

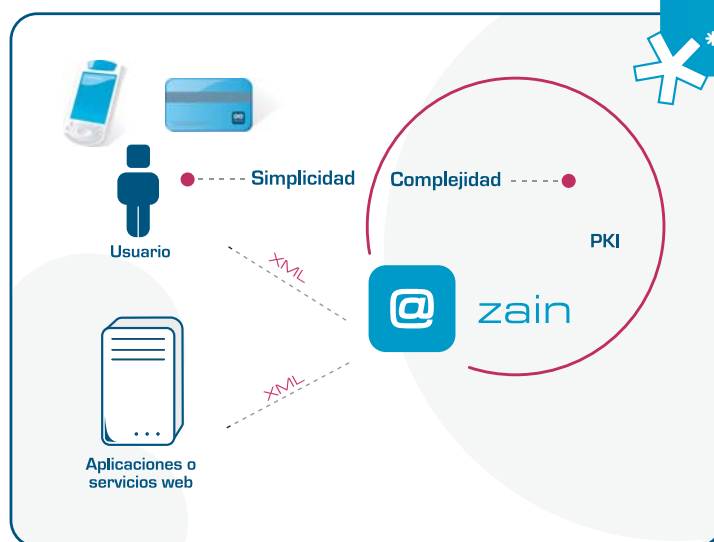
Sinadura Zerbitzuen Plataforma Plataforma de servicios de firma



Zain konfiantzako zerbitzuen plataforma da, segurtasun-zerbitzu global eta estandarizatuen multzoa hartzen duena barne (**kautotzea, baimentzea, sinadura elektronikoa eta datuen babesa**), web-zerbitzu gisa.

Zain es una plataforma de servicios de confianza que incluye un conjunto de servicios de seguridad globales y estandarizados (**autenticación, autorización, firma electrónica y protección de datos**) como servicios Web.

- * Ezartzeko eta mantentzeko erraza
- * Zerbitzu berriak abian jartzeko gutxieneko ahalegina
- * Hardwarearekiko erabateko independentzia
- * Estandar eta premia berriekin bat datorrena
- * Berritasunetara egokitutakoa eta eguneratua
- * Sencillez de implementación y mantenimiento.
- * Minimización de esfuerzo para poner en marcha nuevos servicios.
- * Independencia total del hardware.
- * Alineación con estándares y nuevas necesidades.
- * Adaptación a novedades y actualización.



Zain plataformak aukera emango digu orain arte aplikazioak integratioko ohiko tresnak erabiliz segurtasun-mekanismoz hornitzeak berekin zekarren konplexutasuna gainditzeko. **Plataformaren zerbitzuetara bideratutako arkitekturari** eta informazioa **kudeatzeko sistema** osoari esker, konfiantzako mekanismoak txertatu ahal izan dira negozio-prozesuetan, batzuen eta besteen arteko independentziari bide emanez eta segurtasuneko eta ikuskaritzako politikak modu zentralizatuan kudeatzeko ahalmena eskainiz. Erabateko modularitateak etorkizuneko hazkunde ere bermatuko du, funtzionalitateari nahiz prestazioei begira. Eskalagarritasuna eta jardun-denboraren inguruko eskakizunik zorrotzetara egokitzeko ahalmena ditu ezaugarri.

La plataforma **Zain**, soluciona la complejidad que hasta la fecha suponía el dotar de los mecanismos de seguridad a las aplicaciones mediante el uso de las clásicas herramientas de integración. La **Arquitectura Orientada a Servicios** de la plataforma y su completo **sistema de gestión** de la información simplifican la integración de los mecanismos de confianza en los procesos de negocio, independizándolos unos de otros, y ofreciendo la capacidad de gestión de las políticas de seguridad y auditoria de forma centralizada. Su completa modularidad, garantiza, además, el crecimiento futuro tanto en funcionalidad como en prestaciones, caracterizándose por su escalabilidad y su capacidad para adecuarse a los requerimientos más exigentes de alta disponibilidad.

Zergatik Zain? ¿Por qué Zain?

