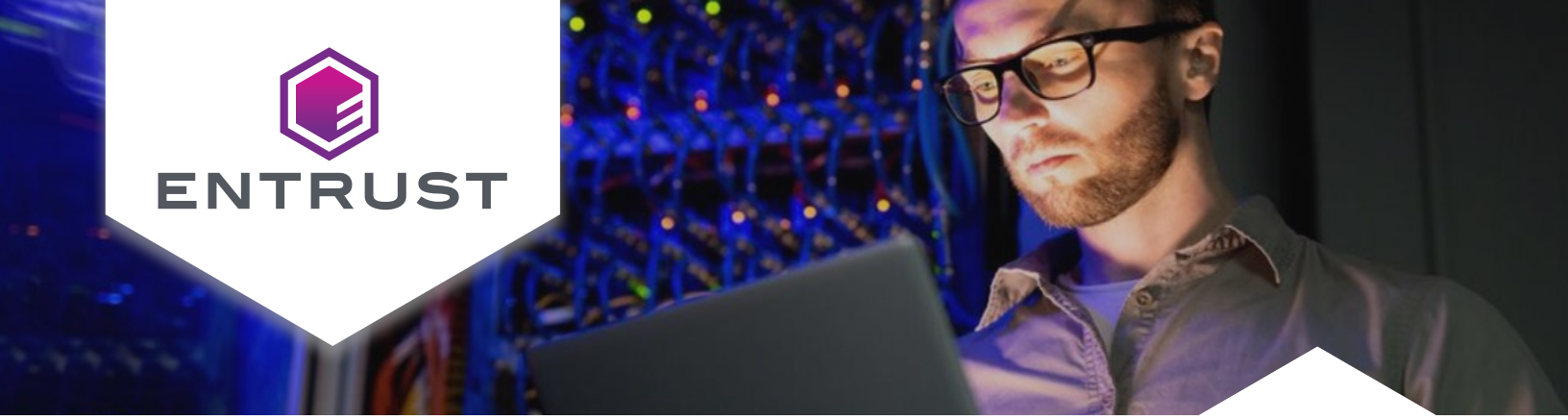

Protecting vTPMs for VMs Running Windows® 11 Using an External KMS

Learn how to protect your vTPM keys for virtual machines on Windows 11 using Entrust KeyControl key management solution (KMS).

Overview

Since the release of **Microsoft Windows® 11**, Trusted Platform Modules (TPMs) have become a mandatory requirement for both virtual and physical machines such as laptops and desktops.

The TPMs underpin the security of the software ecosystem and are used as the root of trust for applications such as BitLocker, which are used to encrypt the disk volumes to prevent unauthorized access if a machine falls into the wrong hands. The TPM works with BitLocker to ensure that the machine hasn't been tampered with while the system is offline.

What Is a TPM?

A TPM is a hardware device that provides cryptographic capabilities (such as random number generation and secure protection of secrets including encryption keys).

Applications can use the TPM to authenticate hardware devices as each TPM chip has a unique, secret asymmetric key burned into the device during manufacturing. This key cannot be exported or transferred to other TPMs and acts as a root of trust for subsequent cryptographic keys generated by the TPM. TPMs conform to the Trusted Platform Module 2.0 specification.

Virtual TPM for Securing Virtual Machines

A virtual TPM (vTPM) emulates a physical TPM, performing the same functions but handling cryptographic operations in software.

Despite this difference, the operating system and its applications behave as if they were interacting with a physical TPM. Running Windows 11 as a virtual machine requires a virtual Trusted Platform Module to be present. Data written to the vTPM is then secured with strong encryption.

Protecting vTPMs for VMs Running Windows® 11 Using an External KMS

The Problem

vTPMs rely on encryption to securely protect the sensitive data stored within them. Most virtualization platforms require a key management system (KMS) to be configured before a vTPM can be added to a virtual machine. The KMS is responsible for managing and safeguarding the cryptographic keys and secrets stored in the vTPM, ensuring secure operation and protection of the virtual machine's data.

The Solution

Entrust KeyControl combines key lifecycle management with a decentralized, vault-based architecture, while providing central policy enforcement and compliance management. This versatile solution supports diverse use cases, ensuring strong security, streamlined governance, and regulatory adherence across the organization.

Data can be protected in line with differing local security policies and in compliance with regulatory mandates.

KeyControl features a centralized dashboard that delivers comprehensive visibility into an enterprise's cryptographic assets, coupled with a policy engine that enables fine-grained control over cryptographic keys and secrets, regardless of their vault locations.

The Entrust Difference

Traditional centralized, monolithic key management solutions no longer effectively meet the needs of organizations that face increasingly complex data security, regulatory, and compliance requirements. Combining visibility with the ability to document usage parameters is essential in ensuring compliance mandates can be met. The KeyControl dashboard offers a feature-rich interface to monitor every aspect of keys and secrets, while ensuring compliance with stringent data sovereignty and residency regulations.

