

Securosys Brings External Key Management to Azure Customers Through Azure Key Vault Managed HSM

Securosys EKM Proxy bridges Azure Key Vault Managed HSM and Securosys Primus HSM or CloudHSM, keeping cryptographic keys under customer control.

ZÜRICH, ZÜRICH, SWITZERLAND, July 8, 2026 /EINPresswire.com/ -- Securosys SA, a Swiss leader in cybersecurity, cloud security, encryption technology, and digital identity protection, today announced the launch of its External Key Manager (EKM) Proxy for Microsoft Azure, enabling organizations in regulated industries to meet data sovereignty and compliance requirements by ensuring encryption keys remain entirely under the customer's control. Securosys now supports Azure Key Vault Managed HSM's external key management feature, empowering European and regulated organizations with greater control over their data and encryption.



The Securosys management team. From the left: Marcel Dasen (Executive VP Engineering), Andreas Curiger (CTO/CSO), Robert Rogenmoser (CEO), Pal Blasko (CFO), and Reto Stäubli (Executive VP Solutions & Services)

Encryption in the Cloud — But Who Holds the Keys?

For organizations in financial services, healthcare, and the public sector, moving sensitive workloads to the cloud has never simply been a technical decision. Compliance and audit requirements in these industries demand demonstrable proof that key material remains under the customer's governance, independent of the cloud provider. Data sovereignty — the principle that organizations retain full control over their data and the keys that protect it — has become a defining requirement for cloud adoption in regulated sectors.

Azure's existing Bring Your Own Key (BYOK) capability allows organizations to generate keys outside Azure before importing them into Azure Key Vault. Securosys already fully supports Azure BYOK, however, the recent external key management integration goes a step further: keys

are never imported into Azure at all. Cryptographic operations are executed within the customer's own HSM environment, which is the level of separation that the strictest regulatory frameworks require.

Cloud Services, Without Surrendering Key Control

The Securosys EKM Proxy connects Azure Key Vault Managed HSM directly to a Securosys Primus HSM, whether deployed on-premises or via Securosys CloudHSM, so that cryptographic operations are executed inside the customer's own certified hardware. Only the results of those operations are returned to Azure. The keys themselves never move.

This allows organizations to run Azure workloads while at all times maintaining independent, auditable control over their key material. The Securosys Primus HSM is compliant with FIPS 140-3 Level 3 and Common Criteria standards, the certifications regulators and auditors look for.

"For years, our customers in banking, healthcare, and government have faced an impossible choice: the agility of the cloud, or the compliance certainty of keeping keys in-house," says Robert Rogenmoser, CEO of Securosys. "With this integration, that trade-off no longer exists. Encryption keys remain in the customer's HSM, under their governance, always, while their teams get every benefit of Azure. That's a genuinely new position for regulated enterprises to be in."

Cloud Agility Without Compliance Compromise

The integration also gives organizations an operational advantage: because keys are never imported into Azure, customers retain the ability to maintain, manage, and govern their key material independently of the cloud platform at all times. The Proxy API is intentionally limited to cryptographic operations, meaning key lifecycle management remains entirely within the Securosys HSM environment. The ability to revoke keys at any time, rendering the associated data unreadable, gives customers the assurance that they remain in control under any circumstance.

Deployment is designed to be straightforward: the EKM Proxy is delivered as a Docker container, configurable via a YAML file, and can be stood up in a customer-controlled environment, whether on-premises or in their own cloud infrastructure. A single proxy instance supports multiple Azure Managed HSM pools, enabling operational segregation between Azure workloads and teams while maintaining a centralized connection to the customer's Primus HSM or CloudHSM environment.

The Securosys EKM Proxy for Azure is available now. Getting started requires an Azure account with Azure Key Vault Managed HSM configured for external key management, a Securosys Primus HSM or CloudHSM partition, and a host environment for the proxy container. Full documentation, including prerequisites, configuration guides, and installation instructions, is available through the Securosys documentation at <https://docs.securossys.com/azure-ekm/overview>.

Martina Alig
Securosys SA
+41 44 552 31 00
martina.alig@securosys.com
Visit us on social media:
[LinkedIn](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/925080458>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.