1482/2020 Foru Agindua, irailaren 9koa, Ogasun eta Finantzetako foru diputatuarena, software bermatzailearen arauzko zehaztapenak eta zehaztapen teknikoak eta software bermatzailearen erregistroko alta-aitorpena arautzen dituena, Ogasun eta Finantzetako foru diputatuaren uztailaren 3ko 274/2023 Foru Aginduak eta Ogasun eta Finantzetako foru diputatuaren abenduaren 5eko 601/2025 Foru Aginduak aldatua

III. ERANSKINA. SOFTWARE BERMATZAILEAREKIN EGINDAKO ERAGIKETAREN ALTA- ETA DEUSEZTAPEN-FITXATEGIEN SINADURA ELEKTRONIKOAREN ZEHAZTAPENAK

(Bizkaiko Aldizkari Ofizialak, 2020ko irailaren 11koak, 2023ko uztailaren 12koak eta 2025eko abenduaren 16koak)

1. Xedea

Eranskin honek ezartzen ditu software bermatzailearekin egindako eragiketaren alta- eta deuseztapen-fitxategien sinadura elektronikoaren zehaztapenak (aurrerantzean, sinatzeko zehaztapenak), foru agindu honen 3. eta 4. artikuluetan aipatzen direnak.

Sinadura elektronikoaren zehaztapenak identifikatzaile bakar batekin identifikatuko dira: https://www.batuz.eus/fitxategiak/batuz/ticketbai/sinadura_elektronikoaren_zehaztapenak_especificaciones_de_la_firma_electronica_v1_2.pdf.

Identifikazio hori nahitaez sartu beharko da software bermatzailearekin egindako eragiketaren alta- eta deuseztapen-fitxategien sinadura elektronikoan, eta dagokion identifikazio-eremua erabiliko da espezifikazioen esparru orokorra zehazteko, bai eta hura baliozkotzeko aplikatu beharreko baldintza orokor eta espezifikoak dituen bertsioa ere.

2. Irismena

2. 1. Jarduleak

Sinadura elektronikoa sortzeko eta baliozkotzeko prozesuko jarduleak honako hauek dira:

— Sinatzailea: nortasun juridikorik gabeko pertsona fisikoa edo juridikoa, sinadura sortzeko gailu bat duena eta software bermatzailearekin alta emateko edo eragiketa baliogabetzeko fitxategi bat sinatzen duena.

— Egiaztatzailea: sinadura elektroniko bat baliozkotzen edo egiaztatzen duen erakundea, pertsona fisikoa zein juridikoa izan, sinadura zehatzaren zehaztapen batzuek eskatzen dituzten baldintzetan oinarrituta.

— Konfiantzazko zerbitzuen emailea: ziurtagiri elektronikoak ematen dituen edo sinadura elektronikoarekin lotutako beste zerbitzu batzuk ematen dituen pertsona fisikoa edo juridikoa.

— Sinadura-zehaztapenen igorlea: dokumentu hau sortzeaz eta kudeatzeaz arduratzen den erakundea; horren bidez, sinatzaileak eta egiaztatzaileak hori bete dute sinadura elektronikoa sortzeko eta baliozkotzeko prozesuetan.

2. 2. Sinadura elektronikorako onartutako formatua

Software bermatzailearekin egindako eragiketaren altako eta deuseztapeneko fitxategien sinadura elektronikorako onartutako formatua FormatoXAdes (XML AdvancedElectronicSignatures) 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 ondorengo bertsioetarako, sintaxiaren aldaketak aztertuko dira, eta profila estandarraren bertsio berrira egokitzea onartuko da, eranskin hau aldatuz.

Orden Foral 1482/2020, de 9 de septiembre, del diputado foral de Hacienda y Finanzas, por la que se regulan las especificaciones normativas y técnicas del software garante y la declaración de alta en el registro de software garante, modificada por la Orden Foral 274/2023, de 3 de julio, del diputado foral de Hacienda y Finanzas y por la Orden Foral 601/2025, de 5 de diciembre, de la diputada foral de Hacienda y Finanzas

ANEXO III ESPECIFICACIONES DE LA FIRMA ELECTRÓNICA DE LOS FICHEROS DE ALTA Y DE ANULACIÓN DE OPERACIÓN CON SOFTWARE GARANTE

(Boletines Oficiales de Bizkaia de 11 de septiembre de 2020, de 12 de julio de 2023 y de 16 de diciembre de 2025)

1. Objeto

Este anexo establece las especificaciones de la firma electrónica de los ficheros de alta y de anulación de operación con software garante (en adelante, especificaciones de firma), a que se refieren los artículos 3 y 4 de esta Orden Foral.