KEY FEATURES

- **Scalable, cost-effective, enterprise-ready** key management solution designed for vTPM and Windows 11
- **Multiple use cases supported**, including virtualization, database protection, cloud key management, tokenization, and secrets management
- **Unified dashboard** for fine-grained visibility of cryptographic keys and secrets
- **Detailed metrics to track compliance** and alert on unauthorized key usage
- **Decentralized vault-based architecture** to support data sovereignty mandates
- **High-availability configuration** for resilient operations and seamless failover
- **Optional upgrade to FIPS 140-3 Level 3** through seamless integration with Entrust nShield hardware security module (HSM)

Learn more about KeyControl at entrust.com

Protecting vTPMs for VMs Running Windows® 11 Using an External KMS

Optional nShield HSM Integration

For organizations requiring higher levels of assurance, KeyControl can be seamlessly integrated with a FIPS 140-3 Level 3 Entrust nShield® HSM. The optional HSM is used to protect the master key for the KeyControl virtual appliance. It's also used in the process when generating cryptographic keys, ensuring high-quality entropy from the HSM's random number generator is used in keys created and managed by KeyControl vaults. Also available as a cloud-based solution: nShield as a Service.

Separation of Roles

In the absence of a key management system, the key management is left solely with the VM administrator.

This approach gives the VM administrator excessive control over keys provisioned for the vTPMs, potentially compromising security. By using an external KMS managed by a security officer, organizations can enforce separation of duties, ensuring that key management and VM administration are handled by distinct roles, significantly reducing risk.

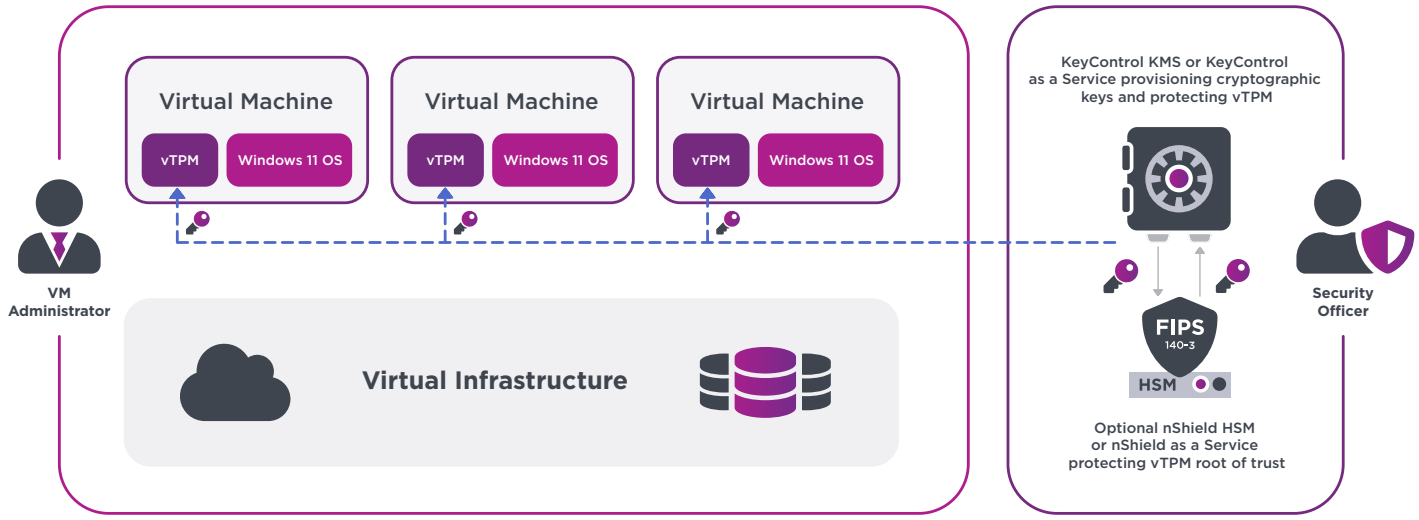

Figure 1: Illustration showing a vTPM for Windows 11 VMs being provisioned by an external key management solution with clear separation of roles. An optional HSM provides a hardware-based root of trust for additional security.

Learn more about KeyControl at entrust.com

Protecting vTPMs for VMs Running Windows® 11 Using an External KMS

Key Benefits

Key Lifecycle Management
Simplifies management of encrypted virtual machines by automating the lifecycle of encryption keys, including key storage, backup, distribution, rotation, and revocation.

HSM Root of Trust
Optional seamless integration with FIPS 140-3 Level 3 validated nShield hardware security modules.

vTPM Support
Provisions cryptographic keys to vTPM on request.

HSM Decentralized Architecture
Supports national and regional data sovereignty mandates. Locate vaults based on business need. Reduced attack surface.

Unified Dashboard
Single unified dashboard, KeyControl Compliance Manager, allows you to view and monitor your organization's cryptographic assets located in one or many vaults.

Wide Range of Use Cases
The flexible vault architecture provides support for a wide range of features and services including KMIP, VM encryption, cloud key management (including BYOK and HYOK deployments), secrets management, privileged access management, tokenization, and database protection.

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