Entrust KeyControl Vault for KMIP

Managing cryptographic keys using the Key Management Interoperability Protocol (KMIP)

Overview

With the emergence of the Zero Trust security framework based on the ”never trust, always verify” principle, encrypting data-at-rest and data-in-transit is a crucial component of cybersecurity.

If a data breach occurs, encrypting sensitive data can be an effective way to reduce the dreaded impacts on your business.

Data encryption relies on the use of cryptographic keys that need to be managed safely and securely over their lifecycle. Any compromise of the key destroys the protection provided by data encryption.

Therefore, key management is just as important as implementing strong encryption. However, managing the cryptographic keys for applications or databases is not a trivial task.

As a comprehensive protocol for the communication between enterprise key management systems and encryption systems, the KMIP was introduced to address that complexity. KMIP is a widely adopted protocol for handling cryptographic keys and secrets for virtualization solutions, databases, endpoints, applications, storage appliances, cloud solutions, and much more.

With Entrust KeyControl Vault for KMIP, businesses have visibility into all keys across on-premises and cloud key management systems, multiple automated workflows for keys documentation, and advanced reporting capabilities.

KEY FEATURES

- Full KMIP support from version 1.0 to 3.0
- Single pane of glass for the management of keys across multiple applications
- Wide range of supported solutions including VMware, vSAN, and VM encryption
- Deployed as a virtual appliance
- High-availability (HA) support with active-active cluster
- Support separation of duties, least privilege, dual control, and multitenancy
- (Optional) Hardware key protection using FIPS 140-2 certified HSMs
- (Optional) Automated compliance engine for PCI DSS, DISA STIG, NIST 800-130, HIPAA, and other standards

