MEI® PKI Token USB

Introducción

Construcción bajo Cumplimiento de Estándares Internacionales

La construcción de los tokens se ha realizado teniendo en cuenta de los principales requisitos de seguridad, bajo rigurosos estándares internacionales, siendo en la práctica nuestra empresa y productos especializados de los primeros y más completos cumplidores de los estándares de certificación. Nuestra empresa proporciona y apoya con patentes a los principales proveedores de la industria.

The *Common Criteria for Information Technology Security Evaluation* (CC) ha concedido el estado de EAL 5+.

El token ha recibido el *Federal Information Processing Standard (FIPS) 140-2 level 2, level 3, FIPS 140 level 4*, un estándar público desarrollado por el gobierno federal de Estados Unidos distinguiendo ambos componentes, harware y software de sistemas informáticos criptográficos, asegurando la evidencia física de la firma electrónica y la autenticación basada en roles.

Los dispositivos MEI®[1] de Kalysis cumplen la *Directiva Comunitaria de la Unión Europea sobre firma digital avanzada*[2].

Los dispositivos criptográficos *Cryptographic Tokens* descritos cumplen la norma comunitaria como *Advanced Electronic Signature Devices* en la máxima escala de seguridad *Secure-Signature-Creation Device (SSCD)* más que como simples *Signature-Creation Devices (SCDev).*

Infraestructura de Clave Pública *Public Key Infraestructure* (PKI): los dispositivos MEI® de Kalysis son aptos para cualquier aplicación PKI, compatibles con cualquier aplicación para tarjetas inteligentes basado el estandar PC/SC o MS CAPI (Requerimientos SCJN):

- Es por ello que son idóneos y *compatibles con el estándar mexicano ITFEA, para el almacenamiento de CURP y RFC en el certificado.*
- *Compatible con la infraestructura de Firma Electrónica de la Suprema Corte de Justicia de la Nación.*

---

[1] *Multi-application Electronic Interface* [MEI®] es una marca registrada de Kalysis.

[2] *Advanced Electronic Signature - an electronic signature which meets the following requirements:*

a. it is uniquely linked to the signer;
b. it is capable of identifying the signer;
c. it is created using means that the signer can maintain under his sole control; and
d. it is linked to the data to which it relates in such a manner that any subsequent alteration of the data is detectable. [Dir. 1999/93/EC]

Equipado con las Características requeridas de Interfaz de Usuario

El MEI PKI Token USB cuenta con el protocolo estándar *Microsoft MiniDriver* que le permite al dispositivo funcionar perfectamente conjuntado en los sistemas operativos Windows sin necesidad de inversión en middleware adicional. El usuario final sólo necesita introducir el token en el ordenador y el driver del periférico se instala automáticamente a través de la función Update de Windows. El diseño MiniDriver funciona con *Windows Microsoft Base Smart Card Provider* para ofrecer soporte nativo para todas las *Microsoft CAPI* y soluciones *CNG*, como *Windows Smart Card Log-on* y *RDP Log-on*.

Certificado por el grupo *PCSC-Lite/LibCCID*, el dispositivo cuenta con suporte integrado para los sistemas operativos Linux y MAC y sus aplicaciones. MEI PKI Token USB trabaja con su propia biblioteca PKCS#11 o con la biblioteca OpenSC PKCS#11 para la integración en populares navegadores Web como Firefox y clientes de correo.

Características

Construcción de chip inteligente de alto rendimiento y alta seguridad	**Chip certificado por Common Criteria EAL 5+** **Algoritmos RSA, AES 256, DES/3DES, SHA-1, SHA-256, aprobados por NIST FIPS CAVP** **Generador de números aleatorios en el hardware del chip criptográfico** **Memoria 64KB EEPROM para almacenar las claves privadas, múltiples certificados y datos sensibles**
Sistema Operativo con IP propietario	**Diseño acorde al estándar internacional FIPS 140-2 level 2 FIPS 140-2 level 3, FIPS 140-2 level 4 certified** **Confidencialidad a través de mensajería segura entre el periférico y la aplicación** **Soporta certificados estándares X.509 v3. Soporta múltiples certificados en un solo dispositivo** **Generación del par de claves, firma y encriptación RSA 2048** **Número de serie universal del hardware de 64 bits**
Hardware del Token USB	**Dispositivo USB 2, velocidad completa** **Compatible con la ISO 7816 1-4 8 9 12, PC/SC y CCID.** **Resistente al agua** **Opciones de personalización: logo, color, y encapsulado**
Middleware confiable con soporte de múltiples sistemas operativos	**Soporta Windows, Linux, y Mac OS** **Compatible con el estándar Windows mini driver, funciona con Microsoft Base Smart Card CSP, soporta *Microsoft smart card enrollement for Windows, smart card user, y smart card logon*** **Soporta el API estándar PKCS #11 & CSP como Netscape, Mozilla, Internet Explorer y Outlook**
Fácil integración con varias aplicaciones PKI	**Dispositivo ideal para almacenar de forma segura e inviolable los certificados digitales, funciona con todas las aplicaciones relacionadas con certificados electrónicos** **Dispositivo de alta seguridad para firma electrónica a través de ordenadores y redes de comunicaciones** **Soporta firma electrónica y encriptación de documentos, correo, y transacciones**

