Hardware Security Module - HSM

Es un dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas. El HSM da velocidad a sus operaciones y permite mejorar la seguridad de todo tipo de aplicaciones, desde la emisión de certificados PKI y encriptación de bases de datos a sistemas que emplean firmas digitales, hasta las comunicaciones vía SSL. Adicionalmente un HSM permite proteger las claves y operaciones criptográficas mediante hardware resistente a cualquier manipulación.

¿Cuál es la función de los hardware security modules?

Los HSM otorgan protección a las transacciones, identidades y aplicaciones mediante la protección de claves criptográficas y la prestación de servicios de cifrado, descifrado, autenticación y firma digital para una diversidad de aplicaciones.

Consideraciones de Seguridad

Como se ha mencionado, el objetivo de un HSM es el almacenado seguro de certificados PKI, que son los datos sensibles de esta tecnología.

La seguridad que proporcionan dichos dispositivos es muy elevada si se siguen ciertas políticas de seguridad.
Las claves protegidas por los HSM sólo están 'completamente protegidas por hardware' si fueron generadas dentro del propio hardware (si se generan fuera y se importan, las copias de dichas claves fuera del dispositivo -obviamente- no podrán ser protegidas por el dispositivo HSM).

Las causas por las que se hacen útiles estos dispositivos son dos: Seguridad y Rendimiento:

Seguridad: En aquellos servidores web que actúan mediante el protocolo criptográfico SSL, los certificados de clave pública, como el que contiene la clave privada (key), son almacenados en el sistema de ficheros del mismo.
Evidentemente, se ajustan los permisos de dichos ficheros para que sólo sean accesibles por el usuario que ejecuta el servidor Web (y evidentemente root), protegiendo al máximo el acceso a dichos ficheros.
Sin embargo, si dicho servidor se viese comprometido, sería posible sacar esos certificados fuera del mismo, pudiendo suplantar el servidor por parte de un usuario malicioso dando lugar a un mega-phising (con certificado válido si además hacemos coincidir el nombre del dominio con el que aparece en el certificado original). Evidentemente y por defecto, esto no es tan sencillo, puesto que además el certificado de clave privado está protegido mediante una clave. Al arranque del servidor web, o le colocamos la contraseña mediante la entrada estándar o harcodeamos en algún otro fichero, la contraseña del certificado privado o lo configuramos sin contraseña. La otra opción es utilizar un módulo HSM para custodiar dicha contraseña, como indicábamos antes. De esta manera, si el servidor es comprometido remotamente, pueden llevarse los certificados pero no la contraseña que los protege, puesto que se encuentra en el HSM. De la misma forma, si no tenemos HSM configurado, la contraseña que protege el certificado, en algún momento se encuentra en memoria, de manera que haciendo un dump de la misma podemos dar con la contraseña. Utilizando módulos HSM, la contraseña no sale del dispositivo, sino que se le pasa el certificado cifrado mediante su API y nos devuelve el resultado ya descifrado para poderlo utilizar por la aplicación en concreto.

Rendimiento: Además de permitir la generación y custodia de la contraseña de los certificados, efectúan las operaciones criptográficas, que suelen ser tareas que consumen muchísimos ciclos de CPU (debido a la necesidad de generar números primos de gran tamaño), mediante un procesador aparte especializado, de manera que libera a servidor de ese tipo de tareas. En general, la efectividad de los módulos HSM es mayor en criptografía de clave pública (o asimétrica) que en criptografía simétrica. En las sesiones SSL se hace uso de ambos tipos de criptografía: al principio de la sesión se utiliza clave pública o asimétrica y una vez negociada la clave a utilizar, se utiliza clave simétrica como se ve en la siguiente figura.

Seguridad y Rendimiento

Permite

- Generar, almacenar y proteger Claves.
- Seguridad basada en el cifrado
- Comunicación segura
- Autenticación y firma digital