Las especificaciones de la firma electrónica se identificarán con un identificador único que será: https://www.batuz.eus/fitxategiak/batuz/ticketbai/sinadura_elektronikoaren_zehaztapenak_especificaciones_de_la_firma_electronica_v1_2.pdf.

Esta identificación se deberá incluir obligatoriamente en la firma electrónica de los ficheros de alta y de anulación de operación con software garante, 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 de alta o de anulación de operación con software garante.

— 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 de alta y de anulación de operación con software garante es el FormatoXAdES (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.

Sinaduraren zehaztapen horietan, ds: eta xades: aurrizkiak erabiliko dira XMLDSig eta XAdES estandarretan definitutako elementuei erreferentzia egiteko, hurrenez hurren.
XAdES formatuan hainbat mota daude; sinadura oinarrizko mota sortzeko prestatu behar da gutxienez, sinadura-zehaztapenei 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 edozein metodo estandarizatu erabil dezake eranskin honen arabera sortutako sinadura 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. Ziurtagiri sinatzailearen jaulkitzaileak konfiantza-zerbitzu kualifikatuen emaileen zerrendan egon beharko du (QTSP). Zerrenda hori hemen dago eskuragarri: https://webgate.ec.europa.eu/tl-browser/# /.

2. 5. Sinatzeko zehaztapenak kudeatzea

Bizkaiko Foru Aldundiari dagokio sinatzeko zehaztapenak mantentzea, eguneratzea, argitaratzea eta zabaltzea.

Zehaztapen horien eguneratzeak Bizkaiko Aldizkari Ofizialean eta esteka honetan argitaratuko dira: www.batuz.eus.

3. Sinadura elektronikoa baliozkotzea

Atal honetan, sinadura elektronikoa sortzeko prozesuan sinatzaileak eta sinadura elektronikoa baliozkotzeko prozesuan egiaztatzaileak kontuan hartu beharko dituzten baldintzak zehazten dira.

3. 1. Indarraldia

Sinadura-zehaztapen horiek baliozkoak dira argitaratzen direnetik bertsio eguneratu berri bat argitaratzen den arte, eta aldi baterako epe bat eman daiteke, bi bertsioak elkarrekin bizi izan daitezen, tartean dauden eragileen plataformak bertsio berriaren zehaztapenetara egokitu ahal izateko. Bertsio berrian aldi horren iraupena zehaztu beharko da; amaitutakoan bertsio eguneratua baino ez da izango baliozkoa.

3. 2. Arau komunak

Sinadura elektronikoan, sinatzailean eta egiaztatzailean parte hartzen duten eragileentzako arau komunak nahitaezko eremua dira, eta sinaduraren zehaztapen guztietan agertu behar dute. Arau horiei esker, sinadura elektronikoa sortzen duen pertsona edo erakundearen eta sinadura hori egiaztatzen duen pertsona edo erakundearen gaineko erantzukizunak ezar daitezke, aurkeztu beharreko gutxieneko baldintzak zehaztuta, betiere izenpetuta sinatzailearentzako baldintzak badira, edo ez izenpetuta, egiaztatzailearentzako baldintzak badira.

3. 3. Sinatzaileak bete beharreko arauak

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 Bizkaia.

Las actualizaciones de estas especificaciones se publicadarán en el Boletín Oficial de Bizkaia y en en el siguiente enlace: www.batuz.eus.

3. 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 la 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

Sinatzaileak bere gain hartuko du sinatu beharreko fitxategian sinaduraren emaitza denboran zehar alda dezakeen eduki dinamikorik ez egotearen ardura. Sinatu beharreko fitxategia sinatzaileak sortu ez badu, pertsona horrek ziurtatu beharko du fitxategiaren barruan ez dagoela eduki dinamikorik (makroak, adibidez).

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

Sinatzaileak, gutxienez, SignedProperties eremuko etiketa hauetan jasotako informazioa eman beharko du (eremu horretan, XMLDsig sinadura sortzeko orduan batera sinatutako propietate batzuk daude); horiek nahitaezkoak dira:

— SigningTime: sinatzaileak sinadura-prozesua noiz egin zuen zehazten du.

— SigningCertificatev2 edo SigningCertificate: ziurtagiri bakoitzean erabilitako segurtasun-algoritmoen eta ziurtagirien erreferentziak jasotzen ditu. Elementu hori sinatu egin beharko da, ziurtagiria ordezteko aukerarik egon ez dadin.