@sinadura / @firma	Zain	Toolkit Izenpe / Izenpe Toolkit-a
<ul style="list-style-type: none"> * Ez du OCSP erantzunik ematen, ez du erabateko sinadurarik ahalbidetzen (ezta horiek baliozkotzea ere): Hortaz, ez ditu Izenperen ikuspegitik ezinbestekoak diren elementuak eta ez luke atzerako bateragarritasunik ahalbidetuko. * MAPen "CertiCA" taldearen bidezko kudeaketa, ez oso arina. * Funtzionaltasun txikiagoa: oraingoz ez ditu onartzen PDF edo s/mime sinadurak. * Ez du artxibo-sinadurarik eskaintzen ("-a") * Bere baimenak ez dio zerbitzua entitate pribatuei ematea ahalbidetzen. 	<ul style="list-style-type: none"> * Eskakizunetara arin egokitzeal * WEB zerbitzuetarako deiak * Estandarretara egokitutakoa * Aplikazioak integrazteko malgutasuna * Izenpen zuzenean eguneratzea * Euskarria 	<ul style="list-style-type: none"> * Liburutegien erabilera, liburutegiko funtzioetarako deiak konfiguratzea * Edukizaille seguruak sortzea * Zerbitzari guztietan liburutegi berria ordezkatzeta * Edukizailleak mantentzea * Talde kudeatzailea prestatzeko premia
<ul style="list-style-type: none"> * No proporciona respuestas OCSP, no permite firma completa (ni validarlas): por lo tanto carece de elementos imprescindibles desde el punto de vista de Izenpe y no permitiría compatibilidad hacia atrás. * Gestión vía grupo "CertiCA" de MAP, poco ágil. * Menor funcionalidad: no soporta hasta la fecha firma de PDF, s/mime. * No proporciona firmas de archivo ("-a") * Su licencia no permite servicio a entidades privadas 	<ul style="list-style-type: none"> * Adaptación a requerimientos ágil * Llamadas a WEB services * Ajustado a estándares * Flexibilidad en la integración de aplicaciones * Actualización directa en Izenpe * Soporte 	<ul style="list-style-type: none"> * Configurar uso librerías, llamadas a funciones de la librería. * Creación de contenedores seguros * Sustitución en todos los servidores de la nueva librería * Mantenimiento de contenedores * Necesidad de formación al equipo gestor.

Nola izan Zain zerbitzuaren bezero? ¿Cómo ser cliente de Zain?

- * Izenpek eskaera egiteko txantiloia emango dizu eta bertan bilduko ditu aplikazioak egoki konfiguratzeko beharrezkoak diren datuak.
- * Aplikazioari dagokion ziurtagiriaren zati publikoa plataforman hartu behar da barne.
- * Aplikazioak sinadurak zerbitzarian egiten baditu, ezinbestekoa da plataformak helburu horretarako erabiliko den ziurtagiria zaintzea. Izenperen ziurtagiri hauetakoren bat izan beharko duzu:
 - Entitatearena
 - Administrazio-organoarena
 - Aplikazioarena
- * Izenpek ongi-etorri-kita emango dizu, eta bertan egongo da aplikazioei alta ematearen inguruko dokumentazioa, baita tutorialak eta adibideak ere.
- * Izenpek aplikazioaren konfigurazioa barne duen txostena emango dio berorren arduradunari.
- * Izenpe proporcionará una plantilla de solicitud en la que se recogerán los datos necesarios para la correcta configuración de las aplicaciones.
- * La parte pública del certificado con el que se presenta la aplicación debe incluirse en la plataforma.
- * Si la aplicación realiza firmas en servidor, es necesario que la plataforma custodie el certificado que se utilizará para dicho fin. Deberás contar con alguno de los siguientes certificados Izenpe:
 - Entidad
 - Órgano Administrativo
 - Aplicación
- * Izenpe proporcionará un Kit de bienvenida que incluye toda la documentación para dar de alta las aplicaciones, tutoriales y ejemplos
- * Izenpe proporcionará un informe con la configuración de la aplicación al responsable de la misma.

