Mantenga su propia clave para una gestión de claves de alta fiabilidad

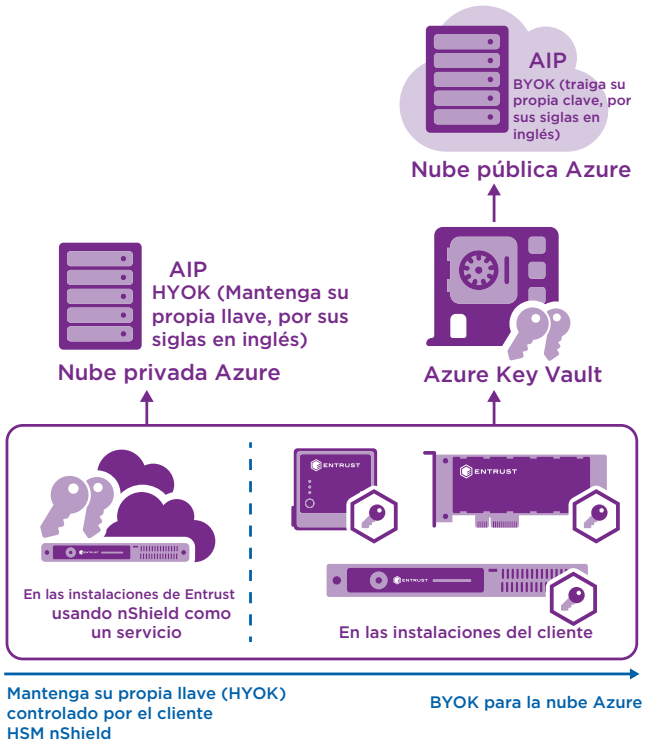
Microsoft y Entrust ofrecen protección consistente de la información y una opción de protección de claves que le permite tener el control en la nube

CARACTERÍSTICAS PRINCIPALES

- Aplicar controles de acceso y uso en los datos que intercambia
- Mantener y proteger sus claves con HSMs que usted controla
- Ofrecer una gestión del ciclo de vida de las claves con certificación FIPS 140-2
- Asegurar que las claves nunca sean visibles para Microsoft

Microsoft Azure Information Protection (AIP) protege los datos que se intercambian en su entorno de trabajo colaborativo incorporando políticas de seguridad aplicables en los recursos de datos, sin importar el tipo de datos. Como servicio en la nube, usted puede ejecutar AIP bajo demanda sin una infraestructura IT y garantizar que su información está protegida dentro de los límites empresariales.

AIP utiliza la criptografía para ofrecer un acceso controlado y una protección constante a sus datos. La seguridad de AIP depende del nivel de protección que se les da a las claves criptográficas más importantes. La vulnerabilidad de las claves criptográficas pone en riesgo sus datos confidenciales.



Los HSMs nShield® de Entrust ofrecen control indispensable para sus claves más importantes, independientemente de si usa AIP de forma local, con una configuración híbrida o totalmente en la nube.

APRENDA MÁS EN ENTRUST.COM/HSM

Mantenga su propia clave para una gestión de claves de alta fiabilidad

El reto: los datos altamente confidenciales requieren que la clave criptográfica permanezca in situ

Aunque mucho contenido se puede atender por medio de las claves almacenadas de forma segura en Azure, algunos contenidos confidenciales no pueden compartirse de ningún modo ni enviarse fuera de su perímetro de seguridad. La seguridad de estos contenidos confidenciales debe mantenerse únicamente de forma local, con acceso y distribución limitados.

Para gestionar la mayoría de datos confidenciales dentro de su propio perímetro de seguridad, AIP ofrece la opción Mantenga su propia clave (HYOK, por sus siglas en inglés) que está habilitada en un componente local, además de un módulo de seguridad de software (HSM) Entrust que proporciona la gestión de claves y que puede establecerse tanto en las instalaciones del cliente como en el entorno nShield como servicio.

Los HSMs nShield® de Entrust crean una jaula cerrada que protege sus claves más importantes y mejora la seguridad de sus datos confidenciales.

La solución: Implementaciones HYOK con el control de claves mejorado de Entrust

Los HSMs nShield de Entrust crean controles firmes en la gestión y el uso de las claves criptográficas que se usan en las implementaciones AIP.

Los HSMs nShield de Entrust le ofrecen una solución de hardware para proteger sus claves más importantes. Los HSMs de nShield protegen y gestionan las claves de forma completamente independiente al entorno de software, lo que le permite tener el control y mantener su propia clave.

Su clave se generará y gestionará dentro de los límites de seguridad de su propio HSM nShield, permitiéndole proteger sus datos más confidenciales.

¿Por qué usar los HSMs de Entrust con AIP y HYOK?

Los HSMs de Entrust le permiten usar AIP a su medida para que se ajuste a sus necesidades de seguridad, ya sea de forma local, en la nube o en una configuración híbrida. Los HSMs nShield:

- Protegen la clave dentro de un límite criptográfico con certificación FIPS 140-2
- Utilizan mecanismos de control de acceso sólidos con separación forzada de tareas, para que la clave solo se use para fines autorizados
- Garantizan la disponibilidad de la clave usando funciones de gestión, almacenamiento y redundancia de claves

Si tiene pensado usar Azure Key Vault para almacenar sus claves y usarlas con AIP, Entrust puede ayudarle a mejorar la seguridad de sus claves. Usted puede generar claves usando los HSMs nShield que controla, y transferirlas de forma segura a Azure Key Vault. La funcionalidad Traiga su propia clave (BYOK) le da el control sobre sus claves y sobre la seguridad de sus datos en la nube.

Mantenga su propia clave para una gestión de claves de alta fiabilidad

HSMs nShield de Entrust

- Protegen las claves en un entorno reforzado a prueba de manipulaciones indebidas
- Aplican políticas de seguridad, separando las funciones de seguridad de las tareas administrativas
- Cumplen con los requisitos normativos del sector público, los servicios financieros y las empresas
- Tienen certificación FIPS 140 Nivel 2 y Common Criteria

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

- Para la generación y administración de claves de gran volumen (o como parte de una implementación híbrida), las tarjetas PCIe integradas del HSM nShield Solo y los dispositivos conectados a la red del HSM nShield Connect ofrecen seguridad de software de alto rendimiento
- Los HSMs nShield Connect pueden implementarse en las instalaciones del cliente o en el entorno nShield como servicio
- Para la generación local de claves de bajo volumen como parte de la funcionalidad BYOK, el HSM nShield Edge ofrece seguridad de hardware conectada por USB

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.

Microsoft

Microsoft ha transformado la forma en que las empresas crean y comparten contenido y crean procesos colaborativos. Los sistemas basados en soluciones de Microsoft maximizan la productividad. Para proteger los datos, Microsoft AIP usa criptografía para establecer entornos empresariales fiables que:

- Gestionan identidades entre las empresas
- Distribuyen certificados para la autenticación
- Controlan los derechos de acceso de los usuarios a las fuentes de datos
- Ofrecen protección total de la información

www.microsoft.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