yubico

Protección de claves criptográficas con el módulo de seguridad de hardware (HSM) más pequeño del mundo

El YubiHSM 2 está disponible como solución de nivel 3 con validación FIPS 140-2 o como solución sin FIPS, ambas con las mismas capacidades. Ambas soluciones garantizan una seguridad de hardware criptográfica sin compromisos para aplicaciones, servidores y dispositivos informáticos a una fracción del coste y tamaño de los HSM tradicionales.

Las claves criptográficas almacenadas en software son vulnerables a las amenazas

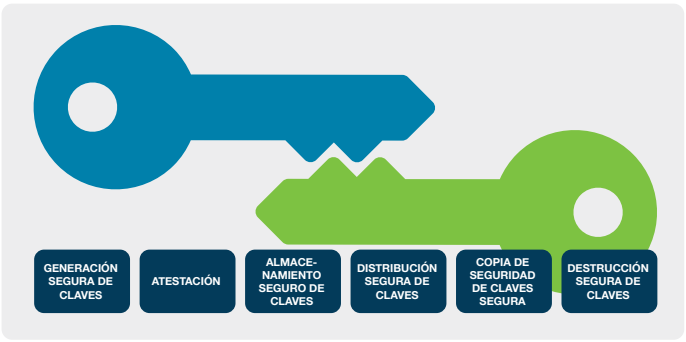
Se espera que el coste de la ciberdelincuencia mundial sea de 6 billones de dólares en 2021, lo que supone un aumento respecto a los 3 billones de 2015.[1] El almacenamiento por software de las claves criptográficas de los servidores es cada vez más v ulnerable a medida que los ataques se vuelven más sofisticados. Por ejemplo, si se compromete una clave privada de una Autoridad de Certificación (CA), un atacante puede fingir que es su sitio web.

The YubiHSM 2 y YubiHSM 2 revolucionan la seguridad eficaz de claves

Garantiza el almacenamiento y las operaciones seguras de claves criptográficas de hardware para aplicaciones, servidores y dispositivos informáticos, al tiempo que elimina el coste y la complejidad de los módulos de seguridad de hardware (HSM) tradicionales. Las soluciones HSM de Yubico son resistentes a las manipulaciones y ofrecen un bajo coste y un alto nivel de seguridad en un factor de forma “nano” portátil que permite un uso flexible en diversos dispositivos y lugares. Con el YubiHSM 2 y el YubiHSM 2 FIPS, las organizaciones pueden evitar que las claves criptográficas sean copiadas por atacantes, malware y personal interno malintencionado. Las empresas pueden realizar una integracion rapida con cualquiera de las dos opciones de HSM utilizando el SDK 2.0 de código abierto.

Protección de hardware segura para claves criptográficas

Las claves criptográficas almacenadas en el software pueden ser copiadas, y son vulnerables a la distribución accidental y al robo a distancia. Si no se implementan procedimientos estrictos, es fácil para los administradores o cualquier personal interno malicioso copiar las claves en memorias USB con el fin de realizar copias de seguridad, enviarlas por ftp o compartirlas con otros a través de un servicio de almacenamiento en la



Protección del ciclo de vida de la clave criptográfica

nube. Además, los atacantes más sofisticados pueden obtener acceso de administrador o desplegar malware troyano que se instala en los servidores, busca claves criptográficas y luego las copia para su venta y distribución en sitios web oscuros como Alphabay.

Las soluciones HSM basadas en hardware permiten el almacenamiento y las operaciones seguras de las claves, ya que impiden la copia y distribución accidental de las mismas, así como el robo a distancia de las claves almacenadas.

- Almacenamiento y operaciones de claves seguras en hardware resistente a la manipulación, con registro de auditoría.
- Amplias capacidades criptográficas que incluyen hashing, envoltura de claves, firma asimétrica, descifrado, atestación y más.

Diseño innovador para un uso flexible

Los HSM tradicionales montados en bastidor y basados en tarjetas no son prácticos para muchas organizaciones debido a los problemas para acomodar el tamaño del HSM y la complejidad de su implementación. Además, el espacio de los bastidores en los centros de datos compartidos suele incluir recintos de servidores físicos con puertas de malla metálica para asegurar el acceso, lo que restringe el espacio disponible.

Con las soluciones HSM de Yubico, las organizaciones pueden asegurar fácilmente servidores, aplicaciones, bases de datos, líneas de montaje, dispositivos IoT, intercambios de criptomonedas y mucho más con un factor de forma “nano” portátil que permite un despliegue rápido y flexible en diversos entornos.

El YubiHSM 2 o el YubiHSM 2 FIPS encaja fácilmente en una ranura USB y queda casi al ras para acomodar los recintos de seguridad física.

