



Confederación
Empresarial de
Bizkaia

Bizkaiko
Enpresarien
Konfederazioa

JORNADA: FIRMA ELECTRONICA, UNA HERRAMIENTA PRACTICA PARA LA EMPRESA

Bilbao, 6 de abril 2011





- Introducción a la firma electrónica



- Aproximación a conceptos técnicos

■ Firma Digital ≠ Firma Electrónica

- Firma digital : es un concepto técnico (matemático)
- Firma Electrónica: es un concepto jurídico



(A) - Emisor del Mensaje.



Encriptación Simétrica



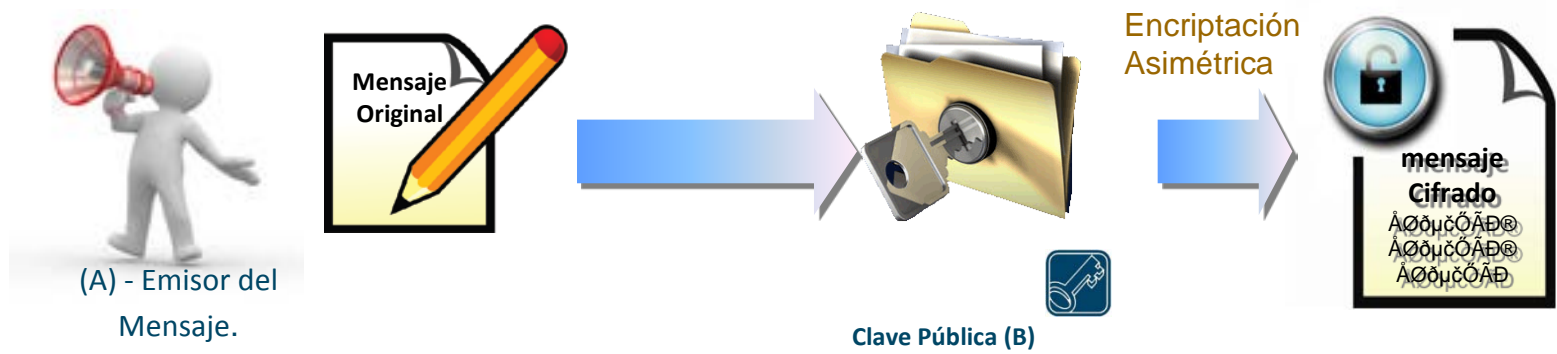
Clave Secreta.

Encriptación simétrica: Se utiliza la misma llave para la encriptación y la descriptación. En otras palabras, los algoritmos en los que la clave en origen y destino es la misma.



