THALES

Luna Key Broker for Microsoft Double Key Encryption (DKE)
Enhanced control and security over sensitive data in Microsoft Azure

Overview

Today's remote working environment relies heavily on the collaborative sharing of information, challenging organizations to maintain the security of confidential data and regulatory compliance while driving employee productivity. For organizations in highly regulated industries such as financial services, governments and healthcare, their sensitive data requires the highest level of control and security.

Thales Luna HSMs and Double Key Encryption for Microsoft 365 work together to enable organizations to protect their most sensitive data while maintaining full control of their encryption keys. The solution uses two keys to protect data. One key is in the customer's control in a FIPS 140-2 Level 3 validated Luna HSM and a second key, which is stored securely in Microsoft Azure. Both keys are required 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 organizations to benefit from the full power of Microsoft 365 collaboration and productivity tools while protecting sensitive data and meeting data privacy regulations and requirements.
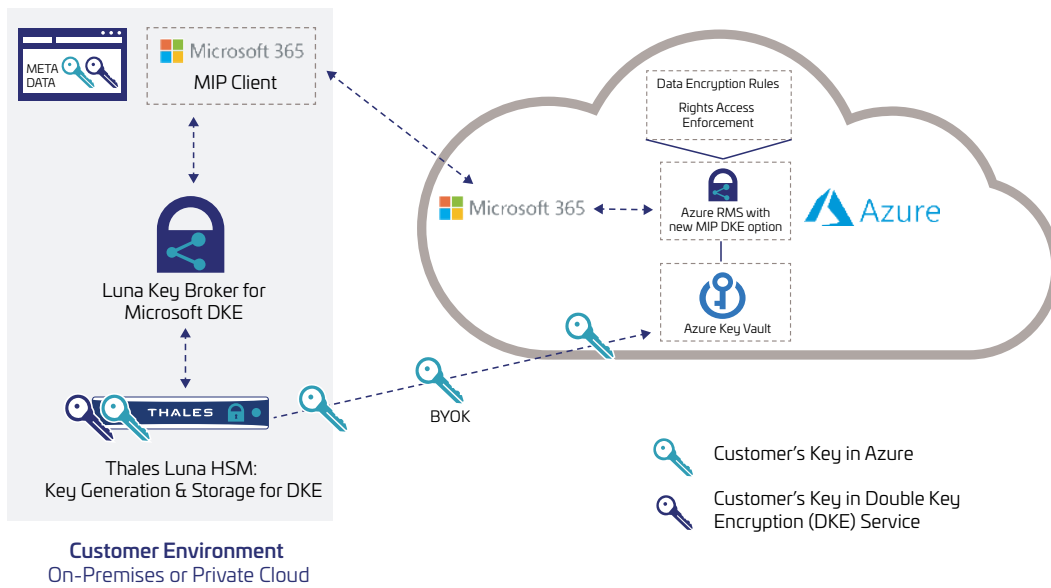
Luna Key Broker for Microsoft DKE

Organizations can protect their most sensitive data with confidence while maintaining full control and ownership of their encryption.

Solution Features and Benefits:

- Enhanced Control Over Data and Keys: Luna Key Broker for Microsoft DKE provides a secure foundation of trust for the double key encryption process. It gives organizations sole control over who has permission to access keys to decrypt protected data.
- Key Life Cycle Management: Secure generation, storage, and protection of encryption keys in a FIPS 140-2 level 3 validated Luna HSM outside of Microsoft Azure.
- Security and Compliance: Help meet internal policy and compliance mandates including regulations such as GDPR, HIPAA and Schrems II. Master encryption keys are held in a Luna HSM separate from where sensitive data resides. This provides a FIPS 140-2 Level 3 root of trust, and ensures separation between sensitive data and encryption keys.
- Flexible Deployment: Luna Key Broker for Microsoft DKE can be deployed either in the cloud, on-premises or in hybrid environments. The solution works with Luna Network HSMs and Luna Cloud HSMs.

Microsoft 365 Encryption with Luna Key Broker for Microsoft DKE

Organizations control the Customer Key in a Thales Luna HSM. This provides a FIPS 140-2 Level 3 validated root of trust, and ensures separation between sensitive data and encryption keys, helping to fulfill compliance and security requirements.

META DATA

Microsoft 365 MIP Client

Luna Key Broker for Microsoft DKE

Thales Luna HSM: Key Generation & Storage for DKE

Customer Environment
On-Premises or Private Cloud

BYOK

Data Encryption Rules
Rights Access Enforcement

Microsoft 365

Azure RMS with new MIP DKE option

Azure

Azure Key Vault

Customer's Key in Azure

Customer's Key in Double Key Encryption (DKE) Service

How it Works

Double Key Encryption (DKE) uses two keys together to access protected data: a Customer Key and a Tenant Key.

Tenant Key: This key is stored in Microsoft Azure and is used to encrypt and protect an organization's sensitive data.

Customer Key: This key remains in the customer's control and is also used to encrypt the data, adding an additional layer of security. The customer key is always protected by a Luna HSM (on-premises or cloud).

To decrypt and view the data, one must have access to both keys. Microsoft can access only one key, ensuring the customer's data is inaccessible to Microsoft.
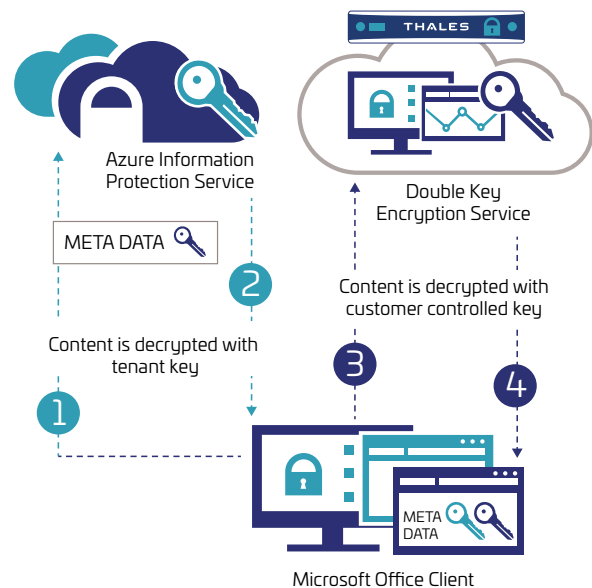
Thales is Here to Help

Thales can help organizations assess and define their DKE strategy and support including integration and deployment. Organizations will need a Thales Luna HSM (on-premises or Luna Cloud HSM service), and the Luna Key Broker for Microsoft DKE for this solution.

Thales Luna HSMs

Thales Luna HSMs have lead the market for more than 25 years, and are the foundation of digital security for traditional and emerging technologies across all environments, including hybrid, multi-cloud. Affording you the flexibility to meet your business needs and compliance needs securely and efficiently, Thales provides a high assurance, FIPS 140-2 Level 3 HSM for any use case, any application, any industry and any environment.

Decryption Flow

Azure Information Protection Service

META DATA

Double Key Encryption Service

Content is decrypted with customer controlled key

Content is decrypted with tenant key

1 2 3 4

Microsoft Office Client

META DATA

Encryption Keys

Customer's Key in Azure

Customer's Key in Double Key Encryption (DKE) Service

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.