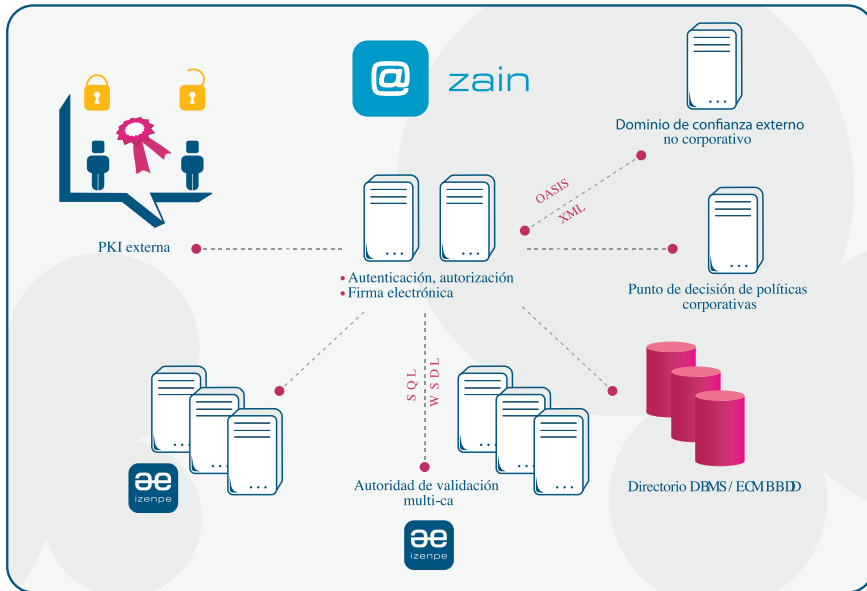
Funtzioak: Funciones:

Zain zerbitzuak gako publikoko azpiegituretan (PKI) oinarritutako konfiantzako zerbitzuen multzoa eskaintzen du, modu estandarrean eta zerbitzuetara bideratuta. Zerbitzu horien erabiltzaile edozein kontsumitzaile-mota izan daiteke, azken erabiltzaile, aplikazio edo beste zerbitzu bat izan.

- * **Kautotzea eta baimentzea.** Kautotzeko eta baimentzeko informazioaren trukea aplikazio korporatiboen eta kanpoko segurtasundomeinuen artean. Horrek web-mailako sarbide bakarraren kontrola ahalbidetuko du (SSO), OASISek definitutako estandarren arabera.
- * **Ziurtagiri digitalak baliozkotzea.** Ziurtagiri-zerbitzuen eskaintzaile ugari ezagutzen ditu eta ziurtagiriei lotutako informazioa uniformetzen. Ziurtagiri estandarrek baliozkotzeko mekanismoak onartzen ditu eta pertsonalizatutako beste edozein mekanismo barne hartzea onartzen du.
- * **Sinadura elektronikoa.** Dokumentu elektronikoa, posta elektronikoa eta web-mezueterako sinadura-formatu gehienak onartzen ditu, sinadura anitzak, denbora-zigilua duten sinadurak eta bititza luzeko sinadurak ere barne direla, sinadura ziurtagiri digitalen indarraldia amaïtu ostean ere baliozkotu ahal izateko.
- * **Datuak zifratzea:** Zifratzeko mekanismoen bidez informazioa babestea, dokumentu elektronikoa izan, posta elektronikoa izan edo web-mezuak izan. Etorkizuneko bertsioetan zifratze-gakoak zaintzeko zerbitzua hartuko da barne, datuetarako sarbidea kontrolatu ahal izateko pertsonen taldeen nahiz konfiantzako sistemen kasuan.
- * **Integrazioko atebidea.** XML datuen elkarren ondoko transformazioen multzoa definitzea eta beren artean konektatzea ahalbidetzen du, plataformako hainbat zerbitzurekin elkarreaginean, prozesuen eta aplikazio edo sareen artean konfiantzako atebide gisa jardunez. Bidegabeko sartzetik gabe aplikazioak integratzea ahalbidetzen du.
- * **Auditoretza eta kontabilitatea.** Plataformako zerbitzu-osagai guztiek sortutako arrasto-informazio osoa modu zentralizatu, uniforme eta seguruan kudeatzen duen zerbitzua. Horien erabilera eta/edo kontsumoko informazioa ere bai.
- * **Objektuen eta entitateen kudeaketa.** Plataformak kudeatzen dituen objektuen eta entitateen ikuspegi uniforme XML formatuan eskaintzen duen broker-a, datuen berariazko formatuak (XML, ASN.1, testua eta abar) eta informazio-iturriak (LDAP, SQL, fitxategiak eta abar) guztiz maskaratu eta horiek web-zerbitzu gisa erabiltzea ahalbidetuz.

