

Thales CipherTrust Cloud Key Management for Double Key Encryption

Enhanced Security and Control
Over Sensitive Data in Microsoft
365 with Microsoft Purview

cpl.thalesgroup.com

THALES
Building a future we can all trust

Microsoft and Thales have partnered to deliver enhanced security and control over sensitive data across the Microsoft 365 suite of modern work productivity tools including Word, Excel, PowerPoint, and Outlook.

Challenges

To obtain data sovereignty in cloud environments, it is a best practice to maintain control and own the keys used to encrypt sensitive data in all applications. This is especially true for Microsoft 365, the online collaboration productivity suite of choice for most enterprises. Today's remote working environment relies heavily on sharing information, challenging organizations to maintain data confidentiality and regulatory compliance while driving employee productivity.

Joint Solution

Organizations in highly regulated industries such as financial services, government, and healthcare can comply with confidentiality and regulations (e.g., GDPR, HIPAA, Schrems II), by leveraging **Thales CipherTrust Cloud Key Management (CCKM)** with Microsoft Purview **Double Key Encryption (DKE) for Microsoft 365** (M365).

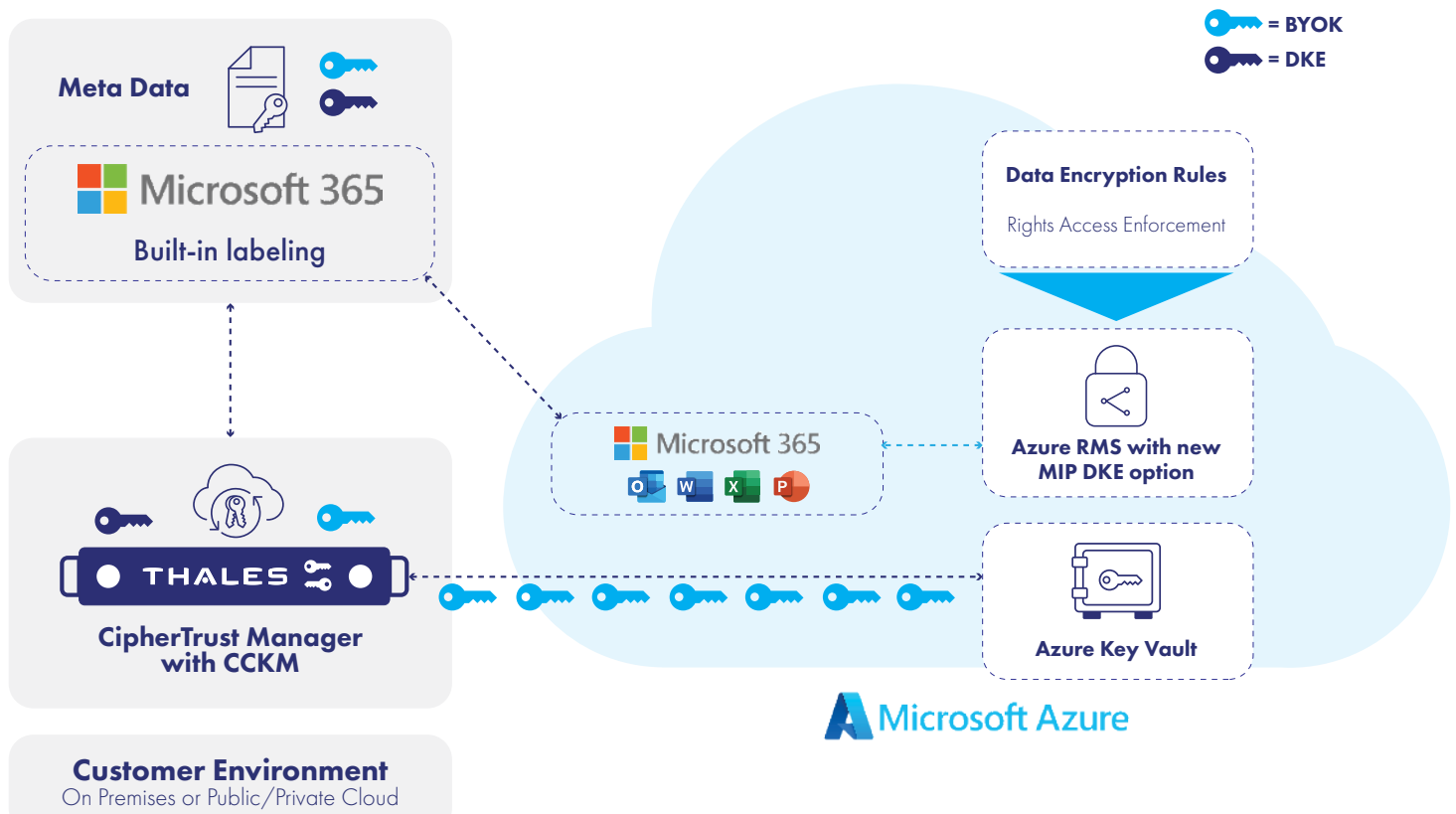
DKE for M365 and CCKM work together to enable organizations to protect their sensitive data while maintaining control of their encryption keys. The solution uses two keys to protect data. Viewing data protected with DKE requires access to both keys. The customer

