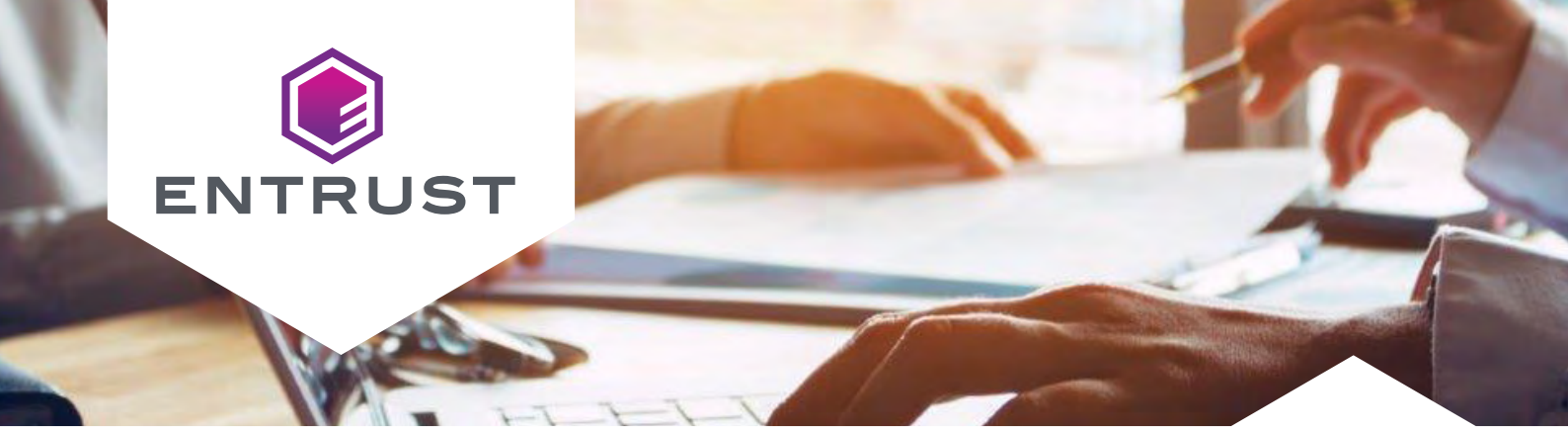


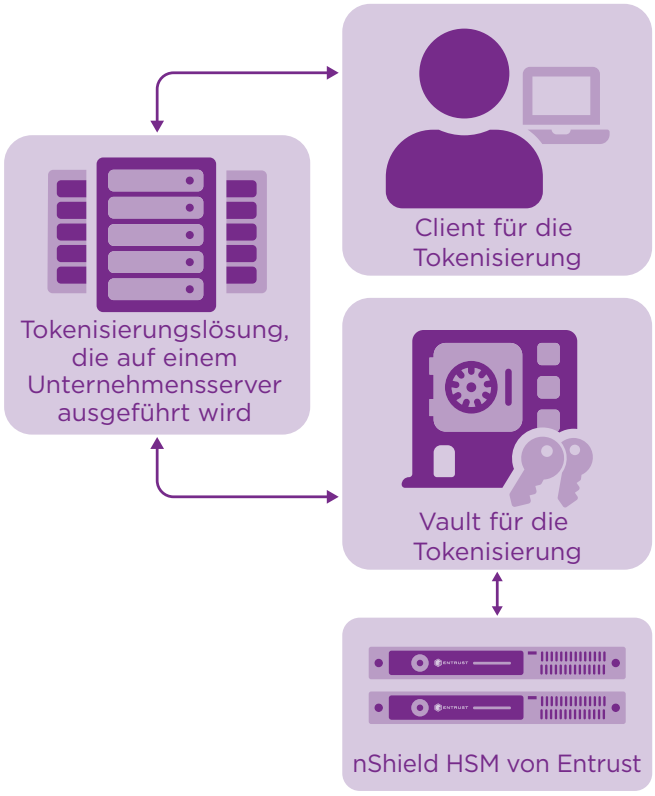
Entrust und führende Anbieter von Tokenisierung gewährleisten Datensicherheit und Compliance

