TicketBAI 1.0 sinadura-politika
Política de Firma TicketBAI 1.0

Bertsioaren data: 2019/12/19

Fecha de versión: 19/12/2019

AURKIBIDEA

ÍNDICE

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 faktururaren 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.

1. INTRODUCCIÓN

1.1 Objeto del documento

Esta Política de Firma TicketBAI (en adelante, Política) representa el conjunto de criterios asumidos por las Diputaciones Forales de Araba/Álava, Bizkaia y Gipuzkoa y por el Gobierno Vasco en relación con la firma electrónica de los ficheros TicketBAI.

La definición, la estructura y los requisitos técnicos del fichero TicketBAI están definidos en el documento "Especificaciones funcionales y técnicas del sistema TicketBAI". A modo de resumen: un fichero TicketBAI contiene los datos de una única factura emitida en formato XML, tanto datos específicos de la factura como otros de control (encadenamiento de facturas, dispositivo que emite la factura, entidad desarrolladora, etc.).

La presente política de firma deberá estar disponible en formato legible, de modo que puedan ser aplicada en un contexto concreto para cumplir con los requerimientos de creación y validación de firma electrónica.

1.2 Referencias

Para el desarrollo de su contenido, se han tenido en cuenta las siguientes especificaciones técnicas:

- 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.

Se ha considerado como normativa básica aplicable:

- REGLAMENTO (UE) N o 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.
- Ley 59/2003, de 19 de diciembre, de firma electrónica.
- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

- 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.

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

- Ley 56/ 2007 o Ley para el Impulso de la Sociedad de la Información.

- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

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 Jarduleak

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.

2. ALCANCE DE LA POLÍTICA DE FIRMA DE TICKETBAI

Esta Política define las condiciones generales para la firma de los ficheros XML con las especificaciones TicketBAI.

Será válida a partir de su fecha de publicación y hasta que se publique una actualización.

La política de firma se identificará con un identificador único que será http://ticketbai.eus/politicafirma. Esta identificación deberá incluirse obligatoriamente en la firma electrónica, empleando el campo correspondiente para identificar la política marco y la versión con las condiciones generales y específicas de aplicación para su validación.

2.1 Actores involucrados

Los actores involucrados en el proceso de creación y validación de firma electrónica son:

- Firmante: persona física o jurídica o entidad sin personalidad jurídica que posee un dispositivo de creación de firma y que firma un fichero TicketBAI.

- Verificador: entidad, ya sea persona física o jurídica, que valida o verifica una firma electrónica apoyándose en las condiciones exigidas por una política de firma concreta.

- Prestador de servicios de confianza: la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.

- Emisor de la Política: entidad que se encarga de generar y gestionar este documento, por el cual se deben regir el firmante y el verificador en los procesos de generación y validación de firma electrónica.

2.2 Formatos admitidos para la firma

Formato XAdES (XML AdvancedElectronicSignatures), según especificación técnica ETSI EN 319 132-1 V1.1.1. Para versiones posteriores del estándar se analizarán los cambios en la sintaxis y se aprobará la adaptación del perfil a la versión del estándar nueva a través de una adenda a la política.

A lo largo de este documento se utilizarán los prefijos ds: y xades: para hacer referencia a elementos definidos en los estándares XMLDSig y XAdES, respectivamente.

Dentro de las distintas clases del formato **XAdES** se deberá adecuar para la generación de, al menos, la clase básica, añadiendo información sobre la política de firma, **clase EPES**.

2.3 Creación de la firma electrónica

Es conveniente realizar la implementación de la creación de la firma electrónica utilizando librerías criptográficas o productos existentes.

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.

No es requerido que la firma incluya Sellado de Tiempo o TimeStamping proporcionados por servicios de TSA en el momento de firma.

2.4 Verificación de la firma electrónica

El verificador puede utilizar cualquier método estandarizado para verificar la firma creada según la presente Política. Las condiciones mínimas que deberán cumplirse para validar la firma serán las siguientes:

1. Garantía de validez de la integridad de la firma.

2. Validez de los certificados en el momento en que se realizó la firma.

3. Certificado firmante expedido bajo una Declaración de Prácticas de Certificación específica, disponible en un repositorio público.

4. El emisor del certificado firmante deberá estar en la lista de Prestadores de Servicios de Confianza Cualificados (QTSP). Esta lista se encuentra disponible en https://webgate.ec.europa.eu/tl-browser/#/.

2.5 Gestión de la Política de firma

El mantenimiento, actualización, publicación y divulgación del presente documento corresponderá a las Diputaciones de Araba/Álava, Bizkaia y Gipuzkoa, y al Gobierno Vasco.

