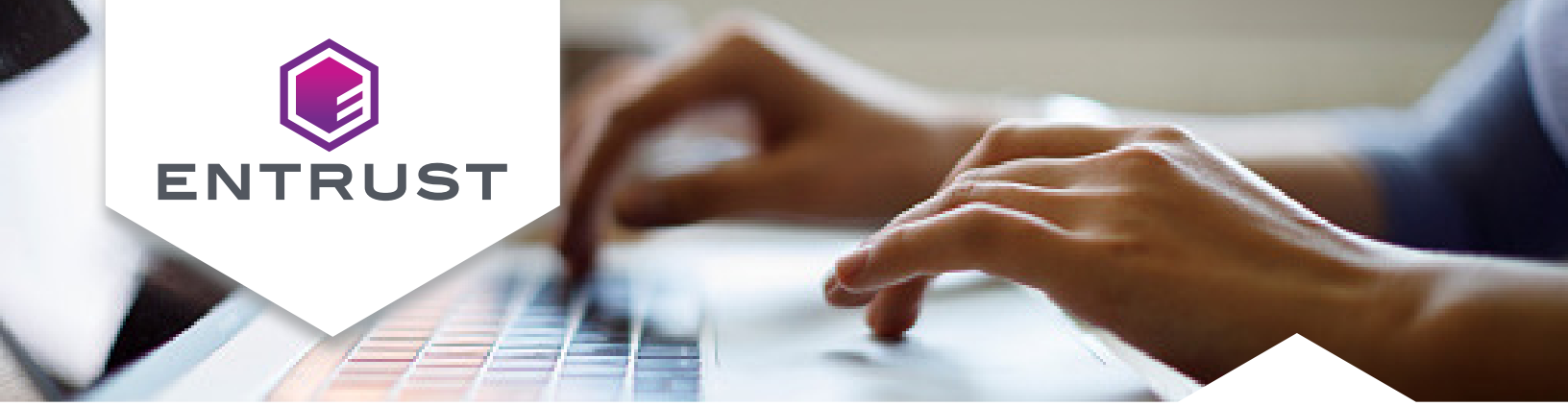


Entrust KeyControl Vault for Cloud Keys

Protecting Microsoft 365 highly sensitive data using Double Key Encryption (DKE)

Overview

Highly sensitive data is often the primary target for malicious actors. The loss of such data can significantly harm an organization's reputation and erode the trust of its customers. Protecting this information is therefore crucial to maintain corporate integrity and customer confidence.

As more companies rely on cloud-based technology, it's vital to ensure highly sensitive data remains protected. Microsoft Double Key Encryption for Azure Information Protection (AIP) helps enterprises protect their most sensitive Microsoft 365 content.

DKE operates on the principle of double encryption within Microsoft 365, where viewing protected data necessitates access to two encryption keys. Crucially, one of these keys is always stored outside of the Microsoft 365 perimeter. Given that Microsoft services are limited to accessing only the key housed in Azure Key Vault, any data protected under this system remains beyond Microsoft's reach. This ensures that users retain complete autonomy and control over their data's privacy and security.

Along with DKE, Entrust KeyControl Vault for Cloud Keys supports businesses to easily manage the keys used for encrypting the data in Microsoft 365.

The KeyControl Vault for Microsoft DKE simplifies management of external cryptographic keys by automating their lifecycle; including key storage, backup, distribution, rotation, and key revocation.

Key Features

- DKE[1] can be used to protect documents using Word, Excel, PowerPoint, and Outlook for Windows
- Double encryption of data using cryptographic keys stored and managed outside of Microsoft 365
- Unified visibility on all keys and control over every key request with full key lifecycle management
- Hardware key protection using FIPS 140-2 Level 3 certified HSMs (optional)
- Automated compliance engine for PCI DSS, DISA STIGs, NIST 800-130, HIPAA, and other standards via KeyControl Compliance Manager

[1] For information on using DKE with Office apps, see https://learn.microsoft.com/en-us/purview/sensitivity-labels-versions

Learn more about Entrust KeyControl at entrust.com

Entrust KeyControl Vault for Cloud Keys

BENEFITS

Combines the benefits of Microsoft 365 with full control over access to highly sensitive data. The KeyControl vault provides maximum control, automation, and management over cryptographic keys for organizations that need to protect their Microsoft 365 data.

- DKE is based on the Hold Your Own Key (HYOK) model, for organizations who want to retain full control over access to their highly sensitive data regardless of where it is stored or processed.
- The entire scope of the external key manager is outside the technical and operational control of Microsoft 365.
- Customers maintain control of the availability, durability, performance, and latency boundaries of key operations.

