Entrust ofrece soluciones de PKI autogestionadas para abordar las necesidades de seguridad específicas de la empresa

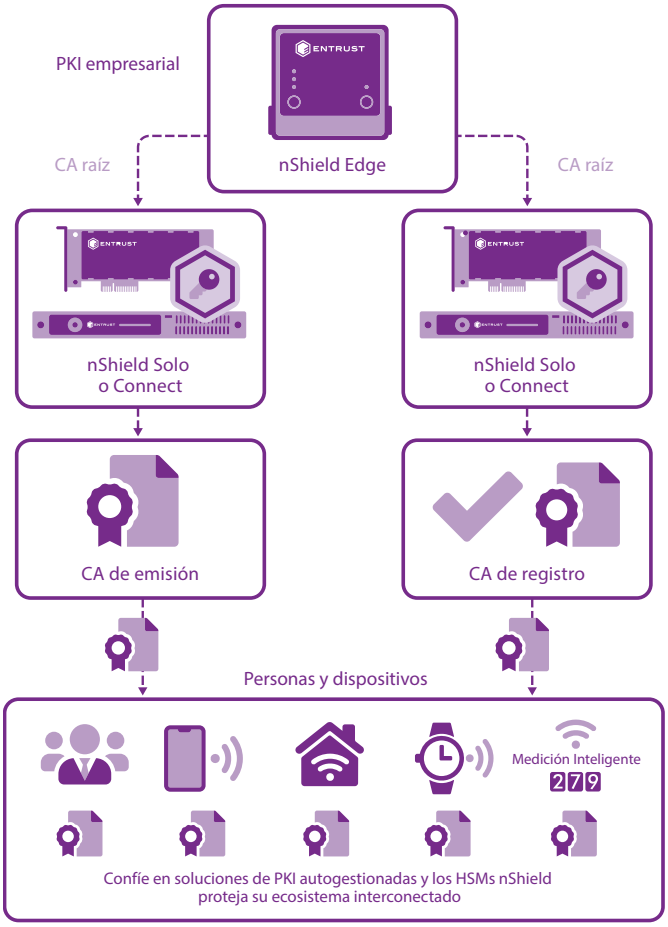
Implemente y mantenga soluciones de administración de identidad seguras con los servicios de Entrust y los módulos de seguridad de hardware

CARACTERÍSTICAS PRINCIPALES

- Proteja la identidad de las personas y del dispositivo
- Desarrolle el proceso y los procedimientos correctos
- Evalúe el estado de las implementaciones de PKI existentes
- Migre las PKI para satisfacer las crecientes demandas
- Facilite la auditoría y el cumplimiento de seguridad

El problema: la creciente adopción de tecnologías interconectadas está ampliando las capacidades de las infraestructuras de clave pública (PKI) existentes e impulsando la necesidad de crear nuevas

El uso creciente de aplicaciones habilitadas para criptografía y el impacto de la Internet de las cosas (IoT) está creando nuevas demandas sin precedentes en las PKI. La expansión de los requisitos de acreditación y la necesidad de administrar la manera como los dispositivos y sensores se conectan de manera segura a ecosistemas de red cercanos está impulsando a las empresas a reevaluar la salud de sus PKI existentes. Junto con los estándares de seguridad cambiantes, las empresas están reconsiderando sus estrategias de implementación de la PKI y, en algunos casos, están rediseñando y migrando a implementaciones nuevas y más sólidas.



APRENDA MÁS EN ENTRUST.COM/HSM

Soluciones de PKI autogestionadas para abordar las necesidades de seguridad específicas de la empresa

El desafío: mantener una sólida raíz de confianza en toda la PKI empresarial que satisfaga las demandas operativas de las aplicaciones más sensibles a la seguridad

Con más aplicaciones sensibles a la seguridad que utilizan PKIs, la seguridad de las claves privadas subyacentes es esencial. Según el Estudio de Tendencias de PKI de 2020 Ponemon Institute, las tres aplicaciones principales que utilizan certificados digitales incluyen SSL/TLS para sitios web públicos, aplicaciones basadas en la nube pública y autenticación de usuarios empresariales. Los certificados digitales permiten la identificación de aplicaciones y dispositivos y la autenticación en ecosistemas confiables. Esto requiere de la protección y administración de un número creciente de claves privadas de manera automatizada y confiable.

