

Verschlüsselung mit Luna-HSM von Thales Strategien für Microsoft Azure



Ihr Unternehmen möchte alle Vorteile der Cloud nutzen, doch einige davon haben ihren Preis. Im Gegenzug für Flexibilität, Skalierbarkeit und Automatisierung wird das Eigentum an kryptographischen Schlüsseln oft an den Anbieter des Cloud-Dienstes abgegeben. Dadurch verlieren Sie die Kontrolle und die Einhaltung von Vorschriften wird erschwert.

Wenn es um kryptographische Schlüssel geht, dreht sich alles um die Kontrolle. Standardmäßig erstellt Azure kryptographische Schlüssel im Auftrag von Kunden und verwaltet deren Lebenszyklus. Vielen Unternehmen, die sensible Daten in der Cloud hosten, sind aufgrund der fehlenden Kontrolle und Hoheit über kryptographische Schlüssel nicht in der Lage, Vorschriften zu erfüllen oder internen Sicherheitsanforderungen zu entsprechen. Daher wünschen sich diese Organisationen die volle Kontrolle darüber, wie und wann kryptographische Schlüssel zum Schutz von und Zugriff auf verschlüsselte Daten verwendet werden.

Thales bietet eine Reihe von Lösungen für die Verschlüsselungsverwaltung auf Grundlage von Luna-HSMs an, um Ihre Daten unabhängig von ihrem Standort zu sichern und zu schützen. Mit Thales erhalten Unternehmen die Flexibilität, Cloud-Dienste zu nutzen, sowie die Möglichkeit, ihre kryptographischen Schlüssel sowohl zu besitzen als auch zu kontrollieren und/oder das Risiko eines unbefugten Datenzugriffs oder Datenverlusts zu reduzieren.

Microsoft Azure Cloud

Microsoft Azure bietet Unternehmen drei verschiedene Optionen, um kryptographische Schlüssel zu erstellen und zu verwalten:

Bring Your Own Key (BYOK)	Erstellen Sie kryptographische Schlüssel in Ihrer eigenen Umgebung und übertragen Sie diese HSM-geschützte Schlüssel (BYOK) anschließend sicher direkt zur Verwendung an Azure Key Vault.
Hold Your Own Key (HYOK)	Kryptographische Schlüssel nutzen Luna-HSM on-premises und ermöglichen Unternehmen damit eine 100%ige Kontrolle über den Zugriff auf verschlüsselte Daten und die Lebenszyklen der Schlüssel – die beste Lösung für interne, kritische und vertrauliche Daten.
Azure Key Vault	Sowohl die Schlüsselerzeugung als auch die Kontrolle über den Lebenszyklus liegen allein beim Anbieter.

BYOK für Microsoft Azure Key Vault mit Luna-HSM

Die Fähigkeit, Schlüssel über die BYOK-Lösung von Thales zu importieren, die in lokalen Luna-HSMs erstellt wurden, ermöglicht eine verbesserte Kontrolle und mehr Sicherheit über kryptographische Schlüssel, die von Azure-Diensten und Anwendungen in der Cloud verwendet werden. Indem Sie Ihre eigenen Schlüssel mit einem

Luna-HSM erstellen, können Sie die Herkunft und Qualität der Schlüssel, die Sie in der Cloud verwenden, leicht überprüfen und so die Sicherheit der Schlüsselverwaltung und der Sicherheitsverfahren Ihres Unternehmens stärken.

Funktionen und Vorteile:

Von Luna-HSM on-premises erstellte Schlüssel werden über die BYOK Utility des Luna-HSM sicher zur Verwendung in Azure Vault importiert – so wird sichergestellt, dass die Schlüssel niemals die sicheren Grenzen des Luna-HSM oder Key Vault im Klartextformat verlassen.

- Sobald die Schlüssel importiert sind, können Sie die Azure Cloud auf die gleiche Weise nutzen und einsetzen wie die von Azure erstellten Schlüssel
- So erhalten Sie eine bessere Kontrolle über die Haltbarkeit des importierten Schlüsselmaterials, da Sie die Originalversion der Schlüssel in Ihrem lokalen Luna HSM außerhalb von Azure Key Vault aufbewahren.
- Gewährleisten Sie den Schutz der in Azure importierten Schlüssel in einer externen manipulationssicheren Hardware gemäß FIPS 140-2 Level 3
- Möglichkeit zur Archivierung einer Kopie der erstellten Schlüssel – Aufbewahrung einer Kopie für zukünftige Audits oder Datenmigration
- Verbessern Sie die Kontrolle über die Lebensdauer und Nutzung der Schlüssel, um Ihre Betriebs- und Compliance-Anforderungen in der Cloud zu unterstützen
- Unterstützt Multi-Cloud-Anwendungsfälle, da die Kunden denselben Schlüssel in mehreren Clouds verwenden können

