HYTRUST

HyTrust KeyControl + VMware vSphere 6.5 VM Encryption = Greater Security Together

White Paper

Table of Contents

White Paper

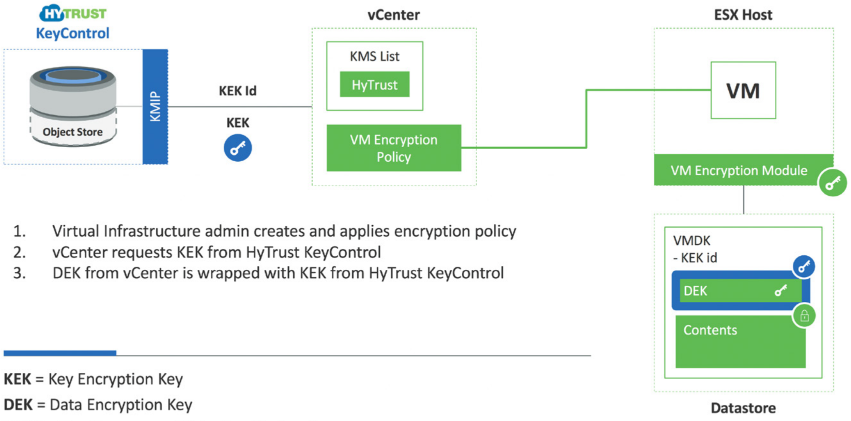
HyTrust KeyControl + vMware vSphere 6.5 VM Encryption = Greater Security Together

If you're familiar with VMware's vSphere 6.5 VM security, you know that data encryption requires an external key manager. But did you know that HyTrust KeyControl has been approved by VMware as a compatible key management solution? HyTrust KeyControl simplifies the process of key management for deployments that do not require sophisticated policy-based key management—but still need to perform to scale to enterprise grade-level performance.

HyTrust KeyControl can deliver keys as a KMIP server to the requesting vCenter KMIP client. Because keys can be issued, revoked, and re-issued—sometimes frequently—the architecture of HyTrust KeyControl has been built to withstand the demands of enterprise deployments.

Best Practices Deployment

HyTrust KeyControl generally should be deployed with at least two key controller nodes (in an active-active, high-availability configuration). If more key controllers are required (for example, in a high-volume key request scenario)—they can be added to the key controller cluster (up to eight per cluster). Since HyTrust KeyControl is delivered as an OVA—deployment is easy. Each data center location (primary and secondary, for example) will have HyTrust KeyControl and a cluster of nodes. This will ensure complete failover protection.



1. Virtual Infrastructure admin creates and applies encryption policy
2. vCenter requests KEK from HyTrust KeyControl
3. DEK from vCenter is wrapped with KEK from HyTrust KeyControl

KEK = Key Encryption Key
DEK = Data Encryption Key
KMIP = Key Management Interface Protocol
BLUE = HyTrust Components **GREEN** = VMware/Customer Components

> "Role based key management (in the HyTrust DataControl product) actually allows us to place encryption control into our clients' hands, simplifying our contract and their audits." [1]
>
> Eric Novikoff, Chief Security Officer, Enki

How It Works

The ESXi host (managed by vCenter) generates and uses an internal key (see diagram above), called the data encryption key (DEK), to encrypt virtual machines and disks. The vCenter server then requests a key from HyTrust KeyControl. This key, known as the key encryption key (KEK), is then used to encrypt the DEK. vCenter Server stores only the each DEK, but the KEK wraps the DEK to protect it.

HyTrust is the only VMware-approved KMIP vendor that VMware has invested in—ensuring a smooth customer experience.

Protection of the HyTrust KeyControl

Given the importance of a key manager in data encryption, the key manager itself must be hyper-secure. HyTrust KeyControl appliance is protected against attacks in four ways:

1. Military-grade encryption of all sensitive information including encryption keys.
2. Whitelisting all OS components in the software.
3. Hardened OS to ensure only the smallest possible attack surface is provided.
4. FIPS 140-2 Level 1 validation and integration with external HSM for a hardware root-of-trust for FIPS 140-2 Level 3 compliance.

Is HyTrust KeyControl Right for My Environment?

HyTrust DataControl takes the elements of HyTrust KeyControl and scales them to a wider set of deployment scenarios. Use the reference table below for a simple guide to determining which solutions are ideal based on your particular deployment scenarios.

[1] - TechValidate TVID: 5F8-42F-649

Product/Capability	HyTrust KeyControl + vSphere 6.5 Encryption Agent	HyTrust KeyControl w/ Support + vSphere 6.5 Encryption Agent	HyTrust DataControl
Encryption of vSphere VMs	●	●	●
Key management	●	●	●
Enterprise support		●	●
Zero downtime rekeying			●
Policy-based enforcement			●
Forensic grade logging			●
Workload boot and clone protection			●
Encrypted backups			●
Audit Ready			●

To learn more about HyTrust KeyControl, as well as other HyTrust products and services, visit:

www.hytrust.com/products/

HyTrust
1975 W. El Camino Real, Suite 203
Mountain View, CA 94040, USA
Phone: 1-844-681-8100
International: 1-650-681-8100