Entrust Double Key Encryption para Microsoft Azure Information Protection

ASPECTOS DESTACADOS

Incremente el control y la seguridad de sus datos confidenciales en entornos híbridos y en la nube

- Aplique dos capas de seguridad a su contenido más crítico en la nube de Azure.
- Cifre los datos de modo que ni siquiera Microsoft tenga acceso a su contenido.
- Mantenga la propiedad y el control pleno de sus claves y del software que las genera.
- Aloje sus claves y almacene sus datos críticos en una ubicación de su elección.
- Administre el acceso de los usuarios a sus claves y al contenido que protegen.

CARACTERÍSTICAS Y BENEFICIOS PRINCIPALES

Entrust Double Key Encryption para Microsoft Azure Information Protection (AIP), brindado por Entrust Professional Services, es un servicio diseñado para ayudar a las empresas a proteger su contenido más crítico en Microsoft 365.

- Se integra con HSM (módulos de seguridad de hardware) de Entrust nShield® certificados con el fin de brindar una base de confianza para la protección de la claves confidenciales de los clientes.
- Las herramientas y el hardware les otorgan a las empresas propiedad y control pleno del software que respalda el proceso de generación de doble clave, sin la presencia de Microsoft en las instalaciones de los clientes.

El cifrado de doble clave (Double Key Encryption) les permite a las organizaciones utilizar entornos informáticos híbridos con niveles adicionales de protección, control y garantías. Como parte de la oferta de Microsoft AIP, esta solución permite a los clientes empresariales determinar quiénes cuentan con permisos para acceder a las claves asociadas y descifrar el contenido. Las empresas pueden almacenar los datos cifrados en sus instalaciones o en la nube, donde son totalmente ilegibles para Microsoft.

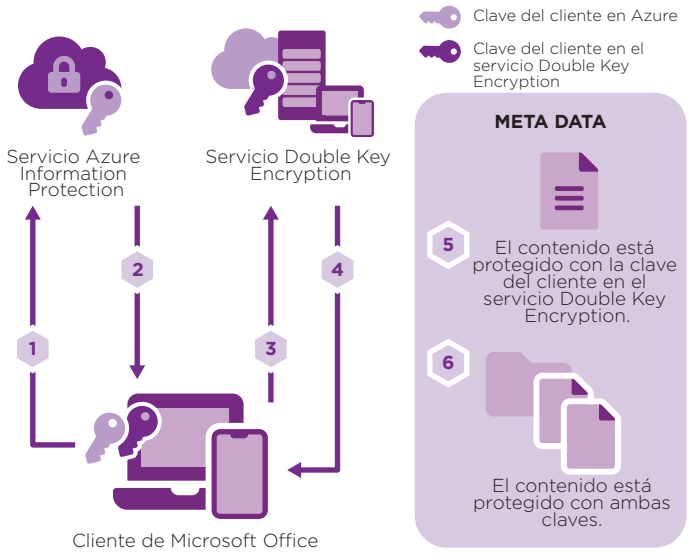
Double Key Encryption reemplaza a Microsoft Hold your Own Key (HYOK) y no requiere que los clientes empresariales administren sus propios servidores de Active Directory and Rights Management. Por el contrario, los clientes pueden ingresar sus propias claves criptográficas en tiempo real.

Double Key Encryption para Microsoft Azure

CÓMO FUNCIONA

Double Key Encryption (DKE) utiliza claves criptográficas de dos componentes para proteger los datos altamente confidenciales de la empresa: una clave de Microsoft y una clave del cliente.

- La clave de Microsoft se utiliza inicialmente para cifrar el contenido del cliente en Azure.
- La clave de Microsoft se cifra con la clave del cliente, protegida mediante un HSM nShield en sus instalaciones.
- Este proceso evita que Microsoft tenga acceso a la clave y al contenido del cliente en Azure.

