securosys

Descripción de los **Productos**

Securosys Primus HSM (Hardware Security Module)

Módulo de seguridad de hardware

Un Módulo de Seguridad de Hardware genera, almacena y gestiona el acceso a las claves de cifrado, identidades digitales (certificados) y activos digitales. En lugar de almacenar esta información crítica en algún lugar de su servidor de red o en un servidor de nube, el HSM los guarda bajo llave de forma segura. Cualquier transacción que utilice estas claves tiene que ser ejecutada dentro del HSM. De esta forma, incluso si su red es violada y acceden a sus archivos personales, la información más crítica, sus identidades y activos digitales, sus certificados y sus claves de cifrado estarán protegidos.

Casos Típicos para la utilización de Securosys Primus HSM:

- PKI y Firma Digital: Asegurar las claves y certificados de los sistemas PKI (Private Key Infrastructure – Infraestructura de Claves Privadas) como Microsoft CA/PKI, PrimeKey EJBCA, Entrust PKI, y SwissPKI.

- Asegurar el acceso a la nube con CASB (Cloud Access Security Broker) utilizando Centraya y plataformas de intercambio de documentos en línea como SecureSafe de DSwiss.

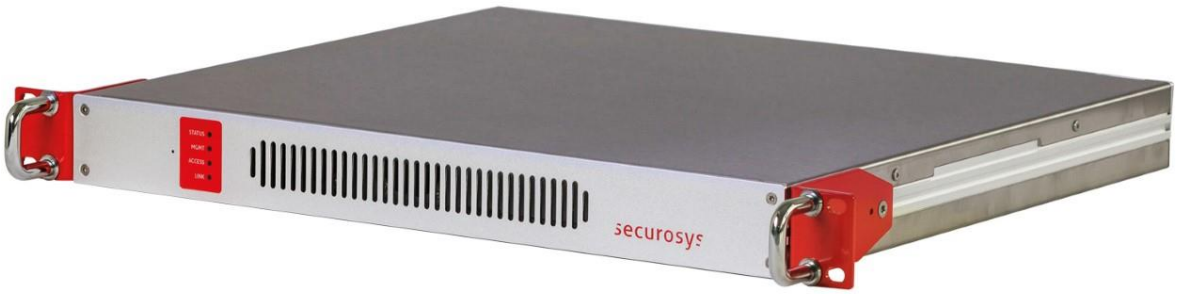
- Plataformas Blockchain y Crypto Currency: Protección de billeteras y Crypto-Billeteras como Bitcoin, Ethereum, Ripple, IOTA, así como nodos y sistemas de blockchain autorizados como Corda de R3 e Hyperledger, en particular con Securosys Transación Security Broker. Ver también Securosys Primus Blockchain HSM.

- Gestión de llaves: Asegurar las claves de los sistemas de gestión de claves de cifrado como Fornetix.

El Primus HSM de Securosys se ofrece en las siguientes versiones:

- Primus X-Series: El Primus X-Series HSM está disponible en cuatro clases de rendimiento diferentes (X200/X400/X700/X1000). Puede almacenar más de 1 millón de claves en 120 particiones de 240MB cada una y es capaz de realizar más de 1200 firmas RSA-4096 por segundo. Es un dispositivo de seguridad de red seguro y a prueba de manipulaciones. El Primus X-Series es ideal para cumplir con los más altos requerimientos de los sistemas de alta disponibilidad. Múltiples HSM pueden ser agrupados como clusters a través de diferentes centros de datos, países, o incluso continentes para proporcionar equilibrio de carga y conmutación por error. Además, cada unidad está equipada con dos fuentes de alimentación redundantes enchufables en caliente (AC o DC).

- Primus E-Series: El Primus E-Series HSM es la solución ideal para un sistema pequeño y sensible a los costos sin sacrificar la funcionalidad ni la utilidad. A menudo se utiliza para reemplazar los engorrosos HSM de tarjetas PCI-e y ofrece un alto rendimiento a un precio excepcional. Está disponible en tres clases de rendimiento (E20/E60/E150) y tiene hasta 50 particiones de 120MB cada una. Siempre es posible una actualización a la serie X de mayor rendimiento. La conexión de los dispositivos a los sistemas existentes es tan fácil como su puesta en marcha. Es fácil de configurar y mantener.



