KeyControl Vault for Cloud Key Management

Control access to cloud-based cryptographic keys using KeyControl and AWS KMS External Key Store (XKS)

Overview

As more companies rely on cloud-based technology, it's vital to ensure systems are secure and confidential data remains protected.

Modern cybersecurity threats and government regulations have led cloud providers to implement cryptographic services to ensure the integrity and confidentiality of data at rest or in transit.

Most AWS services rely on cryptographic services to protect data during transfer or storage.

Regulated industries such as finance, insurance, and healthcare have their options prescribed by security and data-handling policies, government mandates (i.e., data sovereignty), and the overall security posture of the organization.

KEY FEATURES

- Store and manage cryptographic keys outside of the AWS perimeter
- External visibility and control over every key request with full key lifecycle management
- Deployed as a virtual appliance
- 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

Learn more about KeyControl at entrust.com

KeyControl Vault for Cloud Key Management

Data sovereignty legislation in the European Union, informed by the outcome of the Schrems II legal case, has led to many organizations having to think carefully about where their cryptographic keys and encrypted data reside and about the control and access to them. AWS responded by introducing the XKS, which allows organizations to store and manage their cryptographic keys outside of the AWS perimeter.

XKS provides the ability to encrypt data with external keys for most AWS services supporting AWS key managment service, including Amazon EBS, AWS Lambda, and Amazon S3.

Along with XKS, Entrust KeyControl Vault for Cloud Key Management supports businesses to easily manage the keys used for encrypting the data in AWS.

The KeyControl Vault for AWS XKS simplifies management of these keys by automating their lifecycle; including key storage, backup, distribution, rotation, and key revocation.

BENEFITS

Combines the benefits of AWS Key KMS with full control over access to data

The KeyControl Vault provides maximum control, automation, and management over cryptographic keys for organizations that need to protect their data stored in AWS.

- XKS is based on the Hold Your Own Key (HYOK) model, the desired trust model for organizations who want to retain full control over access to their 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 AWS.
- 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 AWS accounts in your organization. The external key store remains transparent for all applications or AWS services encrypting data in the cloud.

KeyControl Vault for Cloud Key Management

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 Key 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 cloud.

Entrust KeyControl Compliance Manager extends vault capabilities beyond a single dashboard view by automating support compliance with industry regulations such as Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), or the General Data Protection Regulation (GDPR). These additions make it easier to demonstrate compliance to auditors, not only for the Cloud Key Management Vault but for all vaults across your organization. Wherever you operate and whatever the regulation, Entrust KeyControl Compliance Manager can help you achieve and maintain compliance, improve your security, and manage your risk.

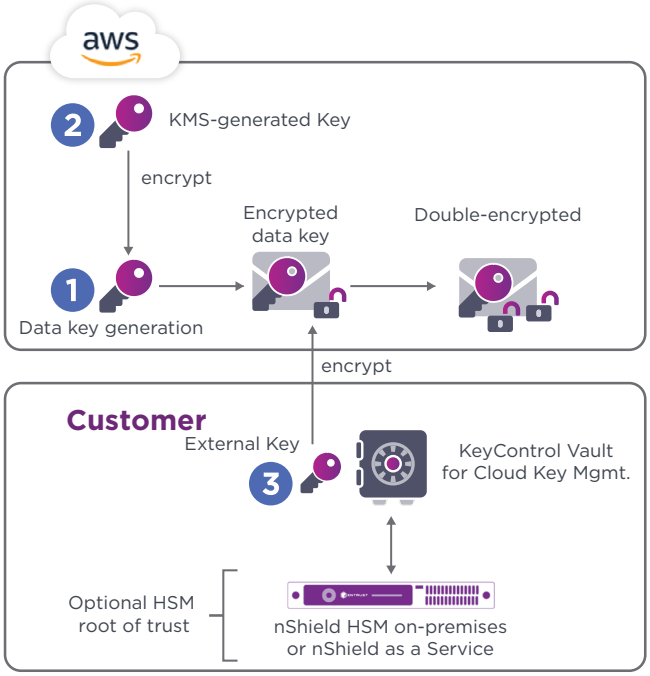
How does it work?

Using the HYOK model, XKS enables cryptographic keys to reside outside the perimeter of AWS.

The AWS Key Management Service (AWS KMS) creates cryptographic keys, called data keys, to encrypt objects used by AWS services.

When XKS is used, data keys are encrypted twice, in accordance with the principle of double-encryption:

1. AWS KMS generates a new data encryption key.
2. AWS KMS first wraps the data key using a KMS-generated key.
3. AWS KMS then wraps the encrypted data key again using the KeyControl Vault. The second encryption is done using an external vault-generated key that never leaves the perimeter of the KeyControl Vault.



Learn more about KeyControl at entrust.com

KeyControl Vault for Cloud Key Management

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 AWS KMS
- An external key provided by the KeyControl Vault