— SignaturePolicyIdentifier: sinadura elektronikoa sortzeko prozesuaren oinarri diren sinadura-zehaztapenak identifikatzen ditu, eta honako eduki hauek izan behar ditu azpibanatzen den elementuetan:

a) Sinadura-zehaztapenen dokumentu honen erreferentzia esplizitua, xades elementuan: SigPolicyId. Horretarako, sinaduraren zehaztapenen bertsio zehatza identifikatzen duen OIDa edo haren kokapenaren URLa agertuko da.

b) Dagokion sinadura-zehaztapenen dokumentuaren aztarna digitala eta erabilitako algoritmoa, <xades: SigPolicyHash> elementuan; horrela, egiaztatzaileak egiaztatu ahal izango du, balio hori kalkulatuz, sinadura hura baliozkotzeko erabiliko diren sinadura-zehaztapenen arabera sortu dela.

SignedProperties eremuan ezar daitezkeen gainerako eremuak aukerakoak dira:

— SignatureProductionPlacev2 edo SignatureProductionPlace: dokumentua sinatu den leku geografikoa definitzen du.

— SignerRolev2 edo SignerRole: pertsonak sinadura elektronikoan duen rola definitzen du. Erabiltzen bada, balio hauetako bat eduki beharko du ClaimedRoles eremuan:

a) "Supplier" edo "igorlea": jaulkitzaileak sinatzen duenean.

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

c) "Thirdparty" edo "hirugarrena": jaulkitzailea edo hartzailea ez den beste pertsona edo erakunde batek sinatzen duenean.

— CommitmentTypeIndication: sinatzailearen ekintza definitzen du sinatutako dokumentuaren gainean (onartu, informatu, jaso, ziurtatu...).

— AllDataObjectsTimeStamp: denbora-zigilu bat du, sinadura sortu aurretik kalkulatua, ds:Reference-n dauden elementu guztien gainean.

— IndividualDataObjectsTimeStamp: denbora-zigilu bat du, sinadura sortu aurretik kalkulatua, ds:Reference delakoetan dauden elementu batzuen gainean.

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. Egiaztatzailearen arauak

El o la firmante se hará responsable de que el fichero a firmar no incluye contenido dinámico que pudiese modificar el resultado de la firma durante el tiempo. Si el fichero a firmar no ha sido creado por el o la firmante, esta persona deberá asegurarse de 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 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 o SigningCertificate: 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:

a) 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.

b) 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: define el lugar geográfico donde se ha realizado la firma del documento.

— SignerRolev2 o SignerRole: 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:

a) “Supplier” o “emisor”: cuando la firma la realiza el emisor o la emisora.

b) “Customer” o “receptor”: cuando la firma la realiza el receptor o la receptora.

c) “Thirdparty” o “tercero”: cuando la firma la realiza una persona o entidad distinta al emisor o la emisora o al receptor o la receptora.

— 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

Sinadura elektroniko aurreratuaren oinarrizko formatuan ez dago baliozkotze-informaziorik, ziurtagiri sinatzaileaz gain. Egiaztatzaileak ezaugarri hauek erabili ahal izango ditu sinadura sortzeko erabili diren sinadura-zehaztapenen baldintzak betetzen direla egiaztatzeko:

— Signing Time: sinadura elektronikoak egiaztatzeko, adierazitako datan ziurtagirien egoera egiaztatzeko adierazpen gisa baino ez da erabiliko; izan ere, denbora-erreferentziak denbora-zigilu baten bidez baino ezin dira ziurtatu (batez ere bezero-gailuetako sinaduren kasuan).

— SigningCertificatev2 edo SigningCertificate: SigningCertificatev2 edo SigningCertificate: ziurtagiriaren (eta, hala badagokio, ziurtapen-katearen) egoera egiaztatzeko eta egiaztatzeko erabiliko da, sinadura sortzen den egunean, baldin eta ziurtagiria iraungi ez bada eta egiaztapen-datuak (CRL, OCSP) eskuratu badaitezke edo PSCk ziurtagiriaren egoera historikoki baliozkotzeko zerbitzu bat eskaintzen badu.

— SignaturePolicyIdentifier: egiaztatu beharko da sinadura sortzeko erabili diren sinadura-zehaztapenak bat datozela zerbitzu horretarako erabili behar denarekin.

Badago itxarote-aldi bat (zuhurtasun-aldia edo graziazko aldia esaten zaiona), ziurtagiria ezeztatu denez egiaztatzeko erabil daitekeena. Egiaztatzaileak denbora hori itxaron dezake sinadura baliozkotzeko edo une berean egin eta gero berriro baliozkotzeko. Izan ere, baliteke atzerapen txiki bat egotea sinatzaileak ziurtagiri bat baliogabetzen duenetik ziurtagiriaren baliogabetze-egoerari buruzko informazioa dagozkion informazio-puntuetara banatzen den 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.