Las actualizaciones de esta Política serán publicadas en el enlace 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 sortz-

3. POLÍTICA DE VALIDACIÓN DE FIRMA ELECTRÓNICA

En este apartado se especifican las condiciones que se deberán considerar por parte del firmante, en el proceso de generación de firma electrónica, y por parte del verificador, en el proceso de validación de la firma.

3.1 Periodo de validez

La presente Política es válida desde su publicación hasta la publicación de una nueva versión actualizada, pudiéndose facilitar un periodo de tiempo transitorio, en el cual convivan las dos versiones, que permita adecuar las diferentes plataformas de los actores involucrados en el proyecto TicketBAI a las especificaciones de la nueva versión. Este periodo de tiempo transitorio deberá indicarse en la nueva versión, pasado el cual sólo será válida la versión actualizada.

3.2 Reglas comunes

Las reglas comunes para los actores involucrados en la firma electrónica, firmante y verificador, son un campo obligatorio que debe aparecer en cualquier Política de Firma. Estas reglas permiten establecer responsabilidades respecto a la firma electrónica sobre la persona o entidad que crea la firma y la persona o entidad que la verifica, definiendo los requisitos mínimos que deben presentarse, debiendo estar firmados, si son requisitos para el firmante, o no firmados, si son requisitos para el verificador.

3.3 Reglas del firmante

El firmante se hará responsable de que el fichero que quiere firmar no contiene contenido dinámico que pudiese modificar el resultado de la firma durante el tiempo. Si el fichero que se quiere firmar no ha sido creado por el firmante, éste deberá asegurarse que no existe contenido dinámico dentro del fichero (como pueden ser macros).

Formato XAdES: se admitirán exclusivamente las firmas **XAdESenveloped**. No se admitirá XAdESenveloping, ni XAdESdettached.

El firmante deberá proporcionar, como mínimo, la información contenida en las siguientes etiquetas dentro del campo SignedProperties (campo que contiene una serie de propiedades conjuntamente firmadas a la hora de la generación de la firma XMLDsig), las cuales son de carácter obligatorio:

- SigningTime: especifica el momento en que el firmante realizó el proceso de firma.
- SigningCertificatev2: contiene referencias a los certificados y algoritmos de seguridad utilizados en cada certificado. Este elemento deberá ser firmado con objeto de evitar la posibilidad de sustitución del certificado.
- SignaturePolicyIdentifier: identifica la política de firma

eko oinarritzat hartu den sinadurapolitika 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:

sobre la que se basa el proceso de generación de firma electrónica, y debe incluir los siguientes contenidos en los elementos en que se subdivide:

- Una referencia explícita al presente documento de política de firma, en el elemento xades:SigPolicyId. Para ello aparecerá el OID que identifique la versión concreta de la política de firma o la URL de su localización.

- La huella digital del documento de política de firma correspondiente y el algoritmo utilizado, en el elemento <xades:SigPolicyHash>, de manera que el verificador pueda comprobar, calculando a su vez este valor, que la firma está generada según la misma política de firma que se utilizará para su validación.

Las etiquetas restantes que pueden agregarse en el campo SignedProperties serán consideradas de carácter opcional:

- SignatureProductionPlacev2: define el lugar geográfico donde se ha realizado la firma del documento.

- SignerRolev2: define el rol de la persona en la firma electrónica. En el caso de su utilización, deberá contener uno de los siguientes valores en el campo ClaimedRoles:

  - "supplier" o "emisor": cuando la firma la realiza el emisor.

  - "customer" o "receptor": cuando la firma la realiza el receptor.

  - "thirdparty" o "tercero": cuando la firma la realiza una persona o entidad distinta al emisor o al receptor.

- CommitmentTypeIndication: define la acción del firmante sobre el documento firmado (lo aprueba, lo informa, lo recibe, lo certifica...).

- AllDataObjectsTimeStamp: contiene un sello de tiempo, calculado antes de la generación de la firma, sobre todos los elementos contenidos en ds:Reference.

- IndividualDataObjectsTimeStamp: contiene un sello de tiempo, calculado antes de la generación de la firma, sobre algunos de los elementos contenidos en ds:Reference.

La etiqueta CounterSignature, refrendo de la firma electrónica y que se puede incluir en el campo UnsignedProperties, será considerada de carácter opcional. Las siguientes firmas, ya sean serie o paralelo, se añadirán según indica el estándar XAdES, según el documento EN 319 102-1.

3.4 Reglas del verificador

El formato básico de firma electrónica avanzada no incluye ninguna información de validación más allá del certificado firmante. Los atributos que podrá utilizar el verificador para comprobar que se cumplen los requisitos de la política de firma según la cual se ha generado la firma son las siguientes:

- 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 ziurtapenzerbitzua 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.

