Proteja las infraestructuras de clave pública con HSMs nShield de Entrust

NFINITY
STRATEGIC TECHNOLOGY PARTNER PROGRAM

Protección de alta seguridad de las claves que sustentan las PKIs

CARACTERÍSTICAS PRINCIPALES

- Proteja la raíz crítica y las claves de CA emisoras dentro de un HSM con certificación FIPS 140-2 Nivel 3 a prueba de manipulaciones indebidas
- Establezca una autenticación sólida para los dispositivos conectados
- Facilite la auditoría y el cumplimiento de las normas de seguridad de datos
- Logre niveles de seguridad y confianza de datos más altos
- Mantenga altos niveles de servicio y agilidad empresarial

El desafío:

La digitalización empresarial y el floreciente Internet de las cosas (IoT) ponen de manifiesto la necesidad de establecer identidades confiables para los usuarios, dispositivos y aplicaciones que accedan a sistemas y datos. Las identidades únicas y rastreables para usuarios y dispositivos permiten mayores ingresos y reducción de costos a través de nuevos productos, servicios y formas de hacer negocios.

CA: Autoridad de certificación VA: Autoridad de validación RA: Autoridad de registro

APRENDA MÁS EN ENTRUST.COM/HSM

Proteja las infraestructuras de clave pública con el HSM nShield

Para capitalizar estas oportunidades y salvaguardar los sistemas y los datos, es fundamental garantizar que:

- Los usuarios que administran el dispositivo o sistema estén autorizados para hacerlo.
- El código que se ejecuta en los dispositivos conectados, incluido el firmware, el sistema operativo y las aplicaciones, sea confiable y no se haya modificado.
- Los datos en tránsito entre dispositivos, personas y aplicaciones sean válidos y estén protegidos de cambios no autorizados
- Las transacciones financieras se puedan proteger y autenticar

Una infraestructura de clave pública (PKI) proporciona un mecanismo mediante el cual se pueden establecer y administrar identidades auténticas para usuarios y dispositivos, también llamados entidades. Una vez autenticadas, estas entidades pueden acceder a sistemas y recursos empresariales críticos, así como a operaciones completas de firma digital. Una PKI se basa en certificados digitales, firmados por una autoridad de certificación (CA), que vinculan una clave pública a un usuario o dispositivo específico. Según este marco, las claves privadas de la CA raíz y emisora son objetivos atractivos que requieren una protección de alta seguridad, ya que representan las claves virtuales del reino.

La solución: PKIs integradas con HSMs nShield de Entrust

Si bien es posible implementar una PKI sin una raíz de hardware de confianza, las claves de CA que se manejan fuera del límite criptográfico de un HSM certificado pueden ser más vulnerables a los ataques que pueden comprometer las capacidades de emisión de credenciales y revocación de certificados de la PKI. El uso de HSMs es una práctica recomendada reconocida para proteger la raíz y emitir claves privadas de CA que sustentan las implementaciones de PKI.

Los HSMs nShield® de Entrust están integrados con los principales proveedores de PKI para ofrecer protección FIPS 140-2 de nivel 3 y Common Criteria EAL 4+ para la raíz y las claves privadas de la CA emisora. Los clientes disfrutan de una postura de seguridad mejorada y pueden demostrar el cumplimiento de requisitos como el Estándar de seguridad de datos de la industria de tarjetas de pago.

La diferencia de nShield

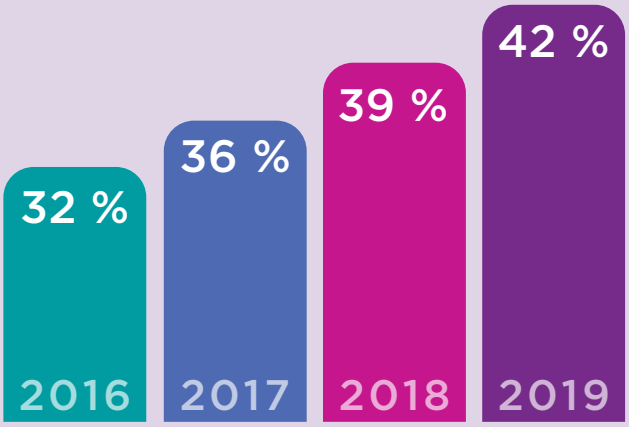
Los HSMs nShield de Entrust ofrecen una forma comprobada, auditable de asegurar claves y material criptográfico valioso. HSMs nShield con certificación FIPS y Common Criteria

- Protegen las claves dentro de un límite criptográfico cuidadosamente diseñado
- Emplean robustos mecanismos de control de acceso con separación obligatoria de tareas, para garantizar que las claves solo sean utilizadas por entidades autorizadas.
- Garantizan la disponibilidad de la clave usando sofisticadas funciones de administración, almacenamiento y redundancia de claves
- Ofrecen un rendimiento alto para admitir un número de aplicaciones en aumento
- Escalan para satisfacer las demandas cambiantes mediante una capacidad de administración mejorada

Los HSM nShield de Entrust están disponibles en varios factores de forma, mientras que nShield como servicio proporciona acceso por suscripción a los HSMs nShield Connect.

Proteja las infraestructuras de clave pública con el HSM nShield

¿Cómo administra las claves privadas para sus CAs de raíz/políticas/emisión?



Los módulos de seguridad de hardware (HSMs)

Fuente: Estudio de tendencias globales de PKI de 2019, Ponemon Institute y Entrust

"Las PKIs de las organizaciones admiten un promedio de 8.5 aplicaciones distintas. todo ello supone que la PKI es el punto central de la TI de una empresa".

Estudio de tendencias globales de PKI de 2019, Ponemon Institute y Entrust

Socios nFinity

Los HSMs nShield de Entrust están integrados con los siguientes proveedores de PKI a través de nuestro programa de socios tecnológicos nFinity. Visite nuestro sitio web para obtener la lista más reciente de socios.

axway
KEYFACTOR
cybertronixx
Microsoft
nexus
DEVICE AUTHORITY
IoT Security Simplified
PrimeKey
digicert®
Red Hat
Entrust Datacard
RSA SECURITY™
HID
HID CORPORATION
SAFELAYER
INSTA
TRUSTONIC
Information Security CORPORATION

Más información

Para saber más sobre los HSMs nShield de Entrust visite **entrust.com/HSM**. Para conocer 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

SOBRE ENTRUST CORPORATION

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.

Más información
entrust.com/HSM

ENTRUST

Contáctenos:
HSMinfo@entrust.com