Administración de claves de alta escalabilidad (HSK)

Administre millones de claves simultáneamente con alto rendimiento

CARACTERÍSTICAS PRINCIPALES

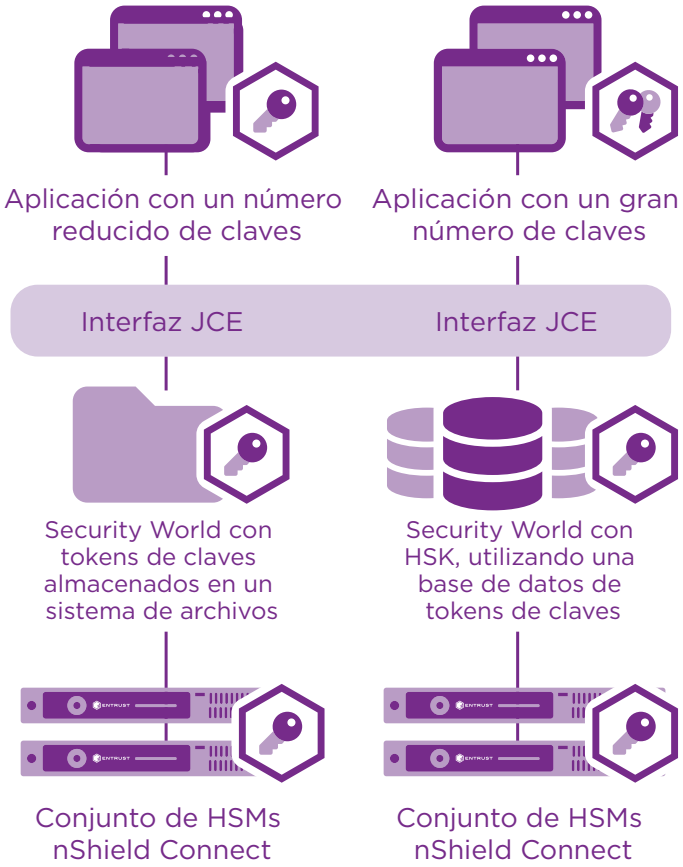
- Una solución de alto rendimiento y altamente escalable para casos de uso específicos de HSMs nShield® de Entrust
- Admite una gran cantidad de claves criptográficas activas simultáneamente
- Evita los cuellos de botella del sistema operativo

Algunos casos de uso de los módulos de seguridad de hardware (HSMs) requieren de la administración de un gran número de claves criptográficas al mismo tiempo. Esto puede causar cuellos de botella en el sistema de archivos de las computadoras conectadas a los HSMs. El almacén de claves de alta escalabilidad (HSK) admite una gran cantidad de claves con alto rendimiento.

Características principales

La solución HSK ofrece las siguientes características:

- Escalabilidad a millones de claves RSA
- El rendimiento permanece esencialmente sin cambios a medida que aumenta el número de claves
- Admite generación de claves RSA, generación de solicitudes de firma de certificado (CSR), creación y verificación de firmas digitales, cifrado y descifrado de datos.
- Sincronización automática entre varias computadoras que realizan llamadas
- Solución extensible personalizable para adaptarse a sus necesidades



APRENDA MÁS EN ENTRUST.COM/HSM

Administración de claves de alta escalabilidad

Cómo funciona

Los HSMs nShield de Entrust proporcionan un desempeño de transacciones de alto rendimiento y admiten miles de transacciones por segundo. (El rendimiento depende del modelo del HSM y de la operación criptográfica específica. Consulte las fichas técnicas de los modelos nShield específicos para obtener los detalles más recientes sobre el rendimiento del HSM).

La arquitectura Security World flexible y segura de Entrust almacena claves criptográficas externas en el HSM, en forma de "tokens". Las claves dentro de los "tokens" están fuertemente protegidas por claves maestras de HSM, utilizando cifrado, restricciones de uso, controles de acceso y seguridad de autenticación. Esto combina una seguridad muy sólida con los beneficios de escalabilidad, equilibrio de carga, conmutación por error, fácil expansión o contracción de la cantidad de HSMs en un grupo, intercambio de HSMs dentro y fuera del grupo y una copia de seguridad sencilla de los tokens de claves sin la necesidad de dispositivos adicionales de copia de seguridad.

La arquitectura estándar de Security World almacena estos "tokens" en los sistemas de archivos de las computadoras que realizan llamadas (con soporte de sincronización), usando un solo archivo por token. Este enfoque se adapta a la mayoría de los casos de uso que normalmente tienen un número limitado de claves activas por computadora del cliente.

En ciertos casos de uso, el rendimiento del HSM nShield puede verse limitado por las latencias presentes en el sistema de archivos del sistema operativo de la computadora que realiza la llamada. HSK proporciona un alto rendimiento cuando hay una gran cantidad de claves mediante el uso de una base de datos, en lugar del sistema de archivos, para almacenar los tokens de claves en la computadora cliente.

El equipo de servicios profesionales (PS) de Entrust lo ayudará a evaluar si el HSK es adecuado para sus necesidades. Los consultores de PS también brindarán soporte para desarrolladores expertos para ayudarlo a integrar HSK en su entorno, incluida la personalización de HSK para satisfacer sus requisitos específicos según sea necesario.

Ejemplos de casos de uso

- Seguridad del correo electrónico corporativo para un gran número de usuarios
- Firma de documentos empresariales
- Internet de las cosas (IoT) con una gran cantidad de dispositivos conectados
- Aplicaciones móviles con una gran cantidad de usuarios finales
- Sistemas de billetera electrónica para intercambios de criptomonedas

Detalles técnicos

- Biblioteca Java Cryptography Extension (JCE), utilizando HSMs nShield
- Opción de servicios web RESTful JSON
- Almacena los "tokens" de claves de HSMs nShield en una base de datos en lugar del sistema de archivos
- Funciona con software de base de datos relacional popular, incluidos MSSQL, Oracle y Derby (con la adición de bases de datos adicionales)
- Funciona con un solo HSM o varios HSMs en un grupo de carga equilibrada

Más información

Para saber más sobre los HSMs nShield de Entrust visite **entrust.com/HSM**. Para saber más sobre las soluciones de seguridad digital de Entrust para identidades, acceso, comunicaciones y datos, visite **entrust.com**

Aprenda más en
entrust.com/HSM

ENTRUST

Contacte con nosotros:
HSMinfo@entrust.com