- CloudsHSM: En lugar de operar el Primus HSM por Ud. mismo en las instalaciones o en su centro de datos, CloudsHSM le ofrece la opción de HSM como un servicio (HSMaaS). CloudsHSM es un servicio de nubes del módulo de seguridad de hardware (HSM). Permite a los usuarios generar claves de cifrado, utilizarlas y almacenarlas de forma segura sin tener que preocuparse por cosas que consumen tiempo como la evaluación, configuración, mantenimiento y actualización de su propio HSM. En cambio, expertos experimentados de Securosys se encargan de ello.
- Decanus Terminal: Decanus permite una gestión fácil y rentable de sus HSM sin comprometer la seguridad. El Terminal de Control Remoto le permite manejar hasta 64 HSM Primus en diferentes lugares del mundo. Decanus se conecta de forma segura a su HSM a través de la red (TCP/IP, AES 256). Ofrece la funcionalidad del panel frontal del HSM Primus en una pantalla táctil. La mayoría de las tareas de configuración, gestión y control pueden realizarse sin necesidad de visitar varios centros de datos. También se puede utilizar para administrar una sola partición en el HSM Primus sin necesidad de encender o confiar en la administración del HSM. De esta manera una organización puede cumplir con las más estrictas políticas de seguridad permitiendo que cada aplicación y unidad de negocio controle completamente su almacén de claves seguro.

El Securosys Primus HSM se conecta a las aplicaciones usando las interfaces JCE/JCA, MS CNG, o PKCS#11. Alternativamente, se puede usar un REST API a través del Securosys Transaction Security Broker.

Transaction Security Broker (TSB)

Agente de seguridad en las transacciones

Almacenar las llaves en un HSM es sólo el comienzo. Hay que asegurarse que sólo pueden ser utilizadas adhiriéndose a ciertas reglas adjuntas a cada llave. Esto hace imposible que aplicaciones corruptas o pirateadas (o administradores) usen las claves, reduciendo drásticamente el riesgo de que le roben sus activos. El Securosys Primus HSM admite agregar tales reglas de forma segura dentro del HSM. La función se denomina "Smart Key Attributes" (SKA) y se puede utilizar para un amplio espectro de aplicaciones, incluidos, entre otros, servicios de firma digital de acuerdo con eIDAS, autorización de transacciones de blockchain y mucho más..
Para facilitar la implementación de los SKA, el Securosys Transaction Security Broker proporciona un REST API y la gestión interna del estado. Es un motor autónomo, que se conecta a una instancia de base de datos externa e integra el Securosys Primus HSM habilitado para SKA - y por lo tanto no es crítico para la seguridad, ya que todas las operaciones relevantes para la seguridad se llevan a cabo en el HSM.
El TSB también puede ser usado sin SKA para proveer un API REST para el Securosys Primus HSM.

Imunes Trusted Execution Environment (TEE)

Entorno de ejecución confiable de Imunes

El concepto básico de un Securosys Imunes TEE es ejecutar códigos de forma segura. Esto supone disponer de un mecanismo para cargar el código de forma segura, proteger el código de la alteración y se extiende a la protección de los datos procesados y su salida. Un TEE debe ser capaz de probar, que una cierta salida fue generada de una entrada específica, cuando esa pieza específica de código fue ejecutada. Por lo tanto, un TEE actúa de manera similar a un notario que atestigua procesos o hechos del mundo real. En el mundo digital la atestación puede realizarse mediante firmas digitales.
Las aplicaciones típicas de la ETE son los motores de políticas, los flujos de trabajo automatizados, el código que debe ser protegido y aislado del malware.

Centurion Network Encryptor.

Encriptador de red Centurion

Utilizando Centurion Network Encryptors, puede asegurar de manera fácil y rentable las comunicaciones de banda ancha. Es la forma más segura de conectar dos o más sitios. A través de su soporte nativo de Ethernet e IP Centurion es ideal como encriptador de capa 2 pero también puede operar en redes portadoras de capa 3 Ethernet, MPLS e IP en cualquier configuración: enlace, punto a punto, punto a multipunto o malla. No se requiere reconfigurar la red ni sacrificar el rendimiento. El caso de uso simple varía de una configuración punto a punto para conectar la sede central a su centro de datos y expandirse a sistemas complejos de sitios múltiples que conectan cientos de sitios. El uso del algoritmo AES de 256 bits estándar y probado de la industria con autenticación simétrica AES-GCM combinada con

verdaderos generadores de números aleatorios con efectos cuánticos da como resultado la solución más segura para cualquier sistema de comunicaciones. Los cifradores de red Centurion operan con anchos de banda de 100Mbit/s a 100Gbit/s