¿Cómo elegir un HSM?

Dado que la elección del HSM depende de la aplicación específica para la que se utilice, en este documento ofrecemos algunas recomendaciones generales esbozando una lista de posibles criterios a tener en cuenta, independientemente de para qué se pretenda utilizar el HSM.

Factores técnicos

1

Rendimiento:

Consulte los factores de rendimiento de cada tipo de HSM, pero céntrese específicamente en su caso de uso: cifrado/descifrado/generación/firma de claves, simétrico, asimétrico, EC, etc. Pregunte por las verdaderas cifras de rendimiento; por ejemplo, si se trata de un HSM conectado a la red, pregunte por la configuración de la red.

2

Escalabilidad:

¿Cuáles son los factores limitantes en términos de escalabilidad, en relación con su aplicación? ¿Necesita un número definido de claves almacenadas en el HSM? ¿Cómo podría añadir otro HSM? ¿Sería fácil hacerlo?

3

Redundancia:

¿Qué ocurre si se rompe un HSM? ¿Qué impacto tendría esto en sus operaciones? ¿Cómo de fácil sería sustituirlo sin pérdida de servicio, etc.?

4

Copias de seguridad:

¿Cómo se llevan a cabo los procesos de copia de seguridad y restauración? ¿Qué esfuerzo le supondría a su organización implantar estos procesos? ¿Es capaz de evitar la pérdida irremediable de sus datos?

5

Soporte de la API:

La API es la conexión con su entorno de Aplicación-Host. A continuación, se ofrecen algunos consejos para responder a las preguntas sobre las API admitidas:

PROJECTNET

Microsoft MS CSP/CNG: La API "estándar" de Microsoft es la forma más sencilla de conectarse a un HSM cuando se utiliza Windows;

JCE: El desarrollador "estándar" de Java.

PKCS#11: El "estándar de la industria", pero hay algunos escollos como los problemas de seguridad conocidos y las extensiones propietarias del proveedor. ATENCIÓN: Las extensiones o mecanismos propietarios de los proveedores son extensiones de la API específicas para cada caso, y no forman parte del estándar PKCS#11. Esto aumentará los costes al cambiar de proveedor.

Software y capacidad de servicio

1

OS / hardware support:

Para ello hay que tener en cuenta diferentes cuestiones. ¿Qué sistemas operativos son compatibles con la tarjeta integrada (PCIe-Driver)? ¿Qué sistemas operativos son compatibles con el HSM conectado a la red? ¿Qué sistemas operativos son compatibles con las herramientas de gestión, por ejemplo, GUI/línea de comandos?

2

Gestión:

¿Se puede gestionar el HSM a distancia? ¿Qué funciones se pueden activar y controlar a distancia?

3

Programabilidad:

La mayor parte de su desarrollo estará en el otro extremo de las API, pero a veces puede ser útil tener la capacidad de escribir aplicaciones que se ejecutan en el dispositivo, para una mayor flexibilidad o velocidad y para especificar su API.

4

Seguridad física:

Hágase la pregunta: ¿Hasta qué punto debe ser su solución resistente a los ataques físicos directos? Si, por la razón que sea, decide que es especialmente importante, quizá quiera buscar "detección y respuesta activa a la manipulación", en lugar de sólo "resistencia pasiva a la manipulación y pruebas".

5

Algoritmos:

¿Es compatible el HSM con el algoritmo criptográfico que desea utilizar, a través de la API seleccionada (primitivas, modos de funcionamiento y parámetros, por ejemplo, curvas, tamaños de clave)?

6

Opciones de autenticación:

Contraseñas; quórum; n-factores; tarjetas inteligentes; etc. Como mínimo, deberías buscar algo que requiera un tamaño de quórum configurable o usuarios autentificados con contraseña antes de permitir las operaciones mediante el uso de una clave.

7

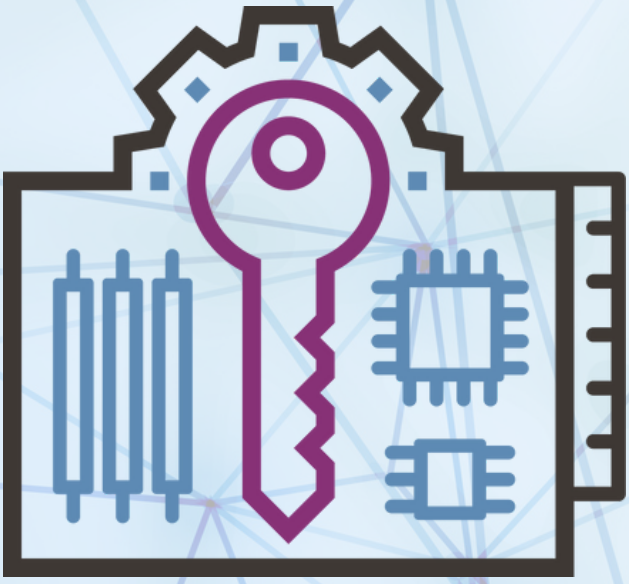
Opciones de política:

Es posible que desee poder definir políticas, como controlar si: las claves pueden exportarse desde el HSM (encriptadas o no); una clave sólo puede utilizarse para firmar/encriptar/desencriptar/...; se requiere autenticación para firmar, pero no para verificar, etc.

8

Capacidad de auditoría:

Incluye tanto las operaciones de tipo HSM (clave generada, algo firmado con la clave Y) como la gestión de problemas de conexión o caídas. ¿Cómo de fácil va a ser integrar los registros en su sistema de monitorización (syslog/snmp/otra salida accesible por la red - o al menos no propietaria)?



info@projectnet.com.pe

PROJECTNET