La solución: las ofertas de PKI autogestionadas de Entrust combinan servicios de consultoría con el hardware de seguridad adecuado para ayudar al cliente desde la definición de los requisitos hasta la implementación y la capacitación

Los requisitos de PKI empresarial suelen ser únicos en función de su negocio, sus clientes y las aplicaciones que admiten. Las ofertas de PKI autogestionadas de Entrust combinan la experiencia técnica en el diseño y la implementación de PKIs organizacionales, con el hardware de seguridad necesario para proporcionar una sólida raíz de confianza para el sistema. Los servicios incluyen la evaluación de requisitos iniciales y el desarrollo de procesos y procedimientos, junto con el diseño, así como la implementación de la infraestructura necesaria para garantizar que los clientes puedan implementar PKIs que cumplan con los requisitos actuales y futuros. La consultoría puede admitir entornos operativos que necesitan alta disponibilidad y redundancia, o entornos de laboratorio para ayudar a los clientes a desarrollar sus propios conjuntos de habilidades de PKI. Para los clientes que implementan PKI por primera vez, las ofertas incluyen documentación y servicios de implementación combinados con hardware de seguridad de soporte. Para los clientes con implementaciones de PKI existentes y en crecimiento, las ofertas incluyen controles de estado y servicios de migración, incluido el servicio de migración SHA junto con hardware de seguridad.

Los módulos de seguridad de hardware (HSMs) nShield® de Entrust aumentan el nivel de garantía de las implementaciones de PKI. Diseñados para proteger y administrar la clave privada subyacente en un entorno aislado certificado, los HSMs nShield de Entrust admiten PKIs de Microsoft, Red Hat, Entrust, RSA e Insta, mediante interfaces de programación de aplicaciones criptográficas estándar (CAPI).

Soluciones de PKI autogestionadas para abordar las necesidades de seguridad específicas de la empresa

Por qué utilizar HSMs de Entrust con PKIs autogestionadas

La implementación de un mayor número de aplicaciones críticas para la seguridad y dispositivos conectados está aumentando la demanda de las PKIs, y se espera que no solo protejan las claves privadas de la autoridad certificadora (CA) raíz de los certificados individuales y de dispositivo emitidos en todos los dominios, sino también su registro. Las PKIs organizativas que no utilizan HSMs para proteger sus claves privadas las dejan vulnerables a interrupciones con posibles consecuencias graves. Los HSMs proporcionan un entorno reforzado que protege las claves críticas para la seguridad contra el robo y el uso indebido, y permite la gestión de su ciclo de vida completo con soporte de conmutación por error. Vincular la emisión de certificados a las verificaciones y aprobaciones de identidad utilizando un HSM ha sido una lección importante aprendida de los compromisos de seguridad de CA. Certificados según estrictos estándares de seguridad, incluidos FIPS 140-2 Nivel 3 y Common Criteria EAL 4+, los HSMs nShield de Entrust:

- Almacenan la CA raíz y las claves de inscripción en un entorno seguro y resistente a manipulaciones indebidas
- Gestionan el acceso de administradores con una política basada en tarjetas inteligentes y autenticación de dos factores
- Cumplen con los requisitos normativos del sector público, los servicios financieros y las empresas

Entrust

Con la simplificación de la administración de las credenciales de identidad en toda la empresa, incluidos los entornos virtualizados, los HSMs nShield de Entrust ayudan a las organizaciones a cumplir con los requisitos en materia de auditoría y cumplimiento, como el Estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS) y la Directiva de servicios de pago (PSD2). Los HSMs nShield están disponibles en los siguientes modelos para satisfacer las necesidades específicas del cliente:

- HSM nShield Edge: HSM portátil con conexión USB para CA raíz fuera de línea y para aplicaciones de desarrollador
- HSM nShield Solo / Solo + / Solo XC: HSM integrado PCI Express de alto rendimiento para servidores
- HSM nShield Connect / Connect+ / Connect XC: HSM de alto rendimiento conectado a la red para centros de datos

Conozca más

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

Entrust es una marca comercial registrada y/o una marca de servicio de Entrust Corporation en Estados Unidos y/o en otros países. ©2020 Entrust Corporation. Todos los derechos reservados. November 2020 • PLB9493