erabiliz gero, honako balioetako bat jarri behar da ClaimedRoles eremuan:

  - “supplier” edo “egilea”: egileak sinatzen badu.

  - “customer” edo “hartzailea”: hartzaileak sinatzen badu.

  - “thirdparty” edo “hirugarrena”: sinatzen duena ez bada ez egilea ez hartzailea.

- CommitmentTypeIndication: zer egin duen sinatzaileak dokumentuarekin (onartu, berri eman, jaso, ziurtatu...).

- AllDataObjectsTimeStamp: denbora-zigilua, sinadura sortu aurrekoa, ezartzen du ds:Reference elementu guztietan.

- IndividualDataObjectsTimeStamp: denbora-zigilua, sinadura sortu aurrekoa, ezartzen du ds:Reference elementu batzuetan.

  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 Egiaztatzaileak bete beharreko arauak

Sinadura elektroniko aurreratuaren oinarrizko formatuan dagoen baliozkotze-informazio bakarra sinatzaile-ziurtagiria da. Egiaztatzaileak honako atributu hauek erabil ditzake sinadura sortzeko aplikatuko den sinadura-politikaren baldintzak betetzen direnez egiaztatzeko:

- Signing Time: sinadura elektronikoak egiaztatzean, data jakin batean ziurtagiriak nola egon diren egiaztatzeko baino ez da erabiliko; izan ere, denbora-erreferentziak denbora-zigiluaz bakarrik ziurtatu daitezke (batez ere sinadura bezero-gailu batez eginez gero).

- SigningCertificatev2: ziurtagiria (behar den kasuetan ziurtapen-katea ere bai) sinadura sortu denean nola egon den egiaztatzeko erabiliko da, baldin eta iraungita ez badago eta egiaztatzeko datuak eskuratu ahal badira (CRL, OCSP) edo, bestela, ziurtapen-zerbitzua egiten duenak ziurtagiriaren egoeraren historia aztertzeko aukera ematen badu.

- SignaturePolicyIdentifier: egiaztatu behar da sinadura sortzeko aplikatu den sinadura-politika bat ote datorren zerbitzu jakin baterako erabili beharrekoarekin.

Badago itxarote-aldi bat (zuhurtasun-aldia edo graziazko aldia esaten zaiona), ziurtagiria ezeztatu denez egiaztatzeko erabil daitekeena. Egiaztatzaileak aldi hori igaro arte itxaron dezake sinadura baliozkotzeko edo, bestela, egin ahala baliozkotu dezake eta gero berriz baliozkotu. Izan ere, gerta daiteke denbora pasatzea sinatzaileak ziurtagiria ezeztatzen hasten denetik ziurtagiriaren ezeztapenaren egoeraren berri behar diren informazio-puntuetara banatu 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 ARKITEKTURAREN EZAUGARRIAK

4.1 Onartzen diren ziurtagiriak

TicketBAI sisteman honako ziurtagiri hauetako bat erabili behar da:

Gailuaren ziurtagiria: gailu bakoitzari identitate berezia eskaintzen dio; bertan instalatuta eta berarekin lotuta dago.

Pertsona fisikoaren edo entitatearen ordezkariaren ziurtagiria: pertsona fisikoa edo pertsona juridikoa nor den frogatzen du.

Enpresaren zigilua: ziurtagiri tekniko hau aplikazio baten bidez erabil daiteke, inor aurrean ez dagoela; gainera, sail edo lantalde bateko pertsona-talde batek ere erabil dezake. Ziurtagiri hau enpresek lanerako erabili ohi duten kautxuzko zigiluaren antzekoa da.

Autonomoaren ziurtagiria: kualifikatu gabeko ziurtagiria, autonomo modura egiten den jarduera ekonomiko baten aitorpena egiten duten pertsona fisikoentzat egiten dena; ziurtagiri honen bidez eskatzailearen IFZ egiaztatzen da.

4.2 Sinaduraren murrizketak arkitekturaren arabera

4.2.1 Bezero-sinaduradun arkitekturak

Arkitektura hauetan sinadura egiten duen softwarea fakturazioaren aplikazioa erabiltzeko baliatzen den gailuan dago. Esaterako, aplikazioa idazmahaian Internet gabe.

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 hauetan sinadura egiten duen softwarea fakturazioaren aplikazioa erabiltzeko baliatzen den gailuan gabe beste batean dago. Beraz, honen bidez bezero-gailutik urruneko beste gailu batean sartzen da sinadura sortzeko.

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

Hauek erabil daitezke sinatzeko: **pertsona fisikoaren ziurtagiria, entitatearen 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 sinadura bezeroan zein zerbitzarian egin daiteke, kasuan kasuko murrizketak kontuan edukiz.

Esaterako, web aplikazioetan:

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

- Zerbitzari-sinadura nabigatzailea sartzen den urruneko zerbitzarian egiten da. Zerbitzari-sinaduradun arkitekturen murrizketa berak aplikatzen dira.

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