

respuesta digital

Jornada:

Aplicaciones y uso de la Firma Digital



respuesta
digital



Relación de Ponentes de la Jornada



Juan Carlos Rodríguez
jcrodriguez@s21sec.com



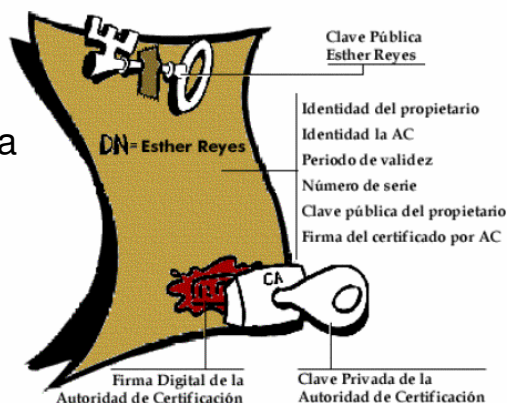
Julian Perez
julianp@ksitdigital.com

Un certificado es un **documento electrónico** emitido y firmado por una **Autoridad de Certificación** que identifica una **clave pública** con su propietario.



- Son utilizados para garantizar la identidad de las personas en las operaciones telemáticas (Internet)
- Su efectividad se basa en la combinación de:
 - * Criptografía
 - * Infraestructura de llaves digitales (PKI)
 - * La legislación vigente

- Los certificados digitales identifican a un sujeto ante accesos y operaciones remotas donde no es posible la comprobación y validación presencial de la identidad de los participantes.

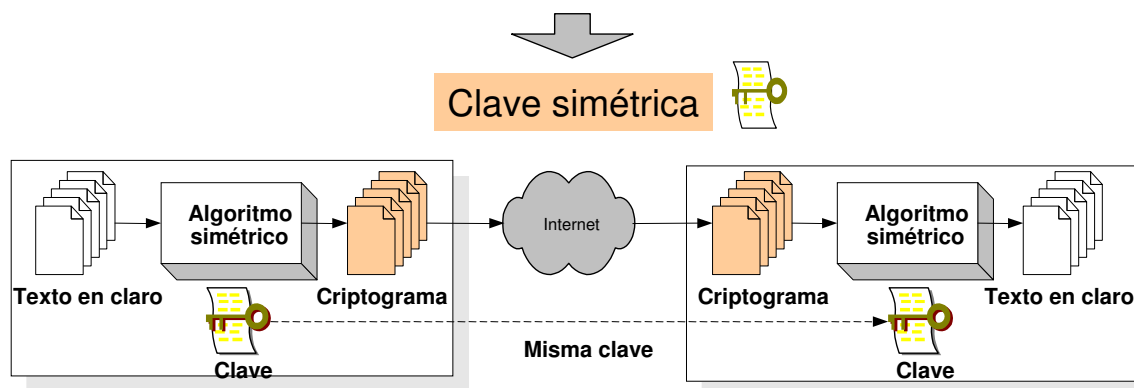


- Son **personales** e **intransferibles** y representan a un individuo como actualmente puede hacerlo la presentación de nuestro DNI junto a nuestra firma manuscrita.

M. Sola

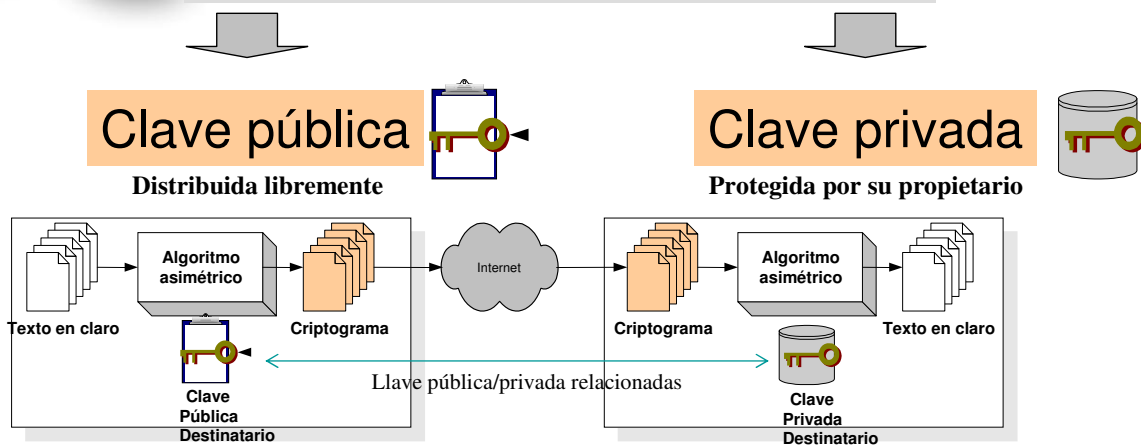
Algoritmos de firma y cifrado y su relación con los Certificados Digitales

La misma clave y algoritmo para cifrar y descifrar la información



Toda la seguridad se basa en la confidencialidad y robustez de la clave

Clave diferente para cifrar y descifrar



En la firma electrónica se invierte el sentido, clave privada para firmar clave pública para verificar la firma

Firma digital electrónica

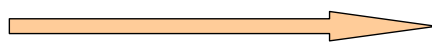
Características:

- **Autenticación.** Se puede comprobar la identidad del firmante
- **Integridad.** Comprueba que el texto no ha sido modificado.
- **No repudio.** El firmante no puede negar haber generado y entregado el documento.