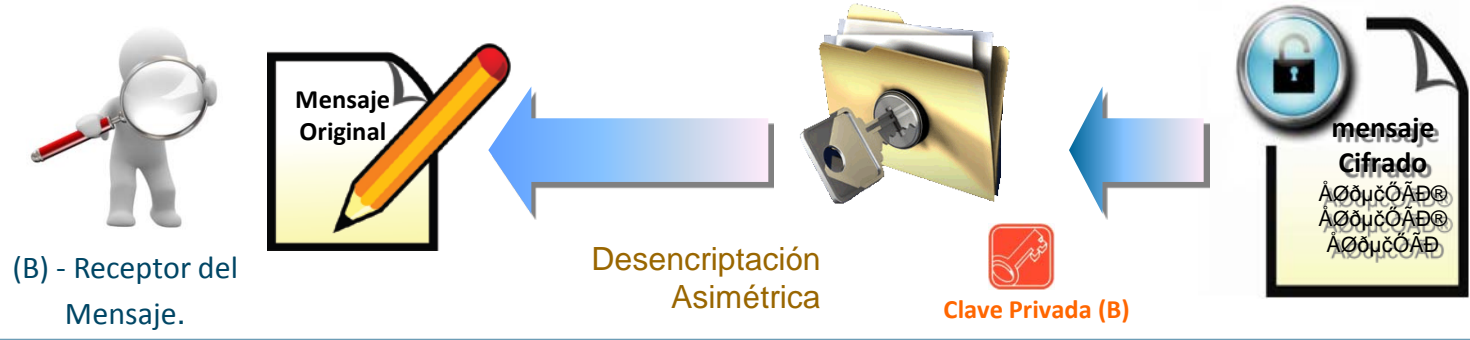
Desencriptación Simétrica

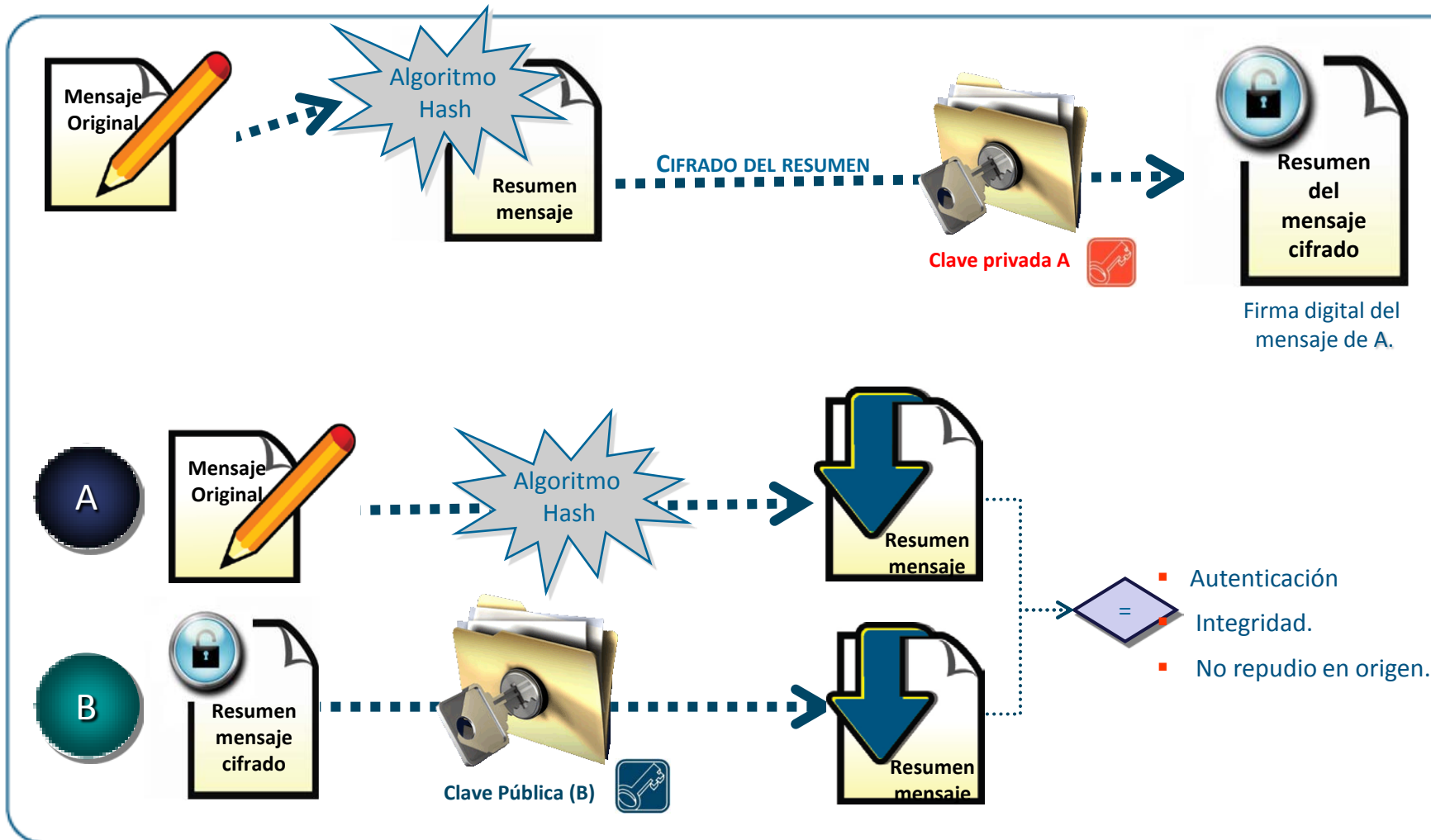




Encriptación Asimétrica: se utilizan algoritmos en los que la clave origen y destino es diferente. A tales efectos, se utiliza una clave pública y una clave privada generados por un procedimiento matemático y relacionadas matemáticamente, de forma que un texto al que se aplica una de las claves sólo puede obtenerse de nuevo al aplicarle la otra clave.

La clave pública es tratada por una Autoridad de Certificación (CA) generando un certificado





- La clave privada del usuario sólo debe ser conocida por el propio usuario y la clave pública puede ser dada a conocer a los demás usuarios.
- Para garantizar la privacidad de las claves privadas se recurre a soporte físicos.
- Para garantizar que una clave pública pertenece a un determinado usuario se utilizan los **certificados electrónicos**.
- Certificado Electrónico: Documento electrónico que asocia una clave pública con la identidad de su propietario, una persona física o jurídica.



Clave Privada.



Clave Privada.
(Soporte Seguro).



Clave Pública.



Clave Pública.

- Un **certificado digital** es un documento digital mediante el cual un tercero de confianza (una autoridad de certificación) acredita electrónicamente la **autenticidad de la identidad** de una persona física, persona jurídica u otro tipo de identidad como lo puede ser, por ejemplo, una URL de un sitio Web y la correspondencia con una clave pública.
- Para ello este tercero de confianza exige los requisitos para identificar con garantías absolutas la identidad acreditada. Si es una persona particular, por ejemplo, le exigirá que se persone con su DNI, en el caso de expedir un certificado para una persona jurídica como una empresa, se le pedirá la correspondiente documentación como lo pueden ser las escrituras de constitución de la sociedad.