HYOK

Volles Vertrauen und umfassende Schlüsselkontrolle

HYOK ist eine Funktion von Microsoft Azure Information Protection, die es Unternehmen ermöglicht, Microsoft-Azure-Cloud-Dienste zu nutzen und komplexe Vorschriften und Richtlinien einzuhalten, indem sie die Eigentümerschaft und Kontrolle über kryptographische Schlüssel nicht aufgeben.

Die Integration zwischen Azure Information Protection und Luna-HSM ermöglicht es Unternehmen, kryptographische Schlüssel in ihren HSM vor Ort zu speichern, im Gegensatz zur Speicherung von Schlüsselmaterial in der Azure Cloud. Damit ist der Zugriff auf interne und hochsensible Daten, die mit Microsoft-Azure-Anwendungen und -Diensten wie Office 365 verbunden sind, nun vollständig unter der Kontrolle des Kunden und dennoch transparent für die Endanwender.

Vorteile von HYOK

Sie erstellen und verwalten Ihre kryptographischen Schlüssel (im Gegensatz zur Standardoption, bei der Azure dies in Ihrem Namen tut) gemäß Ihren eigenen Sicherheitsrichtlinien und behalten dabei die alleinige Kontrolle über die kryptographischen Schlüssel

- 100%ige Sicherheit, dass kryptographische Schlüssel nicht außerhalb Ihrer Kontrolle oder Ihres Wissens weitergegeben oder verwendet werden
- Hilfe bei der Erfüllung interner Richtlinien und Compliance-Vorgaben
- Schützen Sie hochsensible interne Informationen und nutzen Sie gleichzeitig die Vorteile von Microsoft Azure Services wie Office 365
- Der Azure Information Protection Client macht HYOK für Endanwender transparent
- Erzeugung und Speicherung kryptographischer Schlüssel in hochsicheren, FIPS 140-2-zertifizierten Luna-HSM vor Ort

Von Azure erstellte Schlüssel

100%ige Kontrolle durch den Dienstleister

Sicherheitsbewusste Unternehmen müssen den Komfort der von Azure erstellten Schlüssel gegen das Risikoprofil der zu schützenden Daten und Anwendungen abwägen. Für Anwendungen und Daten mit höherer Sicherheitsstufe wird empfohlen, dass Unternehmen die alleinige Kontrolle über die Erzeugung der kryptographischen Schlüssel behalten.

BYOK- und HYOK-Optionen unter Verwendung von Thales-Luna-HSMs bieten Kunden mehr Kontrolle und nutzen gleichzeitig die Vorteile der Microsoft Azure Cloud.

Thales kann auch Ihr Unternehmen unterstützen

Bitte Sie Thales um Unterstützung bei der Bewertung und Definition der Datenschutzstrategie, die am besten zu den Anforderungen Ihres Unternehmens passt, sowie um Tipps für eine schnellere Integration und Bereitstellung.

Zusammenfassung der Verschlüsselungsstrategie mit dem Luna-HSM

Anwendungsfall	Anforderung	Lösung
Unterstützung für Azure-native Dienste wie RMS, Office 365 etc.	Verbesserte Kontrolle über native Azure-Verschlüsselungsdienste	BYOK
kryptographischen Schlüssel müssen stets on-premises verbleiben	Kontrolle des Zugriffs auf kryptographische Schlüssel unabhängig von Azure	HYOK
Nicht kritische Daten	Grundlegender Datenschutz und Einhaltung von Richtlinien	Von Azure erstellte Schlüssel

Über Thales

Die Menschen, denen Sie den Schutz Ihrer Daten anvertrauen, vertrauen beim Datenschutz auf Thales. Beim Thema Datensicherheit stehen Unternehmen immer häufiger vor entscheidenden Momenten. Egal, ob es darum geht, eine Verschlüsselungsstrategie zu entwickeln, Ihre Daten in die Cloud zu übertragen oder Compliance-Anforderungen zu erfüllen – Sie können sich bei der Sicherung Ihrer digitalen Transformation auf Thales verlassen.

Entscheidende Technologie für entscheidende Momente.