!No incluye Confidencialidad!, ya que no se cifra el mensaje

Integridad



Hash

El emisor realiza el Hash (función resumen) del texto en claro y lo envía junto con el mensaje. El receptor realiza la misma función y comprueba el resultado. Si el texto no se ha modificado el resultado obtenido debe ser el mismo.

Autenticación y no repudio



Hash cifrado

Se cifra el Hash con la clave privada del emisor. Sólo el emisor posee esa clave, por lo tanto no puede negar la firma. Cualquiera tercera persona puede comprobar la firma si tiene acceso a la clave pública relacionada con la privada, la cual se distribuye libremente.

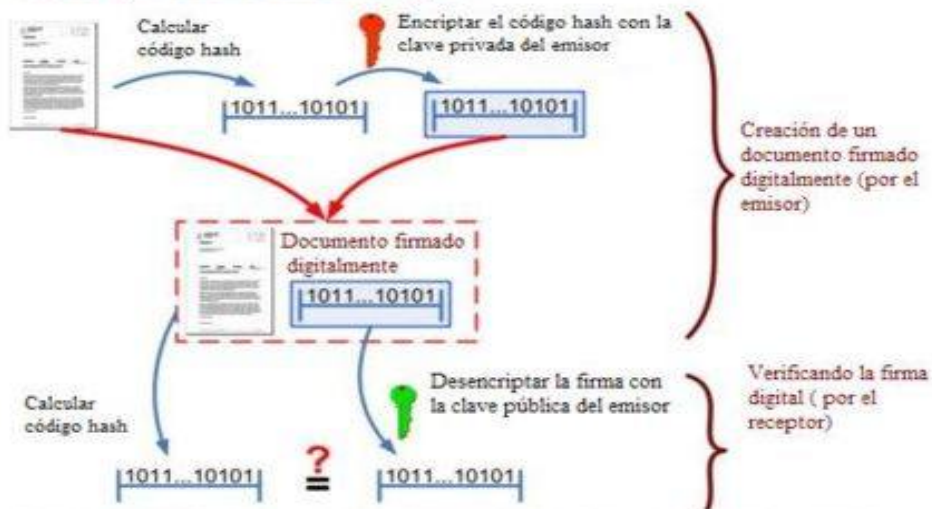
proceso de firma electrónica



proceso de verificación



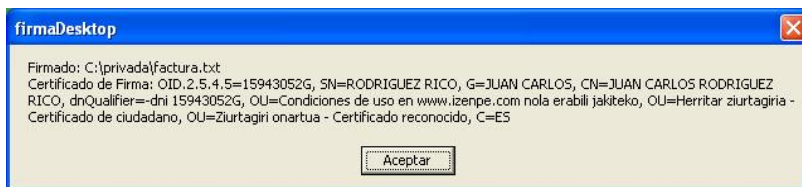
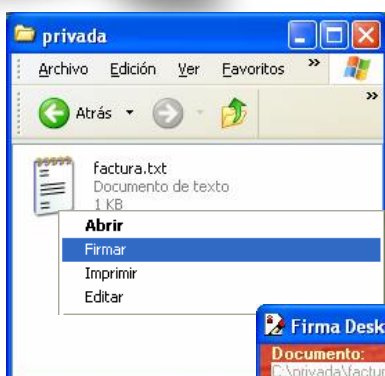
Creando y verificando una firma digital

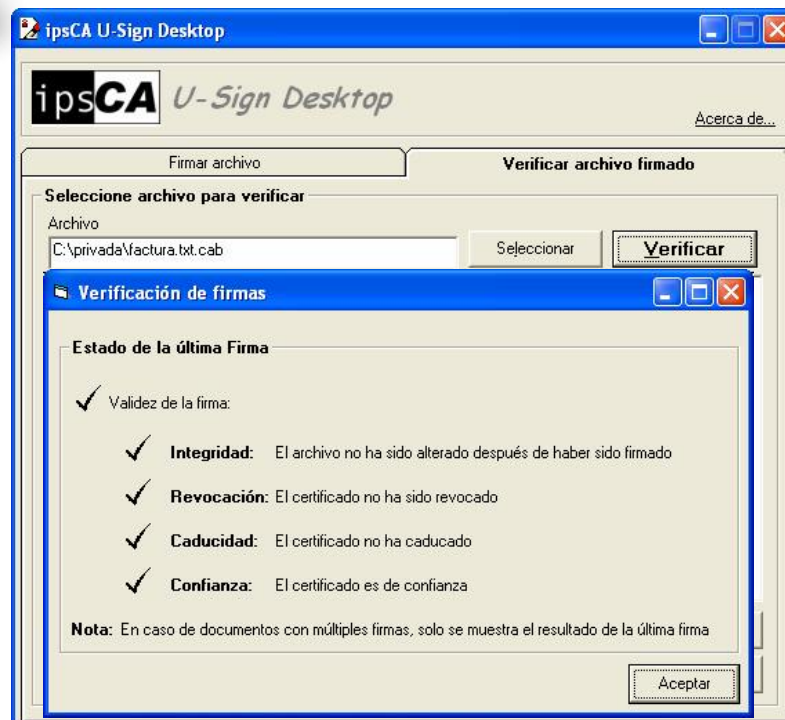


Si el código hash calculado no concuerda con el resultado de la firma digital desencriptada, o el documento fue modificado después de hacer la firma, o la firma no fue generada por la clave privada del emisor del documento

