Firma Electrónica, USB Token y Lectores de Tarjetas Criptográficas de Kalysis

AUTOR: ***Kalysis GRUPO v.1.03***

FECHA: ***Diciembre 2004***

RESUMEN

Kalysis ostenta la patente de los dispositivos adaptadores de tarjetas inteligentes a puerto estándar para dispositivos conectados a Internet orientados a transacciones telemáticas. Cuando el puerto estándar es USB y el chip de una tarjeta inteligente o microprocesador se encuentra contenido el mismo periférico, hablamos de USB Tokens. Los tokens MEI1000 y MEI2000 y los lectores de tarjetas inteligentes MEI100 y MEI200 bajo patente industrial de Kalysis, son dispositivos que involucran tarjetas inteligentes en transacciones telemáticas desde un dispositivo conectado a Internet: por ejemplo, PC, PDA, smartphone, y están amparados en España [Registro de la Propiedad Industrial P200101056].

Documento en versión HTML: http://www.kalysis.com/hardware/mei

Prólogo

Kalysis presenta sus tokens USB de microprocesador y tarjetas criptográficas, además de lectores/grabadores de tarjetas inteligentes empleados en la encriptación de correo electrónico, firma digital, aplicaciones en redes privadas y acceso seguro a servidores de aplicaciones. Este documento recoge la familia MEI® USB Token: MEI1000, MEI2000, y los lectores de tarjetas inteligentes MEI100 y MEI200.

Puede tener acceso a mayor detalle sobre las patentes de Kalysis haciendo click aquí

MEI® Token Criptográfico USB

RESUMEN

MEI® USB token patentado por Kalysis

Su llave para la Era Digital y Firma Electrónica Avanzada

Desde que las redes de negocios llegan a estar más y más conectadas, la necesidad de mejores y más sofisticadas medidas de seguridad en redes de comunicaciones es de primordial importancia. La autenticación del usuario y los métodos de autorización necesitan distinguir entre socios de negocio y clientes, empleados de distintos departamentos, usuarios con acceso remoto, y una miríada de otros factores para asegurar que la persona adecuada obtiene la información correcta.

Los sistemas simples de autenticación de usuario, basados en nombre de usuario y clave, ambos son insuficientes porque no proporcionan la suficiente granularidad entre los sistemas, y fácilmente son perdidos, robados, compartidos y violados. Sistemas más sofisticados de autenticación de usuario -generación dinámica de claves, Infraestructura de Clave Pública Public Key Infraestructure (**PKI**), biometría- proporcionan una incrementada seguridad a menudo a expensas de la usabilidad. Los productos USB Token de Kalysis ofrecen autenticación en coste y eficiencia, verificación y servicios de encriptación que soportan la encriptación del correo electrónico, firmas digitales y certificados, Single Sign On (SSO), aplicaciones **VPN**/**SSL**, **ASP**, y entornos PKI.

Características del USB Token MEI2000

Figure 1 MEI2000. Incluye LED de luz azul bajo la carcasa

- Tarjeta inteligente criptográfica integrada **StarCOS** SPK 2.3 de **G&D**
- Generación del par de claves **RSA 1024-bit** en el dispositivo, la clave privada no puede ser exportada
- Soporte integrado para **RSA**, **DES**, **3DES**, **SHA-1**, **MD5** y otros algoritmos de seguridad y cifrado
- Middleware con soporte **PKCS#11** y **MS CAPI**
- Almacenamiento de múltiples Certificados Electrónicos **X.509 v3**
- Generación de números aleatorios en hardware
- Driver compatible **PC/SC**, firmado por **Microsoft**
- Poderosa conectividad Plug & Play para aplicaciones de PKI
- Firma digital desde hardware
- Soporte para almacén de múltiples claves
- Soporte para múltiples aplicaciones **PKI** y para tarjetas inteligentes
- Certificado de Conformidad **CE** y **FCC**
- Interfaz estándar **USB**
- Card Operating System

