

CRYPTOSEC LAN

Organizaciones por todo el mundo están creando sistemas de información que enlazan empleados, clientes, proveedores y partners, de manera rápida y económica, utilizan recursos de comunicaciones, almacenamiento y procesamiento fuertemente interconectados. Sin embargo, las conexiones bajo demanda de personas y máquinas, en cualquier momento y lugar desafía el modelo de confianza tradicional en seguridad perimetral. Hoy en día las iniciativas en cuestión de seguridad enfatizan la autenticación fuerte, la protección de la propiedad intelectual y de la privacidad del cliente, protegiendo la información teniendo en cuenta la movilidad.

Criptografía y Alta Seguridad

Para desplegar este nuevo nivel de protección, los desarrolladores de aplicaciones y los arquitectos de sistemas están incrementando el uso de criptografía para establecer la identidad, proporcionar confidencialidad e integridad a los datos y construir la confianza. La utilización adecuada de la criptografía para cifrar la información, firmar documentos digitales y respetar los derechos digitales está suficientemente probada. La criptografía depende del uso de las claves; un fallo en la protección y el manejo de estas claves rompería una capa completa de seguridad. Muchas organizaciones cometen el error de depender de seguridad software, dejando las claves desprotegidas en servidores de propósito general, vulnerables a ataques. Allá donde la criptografía se utiliza para proteger datos sensibles, las organizaciones deben desplegar controles de Alta Seguridad para gestionar los riesgos. Un elemento fundamental para fortalecer la seguridad criptográfica es la protección de las claves en el interior de un módulo de seguridad hardware (HSM).

El HSM de Realsec, Cryptosec 2048 tiene la certificación FIPS 140-2 Level 3, es el punto de referencia para los productos de Realsec.

HSM. Estrategia de despliegue

Los HSM forman parte de las mejores prácticas de seguridad criptográfica, pero su papel y su valor van mucho más allá que la simple protección de una clave ante un ataque físico. Los HSM, desplegados correctamente, son proporcionan una base criptográfica de seguridad fácilmente escalable, mejorando el rendimiento del sistema y, a la vez, ser suficientemente robusto y flexible para manejar la dinámica de situaciones que se producen en la vida real. Cada organización tiene su conjunto de aplicaciones con sus requisitos de seguridad y su rendimiento específicos. Estas aplicaciones utilizan tecnologías emergentes que tienden a evolucionar como nuevas oportunidades que pueden evolucionar hacia amenazas.

Para manejar la variedad de necesidades dinámicas de una infraestructura de TI, Realsec ofrece su HSM Cryptosec 2048. Entre las necesidades de securización se pueden destacar:

- Infraestructura Web: La protección de las claves SSL es un elemento de seguridad imprescindible para los servidores Web y los dispositivos de red inteligentes. Cryptosec 2048 combina el procesamiento criptográfico de altas prestaciones con una adecuada administración de claves SSL, pasando las claves privadas desde un software vulnerable a estar protegidas en un dispositivo hardware protegido.
- Aplicaciones: los servidores de aplicaciones se encuentran en el núcleo de una red, manejando tanto datos sensibles como sistemas de seguridad crítica como una PKI. Cryptosec 2048 es una solución para asegurar datos sensibles y firmar claves y código de las aplicaciones.
- Seguridad de Servicios Web: los servicios web atraviesan los firewalls y llegan al núcleo central de la aplicación empresarial, incrementando la vulnerabilidad ante un ataque malicioso. Cryptosec 2048 se puede utilizar para proteger las claves que apuntalan el cifrado y firma XML, así como la capa de transporte SSL.
- Medios de Pago: Cryptosec 2048 es un componente obligado para la funcionalidad de medios de pago, cumpliendo las especificaciones de Visa, Mastercard y Euro6000. De esta manera protege los procesos criptográficos asociados a la autenticación de tarjetas inteligentes.
- Bases de Datos. Cifrando información sensible de la base de datos utilizando un HSM integrado con el software de seguridad para cumplir con las recomendaciones legales e industriales.



CryptosecLAN es un producto orientado a la criptografía de propósito general en formato appliance en cuyo interior se encuentra instalado un HSM Cryptosec 2048. Consta de un servidor rack de 1U con las siguientes características:

- Procesador Intel Core 2 Quad.
- 1 GB de memoria RAM.
- 2 conexiones Ethernet 10/100/1000 Mbps.

Capacidades Criptográficas

- Cifrado de clave simétrica:
 - DES simple, triple DES de doble longitud de clave, triple DES de triple longitud de clave en sus cuatro modos;
 - AES con longitud de clave 128, 192, 256 bits en modos ECB y CBC.
 - SAFER en 64 y 128 bit y en modos K y SK; y en los siguientes modos: ECB, CBC, CFB-64 y OFC-64.
- Funciones Hash:
 - MD5.
 - SHA-1, SHA-2 hasta SHA-512.
 - RIPEMD en 128 y 160 bit.
- Estándar de clave pública RSA con longitud de clave de hasta 4.096 bit.
- Control de tiempo, a efectos de Time Stamping.
- Generación de claves a través de un generador de números aleatorios, según lo especificado en FIPS 186-2 con nota de modificación y aprobado por FIPS 140-2.

Seguridad

- El HSM cumple con la certificación del estándar FIPS 140-2 nivel 3.
- El firmware del módulo impide la salida de datos confidenciales.
- Se imposibilita el acceso a las diversas partes del HSM con sensores que detectan intrusiones o anomalías, borrando la información.
- El HSM está cubierto por una resina epoxi opaca, una cubierta metálica protege el conjunto.
- Sistema seguro para carga y custodia de claves de procedencia externa mediante conexión directa a la placa de un terminal asíncrono.
- La clave maestra del HSM está dividida según el algoritmo m de n y las componentes resultantes se almacenan en tarjetas inteligentes. La autenticación de los administradores y custodios también está basada en este algoritmo e igualmente los datos sensibles se almacenan en el soporte mencionado anteriormente.

Acceso

- Interface PKCS#11 v2.20 (Windows, Linux)
- API propietaria TCP/IP

Permite la administración de usuarios, la carga, borrado y actualización de claves y cálculos criptográficos genéricos como cifrado/descifrado o cálculo/verificación de firma. De acuerdo a las necesidades del Cliente, es posible incorporar a CryptosecLan funciones de su interés, como manejo de bloque de PIN, de códigos de Validación o cualquier otra estándar o de diseño propio.

Igualmente es posible incorporar otros algoritmos criptográficos o de hash, como DSA o distintos algoritmos de la familia SHA.

Estas ampliaciones pueden incorporarse al servidor en cualquier momento, a través de una actualización de firmware.

Características Físicas

Tamaño y Peso:

1U 19 "Rack Mount, 42x36x5cm. Peso: 7.5 Kg

Temperatura Operacional.

10 ° C to 60 ° C sin condensación.

Temperatura del Entorno

- 20 ° C to 60 ° C

Humedad:

10% - 90%

Certificación Estándar:

Federal Communication Commission Part 15 (radio frequency devices)

NATIONAL INSTITUTE OF TECHNOLOGY AND STANDART. FIPS 140-2 LEVEL 3