NFINITY STRATEGIC TECHNOLOGY PARTNER PROGRAM

Optimierte Tokenisierung und Einhaltung von Vorgaben mit nShield-Hardware-Sicherheitsmodulen (HSM) von Entrust

ECKPUNKTE

- Schutz sensibler Data-at-Rest, Data-in-Use und Data-in-Motion
- Reduzierung des Aufwands und der Kosten von Compliance-Prüfungen
- Vermeidung von Anwendungsunterbrechungen durch Tokenisierung, die das Format der Originaldaten beibehält
- Sicherung kryptographischer Schlüssel in einem manipulationssicheren, nach FIPS 140-2 Level 3 zertifizierten Hardware-Sicherheitsmodul
- Generierung von Zufallszahlen mittels einer zertifizierten, konformen Entropiequelle



nShield HSM von Entrust hosten den Master-Root-Schlüssel der Tokenisierungsfunktion und können mit der sicheren Code-Ausführung CodeSafe zudem wichtige Funktionen innerhalb der sicheren Grenzen des HSM ausführen.

Die Herausforderung:

Unternehmen erfassen und übertragen branchenweit mehr sensible Daten als jemals zuvor. Dadurch erhöht sich die Gefahr eines Angriffs durch Cyber-Kriminelle, die mit diesen personenbezogenen Daten Geld machen möchten. Es ist ein zweiter Markt für personenbezogene Daten, Kreditkartennummern und Patientenakten entstanden. Das macht diese Daten besonders anfällig.

Optimierte Datensicherheit und Compliance

Daher setzen Unternehmen auf Tokenisierung, um das Risiko einer Datenoffenlegung zu reduzieren. Bei der Tokenisierung wird ein realer Wert durch einen zufälligen Token ersetzt, der das Format und den Typ der Originaldaten beibehält. Dadurch sind vorhandene Anwendungen und Datenbanken in der Lage, den Token genau wie die ursprünglichen Informationen zu erkennen und zu verarbeiten. Wenn beispielsweise ein Kundendienstmitarbeiter den Datensatz eines Kunden ergänzt, können bestimmte Felder unmittelbar tokenisiert werden. Somit sind sie gegen unbefugten Zugriff geschützt. Je nach Architektur werden die realen Werte entweder verschlüsselt und in einem separaten Vault gespeichert, oder der Token wird mithilfe eines Algorithmus generiert, ohne dass ein Vault zum Einsatz kommt. Dadurch entfällt die Notwendigkeit, die Daten selbst zu speichern.

Die Daten verlieren so für Angreifer an Wert. Entsprechend verbessert Tokenisierung die Sicherheit und reduziert das Diebstahlrisiko. Daher können Vorgaben wie der PCI Data Security Standard leichter eingehalten werden. Durch den Einsatz eines konformen Tokenisierungssystems können Unternehmen den Aufwand für die Einhaltung des PCI DSS nachhaltig verringern.

Ein Unternehmen, das ein Tokenisierungssystem einführt, muss gewährleisten, dass dieses die Rückumwandlung der Token unmöglich macht, damit eine Offenlegung der Originaldaten verhindert wird. Das ist für den Schutz sensibler Daten und die Einhaltung von Datenschutzvorschriften unerlässlich.