Características del USB Token MEI1000

Figure 2 MEI1000. Anverso y reverso. LED externo de luz verde

- Generación del doble factor de autenticación cambio-respuesta **HMAC-MD5** en el dispositivo.
- Middleware con soporte **PKCS#11** y **MS CAPI**
- Almacenamiento de múltiples Certificados Electrónicos **X.509 v3**
- Generación de números aleatorios en hardware
- Driver compatible **PC/SC**, firmado por **Microsoft**
- Número de serie único de 64-bits
- Certificado de Conformidad **CE** y **FCC**
- Aplicación controlada con luz **LED**
- Acceso basado navegador Web a **MEI1000** a través de controles **ActiveX** y applets de **Java**
- Tres niveles de seguridad para acceder a los archivos y derechos administrativos.
- Estrutura de directorio de archivos de dos niveles
- Interfaz estándar **USB**

Kit de Desarrollo de Software

Kalysis ofrece Kit de Desarrollo de Software (SDK) para ambos MEI1000 y MEI2000. El Kit de Desarrollo de Software MEI contiene todos los elementos necesarios para desarrollar sus aplicaciones usando el token MEI de Kalysis. Incluido en el MEI **SDK** se incluye un token MEI, CD con software (incluye código fuente) y Guía para el Desarrollo de Software. Por favor contacte Kalysis o su distribuidor local para solicitar un SDK.

Beneficios

- **Seguridad Superior**: la información clave se mantiene el el token durante la autenticación, el fichero de claves no es accesible. **MEI2000** usa tecnología de tarjetas inteligentes para permitir la generación de claves públicas y privadas en hardware. Las claves privadas no están nunca expuestas al entorno del PC. El algoritmo hash **MD5** realizado en el dispositivo **MEI1000** asegura que las credenciales del personal de seguridad se mantienen seguras dentro, aisladas de hackers, virus y otras amenazas.
- **Compatible**: Soporta Windows98SE/ME/2000/XP/2003, Linux y MAC.
- **Portable**: MEI es Hot Pluggable -no necesita estar conectada desde el arranque del PC-, y puede ser portada en el llavero; simplemente extráigala del puerto **USB** y lleve consigo sus claves y credenciales seguras consigo.
- **Fácil de Usar**: MEI viene con abundantes interfaces de programación. Su popular conector USB y diseño de una pieza es a prueba de polvo, agua, y electricidad estática.
- **Bajo Coste**: MEI actúa como una tarjeta inteligente en aplicaciones **PKI**, pero MEI no necesita un lector especial.
- **Sencillez de Integración**: el middleware MEI soporta los estándares **PKCS#11** y **MS CAPI**, permitiendo una integración sencilla con cualquier software compatible, como **Internet Explorer**, **Outlook**, **Outlook Express** o **Netscape Communicator**.
- **Multi-uso**: MEI puede ser configurado para soportar múltiples claves y aplicaciones.
- **Autenticación de Dos Factores**: La Seguridad puede ser incluso incrementada requiriendo al usuario la entrada de un **PIN** cuando use MEI.

MEI® y PKI

PKI envuelve el uso de certificado digitales, los cuales pueden estar almacenados en discos flexibles. Discos duros y tarjetas "chip". El problema con los disquetes es que ni son un medio fiable ni particularmente convenientes para llevarlos consigo. Los certificados digitales almacenados en los discos duros no son portables y pueden ser copiados fácilmente por usuarios no autorizados. Las tarjetas son convenientes para el usuario, pero requieren la instalación de lectores especiales en cada lugar donde un usuario necesite ser autenticado, lo cual es bastante caro. Con los productos MEI de Kalysis, los usuarios pueden almacenar los certificados digitales y claves privadas en el token MEI. La aplicación obtendrá los certificados digitales y claves privadas del token MEI cuando se adquieran los certificados digitales. No es necesario importar los certificados al ordenador. El dueño del certificado electrónico no necesita preocuparse si su certificado digital puede ser robado, si el sistema del PC fallará, o si un virus infectará la copia de seguridad del certificado electrónico. La seguridad es incrementada más allá requiriendo al usuario introducir el **PIN** de harware del MEI para acceder a los certificados almacenados en el token. MEI puede no sólo autenticar la identidad del usuario en dos direcciones, sino también llevar a cabo la encriptación de datos y otras funciones con certificados digitales. Puede usar de forma cómoda y segura sus certificados electrónicos con MEI.