The KeyControl vault can act as an emergency off switch by blocking access to all sensitive data across all Microsoft 365 accounts in your organization. The external keystore remains transparent for all Microsoft 365 applications.

Protects Your Data With the Highest Level of Assurance

Encryption is the first line of defense for protecting sensitive data processed or stored in the cloud. Entrust KeyControl Vault secures cryptographic keys by generating and storing the keys separately from the data. Moreover, KeyControl Vault can help you achieve the desired security posture and ensure that best practices are followed by implementing separation of duty, least privilege, dual control, and audit trail generation.

Facilitates Compliance With Regulatory Requirements Using KeyControl and DKE

Beyond the cyber-threat risk, an increasingly complex regulatory environment brings its own risks to businesses. Ensuring compliance with legal requirements and standards is sometimes not possible when keys are not segregated from the cloud.

KeyControl, in conjunction with DKE, assists in achieving compliance with a variety of regulations and standards, including the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), Russia's Federal Law No. 242-FZ for data localization, the Privacy Act 1988 in Australia, and the Privacy Act 1993 in New Zealand. This combination provides a robust solution for meeting the stringent requirements of these diverse legal frameworks.

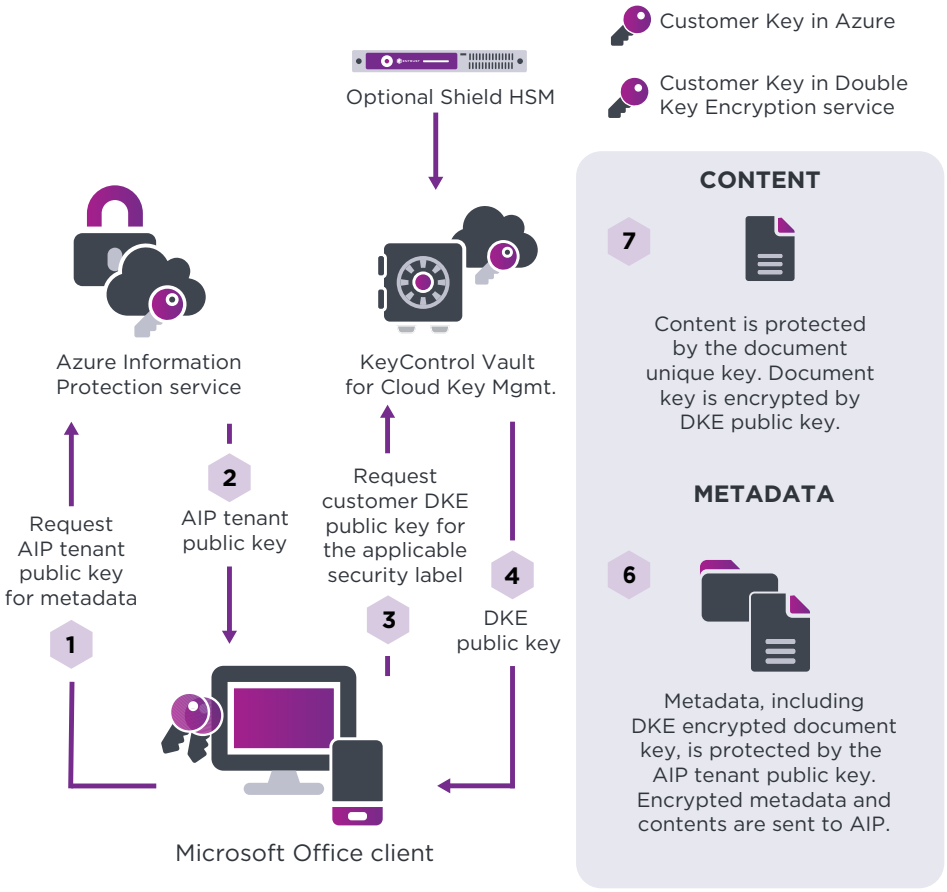
Entrust KeyControl Vault for Cloud Keys

How Does It Work?

Double Key Encryption (DKE) utilizes two component keys to protect highly sensitive data — a key that is in the customer's control and a Microsoft key stored securely in Microsoft Azure. The customer DKE key is generated and protected using a KeyControl vault and, optionally, an Entrust nShield® HSM. The customer DKE key is used to encrypt the organization's sensitive data.

The data is then encrypted again this time with the Azure Information Protection (AIP) key provided by Microsoft. The process ensures third parties including Microsoft do not have access to the customer's content.

- Document content is locally encrypted within the client application, using a unique random AES key per document.
- The unique document key is encrypted using the DKE customer key for the specific security label. The DKE private key is protected using nShield HSMs on-premises.
- The Microsoft key is used to encrypt the document metadata.
- The process prevents Microsoft from having access to the key and the customer content in Azure.