[1]Cybersecurity Ventures

- El factor de forma “nano” permite un despliegue y uso flexibles en distintos dispositivos y ubicaciones
- Despliegue de puerto USB-A totalmente oculto
- Red compartible para su uso por aplicaciones en otros servidores

Bajo coste, alta seguridad ROI

Las claves criptográficas almacenadas en el software son susceptibles de ser atacadas por hackers y malware. Por otra parte, la integracion de los HSM tradicionales puede ser costosa.

Con las soluciones HSM de Yubico, las organizaciones obtienen operaciones y seguridad criptográfica de alto nivel empresarial sin el precio tradicional de los HSM.

- Reducción significativa de la inversión: hasta un 90 % más barato que los HSM tradicionales
- El dispositivo de bajo consumo reduce el consumo de energía de las empresas

Integración rápida, gestión sencilla

Con el YubiHSM 2 SDK, los desarrolladores pueden integrar rápidamente la compatibilidad con la versión FIPS o no FIPS del HSM en productos y aplicaciones empresariales con funciones como la generación e importación de claves, la firma y verificación, y el cifrado y descifrado de datos. Los desarrolladores también pueden hacer accesibles estas funciones a través del estándar industrial PKCS#11.

- Soporte de aplicaciones personalizadas mediante bibliotecas de código abierto. Interfaces mediante YubiHSM KSP, PKCS#11 y bibliotecas nativas
- La gestión remota reduce la complejidad de gestión y los costes

Abordar tipos de uso existentes y emergentes

Intercambio seguro de criptomonedas: el mercado de las criptomonedas está creciendo rápidamente, con un gran volumen de activos que necesitan protección contra los nuevos riesgos de seguridad. Se han violado varios intercambios, todos los cuales podrían haberse evitado con un enfoque de seguridad de mejores prácticas que incluya un módulo de seguridad de hardware. Con el YubiHSM 2 SDK, los desarrolladores que crean soluciones para los intercambios de criptomonedas pueden integrar rápidamente el HSM para proteger las claves criptográficas y mantener segura la información financiera sensible.

Entornos seguros del Internet de las cosas (IoT): el Internet de las cosas (IoT) es un área que está emergiendo rápidamente y en la que los sistemas operan a menudo en entornos hostiles.[2] Las claves criptográficas se utilizan en numerosas aplicaciones de la IoT, con una seguridad insuficiente. Esto se debe, en parte, a que la protección de las claves criptográficas y el registro de certificados en las pasarelas o proxies de IoT ha sido complicado, y a que los HSM tradicionales son demasiado grandes y poco manejables para determinados entornos de IoT, como los coches conectados. Con el SDK de código abierto, los desarrolladores que crean aplicaciones IoT pueden integrarse rápidamente con el YubiHSM 2 o el YubiHSM 2 FIPS ultraportátil para proteger las claves criptográficas y evitar que los entornos IoT críticos sean víctimas de tomas de posesión hostiles.

Servicios en la nube seguros: una seguridad sólida para los entornos en la nube es fundamental, ya que las organizaciones necesitan asegurarse de que sus datos se mantendrán seguros en la nube. El HSM puede desplegarse en un centro de datos y funcionar como un componente de una infraestructura de nube. Las organizaciones pueden estar tranquilas sabiendo que el servicio de alojamiento en la nube de su elección ejecuta el YubiHSM 2 o el YubiHSM 2 FIPS como parte de su oferta.

Servicios de certificados seguros de Microsoft Active Directory: la solución HSM puede proporcionar claves respaldadas por hardware para la implementación de PKI basada en Microsoft de una organización. La implementación del HSM en los servicios de certificados de Microsoft Active Directory no solo protege las claves privadas de la autoridad de certificación, sino que también protege todos los servicios de firma y verificación que utilizan la clave privada.[3]

Resumen

YubiHSM 2 y YubiHSM 2 FIPS permiten a las organizaciones de todos los tamaños mejorar la seguridad de las claves criptográficas a lo largo de todo el ciclo de vida, reducir el riesgo y garantizar el cumplimiento de las normativas. Con el YubiHSM SDK 2.0 disponible como código abierto, las organizaciones pueden integrar fácil y rápidamente la compatibilidad con el HSM seguro en una amplia gama de plataformas y sistemas para casos de uso existentes y emergentes en los que la seguridad sólida es más crítica que nunca.

[2] https://www.smartcard-hsm.com/2017/02/14/IoT_Devices_with_SmartCard-HSM.html

[3] Nota: todos los aspectos del SDK 2.0 de YubiHSM 2 están disponibles como código abierto, excepto el proveedor de almacenamiento de claves (KSP) para su uso con los servicios de certificados de Microsoft Active Directory

Yubico AB
Kungsgatan 44
2 ° piso
SE-111 35 Estocolmo
Suecia

Yubico Inc.
530 Lytton Avenue, Suite 301
Palo Alto, CA 94301 EE. UU.
844-205-6787 (número gratuito)
650-285-0088