

Securosys ermöglicht Azure-Kunden externes Schlüsselmanagement mit Azure Key Vault Managed HSM

08.07.2026, 11:00 | IT, New Media & Software

Pressemitteilung von: *Archiv SEC*



Securosys Geschäftsleitung (v.l.): M. Dasen, A. Curiger, R. Rogenmoser, P. Blasko und R. Stäuble

Der Securosys EKM Proxy verbindet Azure Key Vault Managed HSM mit Securosys Primus HSM oder CloudHSM und gibt Unternehmen in regulierten Branchen die Kontrolle über ihre kryptografischen Schlüssel, ohne dass diese jemals ihre sichere Umgebung verlassen.

Zürich, 8. Juli 2026 – Die Securosys SA, ein führender Schweizer Anbieter im Bereich Cybersicherheit, Cloud-Security, Verschlüsselungstechnologie und Schutz digitaler Identitäten, stellt heute ihren External Key Manager (EKM) Proxy für Microsoft Azure vor. Damit können Unternehmen in regulierten Branchen Anforderungen an Datensouveränität und Compliance erfüllen, indem sichergestellt wird, dass Verschlüsselungsschlüssel jederzeit vollständig unter der Kontrolle des Kunden bleiben. Securosys unterstützt ab sofort das externe Schlüsselmanagement von Azure Key Vault Managed HSM und ermöglicht europäischen sowie regulierten Unternehmen eine noch stärkere Kontrolle über ihre Daten und deren Verschlüsselung.

Verschlüsselung in der Cloud. Aber wer kontrolliert die Schlüssel?

Für Unternehmen aus dem Finanzwesen, dem Gesundheitswesen und dem öffentlichen Sektor war die Verlagerung sensibler Workloads in die Cloud nie eine rein technische Entscheidung. Compliance-Vorgaben und Auditanforderungen verlangen in diesen Branchen den nachweisbaren Beleg, dass kryptografisches Schlüsselmaterial jederzeit unter der Kontrolle des Kunden bleibt und unabhängig vom Cloud-Anbieter verwaltet wird. Datensouveränität, also der Grundsatz, dass Unternehmen die vollständige Kontrolle über ihre Daten und die Schlüssel zu deren Schutz behalten, ist zu einer entscheidenden Voraussetzung für den Einsatz von Cloud-Technologien in regulierten Branchen geworden.

Die bestehende Bring Your Own Key (BYOK) Funktion von Azure ermöglicht es Unternehmen, Schlüssel ausserhalb von Azure zu erzeugen und anschliessend in Azure Key Vault zu importieren. Securosys unterstützt Azure BYOK bereits vollständig. Die neue Integration für externes Schlüsselmanagement geht jedoch einen entscheidenden Schritt weiter: Die Schlüssel werden zu keinem Zeitpunkt in die Azure-Umgebung importiert. Stattdessen werden kryptografische Operationen innerhalb der eigenen HSM-Umgebung des Kunden ausgeführt. Genau diese konsequente Trennung wird

von strengsten regulatorischen Vorgaben verlangt.

Cloud Services nutzen, ohne die Kontrolle über die Schlüssel zu verlieren

Der Securosys EKM Proxy verbindet Azure Key Vault Managed HSM direkt mit einem Securosys Primus HSM, unabhängig davon, ob dieses HSM lokal oder über Securosys CloudHSM betrieben wird. Kryptografische Operationen werden dadurch innerhalb der eigenen zertifizierten Hardware des Kunden ausgeführt. An Azure werden ausschliesslich die Ergebnisse dieser Operationen zurückgegeben. Die Schlüssel selbst werden niemals übertragen.

Dadurch können Unternehmen Azure Workloads nutzen und gleichzeitig jederzeit die unabhängige und überprüfbare Kontrolle über ihr Schlüsselmaterial behalten. Das Securosys Primus HSM erfüllt die Anforderungen von FIPS 140-3 Level 3 sowie der Common-Criteria-Zertifizierung und entspricht damit den Standards, die Regulierungsbehörden und Auditoren erwarten.

