

Thales External Key Management Solutions for Microsoft Azure

Overview

As organizations worldwide increasingly migrate sensitive workloads and data to the public cloud, the demand for robust digital sovereignty solutions has never been greater. Regulatory bodies across the globe are imposing stringent requirements to ensure that enterprises retain control over their data, particularly in sectors such as finance, healthcare, and government. These regulations mandate not only data residency but also uncompromised control over the cryptographic keys that safeguard critical information.

In response to these evolving regulatory landscapes, customer managed key (CMK) solutions provide organizations with a critical capability for maintaining control over sensitive data in public cloud environments. By enabling customers to retain ownership and management of their encryption keys, CMKs help address core digital sovereignty requirements around data control, access governance, and regulatory compliance.

This approach reduces reliance on cloud service providers for key custody, helping organizations align with global standards while confidently advancing their cloud transformation initiatives.

External Key Management in Microsoft Azure Key Vault Managed HSM

Microsoft has introduced enhanced external key management features in Azure, giving organizations direct control over their CMK while using Microsoft's cloud platform. These advancements are tailored to address strict regulatory and data sovereignty demands, especially for customers in highly regulated industries.

The new solution provides:

- **Keys under customer control:** Organizations keep encryption keys in their own HSMs—on premises or with a trusted third-party provider—so Microsoft never has direct access. FIPS 140-3 Level 3 validated protection helps meet stringent security and compliance requirements.
- **Azure Key Vault Managed HSM:** Provides a trusted bridge between Azure services and customer-controlled external HSMs, enabling cloud workloads to use externally held keys without surrendering key custody to the cloud provider.

Thales Luna Hardware Security Modules

Thales enables external key management through a fully externalized cryptographic architecture, where master keys are executed in customer-controlled HSMs via the external key management proxy API, ensuring true sovereignty, auditability, and zero-trust encryption.

This collaboration provides customers with choices in managing their keys by extending their existing key management model with a Customer Managed Key (CMK) / Hold Your Own Key (HYOK) offer.

With Azure Key Vault Managed HSMs and Luna Network HSMs, customers can choose to have data protected with a CMK physically located outside of Azure Cloud. The externally stored key is only accessible via explicit customer authorization. Azure Key Vault Managed HSM supports most Azure services.

Secure your sensitive data and critical applications by storing, protecting and managing your cryptographic keys in Luna Hardware Security Modules (HSMs) - high-assurance, tamper-resistant, network-attached appliances offering market-leading performance.

Easily integrate these network-attached HSMs into a wide range of applications to accelerate cryptographic operations, secure the crypto key lifecycle, and act as a quantum-safe root of trust for your entire crypto infrastructure.