Learn more about KeyControl at entrust.com

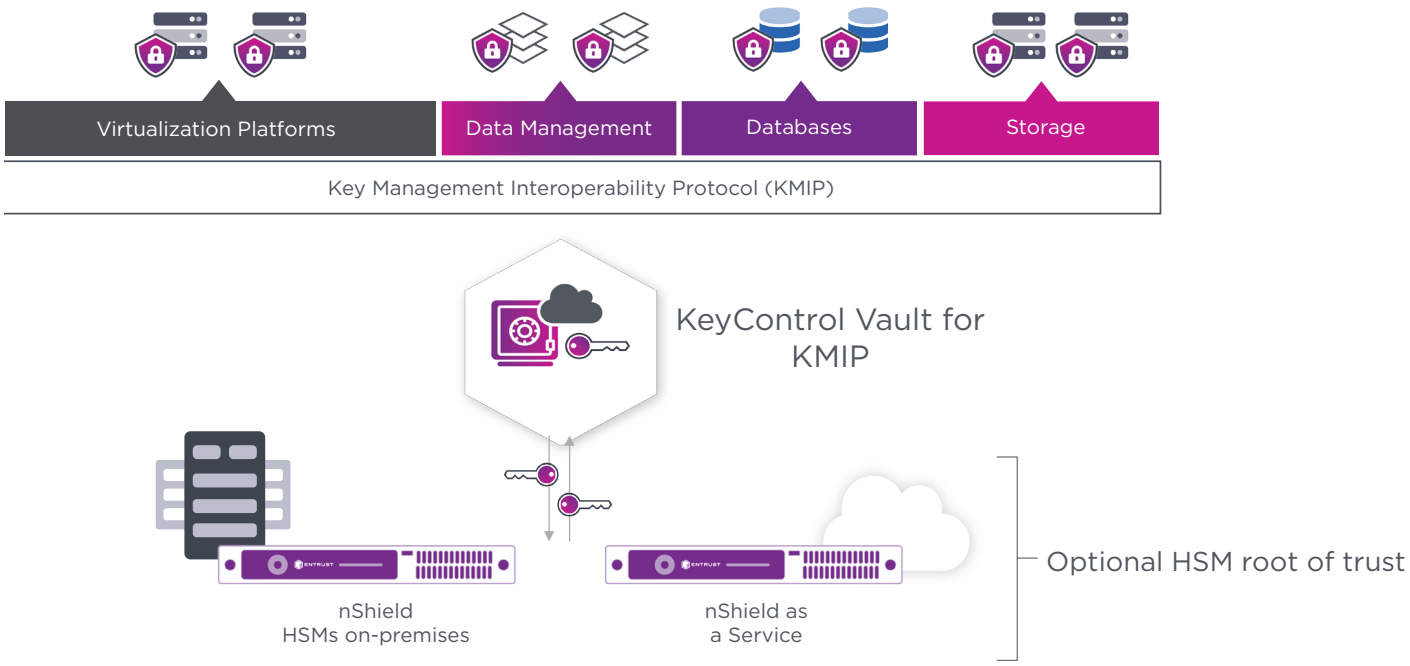
Entrust KeyControl Vault for KMIP

BENEFITS

Create universal key management for third-party solutions

KMIP is a widely accepted industry standard for communicating with endpoint clients and managing key lifecycles, providing key management security for a wide range of KMIP-compatible clients by fully supporting KMIP versions 1.0, 1.1, 1.2, 1.3, 1.4, 2.0, 2.1, 3.0.

KeyControl Vault for KMIP is both VMware and NetApp certified, and interoperable with a wide range of KMIP-compliant clients, including VMware vSphere and vSAN, industry-standard storage arrays such as NetApp, HPE, and Hitachi Vantara, and other KMIP compatible products such as Nutanix, Rubrik, Cohesity, IBM Db2, MySQL, and MongoDB.



Learn more about KeyControl at entrust.com

Entrust KeyControl Vault for KMIP

Simplify key lifecycle management and protect your data with the highest level of assurance

Key management is becoming more complex with the growing number of third-party solutions and the diversification of solutions vendors. Administrators are faced with complex and costly management of disparate cryptographic keys for many different solutions provided by multiple vendors.

With Entrust KeyControl, businesses can easily manage encryption keys at scale. Using Federal Information Processing Standards (FIPS) 140-2 certified encryption algorithms, KeyControl simplifies management of cryptographic keys by providing a single pane of glass and by automating the lifecycle of keys.

The 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.

Facilitate compliance with regulatory requirements using KeyControl Compliance Manager

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 encrypted data.

While KeyControl Vault for KMIP offers a single pane of glass for the management of cryptographic keys and secrets, Entrust KeyControl Compliance Manger extends the vault capabilities by providing an automatic approach to help support compliance with industry regulations such as PCI DSS, HIPAA, and GDPR.

KeyControl Compliance Manager makes an ideal complementary tool by making it easier to demonstrate compliance to auditors, not only for cloud key management vaults but for all vaults across your organization. Wherever you operate and whatever the regulation, KeyControl Compliance Manager can help you achieve and maintain compliance, improve your security, and manage your risk.

Entrust KeyControl Vault for KMIP

How does it work?

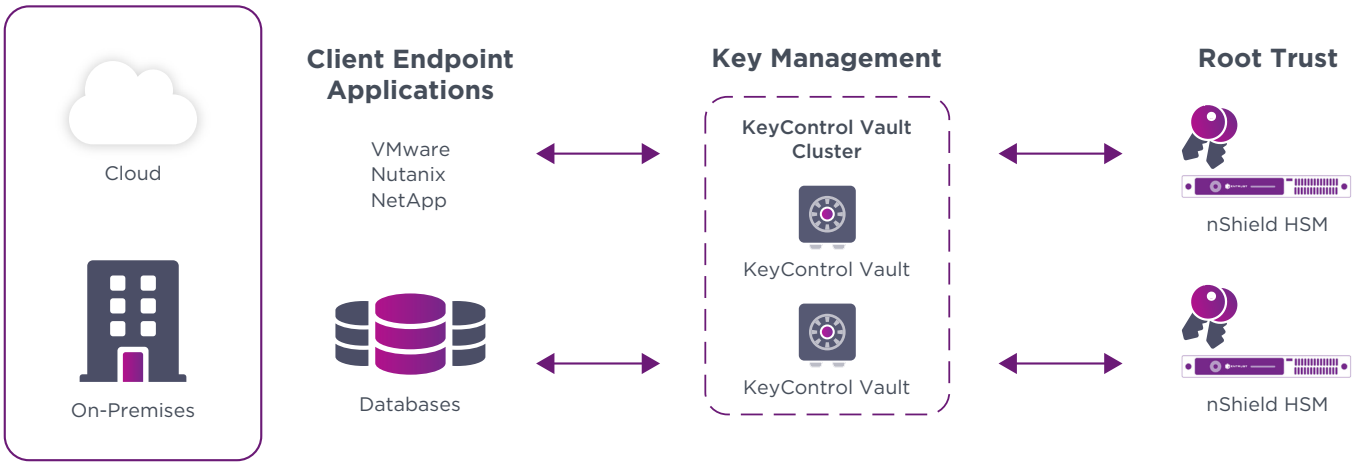
KMIP enables the secure creation and storage of security objects such as symmetric and asymmetric keys, certificates, and user-defined objects in a key management server.