- Signing Time: sólo se utilizará en la verificación de las firmas electrónicas como indicación para comprobar el estado de los certificados en la fecha señalada, ya que únicamente se puede asegurar las referencias temporales mediante un sello de tiempo (especialmente en el caso de firmas en dispositivos cliente).

- SigningCertificatev2: se utilizará para comprobar y verificar el estado del certificado (y, en su caso, la cadena de certificación) en la fecha de la generación de la firma, en el caso que el certificado no haya caducado y se pueda acceder a los datos de verificación (CRL, OCSP) o bien en el caso de que el PSC ofrezca un servicio de validación histórico del estado del certificado.

- SignaturePolicyIdentifier: se deberá comprobar, que la política de firma que se ha utilizado para la generación de la firma se corresponde con la que se debe utilizar para un servicio en cuestión.

Existe un periodo de tiempo de espera, conocido como periodo de precaución o periodo de gracia, para comprobar el estado de revocación de un certificado. El verificador puede esperar este tiempo para validar la firma o realizarla en el mismo momento y revalidarla después. Esto se debe a que puede existir una pequeña demora desde que el firmante inicia la revocación de un certificado hasta que la información del estado de revocación del certificado se distribuye a los puntos de información correspondientes. Se recomienda que este periodo, desde el momento en que se realiza la firma sea, como mínimo, el tiempo máximo permitido para el refresco completo de las CRLs o el tiempo máximo de actualización del estado del certificado en el servicio OCSP. Estos tiempos podrán ser variables según el Prestador de Servicios de Certificación.

3.5 Reglas de uso de algoritmos

Se podrán utilizar cualquiera de los algoritmos basados en RSA admitidos en ETSI TS 119 312 V1.3.1. Como mínimo se exige:

- Tamaño de la clave será estrictamente superior a 1024.

- SHA256 o versiones superiores.

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 zerbitzarisinaduraduna da.

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

4. REQUISITOS ARQUITECTURA TICKETBAI

4.1 Certificados admitidos

La solución TicketBAI requiere de la utilización de alguno de los siguientes certificados:

Certificado de dispositivo: proporciona una identidad única para cada dispositivo, estando instalado y vinculado al dispositivo desde el que se emiten facturas.

Certificado de persona física o de representante de entidad: permiten acreditar la identidad de la persona física o jurídica respectivamente.

Sello de empresa: es un certificado técnico que puede ser utilizado por un aplicativo de forma desasistida, también por un grupo de personas pertenecientes a un departamento o grupo de trabajo. Es un certificado que puede compararse en el mundo físico al uso habitual en el día a día de una empresa de un sello de caucho.

Certificado de autónomo: certificado no cualificado, emitido para personas físicas que declaran actividades económicas como autónomos y cuya función es garantizar el NIF del solicitante de dicho certificado.

4.2 Restricciones de la firma en función de la arquitectura

4.2.1 Arquitecturas con firma en cliente

Se considera arquitectura con firma en cliente, cuando el software que realiza la firma se encuentra ubicado en el dispositivo desde el que se accede a la aplicación de facturación. Por ejemplo, una aplicación de escritorio sin acceso a Internet.

Si se accede de forma remota a otro dispositivo para firmar, se considera arquitectura con firma en servidor.

No existen restricciones en los certificados para este tipo de arquitectura. **Se podrá firmar con: certificado de dispositivo, certificado de persona física, certificado de representante de entidad, sello de empresa o certificado de autónomo**.

4.2.2 Arquitecturas con firma en servidor

Se considera arquitectura con firma en servidor, cuando el software que realiza la firma se encuentra ubicado en un dispositivo distinto desde el que se accede a la aplicación de facturación. Por tanto, el dispositivo cliente accede de forma remota a otro dispositivo para realizar la firma.

De forma complementaria, si la emisión de facturas se realiza en procesos desasistidos (batch) se considera “arquitectura con firma en servidor”.

Se podrá firmar con: **certificado de persona física, certificado de representante de entidad, sello de empresa o certificado de autónomo**.

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. Zerbitzarisinaduradun 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.

En este caso, no se permite la firma con certificado de dispositivo.

4.2.3 Arquitecturas con posibilidad de firma en cliente y en servidor

Las arquitecturas distribuidas podrán elegir entre realizar la firma en cliente o en servidor, siempre respetando las restricciones aplicadas a cada una de ellas.

Por ejemplo, en una aplicación web:

- La firma en cliente se realizaría en el dispositivo que tiene instalado el navegador desde el que se accede a la aplicación. Aplican las restricciones de las arquitecturas con firma en cliente.

- La firma en servidor se realizaría en el servidor remoto al que accede el navegador. Aplican las restricciones de las arquitecturas con firma en servidor.

Una arquitectura no podrá realizar firmas en cliente y servidor de forma simultánea. Debe elegir sólo una de las arquitecturas disponibles