maintains full control of one of their keys using the DKE service. A second key is stored in the Azure Key Vault, which could also be generated by CCKM.

The customer has complete control over their data privacy and security. Protected data is inaccessible to Microsoft because Microsoft services can only access the key stored in Azure Key Vault. Double Key Encryption facilitates secure collaboration in the workplace and helps organizations prevent highly sensitive data from being overshared both internally as well as externally. By design, DKE also prevents Microsoft from being able to read DKE protected data.

To help protect sensitive data, organizations should consider using Microsoft Purview Information Protection with customer-managed keys (BYOK). This approach blends functionality with increased digital sovereignty by allowing the customer to independently store, generate and securely control access to the encryption keys, while still allowing the customer to use the most powerful Microsoft 365 data-over-reasoning services; services that are not available to DKE encrypted content. DKE will help to protect sensitive documents/data from being used by Co-Pilot and allows to protect sensitive documents/data in SharePoint Online and OneDrive for Business.

Thales CCKM - Microsoft DKE Overview



Solution Benefits

CCKM for DKE provides a secure foundation of trust for the double key encryption process. CCKM gives organizations sole control over who has permission to access keys to decrypt protected data and provides enhanced data protection capabilities, including:

Centralized Key Life Cycle Management

CCKM is flexible and built for change. In addition to DKE, CCKM offers additional functionality to securely generate, store, and protect encryption keys for cloud-managed keys, Bring Your Own Key (BYOK), Double Key Encryption (DKE), and Hold Your Own Key (HYOK) encryption keys in one central location.

Meeting Security and Compliance

Help meet internal policy and compliance mandates including regulations such as GDPR, HIPAA and Schrems II, by ensuring master encryption keys are held separate from where sensitive data resides.

Thales Luna HSMs can also be integrated as a part of the solution to form a secure FIPS 140-validated, CC EAL 4+ certified hardware root of trust, ensuring the master keys never leave the secure environment of the HSM. This safeguards the security of data, users, and applications, helps to build trust in the overall ecosystem and meets strict compliance needs.

Increased Efficiency and Operational Resilience

Automate key lifecycle management across clouds and hybrid environments with data protection and key lifecycle and management tools such as a single user interface across clouds, a common set of APIs across clouds, and a single pane of glass view into where your keys are stored across multiple accounts, regions, subscriptions, and projects.

Flexible Deployment Options

CCKM for DKE can be deployed in the cloud, on premises, across hybrid environments, and as a service. Please visit the [Community Edition from MS Marketplace](#) to enable a 90-day free trial, or CCKM as a service from the [Thales DPoD Marketplace](#). Thales also offers the [Luna Key Broker integration for MS DKE](#).

Non-sensitive Data	Sensitive Data	Highly Sensitive Data
Microsoft Managed Keys	Customer Managed Keys BYOK + CCKM	Microsoft 365 DKE + CCKM

About Thales

Today's businesses and governments depend on the cloud, data and software to deliver trusted digital services. That is why the most recognized brands and organizations around the world rely on Thales to help them protect sensitive information and software wherever it is created, stored or accessed – from the cloud and data centers to devices and across networks. As the global leader in data security and software licensing, our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, create more value from their software and deliver seamless digital experiences for millions of consumers every day.