Estructura PKI de MEI®

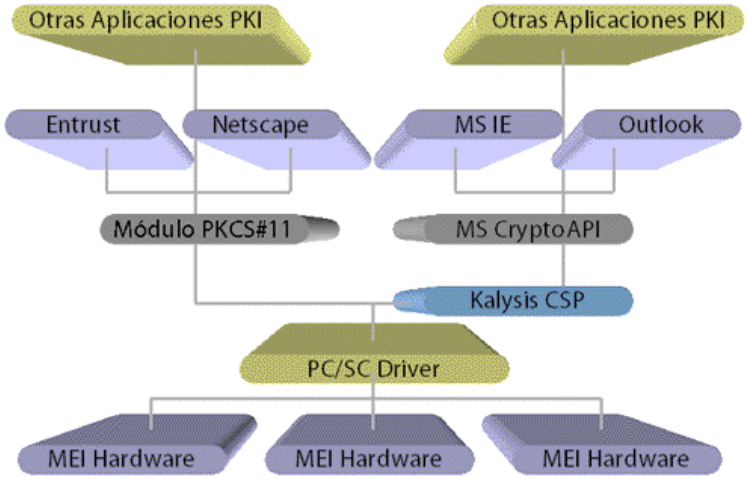

Figure 3 Estructura PKI de MEI®

MEI® Soporta las Arquitecturas Estándares PKI

- **PKCS#11** (Public Key Cryptography Standards de RSA Security Inc)
- **MS CAPI** (Cryptographic Applications Programming Interface de **Microsoft**)

MEI soporta una sencilla integración con cualquier aplicación basada en los estándares PKCS#11 o MS CAPI, no es necesario ningún trabajo de desarrollo. Aplicaciones compatibles pueden almacenar certificados digitales y claves privadas, generar pares de claves **RSA**/**DSA** , llevar a cabo firma digital y funciones de autenticación, encriptar y desencriptar datos con MEI. Internet Explorer, Outlook, Outlook Express, Netscape Navigator y Netscape Messenger son aplicaciones compatibles con los estándares **PKI**.

Aplicaciones de los Lectores y Tokens USB

- Seguridad de la estación de trabajo a través de Windows 2000 smart card logon
- Firma y encriptación de correo estándar con **Microsoft Outlook** / Outlook Express, **Internet Explorer** y **Netscape Messanger**
- Acceso seguro **SSL** a la Web
- Compatibilidad PKI con Windows98SE y superior, Microsoft Internet Explorer y Netscape Communicator
- Logon Seguro en Redes (**Extranets** e **Intranets**)
- Acceso Seguro a Redes Privadas Virtuales (**VPN**).
- Protección Segura de PC
- Protección Segura de Contraseñas

Áreas de Aplicación

- Banca en línea
- Transacciones **B2B**, **B2C**
- Aplicaciones Financieras
- Salud
- Proveedores de Aplicaciones (**ASP**)
- Suscripciones On-line
- Pago de Impuestos / Abono de subsidios
- Aplicaciones Militares y de Gobierno

KALYSIS IBERIA, SL. Plaza de Uncibay, 3, Primera Planta, 29008 Málaga (EMEA)
WEB: KALYSIS.COM sales@kalysis.com Tel. +34 952.60.81.93 Voice/Fax Int. +1 (206) 666-KALY
C.I.F. B92451996. Inscrita en el Registro Mercantil 5 Málaga. T3322, L2234, F45, Hoja MA-63693
Place of Fulfillment Málaga. Court of Jurisdiction Málaga, SPAIN