Die Lösung: Tokenisierung mit nShield HSM von Entrust

Das Verfahren zur Generierung von Token ist der Grundpfeiler einer starken Tokenisierungslösung. Anerkannte bewährte Verfahren zur Tokengenerierung setzen entweder auf Tokenisierung mittels eines Zufallszahlengenerators oder auf Tokenisierung durch Verschlüsselung gepaart mit einer sicheren Speicherung der kryptographischen Schlüssel. Kryptographische Schlüssel müssen gemäß den Vorgaben der PCI DSS verwaltet und geschützt werden. Werden diese Schlüssel für die Generierung von Token und die Detokenisierung verwendet, sollten sie keinen Anwendungen, Systemen, Benutzern oder Prozessen außerhalb des sicheren Tokenisierungssystems zur Verfügung stehen.[1]

nShield®HSM von Entrust können in führende Tokenisierungslösungen integriert werden. Sie legen Referenztabellen mit zufälligen, hochsicheren kryptographischen Schlüsseln fest, die während der Generierung der Token verwendet werden. Der nShield-Zufallszahlengenerator ist eine nach FIPS zertifizierte Entropiequelle. So können Unternehmen äußerst sichere Token erstellen, die von unbefugten Benutzern nicht umgekehrt werden können. Das nShield HSM erstellt und schützt zudem die Schlüssel für die Verschlüsselungstabellen.

Wenn die Tokenisierungsarchitektur einen separaten Vault mit den Originaldaten umfasst, werden die kryptographischen Schlüssel, die zum Schutz der Daten im Vault beitragen, von einem nShield HSM erstellt und gesichert

1. https://www.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf

Optimierte Datensicherheit und Compliance

Warum nShield von Entrust?

nShield HSM von Entrust schützen kryptographische Schlüssel in einer zertifizierten, manipulationssicheren Umgebung. Schlüssel, die außerhalb der kryptographischen Grenzen eines nShield HSM verwendet werden, sind deutlich anfälliger für Angriffe, was zur Offenlegung von Daten führen kann. HSM sind die einzige bewährte und prüfbare Möglichkeit, um wertvolles kryptographisches Material zu schützen. nShield HSM:

- schützen Schlüssel und Zertifikate innerhalb sorgfältig ausgelegter kryptographischer Grenzen
- wenden robuste Zugriffskontrollen an, damit Schlüssel ausschließlich für autorisierte Zwecke verwendet werden
- gewährleisten die Verfügbarkeit von Schlüsseln durch ausgereifte Management-, Speicher- und Redundanzfunktionen, damit bei Bedarf jederzeit auf diese Schlüssel zugegriffen werden kann.
- bieten hohe Leistung für Tokenisierung im großen Umfang
- erfüllen die regulatorischen Vorschriften für Finanzdienstleister, Einzelhandel und weitere Branchen

Weitere Informationen

Mehr Informationen zu den nShield HSMs von Entrust finden Sie auf **entrust.com/HSM**. Auf **entrust.com** erfahren Sie zudem mehr über die digitalen Sicherheitslösungen für Identitäten, Zugriff, Kommunikation und Daten von Entrust.

MICRO FOCUS Voltage

PrimeFactors™ — Applied Data Protection —

Mehr Informationen zu Entrust nShield HSMs

HSMinfo@entrust.com

entrust.com/HSM

ÜBER ENTRUST CORPORATION

Entrust ermöglicht vertrauenswürdige Identitäten und Zahlungen sowie verlässlichen Datenschutz und hält damit die Welt sicher in Bewegung. Ein nahtloses und sicheres Umfeld ist heute mehr denn je unerlässlich, sei es bei Grenzübertritten, beim Einkaufen, beim Zugriff auf E-Government-Dienste oder beim Einloggen in Unternehmensnetzwerke. Entrust bietet für genau diese Interaktionen eine unübertroffene Bandbreite an Lösungen für digitale Sicherheit und die Ausstellung von Berechtigungsnachweisen. Mit 2.500 Mitarbeitern und einem weltweiten Partnernetzwerk ist Entrust für Kunden in über 150 Ländern tätig, die sich bei ihren sensibelsten Operationen auf uns verlassen.

Weitere Informationen auf
entrust.com/HSM

Kontakt:
HSMinfo@entrust.com