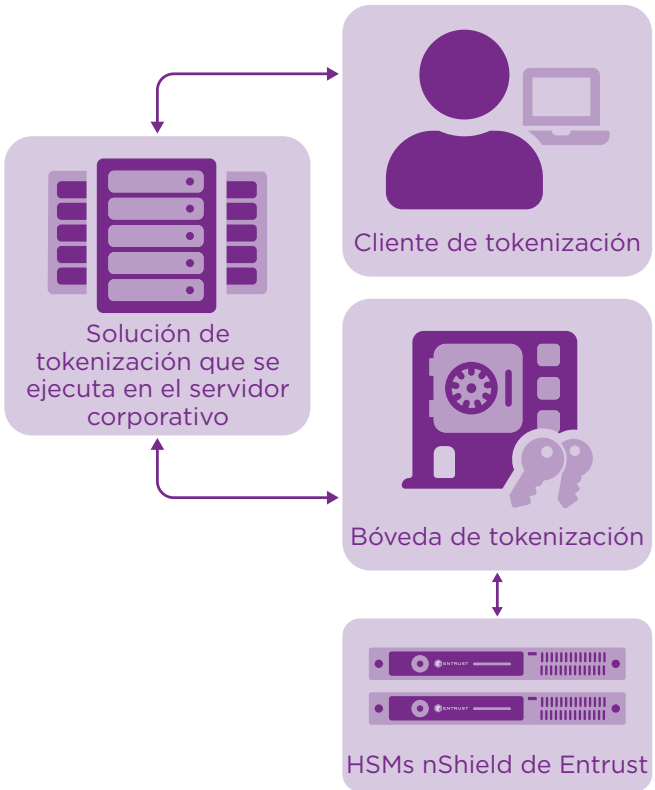
Los proveedores líderes en tokenización y de Entrust mejoran la seguridad y el cumplimiento de los datos

NFINITY
STRATEGIC TECHNOLOGY PARTNER PROGRAM

Tokenización mejorada y cumplimiento con los módulos de seguridad de hardware (HSMs) nShield de Entrust

CARACTERÍSTICAS PRINCIPALES

- Proteja los datos confidenciales en reposo, en uso y en movimiento
- Reduzca el alcance y el costo de las auditorías en materia de cumplimiento
- Evite la interrupción de las aplicaciones que utilizan la tokenización que conserva el formato
- Proteja las claves de cifrado en un módulo de seguridad con certificación FIPS 140-2 Nivel 3 resistente a manipulaciones indebidas
- Genere números aleatorios con una fuente de entropía certificada y compatible



Los HSMs nShield de Entrust alojan la clave raíz maestra para la función de tokenización y también pueden realizar funciones críticas dentro de su límite seguro mediante la ejecución de código seguro de CodeSafe.

El desafío:

En todas las industrias, las empresas están acumulando y transmitiendo más información confidencial que nunca, lo que aumenta el potencial de ataque de los ciberdelincuentes que buscan monetizar datos privados. La disponibilidad de mercados secundarios

APRENDA MÁS EN ENTRUST.COM/HSM

Mejora de la seguridad y el cumplimiento de los datos

para estos datos hace que la información de identificación personal, los números de tarjetas de pago y los registros médicos sean particularmente vulnerables.

En respuesta, las organizaciones han recurrido a la tokenización para reducir el riesgo de exposición de datos. La tokenización sustituye un valor real con un token aleatorio que mantiene el mismo formato y tipo que los datos originales. Esto permite que las aplicaciones y bases de datos existentes reconozcan y procesen el token de la misma manera que la información original. Por ejemplo, a medida que un representante de servicio al cliente agrega al registro de un cliente, los campos específicos se pueden tokenizar inmediatamente para que estén protegidos contra el acceso no autorizado. Dependiendo de la arquitectura, los valores reales se cifran y almacenan en una bóveda separada o, utilizando un enfoque sin bóveda, el token se genera a través de un algoritmo, lo que evita la necesidad de almacenar la información real.

Debido a que los datos se devalúan, la tokenización mejora su seguridad al tiempo que reduce el riesgo de robo. Esto también puede mejorar el cumplimiento de mandatos tales como el Estándar de seguridad de datos de PCI, que señala que las organizaciones pueden reducir efectivamente su alcance de PCI DSS mediante el uso de un sistema de tokenización compatible.

Al implementar un sistema de tokenización, una empresa debe asegurarse de que esté diseñado para evitar la reversión de tokens para revelar los datos originales. Esto es esencial para garantizar que los datos confidenciales permanezcan seguros y que la organización cumpla con los mandatos de privacidad de datos.

La solución: tokenización integrada con HSMs nShield de Entrust

Una solución de tokenización sólida comienza con el proceso de generación de tokens. Las mejores prácticas reconocidas para la generación de tokens requieren una tokenización aleatoria o una tokenización mediante cifrado, junto con el almacenamiento seguro de las claves de cifrado. Las pautas de tokenización de PCI especifican que, "Las claves criptográficas deben gestionarse y protegerse de acuerdo con los requisitos de PCI DSS... Las claves criptográficas utilizadas para la generación y destokenización de tokens no deben estar disponibles para ninguna aplicación, sistema, usuario o proceso fuera del sistema de tokenización seguro".[1]

Los HSMs nShield® de Entrust están integrados con las principales soluciones de tokenización. Establecen tablas de referencia de claves criptográficas altamente aleatorias y altamente seguras, que se utilizan en el proceso de generación de tokens. El generador de números aleatorios de nShield ha sido certificado como una fuente de entropía compatible con FIPS. Esto les permite a las organizaciones crear tokens altamente seguros que no pueden ser revertidos por usuarios no autorizados. El HSM nShield también genera y protege las claves utilizadas para cifrar las tablas de referencia.

Cuando la arquitectura de tokenización incorpora una bóveda separada de datos originales, las claves de cifrado que ayudan a proteger los datos de la bóveda se generan y aseguran en un HSM nShield.

1. https://www.pcisecuritystandards.org/documents/Tokenization_ Product_Security_Guidelines.pdf

Mejora de la seguridad y el cumplimiento de los datos

La diferencia de Entrust nShield

Los HSMs nShield de Entrust protegen las claves de cifrado en un entorno certificado a prueba de manipulaciones indebidas. Las claves que se manejan fuera de los límites criptográficos de los HSMs nShield son significativamente más vulnerables a los ataques, lo que puede llevar a la divulgación de información confidencial. Los HSMs son la única forma comprobada y auditable de asegurar material criptográfico valioso. Los HSMs nShield:

- Protegen las claves y los certificados dentro de límites criptográficos cuidadosamente diseñados
- Usan mecanismos de control de acceso robustos para que las claves solo se utilicen para su propósito autorizado
- Aseguran la disponibilidad mediante el uso de funciones sofisticadas de administración, almacenamiento y redundancia de claves para garantizar que siempre estén accesibles cuando las necesite
- Ofrecen un alto rendimiento para admitir grandes volúmenes de tokenización
- Cumplen con los requisitos reglamentarios y los mandatos de la industria que rigen los servicios financieros, el comercio minorista y otras industrias.

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**

MICRO FOCUS Voltage

PrimeFactors™ — Applied Data Protection —

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

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. Noviembre 2020 • PLB9608