Firma y/o cifrado de documentos del escritorio

Mediante Desktop Firma de Camerfirma





Firma digital en documento WORD

Firma digital incluyendo imagen de firma manuscrita en documento ADOBE

Estimado Joan,

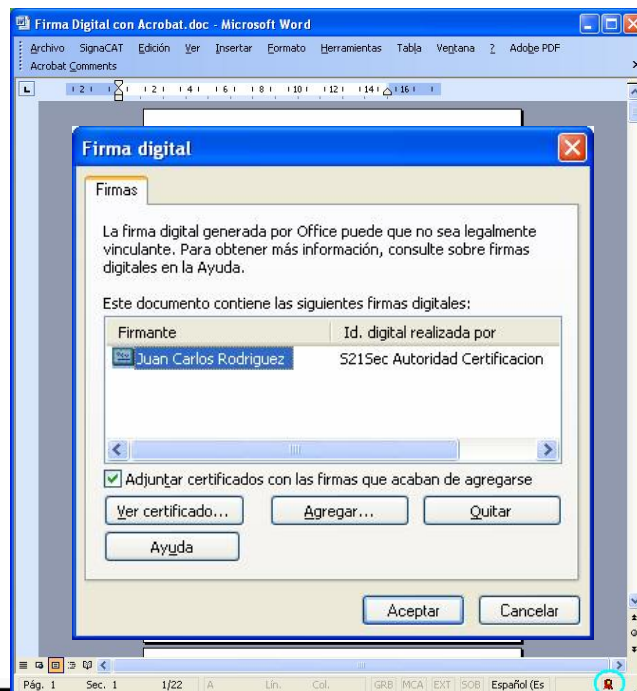
Por la presente te detallo el importe de la factura correspondiente al servicio solicitado.

Cliente: Joan Ayerbe
 Fecha: 21/06/2006
 Concepto: Revisión Pre-ITV
 Importe: 60 Euros
 IVA 7%: 4,2 Euros
 Total Factura: 64,2 Euros

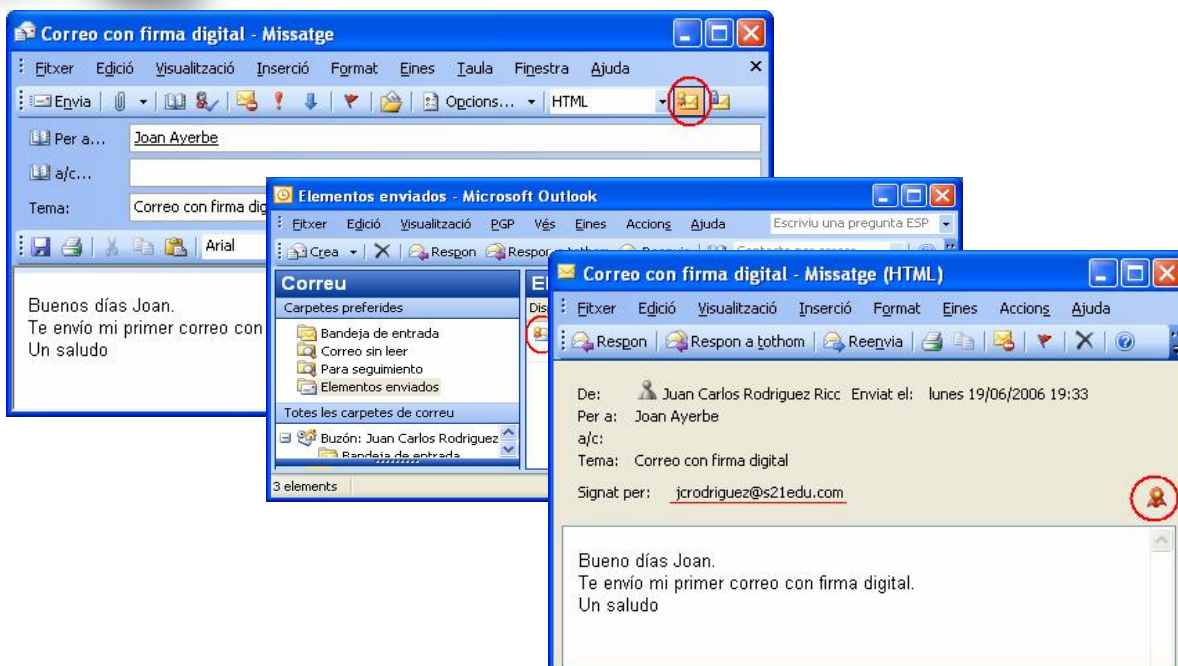


NOMBRE RODRIGUEZ RICO JUAN CARLOS -
 160430E2G
 2006.06.24 11:34:34
 +02'00'

Atentamente:
Juan Carlos Rodriguez



Firma de email's



Los documentos cifrados con un certificado digital solo pueden ser descifrados con la clave privada.