Zain ofrece un conjunto completo de servicios de confianza basados en infraestructuras de clave pública (PKI), de una forma estándar y orientada a servicios, los cuales pueden ser usados por cualquier tipo de consumidor, ya sea usuario final, aplicación u otro servicio.

- * **Autenticación y autorización.** Intercambio de información de autenticación y autorización entre las aplicaciones corporativas y dominios de seguridad externos, haciendo posible el control de acceso único a nivel de web (SSO), mediante los estándares definidos por OASIS.
- * **Validación de certificados digitales.** Reconocimiento de múltiples prestadores de servicios de certificación, uniformizando la información asociada a los certificados. Soporta los mecanismos de validación de certificados estándares y admite la integración de cualquier otro mecanismo personalizado.
- * **Firma electrónica.** Soporta la mayoría de los formatos de firma para documentos electrónicos, correo electrónico y mensajería web; incluyendo firmas múltiples, firmas con sello de tiempo y firmas longevas para poder validar la firma una vez transcurrido el período de vigencia de los certificados digitales.
- * **Cifrado de datos:** Protección de la información mediante mecanismos de cifrado; ya sea documentos electrónicos, correo electrónico o mensajería web. En futuras versiones se incluirá el servicio de custodia de las claves de cifrado, controlando el acceso a los datos para los grupos de personas o sistemas de confianza.
- * **Pasarela de integración.** Permite definir y conectar entre sí un conjunto de transformaciones sucesivas de datos XML, en interacción con los diferentes servicios de la plataforma, actuando de pasarela de confianza entre los procesos y aplicaciones o redes. Posibilita una integración de las aplicaciones con cero intrusiones.
- * **Auditoría y Accounting.** Servicio que gestiona de forma centralizada, uniforme y segura toda la información de traza generada por todos los componentes de servicio de la plataforma, así como la información de uso y/o consumo de los mismos.
- * **Gestión de objetos y entidades.** Broker que ofrece una vista uniforme en XML de los objetos y entidades gestionados por la plataforma, enmascarando totalmente los formatos específicos de los datos (XML, ASN.1, Texto, etc.) y las diferentes fuentes de información (LDAP, SQL, Ficheros, etc.) y permitiendo usarlos como servicio web.



Sinadura electrónico bat sortzen denean, sinatzaileak ez ditu barne hartzen agirian sinaduraren balioa frogatzen duten ebidentziak. Aipatutako ebidentzia elektronikorik automatikoki jasotzen dira sinadura elektronikoko bakoitza egiaztatzeko prozesuan zehar. Ondoren sinadurak egiaztatzeko, ebidentzia horiek funtsezko datu gisa artxibatuko dira. Horiek atera eta hirugarrenek erabili ahal izango dituzte, frogatzeko elementu gisa.

Ebidentzia elektronikoen sinaduraren uneri buruzko informazioa dute beren baitan, baita konfiantzako katea osatzen duten ziurtagiri guztiei eta une horretako ziurtagirien egoerari buruzko informazio fidagarria ere.

Cuando se genera una **firma electrónica**, el firmante no incorpora en el documento las evidencias que otorgan el valor probatorio de dicha firma. Dichas evidencias electrónicas se recogen de forma automática durante el proceso de verificación de cada firma electrónica. Para realizar posteriores verificaciones de las firmas, estas evidencias se archivarán como datos fundamentales, que podrán extraerse y usarse por terceros, como elementos probatorios.