The Entrust KeyControl Vault for KMIP acts as the key management server for clients that retrieve security objects via KMIP. The vault creates and manages security objects like keys and delivers them on-demand to KMIP clients such as hypervisors, tape drives, storage arrays, databases, and backup solutions.

Each KMIP client connects and authenticates to a KMIP vault using a TLS certificate.

Without online access to cryptographic keys, KMIP clients cannot encrypt and decrypt data anymore. For this reason, KeyControl vaults are usually deployed in an active-active cluster across two separate sites for redundancy.

Each KMIP client may connect directly to any of the nodes within the Vault Cluster.



Learn more about KeyControl at entrust.com

Entrust KeyControl Vault for KMIP

Technical Specifications

Supported KMIP Versions:

- KMIP 1.1 – 3.0

Management and Monitoring:

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

Platform support:

- 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, AWS, Azure, KVM, Google Cloud Platform

Certification:

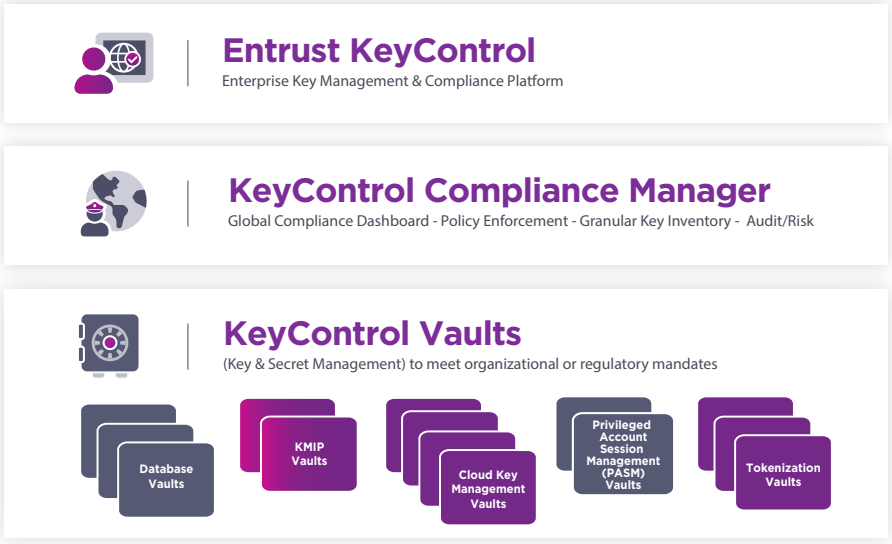
- FIPS 140-2 Level 1 Certified
- FIPS 140-2 Level 3 or eIDAS CC EAL4+ compliance via Entrust nShield HSM on premises or as a service

Deployment media:

- ISO, OVA (Open Virtual Appliance), AMI (Amazon Web Services marketplace), or VHD (Microsoft Azure marketplace)

Entrust KeyControl Product Suite

Entrust KeyControl Vault for KMIP 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

ENTRUST

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