Eigener Schlüssel für hochsichere Schlüsselverwaltung

Microsoft

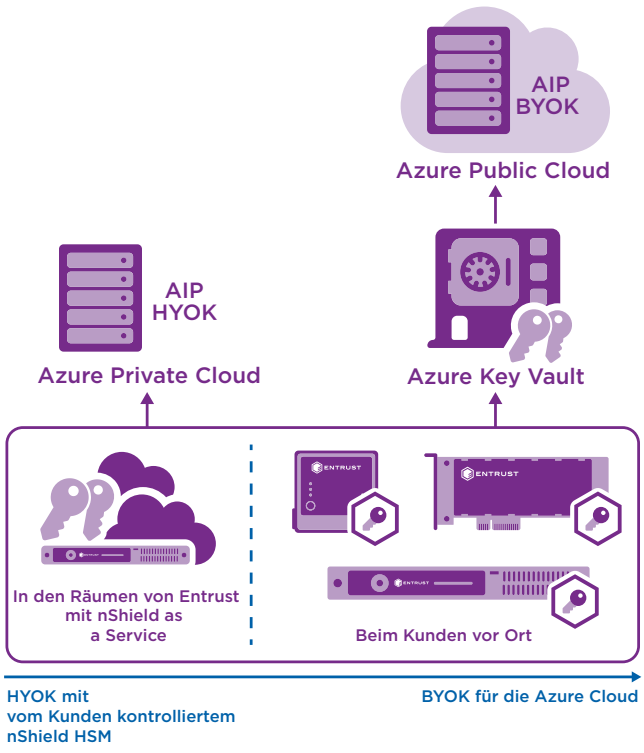
Microsoft und Entrust bieten lang anhaltenden Datenschutz und eine Schlüsselverwaltungslösung, mit der Sie in der Cloud den Überblick behalten

ECKPUNKTE

- Kontrollieren Sie den Zugriff und die Nutzung der von Ihnen ausgetauschten Daten.
- Kontrollieren und schützen Sie Ihrer Schlüssel mithilfe von HSM, die Sie selbst steuern.
- Stellen Sie gemäß FIPS 140-2-zertifizierte Schlüsselverwaltung über den gesamten Lebenszyklus bereit.
- Gewährleisten Sie, dass Schlüssel niemals für Microsoft sichtbar sind.

Microsoft Azure Information Protection (AIP) schützt die in Ihrer kollaborativen Arbeitsumgebung ausgetauschten Daten, indem es unabhängig vom Datentyp durchsetzbare Sicherheitsrichtlinien für die Datenbestände einbettet. Als Cloud-Dienst können sie AIP On-Demand ohne IT-Infrastruktur ausführen und so sicherstellen, dass Ihre Informationen über Unternehmensgrenzen hinweg geschützt sind.

AIP nutzt Kryptographie, damit Sie kontrolliert auf Ihre Daten zugreifen und diese dauerhaft schützen können. Die Sicherheit von AIP hängt vom Schutzniveau der kritischen kryptographischen Schlüssel ab. Die Weitergabe der kryptographischen Schlüssel gefährdet Ihre sensiblen Daten.



Egal, ob Sie AIP vor Ort, in einer Hybridkonfiguration oder vollständig in der Cloud verwenden: nShield® HSM von Entrust bieten Ihnen unverzichtbare Kontrolle über Ihre wichtigen Schlüssel.

WEITERE INFORMATIONEN AUF ENTRUST.COM/HSM

Eigener Schlüssel für hochsichere Schlüsselverwaltung

Die Herausforderung: Hochsensible Daten benötigen einen kryptographischen Schlüssel, der On-Premises aufbewahrt wird

Wenngleich die meisten Inhalte durch sicher gespeicherte Schlüssel in Azure bereitgestellt werden können, dürfen bestimmte sensible Inhalte niemals außerhalb Ihres eigenen Sicherheitsbereichs weitergegeben oder übertragen werden. Die Sicherheit dieser sensiblen Inhalte sollte ausschließlich On-Premises gewährleistet und der Zugriff darauf sowie deren Weitergabe stark eingeschränkt werden.

Damit Sie Ihre sensibelsten Daten innerhalb Ihres eigenen Sicherheitsbereichs verwalten können, bietet AIP die Option Hold Your Own Key (HYOK) an, die durch eine Vor-Ort-Komponente aktiviert wird, wobei die Schlüsselverwaltung über ein Hardware-Sicherheitsmodul (HSM) von Entrust erfolgt, das sich in den Räumlichkeiten des Kunden oder in der as a Service-Umgebung befinden kann.

nShield® HSM von Entrust schaffen einen verschlossenen Raum, der Ihre wichtigen Schlüssel schützt und die Sicherheit Ihrer sensiblen Daten erhöht.