X.509 v3



X.509v3

Certificado de una Entidad

Identificación del titular del certificado



Clave **Pública** del titular

DATOS DE LA AUTORIDAD DE CERTIFICACIÓN



Fechas de expedición y expiración del Certificado

Usos del certificado

Nº de serie: E524 F094 6000 5B80 11D3 3A19 A976 471D

Algoritmo de encriptación empleado para firmar

- ¿Qué es una Autoridad de Certificación?:
 - Dos usuarios que no se conocen podrán confiar entre sí si ambos tienen relación con una tercera parte que dé fe de la fiabilidad de los dos a través de los certificados.
 - La forma en la que esa tercera parte de confianza avalará que el certificado es de fiar es mediante su firma digital sobre el certificado. En otras palabras:
 - Aceptar la precisión de la información certificada.
 - Aceptar la articulación de un proceso en el que se inscriba (firma-creación-datos)
 - Aceptar la articulación de un proceso de verificación (firma-verificación-datos) + (firma-verificación-datos).

OBLIGACIONES DE UNA CA

- Publicar la Declaración de Prácticas de Certificación
- Garantías en cuanto a confidencialidad datos.
- Utilización de Sistemas Fiables de Seguridad.
- Tomar medidas contra la falsificación y custodio de información y procedimientos.
- Mantener un CRL (Listado de Certificados Revocados) actualizado.
- Garantizar un servicio de consulta rápido.

ALGUNAS CA's

- CERES
- CAMERFIRMA
- FIRMAPROFESIONAL
- GEN VALENCIANAA
- C ABOGACÍA
- Agencia Notarial de Certificación
- IZENPE
- CATCERTi
- psCA
- ...



- Aproximación a conceptos legales

- **La Ley 59/2003 de firma electrónica reconoce tres tipos de firma electrónica:**
 - **firma electrónica** es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante . Ejemplo Usuario-Password.
 - **firma electrónica avanzada** firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.
 - **firma electrónica reconocida** equiparada a la firma manuscrita. Esta realizada con un dispositivo seguro de creación de firma y amparada por un certificado reconocido. **LA FIRMA RECONOCIDA TIENE LOS MISMOS EFECTOS JURÍDICOS QUE LA FIRMA MANUSCRITA.**
- Establece las características del Certificado reconocido:
 - Comprobación de la identidad y demás circunstancias.
 - La fiabilidad y garantía de los servicios de certificación.
 - El contenido mínimo debe incluir el certificado:
 - ETSI TS 101862
 - RFC3039

■ Tipos de certificados:

- Certificados de persona física
- Certificados de persona jurídica
- Certificados de atributos..



- Legislación relacionada

■ **LEY 11/2007, de 22 junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.**

Esta nueva ley para reconoce a los ciudadanos su derecho a relacionarse electrónicamente con las administraciones públicas. Los puntos más destacables de la Ley son:

- Los ciudadanos verán reconocidos nuevos derechos en sus relaciones con las administraciones públicas.
- La creación de la figura del Defensor del Usuario.
- Las administraciones tendrán la obligación de hacer estos derechos efectivos a partir de 2009.
- Los trámites y gestiones podrán hacerse desde cualquier lugar, en cualquier momento.
- La administración será más fácil, más ágil y más eficaz.
- Los ciudadanos pasan a tomar el mando en sus relaciones con la administración.
- Es una ley de consenso. En su elaboración han participado todas las administraciones, de ciudadanos, de partidos, de empresas y asociaciones.
- Sólo dos países tienen una norma con un contenido tan avanzado.

■ Sede electrónica

- La sede electrónica es aquella dirección electrónica disponible para los ciudadanos cuya titularidad, gestión y administración corresponde a una Administración Pública, órgano o entidad administrativa en el ejercicio de sus competencias.
- Cada Administración Pública determinará las condiciones e instrumentos de creación de las sedes electrónicas, con sujeción a los principios de publicidad oficial, responsabilidad, calidad, seguridad, disponibilidad, accesibilidad, neutralidad e interoperabilidad
- Las sedes electrónicas dispondrán de sistemas que permitan el establecimiento de comunicaciones seguras siempre que sean necesarias.
- La publicación de los diarios o boletines oficiales en las sedes electrónicas tendrá, en las condiciones y garantías que cada Administración Pública determine, los mismos efectos que los atribuidos a su edición impresa.
- Las sedes electrónicas utilizarán, para identificarse y garantizar una comunicación segura con las mismas, sistemas de firma electrónica basados en certificados de dispositivo seguro o medio equivalente.
- Los sistemas de información que soporten las sedes electrónicas deberán garantizar la confidencialidad, disponibilidad e integridad de las informaciones que manejan.

