Seguridad mejorada: la protección de claves de alta seguridad de Entrust para Red Hat Certificate System

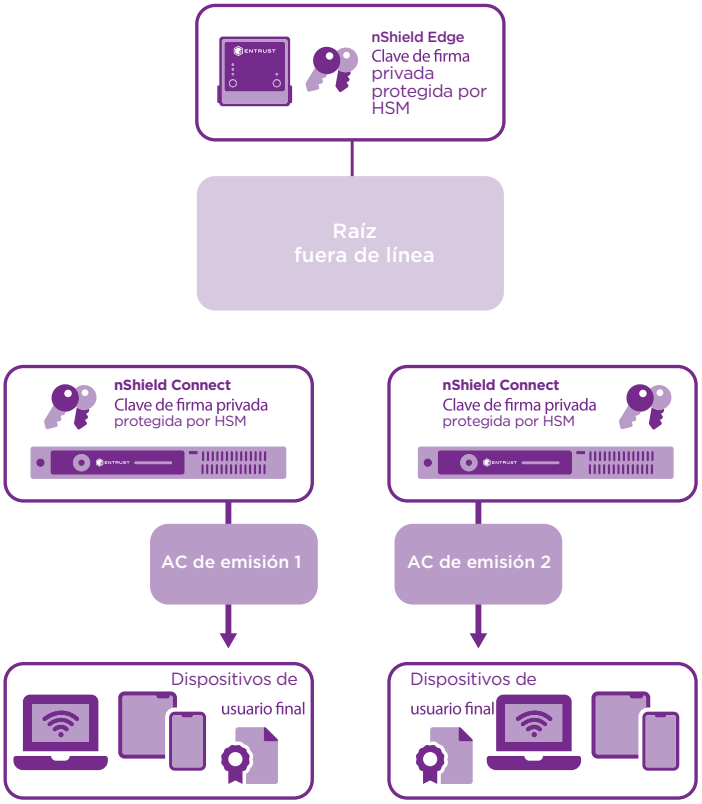
Generar confianza para la infraestructura de clave pública (PKI)

CARACTERÍSTICAS PRINCIPALES

- Amplíe la seguridad de Red Hat Certificate System para las soluciones comerciales de la NSA para aplicaciones clasificadas (CSfC)
- Fortalecer el marco de seguridad gestionando las identidades de los usuarios y manteniendo la privacidad de las comunicaciones
- Proteger las transacciones y las aplicaciones habilitadas para la PKI
- Utilice módulos de seguridad de hardware (HSMs) nShield® de Entrust certificados por NIST FIPS 140-2

El problema: las KPI organizacionales se están ampliando para cumplir con un número cada vez mayor de aplicaciones comerciales

A medida que las brechas de datos se vuelven más sofisticadas, las organizaciones han recurrido a sus PKIs para proteger y controlar el acceso a aplicaciones críticas y datos confidenciales. Dentro de una PKI, la autoridad de certificación (CA) emite credenciales electrónicas para validar las identidades en línea y hacer cumplir los controles de acceso. Analizar la cantidad de certificados digitales utilizados, la importancia y el valor de las aplicaciones que admiten y si las aplicaciones están sujetas a niveles más altos de escrutinio debido al cumplimiento normativo del gobierno o de la industria, son factores críticos para garantizar que la PKI pueda satisfacer las crecientes demandas.



Los HSMs de nShield protegen las claves privadas utilizadas por Red Hat Certificate System.

APRENDA MÁS EN ENTRUST.COM/HSM

Protección de claves de alta seguridad para el sistema de certificaciones de Red Hat

El desafío: establecer una raíz de confianza para los controles de identidad y acceso

La protección de la integridad y seguridad de la CA que sustenta una PKI es de vital importancia para garantizar la confianza en las aplicaciones comerciales y en los datos que protegen. Dado que las PKI admiten cada vez más las topologías cambiantes de acceso de los usuarios, incluidos los dispositivos móviles y de traiga su propio dispositivo (BYOD, por sus siglas), las organizaciones deben asegurarse de que las claves criptográficas privadas estén protegidas y sean gestionadas de manera confiable.