La pérdida o rotura de la tarjeta, o el borrado del certificado del equipo implica

!! La imposibilidad del descifrado de los documentos cifrados con dicha certificado!!

Recuerda también que la renovación de un certificado generalmente se realiza mediante la emisión de una nueva tarjeta (o la descarga de un nuevo certificado), por lo que:

Debes de conservar la tarjeta anterior (o haber realizado una copia del certificado con el par de claves del equipo) para poder descifrar los documentos cifrados con ella antes de recibir la nueva tarjeta o descargar el nuevo certificado.

Responsabilidades y recomendaciones de seguridad en la utilización de certificados digitales

- El par de claves (privada/pública) se genera y almacena en la propia tarjeta y !NO PUEDE SALIR DE LA MISMA!

- Se garantiza con ello que solo el titular de la tarjeta pueda utilizar el certificado que contiene.

- Para las operaciones de firma y/o descifrado es necesario introducir el PIN de acceso a la tarjeta para la utilización de la llave privada



Responsabilidades del titular de la tarjeta

- Es responsabilidad del titular, la custodia de la tarjeta así como garantizar la privacidad del acceso a la misma mediante la selección de un PIN de acceso no predecible y complejo de adivinar.
- El uso de la tarjeta es personal e intransferible y por ello se aplica el principio del NO REPUDIO a las operaciones de firma digital efectuadas con ella.
- Si otro usuario o programa puede tener acceso a la tarjeta criptográfica y a la clave privada que contiene, podrá realizar operaciones de firma digital con el certificado incluido en su nombre, "suplantando" al titular de la tarjeta que finalmente será responsable de las acciones realizadas.
- El titular de la tarjeta deberá de comunicar a la mayor brevedad la pérdida de la tarjeta, para proceder a la revocación del certificado contenido y evitar así su uso fraudulento.



Generalización de la Firma Digital en la documentación

IDEAS NUCLEARES

1. Las soluciones deben cooperar con otras y basarse en estándares probados mundialmente
2. Cualquier aplicación que aporte soluciones de Firma electrónica y cifrado debe tener en cuenta:
Administración – Pyme – CIUDADANOS
3. Firmar facturas es estupendo. Tener la capacidad de firmar TODO, en cualquier momento, contexto, sistema operativo es VITAL para la sociedad y el impacto medioambiental sí será apreciable.
4. DNle como elemento esencial (**atención a otras tarjetas criptográficas**)