- ***Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.***
- Las sedes electrónicas (órganos de la Administración General del Estado y organismos públicos vinculados o dependientes) se crearán mediante orden del Ministro correspondiente o resolución del titular del organismo público, que deberá publicarse en el «Boletín Oficial del Estado».
- Contenido mínimo :
 - Ámbito de aplicación de la sede, que podrá ser la totalidad del Ministerio u organismo público, o uno o varios de sus órganos con rango, al menos, de dirección general.
 - Identificación de la sede, así como del órgano u órganos titulares y de los responsables de la gestión y de los servicios.
 - Información necesaria para la correcta utilización de la sede.
 - Medios disponibles para la formulación de sugerencias y quejas.
 - Normas de creación del registro o registros electrónicos accesibles desde la sede.

■ Nuevo decreto de administración electrónica del gobierno vasco:

Regula la utilización de medios electrónicos, informáticos y telemáticos en los procedimientos administrativos.

La finalidad del nuevo Decreto de Administración Electrónica es desarrollar las bases establecidas en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, y sus normas de desarrollo.

El nuevo Decreto regulará:

- [la sede electrónica de la Administración de la Comunidad Autónoma de Euskadi](#)
- la forma de identificarse y autenticarse por parte de la ciudadanía y de la Administración, en los trámites electrónicos;
- las comunicaciones y las notificaciones electrónicas; el archivo, el documento y el expediente electrónicos.

<http://www.slideshare.net/PIPEJGV/identificacion-y-autenticacion-1>

- **Creación de la sede electrónica:**

- DFG: <https://www.gfaegoitza.net/es/html/25/212.shtml>

La DFB y la DFA tienen preparada la normativa pero todavía no ha sido publicada.

- Orden EHA/962/2007: disposiciones sobre facturación telemática y conservación electrónica de facturas.
- Real Decreto 1496/2003: reglamento que regula las obligaciones de facturación electrónica.
- Directiva 2001/115/CE que simplifica las condiciones impuestas a la facturación electrónica.

■ Ley de contratos del sector público

Artículo 42. Perfil de contratante.

- 1. Con el fin de asegurar la transparencia y el acceso público a la información relativa a su actividad contractual, y sin perjuicio de la utilización de otros medios de publicidad en los casos exigidos por esta Ley o por las normas autonómicas de desarrollo o en los que así se decida voluntariamente, los órganos de contratación difundirán, a través de Internet, su perfil de contratante. La forma de acceso al perfil de contratante deberá especificarse en las páginas Web institucionales que mantengan los entes del sector público, en la Plataforma de Contratación del Estado y en los pliegos y anuncios de licitación.
- 2. El perfil de contratante podrá incluir cualesquiera datos e informaciones referentes a la actividad contractual del órgano de contratación, tales como los anuncios de información previa contemplados en el [artículo 125](#), las licitaciones abiertas o en curso y la documentación relativa a las mismas, las contrataciones programadas, los contratos adjudicados, los procedimientos anulados, y cualquier otra información útil de tipo general, como puntos de contacto y medios de comunicación que pueden utilizarse para relacionarse con el órgano de contratación. **En todo caso deberá publicarse en el perfil de contratante la adjudicación provisional de los contratos.**
- 3. **El sistema informático que soporte el perfil de contratante deberá contar con un dispositivo que permita acreditar fehacientemente el momento de inicio de la difusión pública de la información que se incluya en el mismo.**
- 4. La difusión a través del perfil de contratante de la información relativa a los procedimientos de adjudicación de contratos surtirá los efectos previstos en el [Título I del Libro III](#).



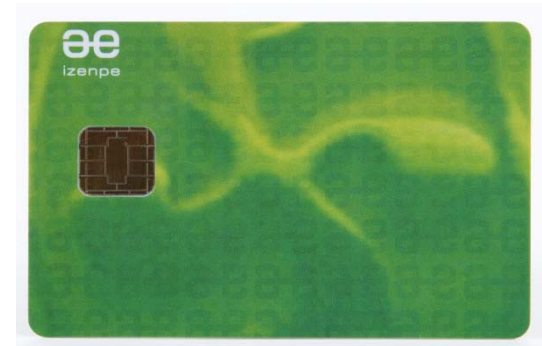
- Infraestructura básica de firma electrónica



- Diferentes certificados,
diferentes finalidades ¿cómo elegir?

■ Certificado de persona física/ciudadano

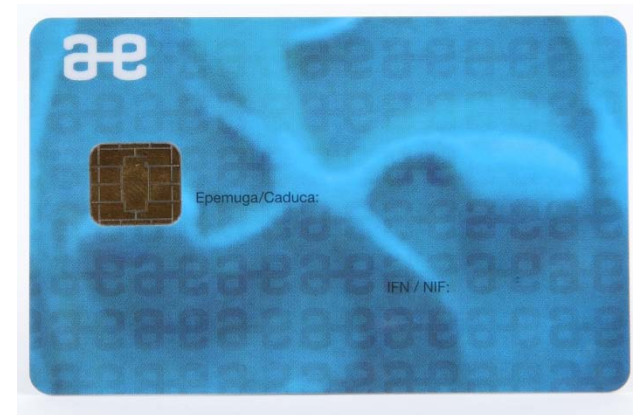
- DNle (tarjeta)
- Certificado ciudadano Izenpe (tarjeta verde/ tarjeta ONA)
- Clase 2 CA de la FNMT (PC/tarjeta)
-



