Soluciones de identidad confiables de Entrust que permiten la transformación empresarial digital

Las soluciones integradas mejoran la seguridad de las implementaciones de la PKI

CARACTERÍSTICAS PRINCIPALES

- Identidades de usuario seguras en aplicaciones empresariales
- Controle el acceso a las implementaciones locales y alojadas
- Administre el ciclo de vida del certificado, incluida la copia de seguridad/ recuperación
- Proporcione una raíz de confianza para proteger las claves privadas confidenciales
- Facilite el cumplimiento normativo con FIPS y Common Criteria
- Admita implementaciones en las instalaciones, en la nube e híbridas

El problema: mayor necesidad de una identidad confiable en un ecosistema en rápida expansión

El Internet de las cosas (IoT), la proliferación de dispositivos móviles y la aparición de nuevos requisitos tales como el respaldo de la emisión de certificados de dispositivo para los programas Traiga su propio dispositivo (BYOK) y la inscripción de dispositivos en red del IoT, hacen que la administración de identidades sólida sea más importante que nunca. Las soluciones de infraestructura

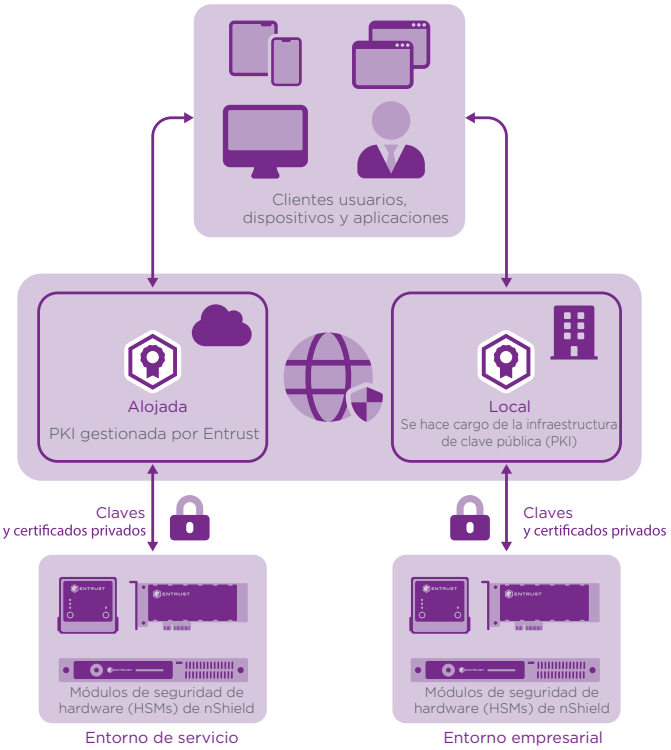

Ilustración de alto nivel de los componentes utilizados en una instalación habitual de administración remota

APRENDA MÁS EN ENTRUST.COM/HSM

Soluciones de identidad confiables de Entrust que permitan la transformación empresarial digital

de clave pública (PKI) son ideales para establecer identidades confiables de usuarios, dispositivos, aplicaciones y servicios para el acceso seguro a sistemas y recursos empresariales críticos, entregando elementos críticos de un entorno seguro.

El desafío: asegurar la gestión de las claves de la autoridad de certificación (CA)

Una protección sólida para las claves privadas utilizadas por las PKI alojadas o locales es esencial para una estrategia de seguridad eficaz. La confiabilidad de una PKI depende de la protección otorgada a las claves privadas en la jerarquía de la CA y los procesos de verificación asociados. Las claves de CA almacenadas y gestionadas en software pueden ser vulnerables a amenazas avanzadas que pueden comprometer su seguridad. La gestión de claves de hardware exclusivo mejora la seguridad y reduce el riesgo de un ecosistema empresarial confiable.

La solución: una solución integrada con una raíz de confianza sólida

Las soluciones de PKI de Entrust establecen y administran la seguridad basada en certificados para aplicaciones comerciales críticas. Entrust Security Manager les permite a los clientes implementar y administrar sus propios certificados digitales. El producto autentica a los usuarios, controla el acceso y protege las aplicaciones criptográficas. Para los clientes que buscan un enfoque de no intervención, Entrust Managed PKI ofrece una solución alojada.

Los módulos de seguridad de hardware (HSM) nShield® de Entrust se integran con las ofertas de PKI de Entrust para proteger la privacidad y la integridad de las claves confidenciales. Las organizaciones que buscan ampliar la seguridad de las PKIs alojadas o en las instalaciones pueden implementar soluciones de Entrust con HSMs nShield, in situ o como servicio, para garantizar que las claves críticas nunca estén expuestas a entidades no autorizadas. Los HSMs nShield generan, almacenan y gestionan de forma segura claves privadas de la CA.

¿Por qué utilizar nShield con Entrust Security Manager y Managed PKI?

Si bien es posible implementar PKIs sin una raíz de hardware de confianza, las claves de CA que se manejan fuera del límite criptográfico de un HSM certificado son significativamente más vulnerables a los ataques que pueden comprometer las capacidades de emisión de credenciales y revocación de certificados de las PKI.

El uso de HSMs se considera una práctica recomendada para las implementaciones de PKI, ya que proporciona una forma comprobada y auditable de proteger material criptográfico valioso. Los HSMs les permiten a las organizaciones:

- Proteger las claves de CA dentro de límites criptográficos cuidadosamente diseñados que emplean robustos mecanismos de control de acceso con separación obligatoria de tareas, para garantizar que las claves solo sean utilizadas por entidades autorizadas.
- Asegurar la disponibilidad mediante el uso de funciones sofisticadas de gestión, almacenamiento y redundancia de claves para garantizar que siempre estén accesibles cuando las necesite
- Ofrecer un rendimiento alto para admitir un número de aplicaciones en aumento

La certificación Entrust Ready de los HSMs nShield asegura interoperabilidad, facilidad de implementación y seguridad mejorada.

Soluciones de identidad confiables de Entrust que permitan la transformación empresarial digital

Los HSMs nShield de Entrust son dispositivos criptográficos de alto rendimiento diseñados para generar, proteger y gestionar material clave confidencial. Certificados según estrictos estándares de seguridad, los HSMs nShield:

- Almacenan las claves en un entorno seguro y a prueba de manipulaciones indebidas
- Cumplen con los requisitos normativos del sector público, los servicios financieros y las empresas
- Aplican políticas en materia de seguridad, separando las funciones de seguridad de las tareas administrativas
- Soporte para criptografía de curva elíptica (ECC) de alto rendimiento

Los HSMs NShield de Entrust están diseñados para ajustarse a las necesidades de rendimiento y presupuesto específicas:

- HSM nShield Edge: HSM portátil con conexión USB para configuraciones de CA raíz fuera de línea de bajo volumen
- HSMs nShield Solo+ y Solo XC: HSMs PCIe integrados de alto rendimiento para servidores y dispositivos de seguridad
- HSMs nShield Connect+ y Connect XC: HSMs de alto rendimiento conectados a la red para entornos de alta disponibilidad
- nShield como servicio: opción de alto rendimiento basada en suscripción para una mayor flexibilidad y rentabilidad

HSMs de Entrust

Los HSMs nShield de Entrust 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.

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