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 la firma 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 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. Algoritmoak erabiltzeko arauak

ETSI TS 119 312 zehaztapenean onartutako edozein sinadura-algoritmo erabili ahal izango da.

3. 5. Reglas de uso de algoritmos

Se podrán utilizar cualquiera de los algoritmos de firma admitidos en la especificación ETSI TS 119 312.

4. Software bermatzailetik eratorritako arkitekturaren betekizunak

4. Requisitos de la arquitectura derivados de software garante

4. 1. Onartzen diren ziurtagiriak

Software bermatzaileak honako ziurtagiri hauetakoren bat erabili beharko du software bermatzailearekin egindako eragiketaren alta- eta deuseztapen-fitxategiak elektronikoki sinatzeko:

— Gailuaren ziurtagiria, fakturazio-gailu bakoitzerako identitate bakarra ematen duena, instalatuta eta fakturak jaulkitzen diren gailuari lotuta.

— Pertsona fisikoaren edo erakundearen ordezkariaren ziurtagiria, pertsona fisikoaren edo juridikoaren nortasuna egiaztatzeko aukera ematen duena, hurrenez hurren.

— Enpresa-zigilua. Ziurtagiri teknikoa da, eta software bermatzaile batek edo sail edo lantalde bateko pertsona-talde batek erabil dezake. Ziurtagiri hau enpresek lanerako erabili ohi duten kautxuzko zigiluaren antzekoa da.

— Autonomoaren ziurtagiria: kualifikatu gabeko ziurtagiria, Pertsona Fisikoen errentaren gaineko zergari buruzko Foru Arauaren arabera ekonomia-jarduerak egiten dituzten pertsona fisikoentzat igortzen dena. Ziurtagiriaren igorpenerako pertsona fisikoak baldintza hori akreditatu beharko du.

4. 1. Certificados admitidos

El software garante deberá utilizar alguno de los siguientes certificados para la firma electrónica de los ficheros de alta y de anulación de operación con software garante:

— 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.

— 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 garante 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 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. Sinaduraren murrizketak arkitekturaren arabera

4. 2. Restricciones de la firma en función de la arquitectura

4. 2. 1. Bezero-sinaduradun arkitekturak

4. 2. 1. Arquitecturas con firma en cliente

Bezeroan sinadura duen arkitekturatzat hartzen da sinadura egiten duen software bermatzailea fakturazio-gailuan bertan dagoenean, bertara sartzen denetik. Esaterako, aplikazioa idazmahaian Internet gabe.

Se considera arquitectura con firma en cliente, cuando el software garante 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 sin acceso a Internet.

Sinatzeko urruneko beste gailu batean sartu behar bada, arkitektura zerbitzari-sinaduraduna da.

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

Honelako arkitekturetan ziurtagiriek ez dute murrizketarik. Hauek erabil daitezke sinatzeko: gailuaren ziurtagiria, pertsona fisikoaren ziurtagiria, erakundearen ordezkariaren ziurtagiria, enpresa-zigilua edo autonomoaren ziurtagiria.

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. Zerbitzari-sinaduradun arkitekturak

Zerbitzari-sinadura duen arkitekturatzat hartzen da sinadura egiten duen software bermatzailea bertara sartzeko erabiltzen den fakturazio-gailuaz bestelako gailu batean kokatuta dagoenean. Beraz, bezeroa fakturatzeko gailua urrunetik sartzen da beste gailu batera sinadura egiteko.

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

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

Hirugarrenei edo hartzaileei fakturazioa egiten dieten enpresen kasuan ezin izango da zerbitzariko gailuaren ziurtagiria erabili.

4. 2. 2. Arquitecturas con firma en servidor

Se considera arquitectura con firma en servidor, cuando el software garante 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 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 o autónoma o certificado de dispositivo.

No se podrá usar el certificado de dispositivo en servidor para el caso de empresas que hagan facturación a terceros o por destinatario o destinataria.

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:

— Aplikaziora sartzeko nabigatzaileak instalatuta duen gailuan egingo litzateke sinadura bezeroan, eta sinadura duten arkitekturen murrizketak aplikatuko lirateke.

— Zerbitzariko sinadura nabigatzailea sartzen den urrutiko zerbitzarian egingo litzateke, eta kasu horretan zerbitzariko sinadura duten arkitekturen murrizketak aplikatuko lirateke.

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

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, 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. Elkarrekikotasun-klausula

Elkarrekikotasun gisa, eranskin honetan jasotako sinadura elektronikoko zehaztapenak betetzat joko dira zergadunek Arabako Foru Aldundiak edo Gipuzkoako Foru Aldundiak ondorio horietarako ezarritako zehaztapenak betetzen dituztenean.

5. Cláusula de reciprocidad

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