- Solicitante = Suscriptor = Poseedor de Claves = persona física
- Firmante= persona física

■ Certificado de persona jurídica

- Certificado entidad Izenpe
- Certificado entidad Camerfirma
-
- Alojado en tarjeta o HSM



- Solicitante = Suscriptor = Persona jurídica
- Poseedor de Claves = persona apoderada para solicitar la firma
- Firmante = Persona jurídica

■ Certificado atributos

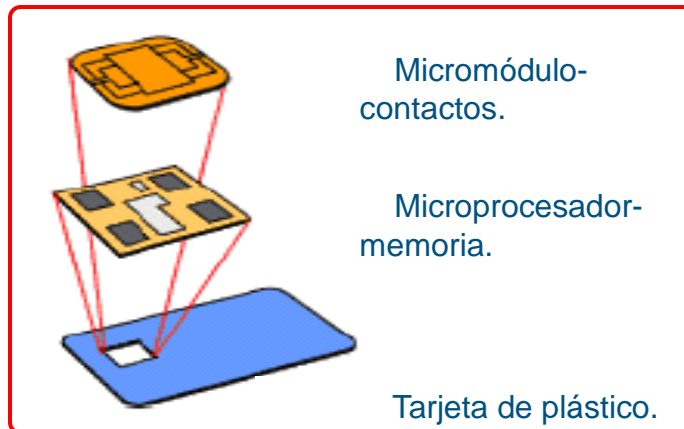
- Condición de colegiado, titular, funcionario,....
 - Certificado corporativo Izenpe
 - Certificado representante Camerfirma
 - Certificado firma profesional
 -
 - Alojado en tarjeta o token usb o microsd
-
- Solicitante = Suscriptor = Persona jurídica
 - Poseedor de Claves = persona física que ostenta los atributos indicados...
 - Firmante= persona física



- Dispositivos seguro de creación de firma

- **Artículo 24 ley 59/2003**
- **Un dispositivo seguro de creación de firma es un dispositivo que ofrece al menos las siguientes garantías:**
 - Que los datos utilizados para la generación de la firma pueden producirse sólo una vez y asegura razonablemente su secreto.
 - Que existe una seguridad razonable de que los datos utilizados para la generación de la firma no pueden ser derivados de los de verificación de firma o de la propia firma y de que la firma esta protegida contra falsificación con la tecnología existente en cada momento.
 - Que los datos de creación de firma pueden ser protegidos de forma fiable por el firmante contra su utilización por terceros
 - Que el dispositivo utilizado no altera los datos o el documento que deba firmarse ni impide que éste se muestre al firmante antes del proceso de firma

- Una tarjeta inteligente (smart card), o tarjeta con circuito integrado (TCI), es cualquier tarjeta del tamaño de un bolsillo con circuitos integrados que permiten la ejecución de cierta lógica programada.
- tarjetas microprocesadas avanzadas en las que hay módulos hardware para la ejecución de algoritmos usados en cifrados y firmas digitales

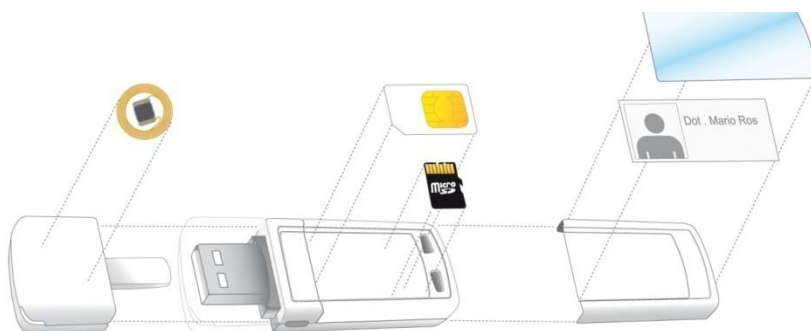


■ Definición:

- Un HSM es un dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas y suele aportar aceleración hardware para operaciones criptográficas.



- Las tarjetas microSD o Transflash corresponden a un formato de tarjeta de memoria flash más pequeña .Mide tan solo 15 × 11 × 0,7 milímetros, lo cual le da un área de 165 mm².
- Principal uso para incorporar a teléfonos móviles, o tokens usb



- Un token de seguridad (también token de autenticación o token criptográfico) es un dispositivo electrónico que se le da a un usuario autorizado de un servicio computarizado para facilitar el proceso de autenticación.

Los *tokens* electrónicos tienen un tamaño pequeño que permiten ser cómodamente llevados en el bolsillo o la cartera y son normalmente diseñados para atarlos a un llavero. Los *tokens* electrónicos se usan para almacenar claves criptográficas como [firmas digitales](#), o [datos biométricos](#) como las huellas digitales. Algunos diseños se hacen a prueba de alteraciones, otro pueden incluir teclados para la entrada de un [PIN](#)





- ¿Qué dispositivo utilizar en cada caso?