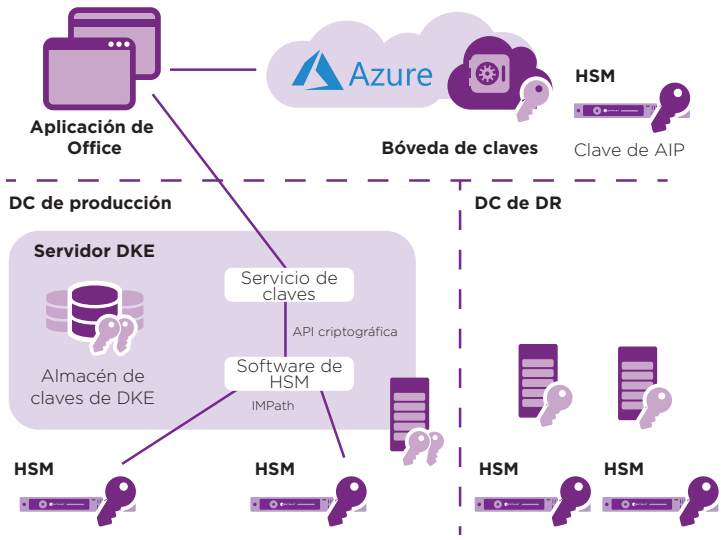


ESPECIFICACIONES TÉCNICAS

Integración con HSM de Entrust nShield

Los HSM de Entrust nShield contienen la clave maestra que protege el servidor de cifrado de doble clave y el almacén de claves. Por lo general, se implementan cuatro HSM nShield entre los entornos de producción y de recuperación ante desastres (DR).

Entrust Double Key Encryption cuenta con el respaldo de FIPS 140-2, Nivel 3. Los Criterios Comunes EAL4+ certificaron a los HSM nShield Solo XC (PCIe) y nShield Connect XC (conectado a la red).



Double Key Encryption para Microsoft Azure

Primeros pasos

Para utilizar Entrust Double Key Encryption para Microsoft AIP, necesitará lo siguiente:

- La solución Entrust Double Key Encryption
- Entrust nShield Solo o nShield Connect HSM

HSM de Entrust

Los HSM de Entrust nShield se encuentran entre las soluciones de módulos de seguridad de hardware de mayor rendimiento, más seguras y fáciles de integrar que existen en el mercado. Esto facilita la conformidad con la normativa y brinda los más altos niveles de seguridad de datos y aplicaciones para las organizaciones empresariales, financieras y gubernamentales. Nuestra incomparable arquitectura de manejo de claves Security World permite un control estricto y granular del acceso y el uso de las claves.

Explore más

Para obtener más información sobre los HSM de Entrust nShield, 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 obtener más información sobre los HSM de Entrust nShield, visite

HSMinfo@entrust.com

entrust.com/HSM

ACERCA DE ENTRUST CORPORATION

Entrust brinda seguridad a un mundo en constante movimiento al garantizar la confianza en las identidades, los pagos y la protección de datos. Hoy más que nunca, las personas exigen experiencias fluidas y seguras al cruzar fronteras, hacer compras, utilizar servicios de gobierno electrónico o acceder a redes corporativas. Entrust cuenta con una gama única de soluciones de seguridad digital y de emisión de credenciales que constituyen el aspecto clave de estas interacciones. Con más de 2500 colaboradores, una red global de socios tecnológicos y clientes en más de 150 países, las organizaciones más confiables del mundo confían en nosotros sin dudarlo.

Explore más en
entrust.com

El logotipo de Entrust y Hexagon son marcas comerciales, marcas registradas o marcas de servicio de Entrust Corporation en los Estados Unidos y en otros países. Todos los demás nombres de marcas o productos son propiedad de sus respectivos dueños. Debido a que estamos mejorando continuamente nuestros productos y servicios, Entrust Corporation se reserva el derecho de modificar las especificaciones sin previo aviso. Entrust es un empleador que ofrece igualdad de oportunidades.
©2020 Entrust Corporation. Todos los derechos reservados. HS21Q3-hsm-double-key-encryption-azure-information-protection-ds

ENTRUST

Oficinas centrales internacionales
1187 Park Place, Minneapolis, MN 55379
Número de teléfono gratuito en EE. UU.: 888 690 2424
Número de teléfono internacional: +1 952 933 1223
hsminfo@entrust.com **entrust.com/contact**