Las evidencias electrónicas comprenden la información acerca del momento que se produjo una firma, todos los certificados que conforman la cadena de confianza y la información fiable del estado de los certificados en dicho instante.

* + Zain buruz+ sobre Zain

Bere funtzioak hainbat zerbitzu-motatan multzoka daitezke:

- * Gakoak kudeaketa. Erregistratzeko, ezeztatzeko, kontsultatzeko eta egiaztatzeko zerbitzuak.
- * Objektuen eta entitateen kudeaketa. Objektu eta entitateei buruzko informazioa erregistratzea, kontsultatzea eta aldatzea, bereziki identifikazioko informazioa denean.
- * Erregistratutako entitateak kautotzeko, baimentzeko eta horien sarbidea kontrolatzeko zerbitzua.
- * Erregistratutako entitateak kautotzea, baimentzea eta horien sarbidea kontrolatzea ahalbidetzen da, sarbide bakarreko kontrolerako eta plataforma osoko federaziorako baimena emanez (erabilzaile, web-zerbitzu eta aplikazioen artean).
- * Sinadura digitala. Sinadura digitalak sortzeko eta egiaztatzeko zerbitzua.
- * Hainbat ziurtagiri-zerbitzu onartzen dira eta sinadurak denboran zehar egiaztatzeko beharrezkoak diren ebidentzia elektronikoen sortzea ahalbidetzen da.
- * Zifratze digitala. Datuak zifratzeko, deszifratzeko, gutun-azaleratzeko eta gutun-azaletik ateratzeko zerbitzuak.
- * Ukorik ez digitala. Ebidentzia digitalak sortzeko eta baliozkotzeko zerbitzua, gehienetan sinadura elektronikorekin batera.

Sus funciones pueden agruparse en diferentes clases de servicios

- * Gestión de claves. Servicios de registro, revocación, consulta y verificación.
- * Gestión de objetos y entidades. Servicios de registro, consulta, y modificación de información sobre objetos y entidades, en particular, información de identificación.
- * Servicios de autenticación, autorización y control de acceso de las entidades registradas.
- * Se permite la autenticación, autorización y control del acceso de las entidades registradas haciendo posible el control de acceso único y federación en toda la plataforma (entre usuarios, servicios web y aplicaciones).
- * Firma digital. Servicios de generación y verificación de firmas digitales.
- * Se reconocen diferentes prestadores de certificación y se permite generar las evidencias electrónicas necesarias para la verificación de firmas a lo largo del tiempo.
- * Cifrado digital. Servicios de cifrado, descifrado, ensobrado y des ensobrado de datos.
- * No-repudio digital. Servicios de generación y validación de evidencias digitales, generalmente acompañadas de firma electrónica.

Zain zerbitzuaren onurak: Beneficios Zain:

