Entrust Double Key Encryption für Microsoft Azure Information Protection

HIGHLIGHTS

Mehr Kontrolle und Sicherheit beim Umgang mit sensiblen Daten in Hybrid- und Cloud-Umgebungen

- Schützen Sie Ihren sensiblen Content in der Azure-Cloud mit zwei Sicherheitsebenen.
- Verschlüsseln Sie Ihre Daten, damit nicht einmal Microsoft auf Ihren Content zugreifen kann.
- Übernehmen Sie die volle Kontrolle mit Ihrem eigenen Schlüssel und einer eigenen Software, die den Schlüssel erstellt.
- Hosten Sie Ihren Schlüssel und sichern Sie Ihre kritischen Daten am Speicherort Ihrer Wahl.
- Bestimmen Sie, wie Ihre User auf Ihren Schlüssel und den dadurch geschützten Content zugreifen dürfen.

WICHTIGSTE FUNKTIONEN UND VORTEILE

Die Entrust Double Key Encryption der Entrust Professional Services dient der Azure Information Protection (AIP). Ihr Unternehmen schützt damit seine sensiblen Daten in Microsoft 365.

- Die Lösung lässt sich in zertifizierte Entrust nShield® HSMs integrieren – als stabiles Fundament zum zuverlässigen Schutz sensibler Kundenschlüssel.
- Die Tools und die Hardware gehören zu 100 Prozent Ihrem Unternehmen. Sie haben also die volle Kontrolle über die Software, auf der die doppelte Verschlüsselung basiert. Gleichzeitig hinterlässt Microsoft im System vor Ort keine Spuren.

Die Double Key Encryption erlaubt es Ihrem Unternehmen, Hybrid-Umgebungen zur Datenverarbeitung zu verwenden – mit zusätzlichen Schutz-, Kontroll- und Sicherheitsebenen. Als Teil des Microsoft-AIP-Pakets gibt Ihnen die Lösung die volle Entscheidungsfreiheit: Bestimmen Sie selbst, wer auf zugehörige Schlüssel zugreifen und Content entschlüsseln darf. Ihr Unternehmen kann seine verschlüsselten Daten im lokalen System oder in der Cloud speichern. Der Content bleibt dadurch vor Microsoft verborgen.

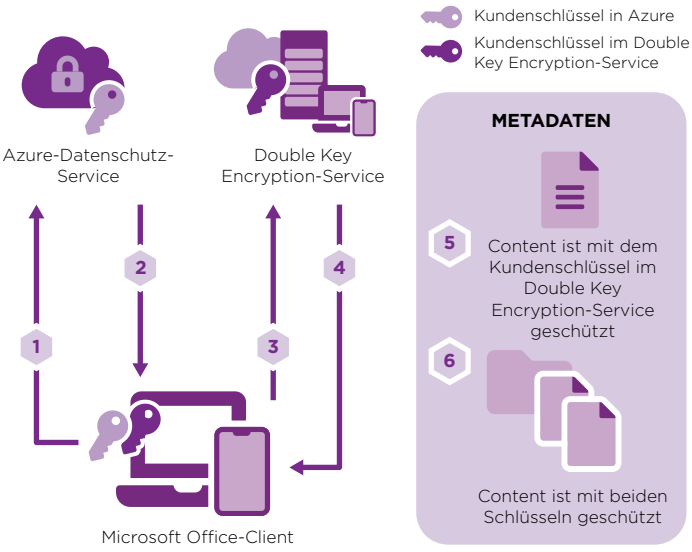
Die Double Key Encryption ersetzt das Microsoft Hold Your Own Key (HYOK)-System. So braucht Ihr Unternehmen keine eigenen Active-Directory- und Rights-Management-Server. Sie erstellen stattdessen in Echtzeit Ihre eigenen kryptographischen Daten.

Double Key Encryption für Microsoft Azure

SO FUNKTIONIERT ES

Die Double Key Encryption schützt im gesamten Unternehmen Ihre sensiblen und kritischen Daten durch eine Verschlüsselung, die aus zwei Komponenten besteht: einem Microsoft- und einem Kunden-Schlüssel.

- Der Microsoft-Schlüssel chiffriert zunächst den Kunden-Content in Azure.
- Anschließend kodiert das System den Microsoft-Schlüssel durch einen Kunden-Schlüssel, der durch ein firmeninternes nShield HSM geschützt ist.
- Der doppelte Schutz gibt Ihnen die Sicherheit, dass Microsoft keinen Zugang zum Schlüssel und zu Ihrem Content in Azure hat.