Die Lösung: HYOK-Bereitstellungen mit erweiterter Schlüsselkontrolle von Entrust

nShield HSM von Entrust wenden strenge Kontrollen bei der Verwaltung und dem Einsatz der in AIP-Bereitstellungen verwendeten kryptographischen Schlüssel an.

nShield HSM von Entrust bieten Ihnen eine Hardwarelösung zum Schutz Ihrer wichtigen Schlüssel. Sie sichern und verwalten diese völlig unabhängig von der Software-Umgebung, so dass Sie die vollständige Kontrolle über Ihren Schlüssel haben.

Dieser wird innerhalb der Sicherheitsgrenzen Ihres eigenen nShield HSM erstellt und verwaltet, so dass Sie Ihre sensibelsten Daten schützen können.

Warum HSM von Entrust mit AIP und HYOK?

HSM von Entrust bieten Ihnen die nötige Flexibilität, um AIP gemäß Ihren Vorgaben zu verwenden und Ihren Datensicherheitsanforderungen gerecht zu werden – ob vor Ort, in der Cloud oder in einer Hybridkonfiguration. nShield HSM:

- sichern den Schlüssel innerhalb gemäß FIPS 140-2 zertifizierten kryptographischen Grenzen.
- nutzen robuste Zugriffssteuerungsmechanismen mit strikter Aufgabentrennung, damit der Schlüssel nur für seinen autorisierten Zweck verwendet wird.
- gewährleisten die Verfügbarkeit von Schlüsseln durch Schlüsselverwaltung,Speicherung und Redundanzfunktionen.

Wenn Sie Azure Key Vault zur Speicherung Ihrer Schlüssel und deren Verwendung mit AIP nutzen möchten, kann Entrust zudem dazu beitragen, die Sicherheit dieser Schlüssel zu verbessern. Sie können sie mit den von Ihnen kontrollierten nShield HSM erstellen und sicher an Azure Key Vault übermitteln. Mit der Bring Your Own Key Funktion (BYOK) haben Sie die Kontrolle über Ihre Schlüssel und die Sicherheit Ihrer Daten in der Cloud.

Eigener Schlüssel für hochsichere Schlüsselverwaltung

nShield HSM von Entrust:

- schützen Schlüssel in einer robusten, manipulationssicheren Umgebung
- setzen Sicherheitsrichtlinien, die Trennung von Sicherheitsfunktionen und Verwaltungsaufgaben um
- halten die regulatorischen Anforderungen für den öffentlichen Sektor, Finanzdienstleistungen und Unternehmen ein
- sind nach FIPS 140-2 Level und Common Criteria zertifiziert

nShield HSM von Entrust sind für spezifische Leistungs- und Budgetanforderungen verfügbar:

- Für die Erstellung und Verwaltung einer großen Anzahl an Schlüsseln (oder als Teil einer hybriden Bereitstellung) bieten eingebettete PCIe-Karten und an das Netzwerk angeschlossene nShield Connect HSM leistungsstarke Hardware-Sicherheit.
- nShield Connect HSM können beim Kunden vor Ort oder in der nShield as a Service-Umgebung eingesetzt werden.
- Für die Erstellung einer geringen Anzahl an Schüsseln On-Premises mithilfe der BYOK-Funktion bietet der nShield Edge HSM bequeme USB-Hardware-Sicherheit.

HSM von Entrust

nShield HSM von Entrust gehören zu den leistungsstärksten, sichersten und am einfachsten integrierbaren HSM-Lösungen am Markt. So erleichtern sie die Einhaltung regulatorischer Vorschriften und bieten höchste Daten- und Anwendungssicherheit für Unternehmen sowie Finanz- und Regierungsbehörden. Unsere einzigartige Security World-Architektur für die Schlüsselverwaltung bietet starke, granulare Schlüsselkontrollen hinsichtlich Zugriff und Nutzung.

Microsoft

Microsoft hat die Erstellung und den Austausch von Inhalten und den Aufbau kollaborativer Prozesse in Unternehmen revolutioniert. Auf Microsoft basierende Systeme maximieren die Produktivität. Microsoft AIP nutzt Kryptographie, um Daten zu schützen und vertrauenswürdige Geschäftsumgebungen zu schaffen, indem es:

- Identitäten unternehmensübergreifend verwaltet
- Zertifikate zur Authentifizierung vergibt
- Benutzerzugriffsrechte auf Datenressourcen kontrolliert
- vollständigen Informationsschutz bietet

www.microsoft.com

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.

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