- * **Zerbitzuetara bideratutako integrazio estrategikoa.** Zain zerbitzuak eskaintzen duen soluzioari esker, segurtasun-funtzioak konfiantzako zerbitzu gisa integra daitezke aplikazioetan, zerbitzuetara bideratutako inguruneetan (SOA). Hori bat dator erabat informazio-sistema korporatiboen ingeniartzatza-prozesuetan nagusi den jardunarekin eta, horri esker, malgutasun gutxiko software-arkitekturen nagusitasunaren etapa itxi ahal izango dugu.
- * **Negozio-prozesuetara gehiago bideratutakoa.** Erabakiak hartzeko prozesuetan, giltzarri da zehatz-mehatz jakitea informazioak une oro duen konfiantzamaile zein den, horien egileak zein diren eta zein atributu dituzten. Zain plataformaren ezaugarri bereizleetako bat da aplikazioei datu horiek hornitzeko gaitasuna izatea, betiere horien logika asko sinplifikatuz, fidagarritasun handiagoa emanez eta horietan aldaketak egitea saihestuz, segurtasun-zerbitzu berriak edo kautotzeko mekanismo berriak aitortzeko dinamikaren bidetik (adibidez: baliozkotzeko autoritateak edo denbora zigilatzea).
- * **Erraztasun eta kontrol handiagoa** Konfiantza-politika komunen multzoa modu zentralizatuan ezartzea eta mantentzea ahalbidetzen du, baita kontrol eta ikuskaritzarako sistema zentralizatu ere. Adibide gisa, ziurtapen-autoritateen (CAen) kopuruarekin zerikusia duen konplexutasuna eta baliozkotzeko mekanismoak (VAK) kentzea nabarmen dezakegu, baita konfiantzako beste domeinu batzuekin aplikazioetara modu gardenean federatzea ahalbidetzea edo negozio-prozesu kritikoetan kriptografiaren erabilera arautzeko gaitasuna eskaintzea ere.
- * **Aplikazioak integratzeko malgutasuna.** Zain plataformak integratzeko metodo guztiak hartzen ditu bere baitan, eta hainbat estrategia ezartzea ahalbidetzen du. Zain plataformako zerbitzuak hiru modutan erabil daitezke:
 - (i) web-zerbitzu gisa, Axis edo .NET bezalako tresna ezagunak erabiliz edo eskaerak eta erantzunak XPath eta XSLT bidez manipulatuaz;
 - (ii) ZAIN plataformaren zerbitzuak modu gardenean kontsumitzen dituen eta aplikazioetan integratuta dagoen API baten bidez, edo
 - (iii) integrazioko atebidea erabiliz, aplikazioak aldatzea saihestuz eta XML Pipeline lengoaiaren bidez datuak modu kateatuan prozesatzeko gaitasunari esker.
- * **Inbertsioa babesten du, estandarren euskarri zabala eskaintzen duelako.** Izaera bera dela eta, Zain ereduak inbertsioa babestea bermatzen du, izan ere, nazioarteko guneetan aitortzen diren eta industrian kontuan hartzen diren segurtasunestandarrik hartzen ditu barne. Hartara, ez ditu baztertzen azken bezero potentzialak, erabiltzaileak nahiz aplikazioak, eta aplikazio gehiagori eskaintzen die, erraz, babesteko mekanismo egokia.
- * **Integración estratégica orientada a servicios.** Zain ofrece una solución que permite integrar las funciones de seguridad en las aplicaciones como servicios de confianza en entornos orientados a servicios (SOA), en clara alineación con la práctica predominante en los procesos de ingeniería de los sistemas de información corporativos y cerrando una etapa de predominio de arquitecturas de software poco flexibles.
- * **Mayor orientación a los procesos de negocio.** En los procesos de toma de decisiones es clave conocer con exactitud cuál es el nivel de confianza que la información tiene en todo momento, quiénes son sus autores y cuáles son sus atributos. Una de las características únicas de la plataforma Zain es su capacidad para suministrar dichos datos a las aplicaciones, simplificando drásticamente su lógica, aportando mayor fiabilidad y evitando la realización de cambios en las mismas, en la dinámica de reconocimiento de nuevos servicios de seguridad o nuevos mecanismos de autenticación (por ejemplo: autoridades de validación o de sellado de tiempo).
- * **Mayor facilidad y control.** Permite el establecimiento y mantenimiento centralizado de un conjunto de políticas de confianza comunes así como un sistema centralizado de control y auditoría. Como ejemplos cabe destacar la eliminación de la complejidad asociada al número de autoridades de certificación (CAs) y los diferentes mecanismos de validación (VAs) el permitir la federación con otros dominios de confianza de forma transparente a las aplicaciones o bien el ofrecer la capacidad para regular el uso de criptografía en los procesos críticos de negocio.
- * **Flexibilidad en la integración de aplicaciones.** Zain cubre la totalidad de métodos de integración, permitiendo la adopción de diferentes estrategias. Los servicios de Zain se pueden usar de tres formas:
 - (i) como servicios web, usando populares herramientas como Axis o .NET o manipulando las peticiones y respuestas mediante XPath y XSLT;
 - (ii) mediante una API integrada en las aplicaciones que consume de forma transparente los servicios de Zain o,
 - (iii) usando la pasarela de integración, que evita modificar las aplicaciones y aporta la capacidad de procesamiento de datos de forma encadenada mediante el lenguaje XML Pipeline.
- * **Protege la inversión, al ofrecer un amplio soporte de los estándares.** Por su propia naturaleza, el modelo de Zain garantiza la protección de la inversión puesto que incorpora los estándares de seguridad reconocidos en foros internacionales y adoptados por la industria, no limitando a los clientes finales potenciales, usuarios o aplicaciones, y ofreciendo el mecanismo de protección adecuado a un mayor número de aplicaciones de forma sencilla