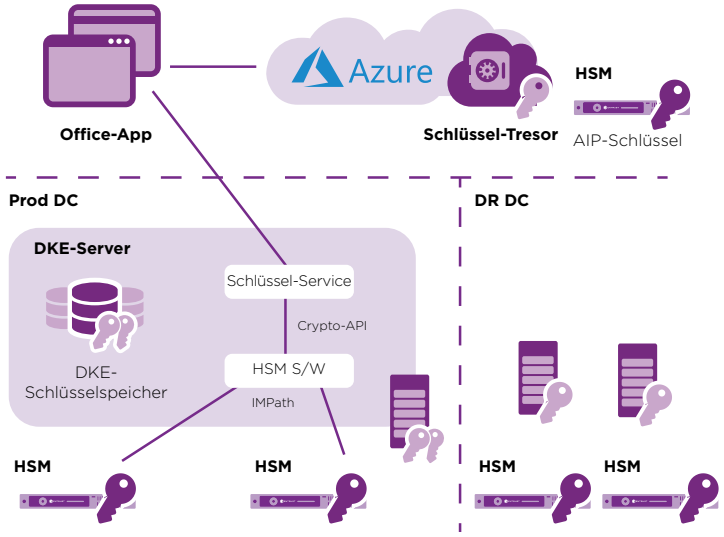


TECHNISCHE DATEN

Integration von Entrust nShield HSMs

Die Entrust nShield HSMs sind Ihr sicherer Ablageort für den Hauptschlüssel, der den Double Key Encryption-Server und den Schlüsselspeicher schützt. Typischerweise kommen vier nShield HSMs zum Einsatz. Sie sorgen für eine systemübergreifende Redundanz und unterstützen Ihre Disaster-Recovery-Umgebungen.

Die Entrust Double Key Encryption basiert auf HSMs, die den Sicherheitsstandards FIPS 140-2 Level 3, den Common Criteria EAL4+ für zertifizierte nShield Solo XC (PCIe)-HSMs und (an Netzwerke angehängte) nShield Connect XC-HSMs entsprechen.



Double Key Encryption für Microsoft Azure

Erste Schritte

Das brauchen Sie für die Microsoft AIP mittels Entrust Double Key Encryption:

- Entrust Double Key Encryption
- Entrust nShield Solo oder nShield Connect HSMs

Entrust HSMs

Die Entrust nShield HSMs zählen zu den leistungsstärksten, sichersten und am einfachsten zu integrierenden HSM-Lösungen auf dem Markt. Sie erleichtern die Compliance mit Vorschriften und stellen die höchste Stufe der Daten- und Anwendungssicherheit dar – in Unternehmen, Finanzinstituten und Verwaltungsorganen. Unsere Security World-Architektur ist eine einzigartige Lösung zur Schlüsselverwaltung. Sie können darüber den Zugriff auf Ihre Schlüssel und deren Nutzung effektiv steuern und genau anpassen.

Mehr erfahren

Weitere Informationen zu den Entrust nShield HSMs finden Sie unter **entrust.com/HSM**. Möchten Sie mehr darüber erfahren, wie Entrust Ihre Identitäten, Zugriffe, Kommunikationskanäle und Daten schützt? Besuchen Sie unsere Website unter der Adresse **entrust.com**.

Weitere Informationen zu den Entrust nShield HSMs:

HSMinfo@entrust.com

entrust.com/HSM

ÜBER DIE ENTRUST CORPORATION

Entrust steht für Sicherheit im globalen Geschäftsverkehr durch verlässliche Identitätsprüfungen, Zahlungen und Maßnahmen zum Datenschutz. Die Menschen legen immer mehr Wert auf eine nahtlose und sichere User und Customer Experience – ob sie verreisen, Käufe abschließen, auf elektronische Verwaltungsdienste zugreifen oder Unternehmensnetzwerke nutzen. Entrust bietet Ihren Kunden und Usern eine einmalige Bandbreite digitaler Lösungen für durchweg sichere und authentifizierte Transaktionen. Die renommiertesten Unternehmen weltweit vertrauen Entrust. Wir beschäftigen über 2.500 Kollegen, unterhalten ein globales Partnernetzwerk und haben Kunden in über 150 Ländern der Welt.

Weitere Informationen unter:
entrust.com

ENTRUST

Kontakt:

One Station Square
Cambridge CB1 2GA
+44 1223 723600
SALES +44 1223 723711
hsminfo@entrust.com entrust.com/contact