



## 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

## Especificaciones de la firma electrónica de los ficheros TicketBAI

### 1. Objeto

Este anexo establece las especificaciones de la firma electrónica de los ficheros TicketBAI (en adelante, especificaciones de firma).

Las especificaciones de la firma electrónica se identificarán con un identificador único que será: <https://ticketbai.araba.eus/tbai/sinadura/> Esta identificación se deberá incluir obligatoriamente en la firma electrónica de los ficheros TicketBAI, empleando el campo correspondiente identificativo para determinar el marco general de especificaciones y la versión con las condiciones generales y específicas de aplicación para su validación.

### 2. Alcance

#### 2.1. Actores involucrados

Los actores involucrados en el proceso de creación y validación de la 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 o verificadora: entidad, ya sea persona física o jurídica, que valida o verifica una firma electrónica apoyándose en las condiciones exigidas por unas especificaciones de firma concreta.
- Prestador o prestadora de servicios de confianza: la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.
- Emisor o emisora de las especificaciones de firma: entidad que se encarga de generar y gestionar este documento, por el cual se deben regir el o la firmante y el verificador o la verificadora en los procesos de generación y validación de firma electrónica.

#### 2.2. Formato admitido para la firma electrónica

El formato admitido para la firma electrónica de los ficheros TicketBAI es el FormatoXAdES

AdvancedElectronicSignatures), ETSI EN 319 132-1 V1.1.1, ETSI TS 103 171 V2.1.1 eta ETSI TS 101 903 V1.4.2 zehaztaperen teknikoaren arabera. Estandarraren hurrengo bertsioetarako, sintaxian egindako aldaketak aztertuko dira eta profila estandarren bertsio berrira egokitzea onartuko da eranskin hau aldatuz.

Zehaztaperen hauek ds: aurrizkia erabiliko da XMLDSig estandarrean zehaztutako elementuak aipatzeko eta xades: aurrekia XAdES estandarrean zehaztutakoak aipatzeko.

XAdES formatuan hainbat mota daude; sinadura oinarritzko 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 erabili dezake eranskin honekin bat etorritik 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 ziurtaperen 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 zehaztaperenak kudeatzea

Sinadura zehaztaperenak mantentzeko, eguneratzeko, argitaratzeko eta hedatzeko ardura Arabako Foru Aldundiak dauka.

Zehaztaperen hauek eguneratzeak Arabako Aldizkari Ofizialean eta hemen argitaratuko dira:

<https://ticketbai.araba.eus/tbai/sinadura/>

(XML AdvancedElectronicSignatures), según las especificaciones técnicas ETSI EN 319 132-1 V1.1.1, ETSI TS 103 171 V2.1.1 y ETSI TS 101 903 V1.4.2. Para versiones posteriores del estándar se analizarán los cambios en la sintaxis y se aprobará la adaptación del perfil a la nueva versión del estándar a través de la modificación del presente anexo.

A lo largo de estas especificaciones de firma 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 las especificaciones 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.

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 o la verificadora puede utilizar cualquier método estandarizado para verificar la firma creada según el presente anexo. 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 o la emisora 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 las especificaciones para la firma

El mantenimiento, actualización, publicación y divulgación de las especificaciones de firma corresponderá a la Diputación Foral de Álava. Las actualizaciones de estas especificaciones se publicarán en el Boletín Oficial de Álava y en el siguiente enlace:

<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 zehaztaperen 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 zehaztaperentara moldatu ahal izango dituzte. Trantsizioaldi horren iraupena bertsio berriari 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 zehaztaperen 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.

### 3. Política de validación de la firma electrónica

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

#### 3.1. Periodo de validez

Estas especificaciones de firma son válidas 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 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 o verificadora, son un campo obligatorio que debe aparecer en todas las especificaciones 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 verifica, definiendo los requisitos mínimos que deben presentarse, debiendo estar firmados, si son requisitos para el o la firmante, o no firmados, si son requisitos para el verificador o la verificadora.

#### 3.3. Reglas del firmante

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

Formato XAdES: se admitirán exclusivamente las firmas XAdESenveloped. No se admitirá XAdESenveloping, ni XAdESdettached. El o la 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 o la firmante realizó el proceso de firma.

- SigningCertificateV2 edo SigningCertificate<sup>1</sup>: ziurtagiriak eta haietan erabilitako segurtasun algoritmoak. Elementu hau sinatu egin behar da, ziurtagiria ordeztzeko 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 azterna 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<sup>2</sup>: non sinatu den dokumentua.
- SignerRoleV2 edo SignerRole<sup>3</sup>: 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.

- SigningCertificateV2 o SigningCertificate<sup>1</sup>: 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 las especificaciones de firma sobre las que se basa el proceso de generación de la firma electrónica, y debe incluir los siguientes contenidos en los elementos en que se subdivide:
  - Referencia explícita al presente documento de especificaciones de firma, en el elemento xades:SigPolicyId. Para ello, aparecerá el OID que identifique la versión concreta de las especificaciones de firma o la URL de su localización.
  - La huella digital del documento de especificaciones de firma correspondiente y el algoritmo utilizado, en el elemento <xades:SigPolicyHash>, de manera que el verificador o la verificadora pueda comprobar, calculando a su vez este valor, que la firma está generada según las mismas especificaciones de firma que se utilizarán para su validación.