- Los certificados de persona física se suelen alojar en tarjetas criptográficas
- Los certificados de entidad se pueden alojar en tarjeta criptográfica o en hsm, es conveniente alojarlos en hsm cuando se utilizan en procedimientos intensivos (ej la facturación, visado de documentos,...)
- Certificados de atributos / corporativos:
 - Tarjetas cuando a la tarjeta se le da otra utilidad (control de entrada)
 - MicroSD para el personal que dispone de mucha movilidad, ya que la microSD se puede alojar a su vez en un móvil o en un token usb que se puede conectar al PC.



- Validación de la firma

- Siempre que recibimos un documento firmado electrónicamente, es obligación del receptor comprobar la validez de la firma. ¿Cómo?
- Es una operación que se realiza automáticamente en dos pasos
 - Comprobación matemática
 - Comprobación de la validez del certificado
 - CRL
 - OCSP

- Cuando una autoridad de certificación emite un certificado digital lo hace con un periodo máximo de validez.
- Sin embargo, existen otras situaciones que pueden invalidar el certificado digital aún cuando no ha caducado, de manera inesperada:
 - El usuario del certificado cree que su [clave privada](#) ha sido robada.
 - Desaparece la condición por la que el certificado fue expedido. Por ejemplo, el cambio de apoderado de una entidad jurídica.
 - El certificado contiene información errónea o información que ha cambiado. Por ejemplo, una errata en los apellidos.
 - Una orden judicial.
 - Etc.

■ ¿Cómo comprobar si un certificado es válido?

■ Mediante CRLs.

Acrónimo de "Certificate Revocation List", es una lista de certificados (más concretamente sus números de serie) que han sido revocados, ya no son válidos y en los que no debe confiar ningún sistema de usuario. Dicha lista está firmada digitalmente por la autoridad de certificación. Se utilizan la extensión CRLDistributionPoints presente en los certificados

■ **Ventaja:** se pueden consultar sin necesidad de una conexión permanente con cada autoridad de certificación. Basta establecer dicha conexión con cierta periodicidad para descargar las CRL actualizadas.

■ **Desventajas:** Existe el peligro de que un certificado este revocado pero no aparezca en la CRL del tercero (no actualizada). Además las CRL crecen en tamaño por lo que podrían ser ineficientes.

■ Mediante protocolo OCSP.

Protocolo de consulta *en línea* (proporcionado por la autoridad de validación) que aporte información al momento sobre cada certificado en concreto



