

KIT DE FIRMA Y AUTENTICACIÓN EN SISTEMAS WEB



El KIT que KSI Seguridad Digital ha creado es independiente del servidor web donde vaya a implantarse.

Este sistema permite implantar:

- Autenticación.
- Firma de formularios.
- Firma de ficheros.

PARTE SERVIDORA

Las librerías de KSI, incluidas en el KIT, ofrecen múltiples funcionalidades como se puede ver en la Hoja de Producto del API.

Las características más importantes:

- Firmar y verificación utilizando los estándares más extendidos: PKCS#7/CMS, CAdES, XAdES, PDF. En curso la firma inyectada en ficheros Microsoft Office y OpenOffice.
- Validación de certificados en tiempo real accediendo al OCSP Responder de la entidad emisora de los certificados
- Validación de certificados mediante comprobación de CRL.
- Capacidades de cifrado y descifrado orientadas a seguridad adicional
- Cumplimiento de formatos como Facturae determinados por la AEAT
- Capacidad de firma completa (con validación y sellado de tiempo)



KIT DE FIRMA Y AUTENTICACIÓN EN SISTEMAS WEB

PARTE CLIENTE

En la parte cliente puede ser utilizado con navegadores como Microsoft Internet Explorer (ActiveX) o cualquier otro navegador que sea capaz de ejecutar applets de Java (Firefox).

El ActiveX y el Applet permiten la firma de formularios, firma de ficheros y procesos de autenticación, siendo respaldado en la parte servidora por el API KSI para la correcta verificación de la firma y del firmante, de la validación OCSP y en su defecto de la comprobación en el fichero local de CRL.

ActiveX

El ActiveX de KSI es un código firmado que encapsula todas las capacidades del API para aportar todas las capacidades de firma. Puede acceder a los certificados digitales, en modalidad **software** o en **dispositivos criptográficos** como el **DNIE**.

Ha sido probado en todos los sistemas windows, incluyendo Windows Vista, aún cuando Internet Explorer tenga activado el modo protegido.

APPLET KSI

El Applet de KSI es un código Java firmado que aporta todas las capacidades de firma. Puede acceder a los certificados digitales, en modalidad **software** o en **dispositivos criptográficos** como el **DNIE**.

CARACTERÍSTICAS TÉCNICAS

Diseñado para servidor con S.O. Windows o Linux

Necesario el API de KSI Seguridad Digital en servidor

Applet y/o ActiveX de KSI para el Navegador de la parte cliente

Capacidad de validación OCSP y/o CRL de las CA cuyos certificados vayan a ser utilizados.