Especificaciones

Especificaciones de producto

Sistemas operativos soportados[3]	• **Windows 32 y 64 bit, Windows XP SP3, Server 2008, 7…** • **Linux 32 y 64 bit** • **Mac OS X (10.5 y superior)**
Middleware	**Microsoft Windows MiniDriver** **Windows middleware para Windows CSP** **Librería de acceso directo para PKCS#11 bajo Windows, Linux y MAC**
Estándares	**Almacenamiento de Certificado X.509 v3, SSL v3, IPSec, ISO 7816 1-4 8 9 12, CCID**
Algoritmos criptográficos	**RSA 512 / RSA 1024/ RSA 2048 bit** **ECDSA 192 / 256 bit** **DES / 3DES** **AES 128/ AES 192/ AES 256 bit** **SHA-1 / SHA-256**
Funciones criptográficas	**Generación en el dispositivo del par de claves** **Firma digital y verificación en el dispositivo** **Encriptación y desencriptación de datos en el dispositivo**
APIs Criptográficas	**Microsoft Crypto API (CAPI), Cryptography API: Next Generation (CNG)** **Microsoft Smart Card MiniDriver** **PKCS#11** **PC/SC**
Procesador	**16 bit smart card chip (COMMON CRITERIA EAL 5+ certified)**
Espacio de memoria	**64KB (EEPROM)**
Durabilidad	**Al menos 500.000 ciclos de lectura/escritura**
Retención de datos	**Más de 10 años**
Conectividad	**USB 2.0 velocidad completa, Conector tipo A**
Interfaz	**ISO 7816** **CCID**
Consumo energético	**Menos de 250mW**
Temperatura de operación	**0°C ~ 70°C** **(32°F ~ 158°F)**
Temperatura de almacenamiento	**-20°C ~ 85°C** **(-4°F ~ 185°F)**
Humedad	**0% ~ 100% sin condensación**

[3] **FreeBSD, GNU/Linux, Mac OS X 10.5 Leopard, Mac OS X 10.6 Snow Leopard, Mac OS X 10.7 Lion, Windows 7, Windows 7 - 64 bits, Windows 2008, Windows 2008 - 64bits, Windows Vista, Windows Vista - 64 bits, Windows Server 2003 Windows Server 2003 64 bits, Windows 2000, Windows XP.**

Especificaciones de encapsulado

Dimensiones	**53,3mm x 16,5mm x 8,5mm**
Peso	**4,5 gramos**
Color	**Azul**
Material	**PC (Policarbonato)**
Logo	**Pestaña en el perfil frontal** **Dimensiones: 20mm x 6mm**
Número de Serie	**Impreso en tinta en lado posterior o en conector USB**
Personalización	**Serigrafía en el dispositivo con la leyenda:** "Poder Judicial de la Federación"

Ventajas de la oferta económica

Actualizaciones de los drivers en caso de nuevas versiones (algo frecuente en sistema operativo Windows) sin coste.

Licencia de por vida: los dispositivos no necesitan licencias de uso que otros fabricantes establecen según ciclos temporales; esto es, se entregan con licencia completamente pagada, por lo cual no existen costes ocultos de mantenimiento.

Garantía: 18 meses.

Experiencia del Proveedor: en donde la criptografía ha experimentado un mayor desarrollo, Kalysis se ha especializado en dispositivos de firma electrónica desde hace más de diez años. Proveedor de los Colegios de Ingenieros en Telecomunicación (superior y técnica) de España, Universidad Nacional de Educación a Distancia, UME (Unidad Militar de Emergencias), IBM, Novartis Farmacéutica, Telefónica de España, etc. ha tenido oportunidad de participar en numeros proyectos de firma electrónica, desde el ámbito de la justicia hasta la firma de proyectos, documentos y transacciones.

Soporte Técnico y a la Implantación: nuestra empresa se ofrece a apoyar desinteresadamente el despliegue de los proyectos de firma electrónica de la entidad, para conseguir tanto el éxito técnico, como el éxito en la implantación.