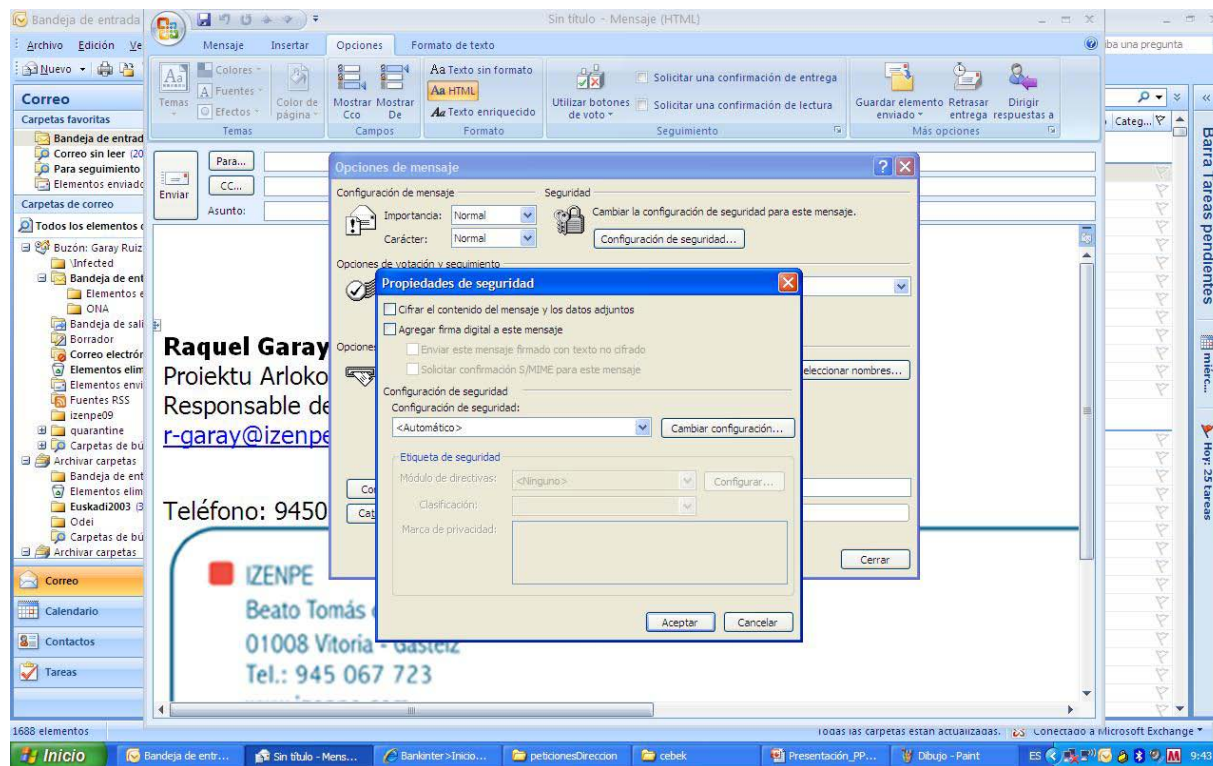
■ Pausa-Cafe



- Ejemplos prácticos de aplicaciones de firma

Firma y cifrado de correo electrónico: variantes y necesidades
Utilidades: smart card log on, VPN
Firma de documentos PDF
Aplicaciones de firma: Sinadura, Idazki y otras
Notificación electrónica: sms certificado, contrato certificado
Portafirmas.

Los clientes de correo electrónico nos ofrecen la opción de firmar y cifrar correo electrónico .



Se puede habilitar la apertura de la sesión de windows en base a certificados, en este caso cuando el dispositivo físico que aloja el certificado no esta presente, la sesión se cierra.



Un pdf firmado se puede visualizar con cualquier reader de adobe, sin embargo para generar una firma es necesario disponer de un herramienta:

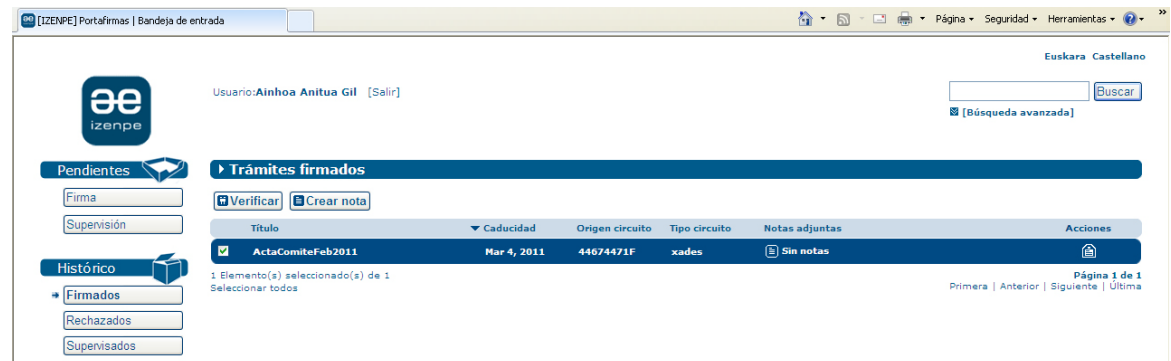
Writer de adobe

Sinadura

Idazki



- Nuevo servicio que permite la implementación de circuitos de firma sencillos, acta de reunión, aprobación de gastos,....



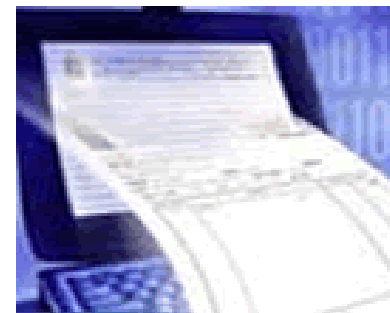
El envío de correo electrónico y SMS se ha convertido en una herramienta de trabajo habitual, sin cuya existencia no concebimos nuestra realidad laboral. Sin embargo estos medios no proporcionan garantías verificables de la comunicación intercambiada.

Izenpe proporciona una plataforma de comunicación certificada que garantiza mediante un certificado, el contenido íntegro de la comunicación, la fecha de envío y la fecha de entrega del mensaje, así como la constancia de lectura del mensaje por el destinatario.

La utilización de la plataforma de comunicación certificada facilita la realización de notificaciones fehacientes de forma “instantánea”, evitando costosos procesos de envío de cartas certificadas y buro fax

Una factura electrónica es...