Evolución de Infraestructuras y momento actual

MAYOR SEGURIDAD MUNDIAL Y AHORRO DE PAPEL

APLICACIONES

DATOS PERSONALES

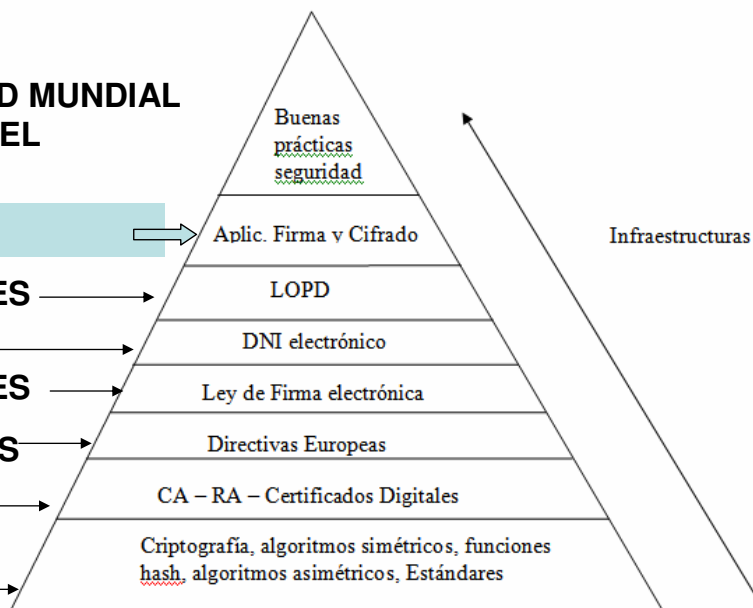
DNI en Europa

NORMAS ESTATALES

NORMAS EUROPEAS

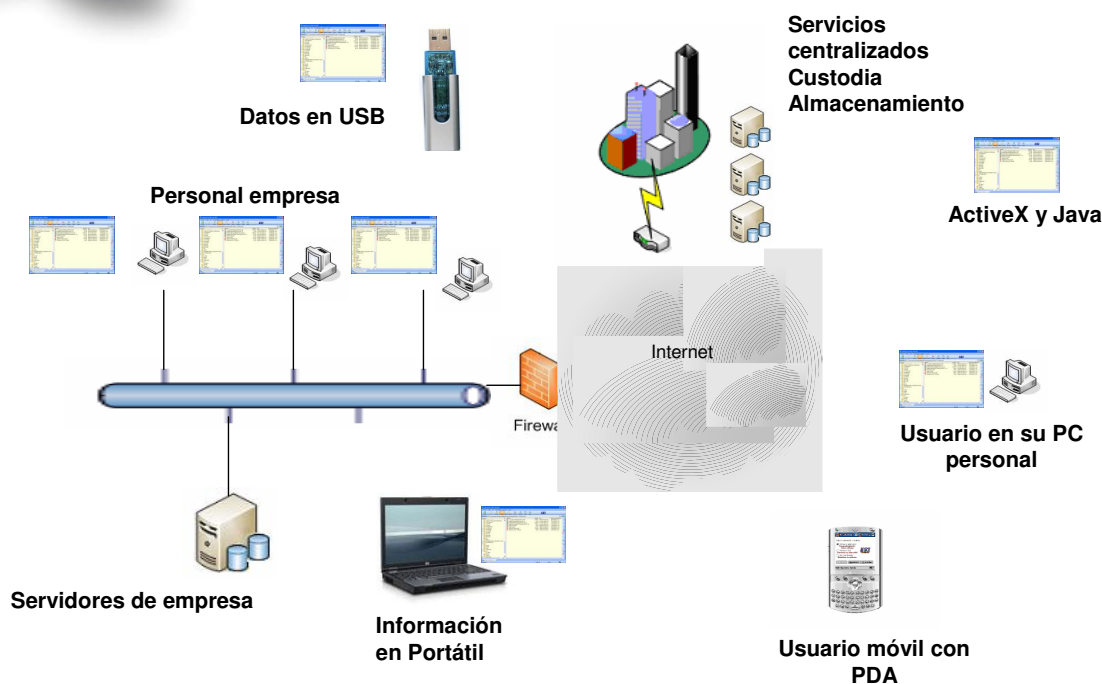
CERTIFICADOS

CRIPTOGRAFIA



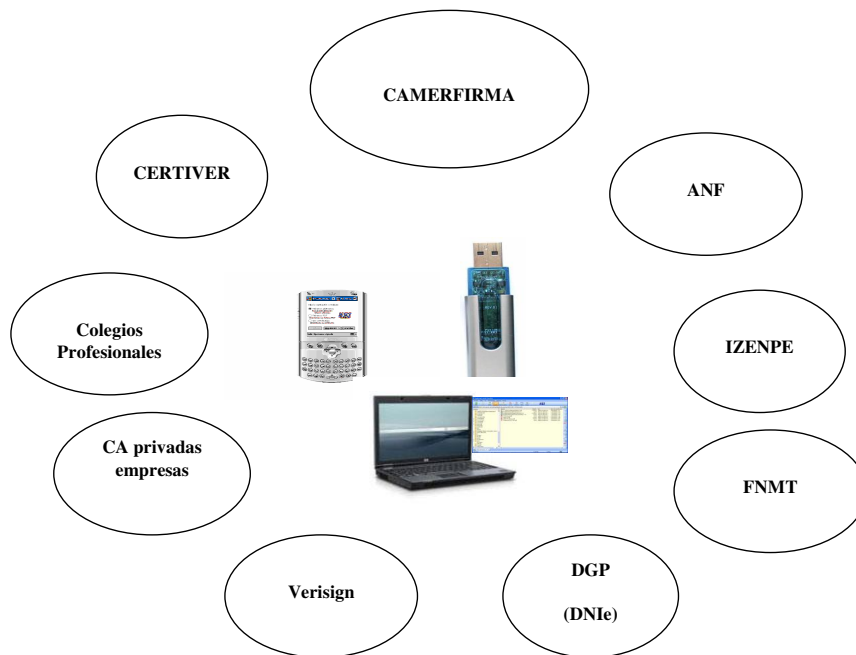
Infraestructuras en avance

Firmar y asegurar en todos los contextos



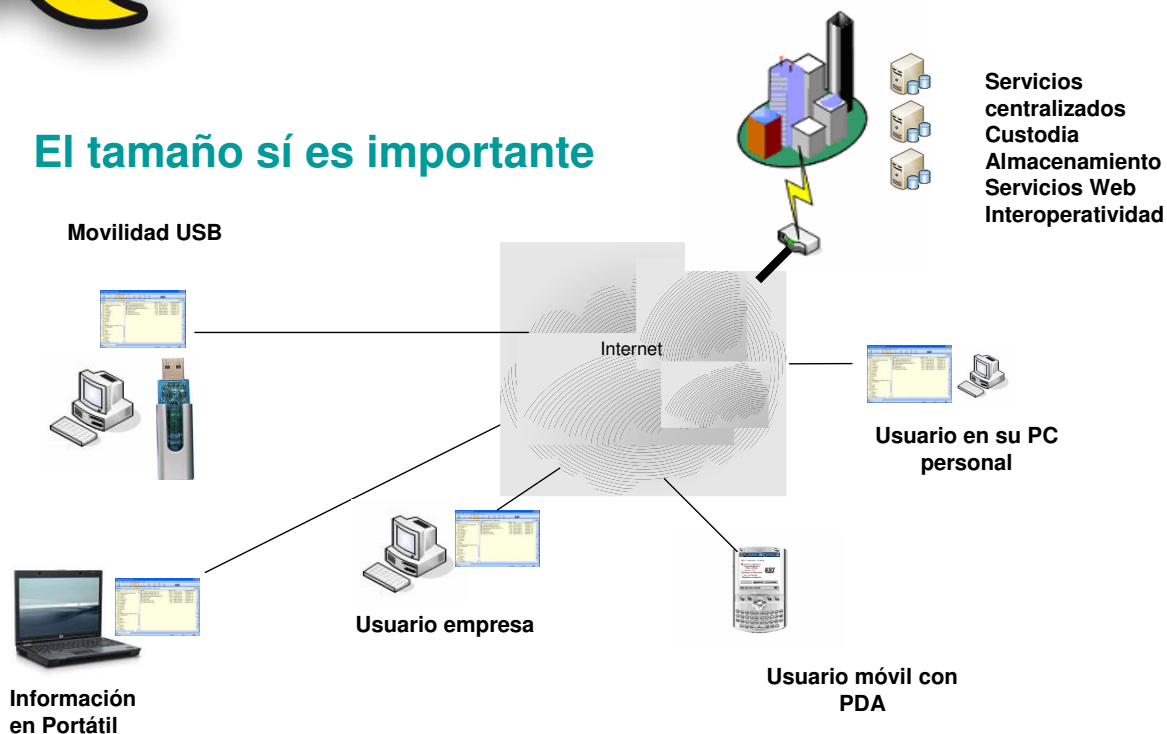
Autoridades – Servicios - Soluciones

- **Autoridades Certificación**
- **Servicios validación, Tiempo y Custodia**
- **Aplicaciones en distintos sistemas operativos**



Centralizado y distribuido

El tamaño sí es importante



ESTANDARES – Estándares – estándares - estándares

- Firmar en todos los formatos que sean estándares
- PDF, CADES (CMS) y XAdES (XML)
- Balances, Informes, Historiales médicos, Nóminas, Memorándums, Currículums, Instancias, Registros, Campos, Recetas, email, Logs, Backup, Libros, Vídeos, música...

¡Todo puede ser firmado!

¡Podemos decir adiós a la información anónima con un ahorro enorme de papel y el impacto ambiental derivado!

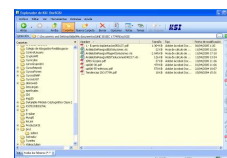
Hagamos aplicaciones interoperables

- Aplicaciones autónomas Linux – Windows - MAC
- Aplicaciones en PDA y dispositivos móviles
- Integrar la firma en todo el software de Gestión
- Firmar y/o cifrar en cualquier momento y lugar, con y sin conexión a Internet y cualquier tamaño de información.

• Firma avanzada y firma reconocida

Firma cotidiana en cualquier lugar

- Con la administración pública
- Con empresas
- En nuestro entorno personal
- Validación certificados
- Sellos de Tiempo
- Validar en cualquier lugar una firma



Con la firma electrónica ocurrirá como con las tarjetas bancarias.