Aplicaciones MEI® PKI

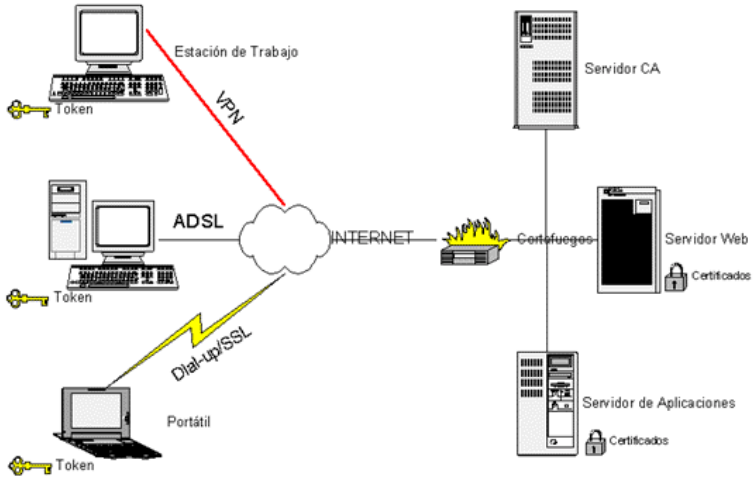

Figure 4 Sistemas de seguridad en las comunicaciones con MEI®

MEI1000 Diagrama de Flujo de Autenticación de Dos Factores

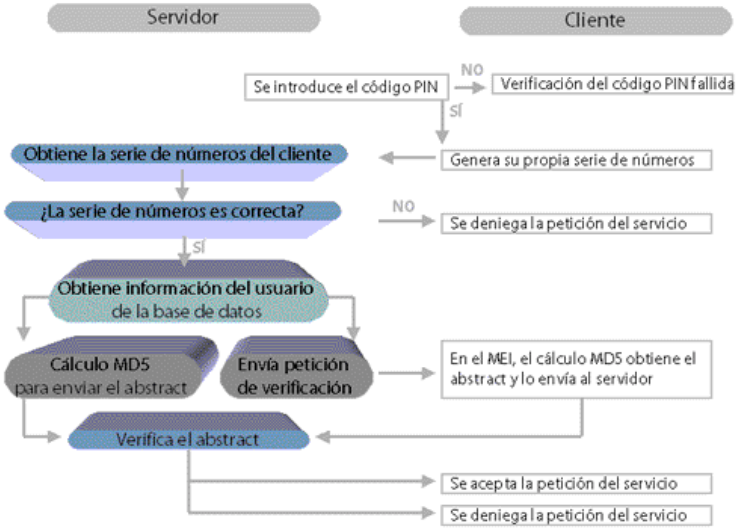

Figure 5 Esquema de flujo challenge-response para firma electrónica avanzada con MEI®

MEI1000 adopta un mecanismo intercambio-respuesta en todo el proceso de autenticación. Para verificar la identidad del usuario en la red, el cliente envía primero una petición de verificación al servidor. Después de recibir la petición, el servidor genera un número aleatorio y envía este número al cliente a través de la red (esto es, intercambio) El cliente dirige el número aleatorio recibido al MEI1000, éste lleva a cabo el cálculo **HMAC-MD5** con el número aleatorio y la clave almacenada en el token MEI1000, y enseguida envía el resultado del cálculo al servidor (esto es, respuesta). Al mismo tiempo el servidor lleva a cabo el cálculo **HMAC-MD5** con el número aleatorio y la clave correspondiente almacenada en la base de datos del servidor. El cliente se considera un usuario legítimo si el cálculo resultante desde el servidor es el mismo que el devuelto por el cliente

