Encryption Strategies for Microsoft Azure Using Thales Luna HSMs

Your organization is looking to leverage all of the advantages the cloud has to offer, but some of the benefits come at a price. In return for flexibility, scalability and automation, data and encryption key ownership is often given up to the cloud service provider, taking the control out of your hands and increasing compliance complexity.

When it comes to encryption keys and protecting sensitive data, it is all about enhanced control and following security best practices. By default Azure generates encryption keys on behalf of customers and manages their lifecycle. For many organizations hosting sensitive data in the cloud, this lack of sole control and ownership over encryption keys does not meet their compliance or internal security requirements. Instead these organizations want full control over how and when encryption keys are used to protect and access encrypted data.

Thales offers a number of encryption management solutions based upon Thales Luna HSMs to secure and protect your data regardless of its location. With Thales, you have the flexibility to leverage cloud services, the ability to both own and control your encryption keys, and/or reduce the risk of unauthorized data access or data loss.

Microsoft Azure Cloud

Microsoft Azure offers three different encryption key generation and management options:

Bring Your Own Key (BYOK) Tenant root keys generated by customer	Create encryption keys in your own environment and then securely bring those Luna HSM protected keys directly into Azure Key Vault for use.
Double Key Encryption (DKE) Additional security using two keys: one created and held by Microsoft in Azure, and another created and held outside of Azure by the customer	Encryption keys utilizing Luna HSMs providing organizations with 100% control over access to encrypted data and key lifecycles – best solution for highly sensitive content that requires additional protection.
Keys Generated by Microsoft Tenant root keys generated by Microsoft	Both key generation and lifecycle control rest solely with Microsoft.

BYOK for Microsoft Azure Key Vault with Luna HSMs

Tenant Root Keys Generated by Customer

The ability to import keys generated in Luna HSMs via the Thales BYOK solution provides enhanced control and security over encryption keys used by Azure Services and applications running in the cloud. By generating your own keys with a Luna HSM, you can easily verify the origin and quality of the keys you are using in the cloud, strengthening the security of your organization's key management and security practices.

BYOK Features & Benefits:

- **Verify Origin and Quality of Keys Being Brought to the Cloud:** Keys generated by Luna HSMs are securely imported for use in Azure Vault via the Luna HSM BYOK Utility ensuring the keys are always protected. Once keys are imported you're able to use and leverage the Azure cloud in the same manner as Azure generated keys.
- **High Quality Entropy Results in Strong Keys/Identities:** Securely create and control encryption keys separate from where sensitive data is being hosted. Enhance control over key lifetimes and usage to support your operational and compliance requirements in the cloud.
- **Secure Copy of Key in Your Possession:** Ensure protection of imported keys to Azure in an external FIPS 140-2 Level 3 validated Luna HSM root of trust. You also have the ability to archive a copy of the generated keys – retaining a copy for future audit or data migration.
- **Supports Multi-Cloud Uses Cases:** You're able to use the same key in multiple clouds.

Luna Key Broker for Microsoft DKE

Double Key Encryption (DKE) Protection Provides Additional Security for Your Data by Using Two Keys

Protect your most sensitive data while maintaining full control and ownership of your encryption keys outside of Azure cloud. The solution uses two keys to protect data. One key is created and managed securely by you in a FIPS 140-2 Level 3 Luna HSM and another one created and held by Microsoft in Azure. DKE requires both keys to access protected data, ensuring that Microsoft and other third parties never have access to the protected data on their own.

This enhanced data protection capability enables Microsoft customers to benefit from the full power of Microsoft 365 collaboration and productivity tools while protecting sensitive data and meeting data privacy regulations and requirements.

DKE Features and Benefits:

You generate and manage your encryption keys (vs. the default option of having Microsoft do so on your behalf) according to your own security policies while maintaining sole control of encryption keys.

- **Enhanced Control Over Data and Keys:** Have confidence that encryption keys are not shared or used outside of your control or knowledge as Microsoft will never have access to protected data on its own. Only you have the ability to decrypt protected data.
- **Flexible Deployment:** Luna Key Broker for Microsoft DKE can be deployed either in the cloud or on-premises.
- **Security and Compliance:** Help meet internal policy and compliance mandates including regulations such as GDPR, HIPAA and Schrems II. Customer held keys are maintained separate from where your sensitive data resides by generating, managing and storing encryption keys in high assurance FIPS 140-2 Level 3 validated Luna HSM.

Microsoft Generated Keys

Tenant Root Keys Generated by Microsoft

As a security conscious enterprise, the convenience of Microsoft Azure generated keys needs to be balanced against the risk profile of the data and applications being protected. For higher assurance applications and data, it is recommended that organizations retain sole control over the generation of encryption keys.

DKE and BYOK options using Thales Luna HSMs make it easy for organizations to follow security and key management best practices, while still realizing the benefits that hosting data in Microsoft Azure has to offer.

Luna HSM Encryption Strategy Summary

Use Case	Need	Solution
Compliance mandate for secure key generation	Additional control over lifecycle operations with a FIPS 140-2 Level 3 validated Luna HSM	BYOK
Multi-Cloud support	Ability to use the same key in multiple clouds	
Support for Azure native services	Enhanced control over Azure encryption services such as RMS, Microsoft 365, etc.	
Compliance mandate to hold keys separate from the cloud service provider	With DKE customer held keys are maintained in the customer's environment and remain separate from the cloud provider in a FIPS 140-2 Level 3 validated Luna HSM	DKE
Sole control over the ability to de-crypt protected data	Control access to encryption keys independent of Azure	
Support for Microsoft 365	Enhanced control over native Microsoft 365 encryption services	
Non-Critical Data	Basic data protection and policy compliance	Keys generated by Microsoft

Thales Can Help

Contact Thales to help you assess and define the data protection strategy that best suits your organizational requirements, and for integration guides to help speed your deployment.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

> cpl.thalesgroup.com <

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us