Generalización gradual

Consultoría de implantación en Firma y Cifrado

Es una necesidad real y es un modo eficaz de comenzar a avanzar

- Orientada a la PYME
- Todas las áreas de la empresa lo requieren
- Necesidad de formación, sensibilización y Políticas de firma y cifrado
- Facilita uso eficaz herramientas y certificados
- Implantación inmediata de aplicaciones

Formación y aplicaciones (todo en uno)

Distribución masiva de Información firmada



- Versiones Escritorio en Windows Módulos: (PDF, XML, Asesorías)

- Plataforma servidor Linux y Windows basada en Software Libre

Proyecto desarrollado en colaboración con EDATALIA

Desarrolladores se suman al proceso en régimen de colaboración con KSI

- Librerías Windows
- Librerías Linux
- Firma y Cifrado

Objetivos:

- eCalidad, LOPD, GAMP4, HIPAA, CFR 21 PART 11
- Firma y/o cifrado en el interior de la empresa
- Firma y/o cifrado para el transporte
- Distribución documental firmada o cifrada- Reducción papel
- Añadir Firma en software propio (ERP – Nominas – otros)

Libro descargable como PDF

- Firma electrónica
- Cifrado
- Seguridad documental
- DNle y otras tarjetas
- Factura electrónica
- Normas legales
- Formatos estándares

colaboración con INTECO



Seguridad documental, firma digital y DNle en Europa

Julián Pérez Muñoz
Pablo F. Pérez Trullós
Pedro J. Latasa López
Santiago Castaño Matilla



WWW.KSITDIGITAL.COM

Descargue libremente:

- Libro
- Manuales
- Aplicación ESecure

mapa del sitio | accesibilidad | contacto | maximizar/restaurar tamaño

SOLUCIONES AVANZADAS DE SEGURIDAD DIGITAL

usted está aquí: inicio

Servicios
KSI Seguridad Digital es una empresa dedicada al ámbito de la Seguridad informática.