Learn more about Entrust KeyControl at entrust.com

Entrust KeyControl Vault for Cloud Keys

Internal and External Key Management

Thus, each double-encrypted data key cannot be used to decrypt an object without access to both:

- An internal key provided by the Azure Key Vault
- An external key provided by the KeyControl vault

The external and internal keys are both needed when an Office application needs to decrypt the encrypted data.

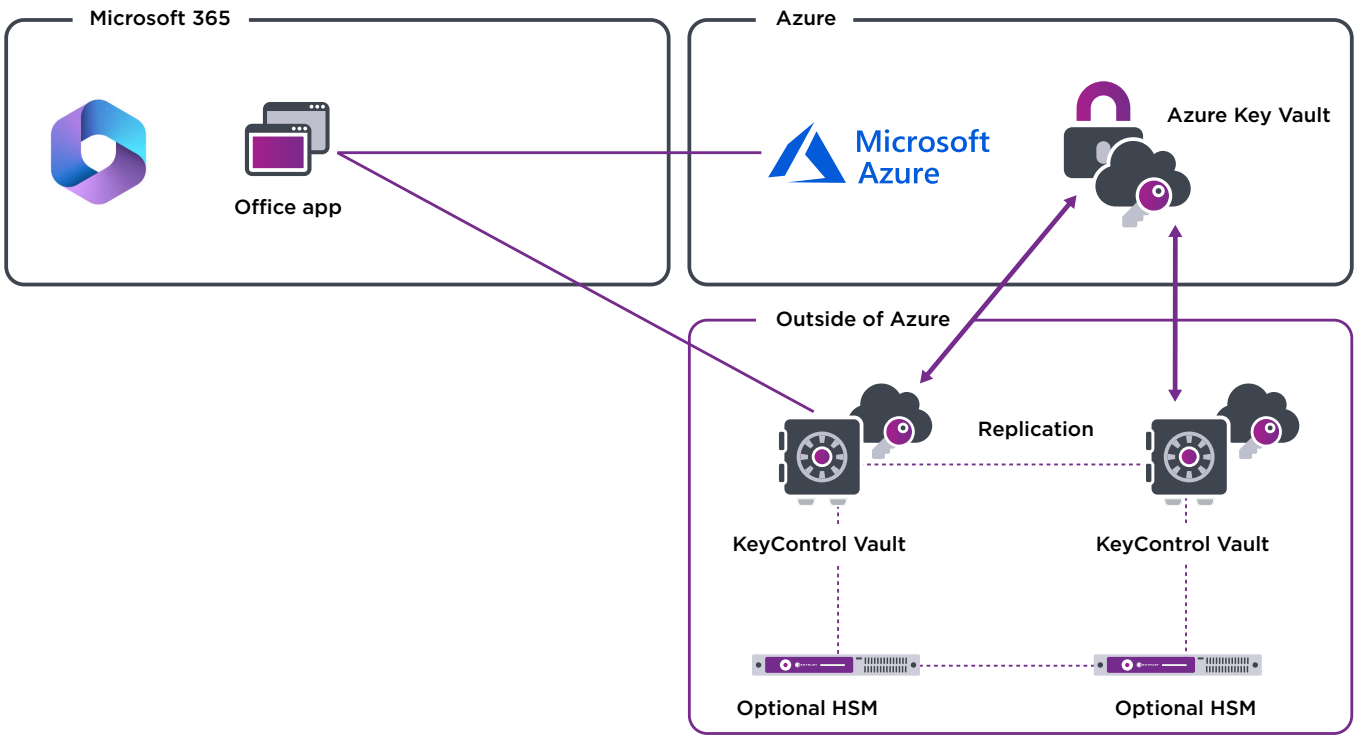
Without online access to external keys, the Office app cannot encrypt and decrypt data.

A typical architecture includes the following components for enhanced redundancy and security:

- Two KeyControl vaults configured in an active-active cluster, strategically deployed across two geographically distant sites for improved fault tolerance and high availability.
- Two nShield hardware security modules (HSMs) set up for redundancy, and distributed across two separate, distant locations to ensure continuous operation and data protection.

The KeyControl vaults act as an external key service by interacting with Azure.

Using KeyControl vault with DKE, the customer fully owns the creation, rotation, replication, and deletion of external keys.