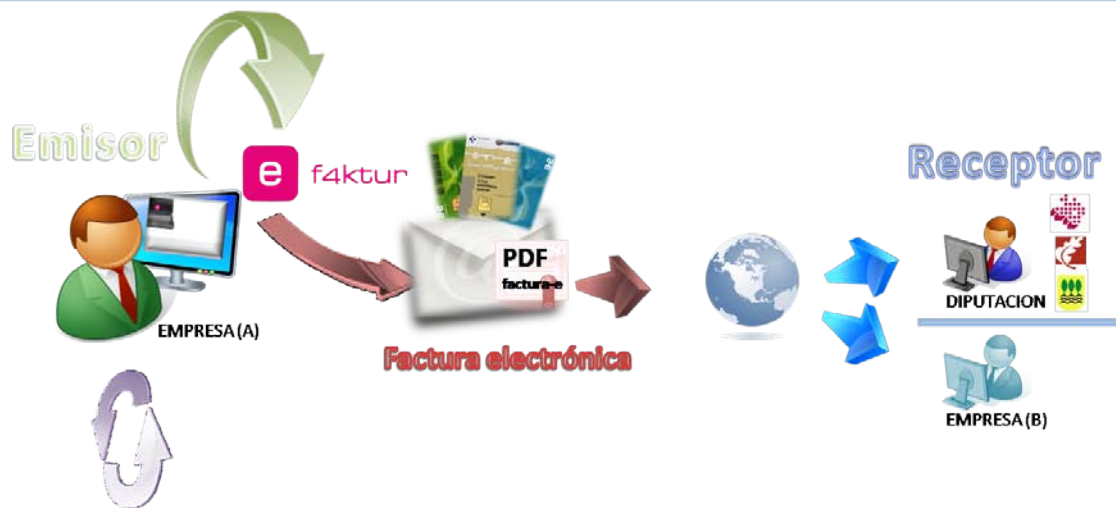
- ... un documento tributario generado por medios telemáticos (de un ordenador a otro) en formato electrónico (fichero informático) que reemplaza a la factura en papel
- ... que conserva el mismo valor legal con unas condiciones de seguridad que no tiene la factura en papel (autenticidad e integridad)
- ... y se transmite desde el emisor al receptor por medios telemáticos firmada electrónicamente con un certificado electrónico reconocido





- Es una **iniciativa de las Diputaciones Forales Vascas** para dotar de forma **gratuita** a emisores de facturas una solución de factura electrónica que permite de forma **sencilla y práctica** trabajar entre empresas y con las administraciones vascas.
- Es una herramienta dirigida a emisores de facturas.
- ef4ktur está dirigido a PYMEs, microPYMEs y trabajadores autónomos.

- Se puede instalar en plataformas windows, Linux y Mac.
- Es software libre con licencia EUPL.
- Permite la creación de facturas electrónicas en formato PDF o FACTURAE.
- Envía las facturas a través del correo electrónico o servicios web desarrollados por los receptores.
- Permite la importación de datos desde otros sistemas.
- Permite la firma de facturas con certificados reconocidos, software o almacenados en tarjeta criptográfica.



www.izenpe.com
www.ef4ktur.com
cau-izenpe@izenpe.net
902 542 542



■ ¿Cómo implantar la firma electrónica en mi empresa?



- Necesidades y Requisitos

Agentes que intervienen

AGENTES QUE INTERVIENEN

Empresa

TICs

PSC

MISIÓN DE LOS AGENTES

Detectar colectivos y servicios de interés

Dotar de herramientas adecuadas.
Formar al personal técnico

Proveer certificados y servicios asociados
Adaptar soluciones al sector

- Seleccionar un piloto inicial
 - Escala reducida en el área que suponga una ganancia directa para nuestra empresa.
 - Proyectos de no retorno inversión inmediato

- Estudiar los productos del mercado
 - Estudiar las herramientas TIC
 - Estudiar el tipo de certificados y el tipo de PSC

■ Entorno interno:

- Intranet (nota de gastos, solicitud de vacaciones, solicitud de compras) :
 - Certificado corporativo tarjetas
 - Portafirmas
- Factura electrónica (emisión)
 - Certificado de entidad en software o tarjeta
 - Ef4ktur
- Junta accionistas/Consejo administración
 - Certificado de entidad en software
 - Servicio de acreditación de documentación
- Movilidad
 - Aplicaciones internas
 - Corporativos en microSD

	Izenpe	Ceres	Camerfirma	Firma Profesional	Ancert
Ciudadano	X	X	X		X
P. Jurídica	X	X	X	X	X
Corporativo	X		X	X	



■ Planificación

FASES DEL PROYECTO

Impulso al proyecto

Desarrollo del proyecto

Despliegue de las entidades de
registro

Atención a la base instalada

COLABORACIÓN DEL PSC

Información
Orientación

Consultoría jurídica Consultoría
técnica

Planificación emisión
Despliegue inicial

Mantenimiento ciclo de vida de los
certificados
Atención al usuario



- Desarrollo en base a servicios

■ Plataformas de firma

- Independizan del tipo de certificado
- Independizan del formato de firma

■ Plataformas de custodia

- Los documentos firmados electrónicamente tienen que ser custodiados
- Custodiar el fichero
- Custodiar la firma, que requiere de actuación activa de refirma...

- **Cambios organizativos resultantes de la digitalización**
- **Cambios procedimentales**
- **Problemáticas relativas a la desmaterialización:**
 - Firma electrónica
 - Archivado de datos
 - Protección de datos



**Confederación
Empresarial de
Bizkaia**

**Bizkaiko
Enpresarien
Konfederazioa**

MUCHAS GRACIAS
www.izenpe.com