Noticias

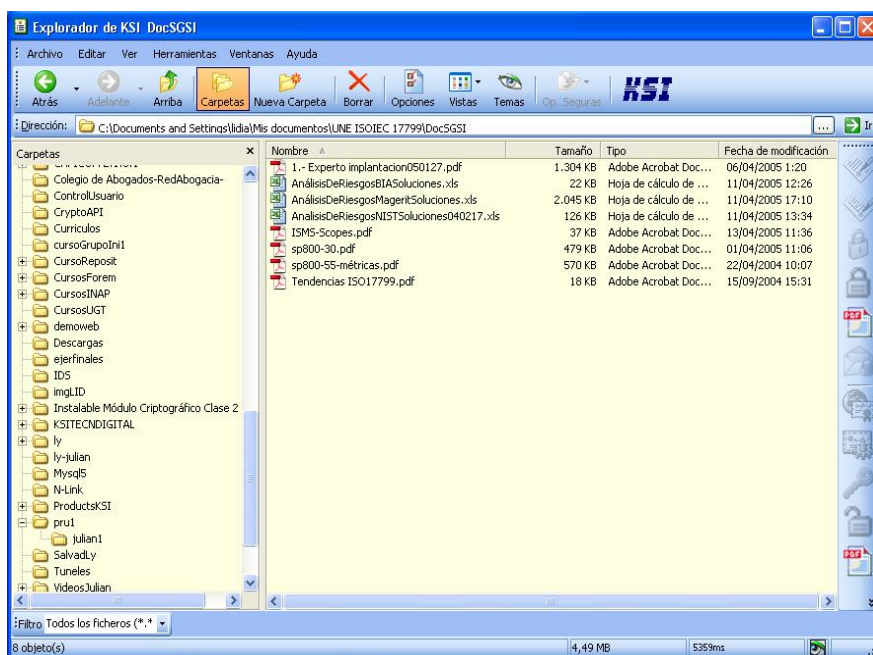
Seguridad documental, Firma Digital y DNle en Europa
El libro Seguridad Documental, Firma Digital y DNle en Europa se extiende con rapidez por España con cientos de descargas de muchos países europeos y americanos

Ilustre Colegio de Graduados Sociales de Navarra y KSI
Las dos entidades firman un acuerdo de SOCIOS TECNOLÓGICOS en materia de SEGURIDAD DIGITAL en sus aspectos de firma electrónica, cifrado de la información y facturación electrónica

APLICACION ESECURE

Acciones:

- Firma
- Cifrado
- Verificación
- Correo seguro
- Borrado seguro
- Firma múltiple
- Descifrado
- DNle
- Tarjetas criptográficas.
- Multiformato



ESECURE PDA

Acciones:

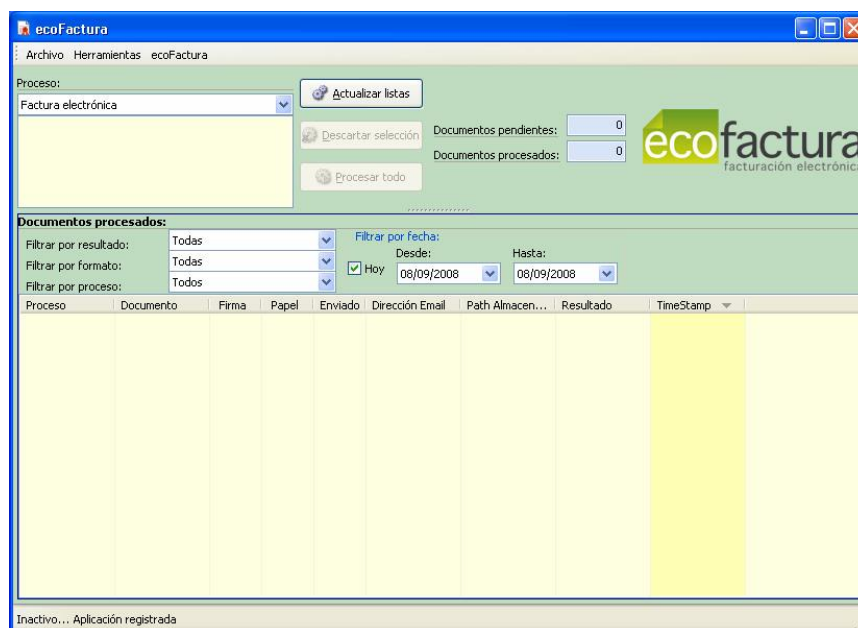
- Firma
- Cifrado
- Descifrado
- Verificación
- Compatibilidad con PC



Distribución ficheros firmados

Acciones:

- Firma
- Cifrado
- Envío por correo
- PDF y XML
- Firma múltiple
- Multiproceso
- Firma avanzada
- Firma reconocida

