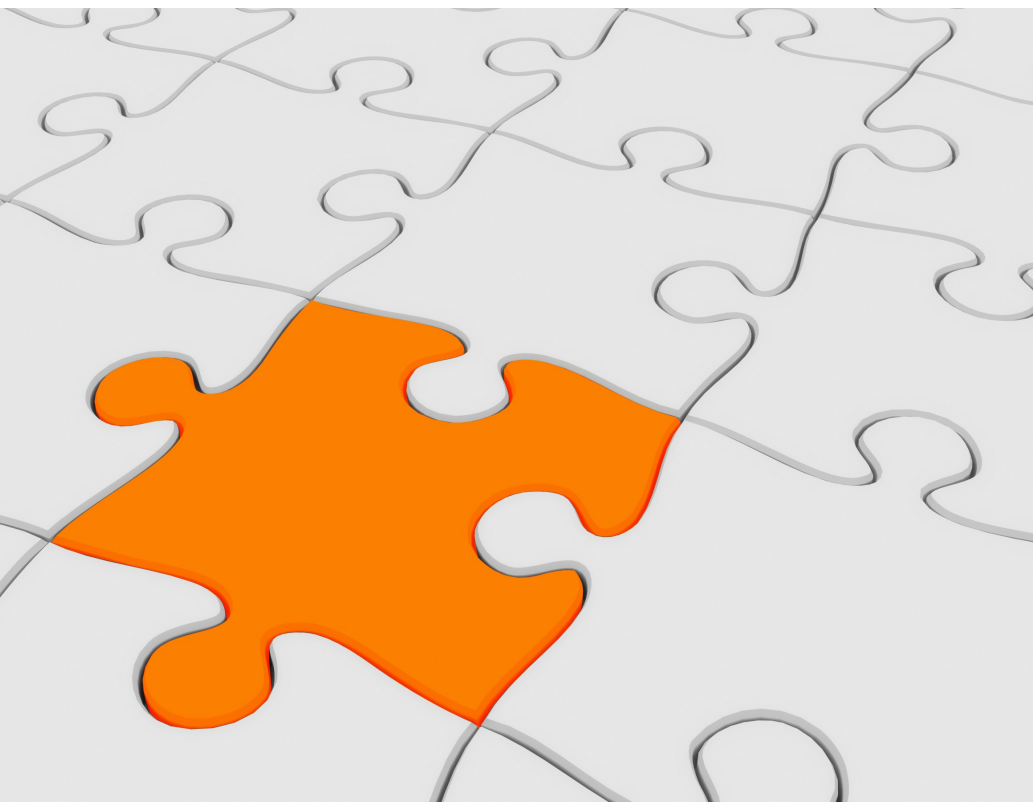


# API DE FIRMA ELECTRÓNICA Y CIFRADO



“API es  
la pieza  
perfecta para  
complementar  
sus  
aplicaciones”

La **Librería de Seguridad** de KSI para desarrolladores aporta todos los **estándares necesarios** para la utilización de distintos tipos de **cifrado** en las aplicaciones (**Simétrico y Asimétrico**) además de todas las capacidades de **Firma electrónica** que hoy día necesitamos aportar a sistemas de: documentación, de contabilidad e informes, de nóminas y trabajo en grupo, de almacenamiento seguro, y aquellos orientados a cumplir **normativas legales** como CFR 21, HIPAA, GAMP4, LOPD, LFE y aquellas normativas orientadas a implantar la **Factura electrónica** en Europa siguiendo recomendaciones de la CEE y estándares de organizaciones como ETSI (**European Telecommunications Standards Institute**).

La licencia de la aplicación ESecure, que reciben dentro del pedido del API, tiene características avanzadas y su **licencia no caduca**. Ello representa una prueba viva de la capacidad de las librerías y de su estandarización, ya que la información firmada va a poder **validarla en múltiples sistemas de terceros como Autoridades de Certificación**.

---

## CARACTERÍSTICAS DEL API

Librería de programación que puede ser utilizada en Windows, Linux y PDA

---

Utiliza certificados estándar **X.509 v3** que estén situados en distintos tipos de almacenes de certificados

---

Librería en formato binario para los distintos sistemas operativos con capacidades de firma y cifrado, con una compilación específica para se usada desde Java vía JNI

---

Librería utilizable para la **firma y cifrado de strings** para facilitar la firma de formularios completos, subformularios o campos específicos de BBDD

---

Cualquier fichero puede ser firmado, **independientemente de su tamaño**, siguiendo distintos formatos de plena actualidad en todo el mundo (PKCS#7, PDF, CMS-CADES, XML-XAdES)

---

## FUNCIONALIDADES BÁSICAS DEL API

- Verificación de firmas incluyendo sellado de tiempo y validación OCSP de certificados
- Extracción de la información firmada tras la verificación
- Firma de ficheros **independientemente de su formato y tamaño**
- Soporte **PKCS#7, PDF, CMS (CADES), XML (XAdES, XMLDSig)**
- Sello de tiempo seguro proveniente de una **TSA** (TimeStamping Authority) y servicios de tiempo provenientes de un servidor **NTP**
- Firma y verificación de Strings
- **Acceso a CryptoAPI** de Windows (funcionalidad sólo para Windows)
- Capacidad de caché OCSP en firmas de lotes con el mismo certificado (ejemplo Facturación electrónica)
- Uso transparente de tarjetas criptográficas en firma y cifrado en Windows a través de CryptoAPI y librerías PKCS#11 de fabricantes

---

## VERSIONES DEL API

El API puede ser adquirido bien con todos los formatos de firma o sólo con alguno de ellos (**PDF, CADES, XAdES**). En sistemas Windows las distintas modalidades se complementan con un sistema de protección anticopia por PC denominado **Secure**.