Denbora-zigilu elektronikoa El sello de tiempo electrónico

Denbora-zigiluek modu ukaezinean bermatzen dute data jakin batean dokumentu elektronikoa izan bazela (esate baterako, kontratuen, ikerketari buruzko datuen, jabetza intelektualaren edo historial klinikoaren kasuan). Denbora-zigiluaren fidagarritasuna honetan datza: konfiantzako hirugarren batek (TTP), gehienetan denbora zigilatze autoritate (TSA) deitu ohi denak, erlazionatzen du data zehatz bat dokumentu elektronikoarekin, eta inoiz ez sinatzaileak berak.

Denbora-zigiluak ukorik eza edo ukaezintasuna ematen die dokumentu elektronikoari, sinadura elektronikoarekin batera erabiliz gero. Ikuspegi teknikotik begiratuta, denborazigilua beharrezkoa da:

- * sinadura bat ziurtagiri digital jakin batek (iraungi egin delako edo ezeztatu egin delako) balioa galdu aurretik edo ondoren sortu den zehazteko, eta
- * sinadura hori denboran zehar egiaztatu ahal izateko, hain zuzen ere, sinadurari balio frogatzailea ematen dioten ebidentzia elektronikoak iraungitzen direnetik aurrera.

Los sellos de tiempo avalan de forma irrefutable la existencia de un documento electrónico en una fecha concreta (p.e. **contratos, datos sobre investigación, propiedad intelectual, historial clínico**). La fiabilidad del sello de tiempo se fundamenta en que es una **Tercera Parte de Confianza (TTP)**, habitualmente denominada **Autoridad de Sellado de Tiempo (TSA)**, quien relaciona una fecha concreta con el documento electrónico y nunca el propio firmante.

El sello de tiempo, usado juntamente con la firma electrónica, confiere a los documentos electrónicos el carácter de no repudio o de **irrefutabilidad**. Desde la perspectiva técnica, el sello de tiempo es necesario para:

- * determinar si una firma se ha generado antes o después de que un certificado digital pierda su validez (por expiración o revocación) y
- * para poder verificar dicha firma a lo largo del tiempo, más allá de la fecha de expiración de las evidencias electrónicas que otorgan el valor probatorio a la firma.

Sinadura elektronikoen motak Tipos de firmas electrónicas

XAdES (ETSI TS 101 903) eta CAAdES (ETSI TS 101 733) estandarrek lau sinadura-mota bereizten dituzte:

- * Oinarrizko sinadura (ES). Sinaduraren data ez du denbora-zigilurik eta sinatzaileak berak aitortzen du sinaduraren data.
- * Denbora-zigilua duen sinadura (ES-T). TSA batek bermatzen du sinaduraren data.
- * Baliozkotzeko informazio osoa duen sinadura (ES-C). Ziurtapen-kateari buruzko informazioa eta ziurtagiriaren egoerari buruzko informazioa eranstean ditu.
- * Ebidentzia elektronikoak dituen sinadura, edo artxibo-sinadura (ES-A) izenarekin ezagutzen dena. Denbora-zigilua duen baliozkotzeko informazio osoa barne hartu ondoren, sinadura hurrenez hurren freskatuko da denbora-zigilu gehigarriekin, ziurtagiriak iraungi baino lehen edo algoritmo kriptografikoek fidagarritasuna galdu baino lehen. Gisa honetako sinadurak dira bizitza luzeko sinadura elektronikoetarako oinarri.