Especificaciones Técnicas de MEI1000 y MEI2000

	MEI1000	MEI2000
Sistemas Operativos Soportados	Windows 98SE/ME/2000/XP/Server 2003, MAC, Linux	
Certificados Estándares	x.509 v3	
API y Soporte de Estándares	PKCS#11, MS CAPI	PKCS#11, MS CAPI
	PC/SC, API propia	PC/SC, ISO 7816-3/4
	SSL v3, IPSec/IKE	SSL v3, IPSec/IKE
Espacio de Almacenamiento	8k, 32k	32k
Algoritmo de Hardware	HMAC-MD5	RSA, DES, 3DES, MD5, SHA-1
Disipación de Energía	<250mW	
Temperatura de Operación	0º C - 70º C	
Temperatura de Almacenamiento	-40º C - 85º C	
Dimensiones	50x17x7 mm (Caja A1)	
Peso	6 gramos (Caja A1)	
Tasa de Humedad	0 a 100% sin condensación	
Tipo de Conector	USB tipo A (Universal Serial Bus)	
Caja Externa	Molde de Plástico Duro	
Retención de datos de la Memoria	Al menos 10 Años	
Reescritura de las Celdas de Memoria	Al menos 1.000.000 de veces	Al menos 100.000 veces

Figure 6 Características de los dispositivos MEI1000 y MEI2000

Lectores de Tarjetas Inteligentes MEI100 y MEI200

Figure 7 MEI100. Conector de tarjetas inteligentes SIM a puerto USB

Figure 8 MEI200. Conector de tarjetas inteligentes a puerto USB/Serie

- Lector/Grabador de tarjetas inteligentes
- Soporta todas las tarjetas **ISO 7816-4**
- Soporta tarjetas inteligentes en formato **SIM** y en tamaño completo
- Soporta ambos puertos **USB** y **Serie** (incluso ambos en el **MEI200 TWIN**)
- Bajo coste y diseño compacto, portátil
- Driver **PC/SC** compatible, firmado por Microsoft
- Soporta múltiples plataformas de PC
- Soporta múltiples lenguajes de programación
- Automáticamente reconoce el tipo de tarjeta IC y selecciona el protocolo de comunicaciones adecuado
- Velocidad de transferencia: 9.600 bps por defecto, máxima 115.2000 bps
- Peso: **MEI200**: 60 gramos, **MEI100**: 15 gramos

El lector MEI® soporta automáticamente todas las aplicaciones para tarjetas inteligentes y **PKI**

Especificaciones Técnicas de los Lectores MEI100 y MEI200

Temperatura de Operación	0 - +70º C
Inserción Máxima de Tarjetas	Al menos 100.000 veces
Frecuencia de la Tarjeta	3MHz
Corriente de la Tarjeta	0 - 50 mA
Interfaz	PC, puerto USB o Serie*
Alimentación	Provista por el puerto USB o Serie*
Protocolo de Comunicaciones	T=0, T=1
Estándares	ISO7816-3, PC/SC
Tasa de Interfaz	T=0: 9.600 baudios (bps) T=1: 9.600 - 115.200 baudios (bps)
Sistemas Operativos Soportados	Windows 98/ME/2000/XP/2003, Linux, MAC

Figure 9 Características de los lectores MEI100, MEI200, y MEI 200 TWIN

Cotización y Contacto

Cumplimente este formulario para solicitar una cotización de los dispositivos MEI® mencionados en este documento.

Puede ponerse en contacto a través del teléfono: **95.260.81.93** o el correo electrónico: **info @ kalysis.com**

Kalysis mantiene su documentación técnica en formato SGML/XML, por lo que si lo desea puede descargar estos contenidos en formato PDF de impresión.

GLOSARIO

Firma Digital Avanzada — 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]

Los dispositivos MEI® de Kalysis cumplen la **Directiva Comunitaria** sobre firma digital avanzada.

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

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)

PKI — 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.**

Index

[i] Para más información sobre nuestros productos visite nuestro sitio web: http://www.kalysis.com