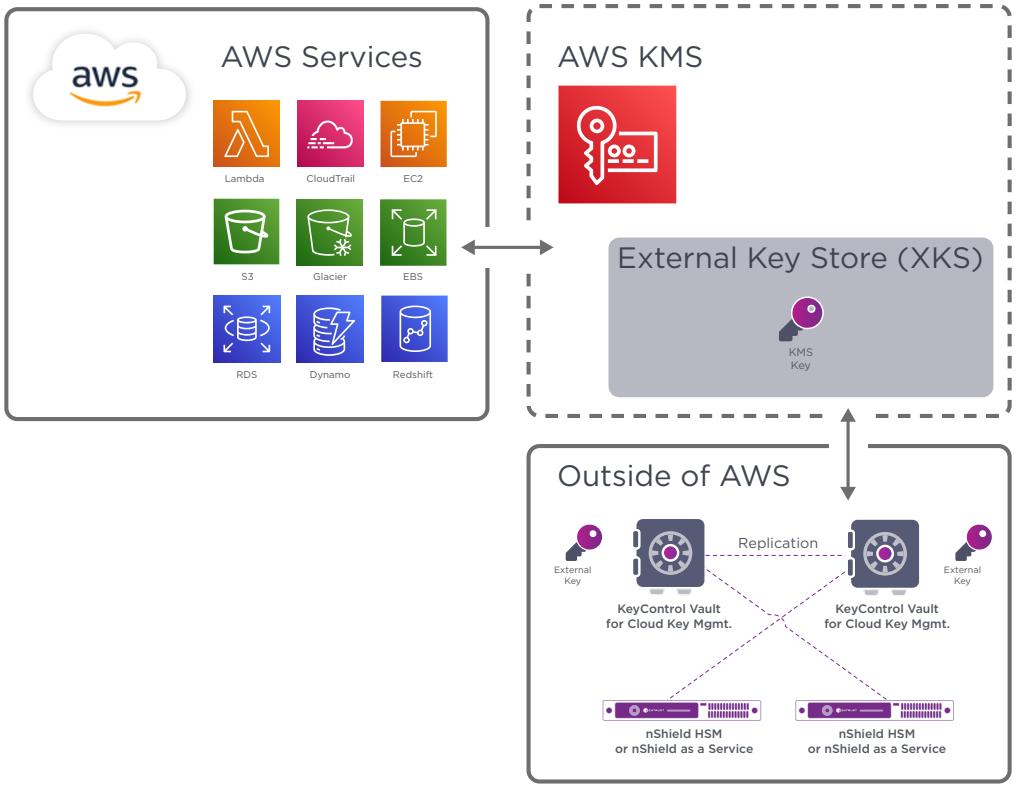
Using the concept of envelope encryption, the AWS service encrypts the data and then stores the double-encrypted data key alongside the encrypted data. The external and internal keys are both needed when an AWS service needs to decrypt the encrypted data.

Without online access to external keys, AWS services cannot encrypt and decrypt data. For redundancy two KeyControl Vaults are usually deployed in an active-active cluster across two separate sites.

The KeyControl Vaults act as an external key store proxy by interacting with AWS KMS.

XKS can be used with any AWS services that support “customer managed keys” to protect the resources in that service. Using KeyControl Vault with AWS XKS, the customer fully owns the creation, rotation, replication, and deletion of keys.

XKS Typical Architecture



Learn more about KeyControl at entrust.com

KeyControl Vault for Cloud Key Management

Technical Specifications

Supported AWS services:

- Most AWS services supporting AWS KMS customer managed keys including Amazon EBS, AWS Lambda, Amazon S3, and over 100 more services

Supported cryptographic algorithms for external keys:

- AES 256-bit key (256 random bits)

Management and monitoring:

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

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

Deployment media:

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

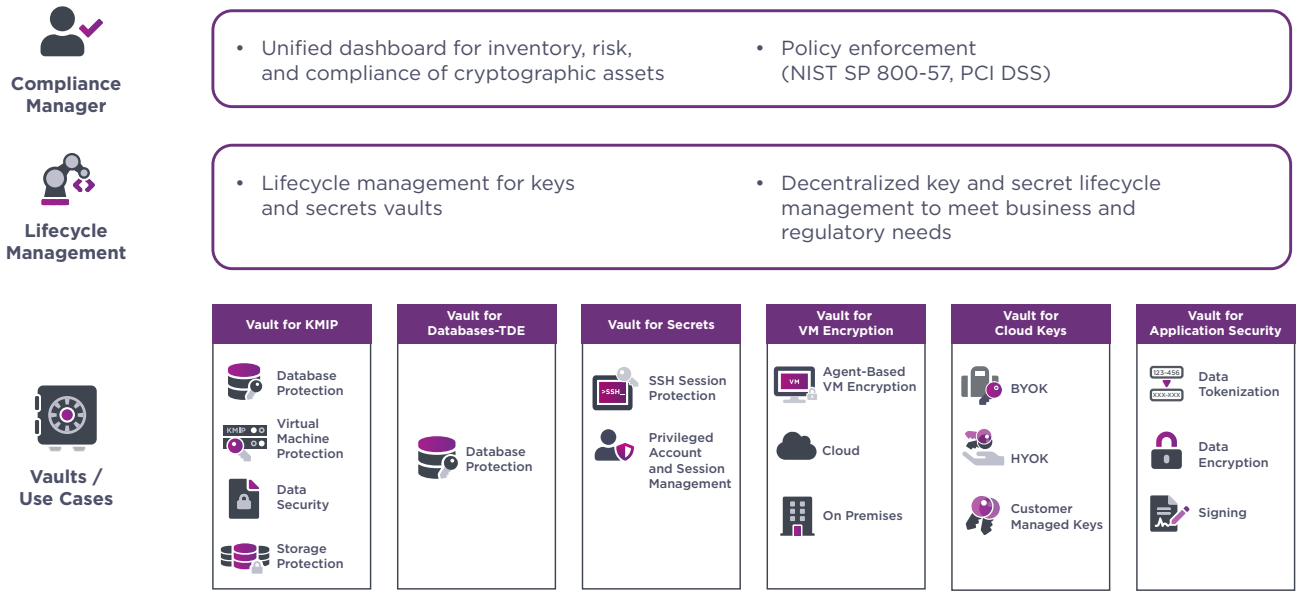
Certifications:

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

KeyControl Vault for Cloud Key Management

Entrust KeyControl Platform

Entrust KeyControl Vault for Cloud Key Management 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