Learn more about Entrust KeyControl at entrust.com

Entrust KeyControl Vault for Cloud Keys

Technical Specifications

Supported Office applications:

- Word, PowerPoint, Outlook, Excel
  For information on using DKE with Office apps, see https://learn.microsoft.com/enus/purview/sensitivity-labels-versions

Support external keys:

- RSA-2048, RSA-3072 and RSA-4096

Management and monitoring:

- Centralized management with Web UI and Rest API
- Syslog and Splunk integration

Certifications:

- FIPS 140-2 Level 3 or eIDAS CC EAL4+ compliance via Entrust nShield HSM on premises or as a service

Platforms supported:

- Private cloud platforms: vSphere, vCloud Air (OVH), VCE, VxRail, NetApp, Nutanix
- Public cloud platforms: AWS, IBM Cloud, Microsoft Azure, VMware Cloud (VMC) on AWS, Google Cloud Platform (GCP)
- Hypervisor support: ESXi, KVM, Nutanix, Hyper-V

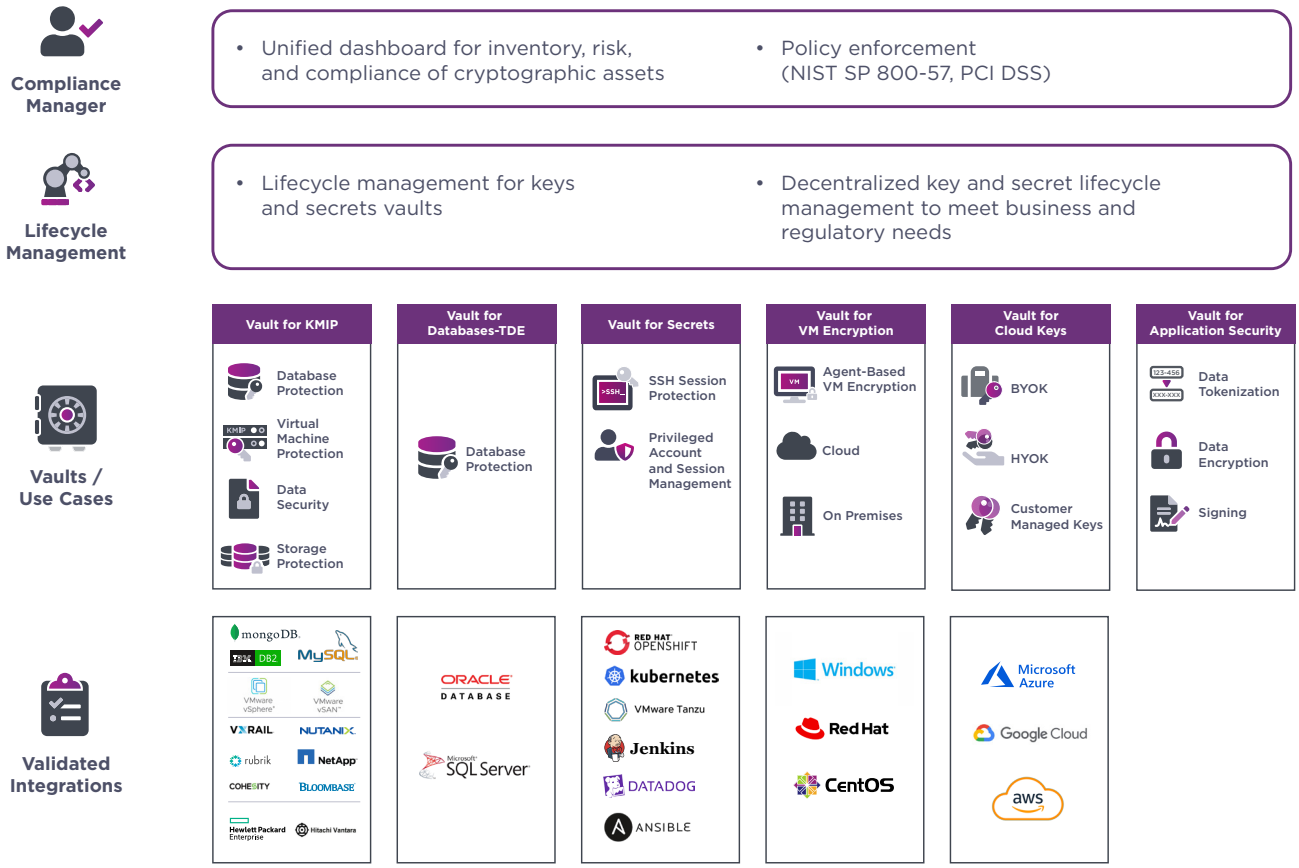
Deployment media:

- ISO, OVA (Open Virtual Appliance), AMI (Amazon Web Services Marketplace), VHD (Microsoft Azure Marketplace), and GCI (Google Cloud Marketplace)

Entrust KeyControl Vault for Cloud Keys

Entrust KeyControl Platform

Entrust KeyControl Vault for Cloud Keys is part of a suite of products designed to manage key lifecycles at scale for encrypted workloads in virtualized environments across on-premises, multi-cloud, and hybrid deployments.



Learn more at
entrust.com

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223