Los estándares XAdES (ETSI TS 101 903) y CAAdES (ETSI TS 101 733) distinguen entre cuatro tipos de firma:

- * Firma básica (ES), cuya fecha de firma no está sellada temporalmente, sino que es el firmante quien declara la fecha de firma.
- * Firma con sello de tiempo (ES-T), cuya fecha de firma está avalada por una TSA.
- * Firma con información completa de validación (ES-C), añade información sobre la cadena de certificación y la información del estado de los certificados.
- * Firma con evidencias electrónicas, o también conocida con la firma de archivo (ES-A). Una vez incorporada la información completa de validación con sellado de tiempo, la firma se refrescará sucesivamente con sellos de tiempo adicionales antes de que los certificados expiren o de que los algoritmos criptográficos pierdan fiabilidad. Este tipo de firmas son la base para las firmas electrónicas longevas.

Ezaugarri teknikoak Características técnicas



- * Web-zerbitzuen azpiegitura: WSDL, UDDI eta SOAP
- * Segurtasun-zerbitzuak: OASIS WSS, SSL/TLS, OASIS SAML eta OASIS DSS sinadura elektronikoko zerbitzua. Etorkizuneko bertsioetan OASISen XACML, Liberty ID-WSF/WS-Trust/WS-Federation estandarrek eta XKMS gakoaren kudeaketa hartuko dira barne.
- * Gutun-azal digitaleko estandarrek: PKCS#7, IETF CMS, ETSI TS 101733 - CAAdES, W3C XML-DSig, W3C XML-Enc, ETSI TS 101903 - XAdES, PDF dokumentuetarako sinadura, IETFren arabera eta S/MIME.
- * Denbora-zigilu digitalerako euskarria: Denbora zigilatze IETF TSP protokoloa.
- * Ziurtagiri digitalen egoera egiaztatzea: CRLen, IETFren OCSP protokoloaren eta pertsonaliza daitezkeen bestelako mekanismoen bidez.
- * Direktorio-euskarria: LDAP protokoloa.
- * Onartutako datu-baseen sistemak: Oracle, Microsoft SQL Server edo MySQL.
- * Dokumentu-kudeatzailearen euskarria: HTTP/WebDAV protokoloa. Kontsultatu onartutako DMS/ECM-etarako.
- * HSM euskarria: PKCS #11 gailuak, Safelayer-ek homologatutakoak.
- * Infrastruktura de servicios web: WSDL, UDDI y SOAP.
- * Servicios de seguridad: OASIS WSS, SSL/TLS, OASIS SAML y Servicio de firma electrónica OASIS DSS. En futuras versiones se incorporarán los estándares de OASIS XACML, Liberty ID-WSF/WS-Trust/WS-Federation y gestión de claves XKMS.
- * Estándares de sobre digital: PKCS#7, IETF CMS, ETSI TS 101733 - CAAdES, W3C XML-DSig, W3C XML-Enc, ETSI TS 101903 - XAdES, Firma para documentos PDF según IETF y S/MIME.
- * Soporte de sellado de tiempo digital: Protocolo de Sellado de tiempo IETF TSP.
- * Verificación de estado de certificados digitales: Mediante CRLs, protocolo OCSP de IETF y otros mecanismos personalizables.
- * Soporte de directorio: Protocolo LDAP.
- * Sistemas de Base de Datos soportados: Oracle, Microsoft SQL Server o MySQL. Dokumentu-kudeatzailearen euskarria: Dokumentu-kudeatzailearen euskarria: Protocolo HTTP/WebDAV. Consultar para DMS/ECMs soportados.
- * Soporte de HSM: Dispositivos PKCS #11 homologados por Safelayer.



zain

Beato Tomás de Zumárraga 71 - 1ª Planta . 01008 . Vitoria - Gasteiz
www.izenpe.com . info@izenpe.com . Tel.: 945 017 490