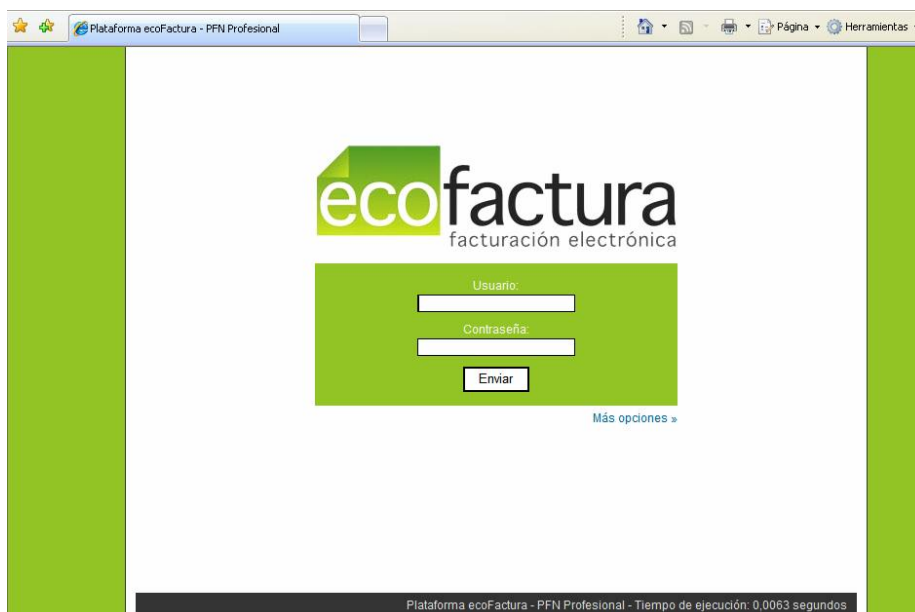


Familia de productos desarrollada en colaboración con EDATALIA

Plataforma ecoFactura PFN

Acciones:

- Firma
- Cifrado
- Verificación
- Envío correo
- Firma múltiple
- Descifrado
- Publicación de ficheros firmados
- Multiformato
- Gestión documental web



Plataforma de software libre desarrollada en colaboración con LITO dentro del Proyecto KSI-EDATALIA

Plataforma ecoFactura PFN

Acciones:

- Firma por usuarios
- Cifrado y descifrado en servidor
- Verificación de firmas
- Alternativa a correo
- Multiformato
- Trazabilidad

The screenshot shows the 'ecoFactura' web application interface. At the top, there's a navigation bar with 'Área de Administrador', 'Buscador', 'Ayuda', and 'Salir'. Below that, a search bar is visible. The main content area displays a table of files and folders. The table has columns for 'Nombre', 'Tipo', 'Tamaño', 'Fecha', 'Permisos', and 'Acciones'. The files listed include 'documentos', 'Actima', 'Base de Facturación', 'Base de Lominas', 'Crealia', 'KSI', 'MMI', and 'PuntoGlobal'. The 'Tipo' column shows 'CONTENIDO' for folders and 'VACÍO' for empty folders. The 'Fecha' column shows dates from August 2008. The 'Permisos' column shows the number of files in each folder (e.g., 777 for 'documentos'). The 'Acciones' column contains icons for file operations like view, download, and delete.

Nombre	Tipo	Tamaño	Fecha	Permisos	Acciones
documentos			01:15 31-08-2008	777	
Actima	CONTENIDO	-	00:23 25-08-2008	755	
Base de Facturación	CONTENIDO	-	20:58 27-08-2008	755	
Base de Lominas	CONTENIDO	-	01:17 31-08-2008	755	
Crealia	CONTENIDO	-	21:22 23-08-2008	755	
KSI	CONTENIDO	-	18:33 29-08-2008	755	
MMI	VACÍO	-	18:55 07-08-2008	755	
PuntoGlobal	VACÍO	-	14:48 23-08-2008	755	

Plataforma de Software Libre desarrollada en colaboración con LITO

Colaborar para un mundo de Firma

- Con Institutos de Formación Profesional (Convenios con KSI)
- Con Colegios Profesionales (Proyectos de firma y eFactura)
- Con INTECO en soluciones extrapolables y Common Criteria
- Con XION en el mundo de la movilidad e interoperabilidad
- Con Masbytes en servicios ASP sobre eFactura
- Con consultoras jurídicas y del mundo de la calidad
- Con empresas y desarrolladores del mundo del software libre
- Con Edatalia en el universo de la eFactura e interoperabilidad
- Con desarrolladores de ERP y herramientas de Gestión
- Con centros de formación nacional
- Con NGA formando a sector médico cursos online en España

La firma se desarrolla poderosamente en procesos de colaboración.

El ciudadano puede colaborar con KSI descargando sin coste nuestras soluciones, documentos y herramientas

KSI Seguridad Digital y orientación al mundo

“Generalizar la firma y cifrado en todos los estamentos y ámbitos de la sociedad no puede hacerse sin el concurso de los ciudadanos.

El DNle en distintos países fraguará soluciones que tenderán a formarlos y apoyarlos y KSI estará en ellos con soluciones en cada idioma.

Construimos soluciones llave en mano e impulsamos que los desarrolladores integren la firma en beneficio de la generalización y facilidad de uso mediante colaboraciones especiales.

www.ksitdigital.com

- **Descanso**

Prácticas:

- *Obtención del “Hash” de un fichero*
- *Conexión Web SSL a un servidor con certificado de una AC de confianza y AC desconocida*

- *Firma de documentos con un programa de escritorio*
- *Firma de documentos con Adobe Acrobat*
- *Firma de documentos con Office 2003*
- *Firma de mensajes de correo electrónico con Outlook*
- *Entorno de firma electrónica “Esecure KSI”*

Gracias por su
asistencia y atención