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

- SignatureProductionPlaceV2 o SignatureProductionPlace<sup>2</sup>: define el lugar geográfico donde se ha realizado la firma del documento.
- SignerRoleV2 o SignerRole<sup>3</sup>: 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 o la emisora.
  - “Customer” o “receptor”: cuando la firma la realiza el receptor o la receptora.
  - “Thirdparty” o “tercero”: cuando la firma la realiza una persona o entidad distinta al emisor o la emisora o al receptor o la receptora.

---

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

2 SignatureProductionPlaceV2 - ETSI EN 319 132 , SignatureProductionPlace - ETSITS 101 903, ETSITS 103 171.

3 SignerRoleV2 - ETSI EN 319 132 , SignerRole - ETSITS 101 903, ETSITS 103 171.

---

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

2 SignatureProductionPlaceV2 - ETSI EN 319 132 , SignatureProductionPlace - ETSITS 101 903, ETSITS 103 171.

3 SignerRoleV2 - ETSI EN 319 132 , SignerRole - ETSITS 101 903, ETSITS 103 171.

- 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.

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

### 3.4. Egiaztatzaileak bete beharreko arauak

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

- Signing Time: sinadura elektronikoa 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 graziako aldia) ziurtagiria ezeztatu den ala ez egiaztatu daiteke. Hain zuzen ere, egiaztatzaileak aldi hori igaro arte

- CommitmentTypeIndication: define la acción del o de la 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 o de la verificadora

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 o la verificadora para comprobar que se cumplen los requisitos de las especificaciones de firma según la cual esta se ha generado, son los siguientes:

- 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 pueden asegurar las referencias temporales mediante un sello de tiempo (especialmente en el caso de firmas en dispositivos cliente).
- SigningCertificatev2 o SigningCertificate: 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 de 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 las especificaciones de firma que se han utilizado para la generación de la firma se corresponden 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

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 arabera alda litezke.

### 3.5. Algoritmoak erabiltzeko arauak

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

certificado. El verificador o la verificadora 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 o la 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. Requisitos derivados de la arquitectura del software TicketBAI

### 4.1. Certificados admitidos

El software TicketBAI deberá utilizar alguno de los siguientes certificados para la firma electrónica de los ficheros TicketBAI:

- Certificado de dispositivo, el cual proporciona una identidad única para cada dispositivo de facturación, estando instalado y vinculado al dispositivo desde el que se emiten facturas o justificantes.
- Certificado de persona física o de representante de entidad, los cuales permiten acreditar la identidad de la persona física o jurídica respectivamente.
- Sello de empresa, el cual constituye un certificado técnico que puede ser utilizado por un software TicketBAI de forma desasistida, o 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 o autónoma: certificado no cualificado, emitido para personas físicas que desarrollen una actividad económica de acuerdo



da, Pertsona fisikoaren errentaren gaineko zergaren Foru Arauan ezartzen denarekin bat etorritz. 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, autonomoaren ziurtagiria edo gailuaren ziurtagiria.

Arkitektura zerbitzarian duten hirugarrenei fakturazioa egiten dieten enpresen kasuan, fitxategiak elektronikoki sinatzeko enpresa-zigilua erabiltzea gomendatzen da.

### **4.2.3. Bezero sinadura eta zerbitzari sinadura erabil daitezkeen arkitekturak**

Arkitektura banatuetan, bezero sinadura zein zerbitzari sinadura hauta daiteke, bakoitzaren murrizketak kontuan edukiz.

con lo previsto en la Norma Foral del Impuesto sobre la Renta de las Personas Físicas, y para cuya emisión, se exigirá la acreditación por la persona física de esta circunstancia.

## **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 TicketBAI que realiza la firma se encuentra ubicado en el propio dispositivo de facturación desde que se accede al mismo. Por ejemplo, una aplicación de escritorio.

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 o autónoma.

### **4.2.2. Arquitecturas con firma en servidor**

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

De forma complementaria, si la emisión de facturas o justificantes 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-autónoma o certificado de dispositivo.

Para el caso de empresas que hagan facturación a terceros con arquitectura en servidor se recomienda el uso del sello de entidad para la firma electrónica de los ficheros.

Se ha de tener en cuenta que el certificado de dispositivo sólo se puede utilizar en nombre propio.

### **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.

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 sartzten 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 arkitekturretako bat hautatu behar da.

## 5. Elkarrekikotasuna

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

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, aplicándose las restricciones de las arquitecturas con firma en cliente.
- La firma en servidor se realizaría en el servidor remoto al que accede el navegador, aplicándose en este caso 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.

## 5. Cláusula de reciprocidad

A título de reciprocidad, se entenderán cumplidas las especificaciones de firma electrónica contenidas en este anexo cuando los contribuyentes cumplan las especificaciones que a estos efectos hayan sido establecidos por la Diputación Foral de Gipuzkoa o por la Diputación Foral de Bizkaia.