Optionspaket für Cloud-Integration

Erstellen und kontrollieren Sie kryptographische Schlüssel in Ihrem nach FIPS 140-2 zertifizierten HSM und exportierten Sie diese anschließend sicher in die Cloud

HIGHLIGHTS

Nutzer öffentlicher Cloud-Dienste können kryptographische Schlüssel in ihrer eigenen Umgebung erstellen und kontrollieren, während sie diese ganz nach Bedarf in der Cloud ihrer Wahl verwenden.

- Kontrollieren Sie Ihre kryptographischen Schlüssel in Multi-Cloud- und hybriden Cloud-Umgebungen.
- Sichere Schlüsselerstellung mithilfe eine starken Entropiequelle
- Langfristiger Schlüsselschutz durch FIPS-zertifizierten HSM
- Unterstützung von Amazon Web Services, Google Compute Engine und Microsoft Azure

Schützen Sie Ihre Schlüssel in der Cloud durch höchste Sicherheit

Schützen Sie Ihre Marke und Ihre Daten

nShield-HSM von Entrust sind anhand höchster Sicherheitsstandards wie FIPS 140-2 und Common Criteria validiert und schützen Ihre Daten sogar in den herausforderndsten und anspruchsvollsten Sicherheitssituationen On-Premises und in der Cloud.

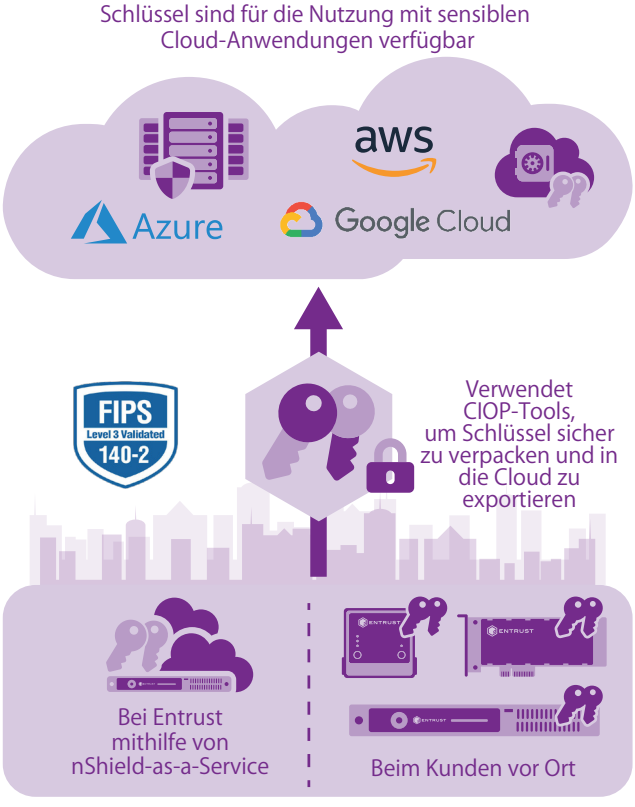

Abbildung 1. Kryptographische Schlüssel werden in einem nShield-HSM erstellt, verpackt und sicher in die Cloud exportiert.

WEITERE INFORMATIONEN AUF ENTRUST.COM/HSM

Optionspaket für Cloud-Integration

Unterstützte Cloud-Anbieter

Mit den Tools des Optionspaket für Cloud-Integration (CIOP) erstellen Sie mittels eines nShield-HSM Ihre eigenen kryptographischen Schlüssel. Diese werden anschließend verpackt und sicher zu den folgenden Cloud-Anbietern exportiert:

- Amazon Web Services (AWS)
- Google Compute Engine
- Microsoft Azure Key Vault (mit dem Azure-BYOK-Mechanismus)

Für Kunden, die noch mehr Sicherheit wünschen, bietet Microsoft nCipher BYOK an. Die BYOK-Methode von nCipher stellt zusätzlich sicher, dass die erstellten Schlüsselberechtigungen bei der Übertragung in den Microsoft Azure Key Vault erhalten bleiben. Ferner nutzt Microsoft nCipher Security World, um die Schlüssel auf eine bestimmte Azure-Region begrenzen. Für diese Methode ist ein Erwerb des CIOP nicht erforderlich. Weitere Informationen finden Sie in **Import HSM-protected keys for Key Vault (nCipher)** .

Schlüsselkontrolle in hybriden und Multi-Cloud-Umgebungen

Das Optionspaket für Cloud-Integration bietet Kunden die Kontrolle und Sicherheit, sie für die Bereitstellung von hybriden oder Multi-Cloud-Umgebungen oder einer einzelnen Cloud von einem einzigen Cloud-Anbieter benötigen. Indem Sie in der Cloud Ihre eigenen Schlüssel verwenden, umgehen Sie die Schwierigkeiten, die mit anbieterabhängiger Verschlüsselung einhergehen und die Migration von einem Cloud-Anbieter zum anderen erschweren können.

Unterstützte Konfigurationen

- Erfordert nShield Security World Software v12.60 und Firmware v12.60 oder höher für Azure BYOK
- Erfordert nShield Security World Software v12.40 Software für AWS und Google Compute Engine
- Diese Version wurde auf Kompatibilität mit einer Reihe von Plattformen getestet, darunter:
  - Microsoft Windows Server 2019 x64 und 2016 x64
  - Microsoft Windows 10 x64 und 7 x64
  - RedHat Enterprise Linux 7 x64 und AS/ES 6 x86/x64
  - SUSE Enterprise Linux 12 x64 und 11 x64
  - Oracle Enterprise Linux 7.6 x64 und 6.10 x64
- Unterstützte HSM
  - Mit allen aktuellen nShield-Modellen kompatibel

Weitere Informationen

Mehr Informationen zu den nShield HSM 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.

Weitere Informationen auf
entrust.com/HSM

ENTRUST

Kontakt:
HSMinfo@entrust.com