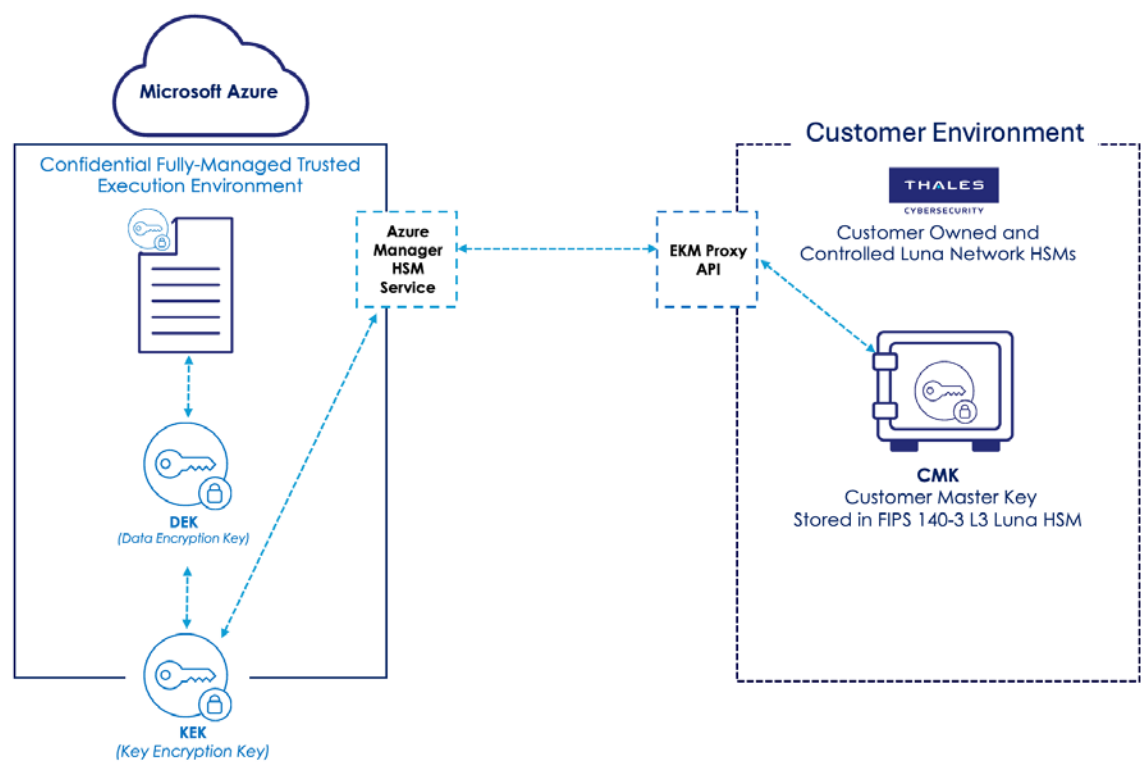
Benefits

- Demonstrate compliance with privacy regulations such as GDPR, PCI-DSS, and Schrems II
- Improve operational sovereignty by keeping key control outside the cloud provider environment
- Reduce threat surface by owning and controlling your own customer-managed keys
- Strengthen separation of duties between Azure operations and customer-controlled cryptographic services
- Support flexible deployment across on-premises, hosted, and hybrid environments

Gain Strong Key Control and Security with Hold Your Own Key (HYOK)

Microsoft External Key Management (EKM) allows enterprises to retain full control of encryption keys (KEK/CMK) by externalizing them to customer-operated HSM infrastructure, integrated through the external key management proxy API. This service offers a crucial layer of separation of duty and control. All critical key operations (wrap/unwrap) are executed in customer-controlled HSMs. Microsoft never holds the keys.

Encryption Flow Diagram



How it Works

In this model, Azure services use DEKs to encrypt and protect sensitive data, while Azure Key Vault Managed HSM orchestrates the key operations that support the encryption process within a Confidential Computing environment. The external key management proxy API provides a secure interface between Azure and the customer’s external key system, allowing Azure to request cryptographic services without direct access to the underlying keys.

All cryptographic operations are executed within the customer’s Luna HSM, keeping control of key usage firmly in the customer’s hands. By separating cloud-based data processing from externally controlled key operations, this approach enhances security, supports compliance objectives, and reinforces digital sovereignty.

Layer	Description	Location	Control
DEK	Encrypts application data	Azure service	Microsoft
KEK	Encrypts (wraps) DEK	Azure service	Microsoft
CMK	KEK used as root key in Azure services. CMK wraps/encrypts the KEK.	Thales Luna HSM	Customer

In this model, source keys are generated and controlled in the customer owned and controlled Thales Luna HSM in their own environment, then linked for use with Azure services through external key management.

The customer retains accountability for key ownership and access decisions, while Thales enforces those controls. Azure uses the keys only when explicitly authorized.

Increased Efficiency

By combining Managed HSM's external key management with Thales Luna HSMs, organizations can improve operational efficiency while maintaining strong key control. This model allows customers to centralize cryptographic key management across cloud and hybrid environments, integrate with a broad range of applications, and streamline deployment through existing automation and management tools. Because Thales Luna HSMs are designed for high performance and scalability, customers can support demanding encryption workloads without introducing unnecessary operational complexity, helping security and IT teams move faster while preserving compliance and sovereignty requirements.

Align with Best Practices

Deliver compliance, best security practices and control of your data by separating encryption key control from data encryption and decryption operations. Gain operational insights on encryption key usage with reports and logs provided by Thales.

Integrate with Your Automation Initiatives

Thales Luna HSM capabilities are available programmatically using RESTful APIs, enabling DevOps and IT teams with the power of centralized cloud encryption management to work with the organization's automation and self-service initiatives.

Thales is Here to Help

[Contact Thales](#) to help you assess and define the data security strategy that best suits your organizational requirements.

[View the Thales Integration Guide.](#)

Thales is also working to integrate the Microsoft solution with its [CipherTrust Data Security Platform](#). Contact Thales if you would like to [learn more](#).

About Thales

Thales is a global leader in cybersecurity, helping the most trusted companies and organizations around the world protect critical applications, sensitive data, and identities anywhere at scale. Through our innovative services and integrated platforms, Thales helps customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.