La solución: Red Hat y Entrust brindan juntos una protección sólida de las identidades digitales

Red Hat Certificate System emite, gestiona y valida las identidades digitales que se utilizan para vincular personas, dispositivos o servicios a sus claves privadas correspondientes. La validez de cada certificado emitido depende de la protección de la clave CA que emite las identidades. Cuando el proceso de emisión se ejecuta en un servidor utilizando una clave almacenada localmente en un archivo, esa clave puede ser vulnerable a la duplicación, modificación y sustitución. Hoy en día, la mayoría de las CA se utilizan para emitir certificados para su uso dentro de una organización. Internamente, los certificados se utilizan normalmente para realizar autenticación por cable e inalámbrica, conexiones de seguridad de capa de conexión/transporte seguro (SSL/TLS) y autenticación de red privada virtual (VPN). Dado que las aplicaciones en expansión necesitan los servicios de una PKI, las demandas de las CA y la necesidad de una seguridad mejorada son primordiales.

Los HSMs nShield de de Entrust aumentan el nivel de seguridad de la PKI al proteger la raíz privada y las claves de CA de firma. Los HSMs nShield protegen los procesos de emisión, gestión y validación, lo que les permite a las organizaciones fortalecer la solución de identidad y acceso. Los HSMs nShield se integran fácilmente con Certificate System de Red Hat utilizando interfaces de programación de aplicaciones criptográficas estándar (CAPI). Cuando se utilizan los HSMs nShield de Entrust, todo el procesamiento de validación y emisión de certificados se produce dentro de los límites protegidos del HSM. Las claves de firma y raíz privadas nunca son accesibles o en un formato legible fuera del HSM. Incluso durante los procesos de copia de seguridad, archivo y recuperación, los HSMs nShield garantizan que las claves privadas no sean susceptibles de manipulación y/o compromiso.

Protección de claves de alta seguridad para el sistema de certificaciones deRed Hat

¿Por qué utilizar HSMs de Entrust con Certificate System de Red Hat?

La identificación de brechas, la recuperación y la planificación de contingencias son pasos importantes que se pueden tomar para fortalecer la seguridad de una PKI. Una PKI reforzada y de alta seguridad proporciona un entorno que protege las claves críticas para la seguridad contra robos y usos indebidos. Vincular la emisión de certificados a las verificaciones y aprobaciones de identidad utilizando un HSM nShield de Entrust, ha sido una lección importante aprendida de los compromisos de seguridad de CA anteriores.

Certificados según estrictos estándares de seguridad, incluidos FIPS 140-2 Nivel 3 y Common Criteria EAL4+, los HSMs nShield:

- Almacene las claves para firmar y emitir certificados digitales en un entorno seguro y resistente a manipulaciones indebidas
- Gestione el acceso de administradores con una política basada en tarjetas inteligentes y autenticación de dos factores
- Cumpla con los requisitos normativos del sector público, los servicios financieros y las empresas

HSMs de Entrust

Los HSMs de Entrust nShield se encuentran entre las soluciones de HSMs de mayor rendimiento, más seguras y fáciles de integrar que se encuentran disponibles, lo cual facilita el cumplimiento normativo y ofrece los niveles más altos de seguridad de datos y aplicaciones para organizaciones empresariales, financieras y gubernamentales. Nuestra exclusiva arquitectura de gestión de claves Security World proporciona controles sólidos y granulares sobre el acceso y uso de claves.

Red Hat

Red Hat es el proveedor mundial líder de soluciones de código abierto para empresas. Además de sistemas de certificaciones de Red Hat, las soluciones incluyen las plataformas Red Hat Enterprise Linux, Red Hat OpenStack y Red Hat OpenShift, entre una amplia gama de servicios y administración. Los HSMs nShield de Entrust están certificados con Red Hat Certificate System. **www.redhat.com**

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**

Para saber más sobre los HSMs nShield de Entrust

HSMinfo@entrust.com

entrust.com/HSM

ACERCA DE ENTRUST

Entrust ayuda a que el mundo se mueva de forma segura al permitir la protección fiable de identidades, pagos y datos. Hoy más que nunca, las personas exigen experiencias seguras y sin problemas, ya sea que crucen fronteras, realicen una compra, accedan a servicios de gobierno electrónico o inicien sesión en redes corporativas. Entrust ofrece una variedad incomparable de soluciones de seguridad digital y emisión de credenciales en el núcleo de todas estas interacciones. Con más de 2500 colegas, una red de socios globales y clientes en más de 150 países, no es de extrañar que las organizaciones más confiables del mundo confíen en nosotros.

Aprenda más en
entrust.com/HSM

ENTRUST

Contáctenos:
HSMinfo@entrust.com