„Seit Jahren stehen unsere Kunden aus dem Bankenwesen, dem Gesundheitswesen und dem öffentlichen Sektor vor einer scheinbar unlösbaren Entscheidung: Entweder sie profitieren von der Agilität der Cloud oder von der Compliance-Sicherheit, die sich durch die Verwaltung ihrer Schlüssel im eigenen Unternehmen erreichen lässt“, sagt Robert Rogenmoser, CEO von Securosys. „Mit dieser Integration entfällt der Zielkonflikt. Die Verschlüsselungsschlüssel verbleiben jederzeit im HSM des Kunden und unter dessen Kontrolle, während gleichzeitig alle Vorteile von Azure genutzt werden können. Das eröffnet regulierten Unternehmen völlig neue Perspektiven.“

Cloud-Agilität ohne Kompromisse bei der Compliance

Die Integration bietet Unternehmen zudem einen weiteren operativen Vorteil: Da die Schlüssel niemals in die Azure-Umgebung importiert werden, behalten Kunden jederzeit die Möglichkeit, ihr Schlüsselmaterial unabhängig von der Cloud-Plattform zu verwalten und zu kontrollieren. Die API des EKM-Proxys ist bewusst auf kryptografische Operationen beschränkt. Das Management des gesamten Schlüssel-Lebenszyklus verbleibt vollständig innerhalb der Securosys-HSM-Umgebung. Darüber hinaus können Schlüssel jederzeit widerrufen werden, wodurch die zugehörigen Daten unlesbar werden. So erlangen Kunden Gewissheit, unter allen Umständen die Kontrolle zu behalten.

Auch die Bereitstellung ist einfach: Der EKM-Proxy wird als Docker-Container ausgeliefert, über eine YAML-Datei konfiguriert und kann sowohl lokal als auch in der eigenen Cloud-Infrastruktur des Kunden betrieben werden. Eine einzelne Proxy-Instanz unterstützt mehrere Azure Managed HSM Pools. Dadurch lassen sich Azure Workloads und Teams organisatorisch voneinander trennen, während gleichzeitig eine zentrale Verbindung zum Primus HSM oder zur CloudHSM-Umgebung des Kunden bestehen bleibt.

Der Securosys EKM-Proxy für Azure ist ab sofort verfügbar. Für die Inbetriebnahme werden ein Azure-Konto mit für External Key Management konfiguriertem Azure Key Vault Managed HSM, eine Securosys Primus HSM- oder CloudHSM-Partition sowie eine Host-Umgebung für den Proxy-Container benötigt.

Die vollständige Dokumentation mit allen Voraussetzungen, Konfigurationsanleitungen und Installationshinweisen steht unter <https://docs.securosys.com/azure-ekm/overview> zur Verfügung.

Securosys SA

Max-Högger-Strasse 2
8048 Zürich
Schweiz

MartinaAlig (Marketing Director)

0445523100

martina.alig@securosys.com

www.securosys.com/de/

Portrait

Securosys SA, mit Hauptsitz in Zürich, Schweiz, ist ein renommierter Branchenführer, der sich auf Cybersicherheit, Verschlüsselung und den Schutz digitaler Identitäten spezialisiert hat. Die Firma wurde 2014 gegründet, und ihre Hardware-Sicherheitsmodule (HSMs) sichern täglich Transaktionen von über 100 Milliarden Euro auf dem Schweizer Bankenplatz SIC (unter Aufsicht der Schweizerischen Nationalbank) sowie die Schweizer Börsen SIX und SDX. Über die Hälfte der weltweiten Tier-1-Banken sowie viele weitere Technologiefirmen vertrauen den von Securosys in der Schweiz entwickelten und produzierten HSMs.

Die umfassenden HSM-Lösungen von Securosys, die sowohl für den Einsatz vor Ort als auch in der Cloud als SaaS verfügbar sind, sind nach den höchsten Sicherheitsstandards wie FIPS und Common Criteria zertifiziert. Die HSMs von Securosys sind auf verschiedene Branchen zugeschnitten wie das Finanzwesen, das Gesundheitswesen, Behörden und weitere Industrien. Sie bieten unübertroffene Funktionen wie unabhängige, kryptografisch sichere Partitionen, patentierten, richtlinienbasierten, individuellen Schlüsselschutz und Cloud-Tauglichkeit. Die Geräte unterstützen hybride Signaturen und ermöglichen so einen nahtlosen Übergang von klassischer zu Post-Quantum-Kryptografie (PQC). Dank dieser Innovationen gelten die HSMs von Securosys als verlässliche Wahl für die sichere Schlüsselgenerierung, -verwaltung, -verschlüsselung und digitale Signatur in unterschiedlichsten Anwendungsbereichen.

News-ID: 1317342 • Views: 91 (Stand: 06.08.2026)

Link zur Pressemitteilung:

<https://www.openpr.de/news/1317342/Securosys-ermoeslicht-Azure-Kunden-externes-Schlüsselmanagement-mit-Azure-Key-Vault-Managed-HSM.html>