# Entrust Cryptographic Security Platform

## Key and Secrets Management

## Overview

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 offering fine-grained policy controls and ensuring compliance mandates can be met. The Entrust Cryptographic Security Platform provides a feature-rich dashboard to monitor every facet of a key or secret while addressing the rigors of data sovereignty and residency regulations.

The platform combines key lifecycle management and a decentralized vault-based architecture with a comprehensive central policy and compliance management capabilities for a wide range of use cases.

**Versatile Key and Secret Vaults:** A decentralized security model helps mitigate aggregation risks across a cryptographic ecosystem. Data can be protected in line with differing local security policies and comply with regulatory mandates.

**Compliance Dashboard:** The Compliance Manager provides centralized visibility of an enterprise's cryptographic assets and a policy engine that allows fine-grained control of all cryptographic keys and secrets regardless of the vault locations.

## The Solution

Entrust's Cryptographic Security Platform addresses the growing need for comprehensive cryptographic asset management in an increasingly complex digital landscape. It unifies cryptographic management by combining the rich capabilities to operate PKI, certificate lifecycle management, key management, secrets management, and HSMs – all from a single cohesive system.

By integrating these critical components, the Cryptographic Security Platform offers unparalleled security, visibility, compliance, and operational efficiency for organizations dealing with securing an increasing number of machine identities, helping them protect sensitive data while fulfilling complex cryptographic requirements.

### Key Features

- Scalable, cost-effective, enterprise-ready key management system that supports a wide range of use cases
- Unified dashboard for fine-grained visibility of keys and secrets
- Detailed metrics to identify level of compliance and alert on prohibited key usage
- Decentralized vault-based architecture
- Full key lifecycle management
- Full HA configuration for resilient backup and recovery
- Optional upgrade to FIPS 140-3 Level 3 root of trust through seamless integration with Entrust nShield hardware security module (HSM)

ENTRUST

SECURING A WORLD IN MOTION

# Redefining Key and Secrets Management

## Highlights

### Vault Architecture

The flexible Cryptographic Security Platform architecture supports the following vault options for managing keys and secrets:

### Vault for KMIP

Provides a vault for KMIP workloads utilizing cryptographic keys including virtualization platforms, backup & recovery, database, and storage workloads.

### Vault for Databases

Provides key lifecycle management for encrypted SQL databases using transparent database encryption (TDE).

### Vault for Cloud Key Management

Provides organizations with control of their cryptographic keys while leveraging the benefits of the cloud. Supports customer-managed keys including Bring Your Own Key (BYOK) and cloud-managed keys (or native keys) and externally-stored keys including Hold Your Own Key (HYOK).

### Vault for Cryptographic APIs

Addresses a wide range of data protection use cases by providing data encryption, data tokenization, data signature with format-preserving encryption (FPE), data masking, and key management.

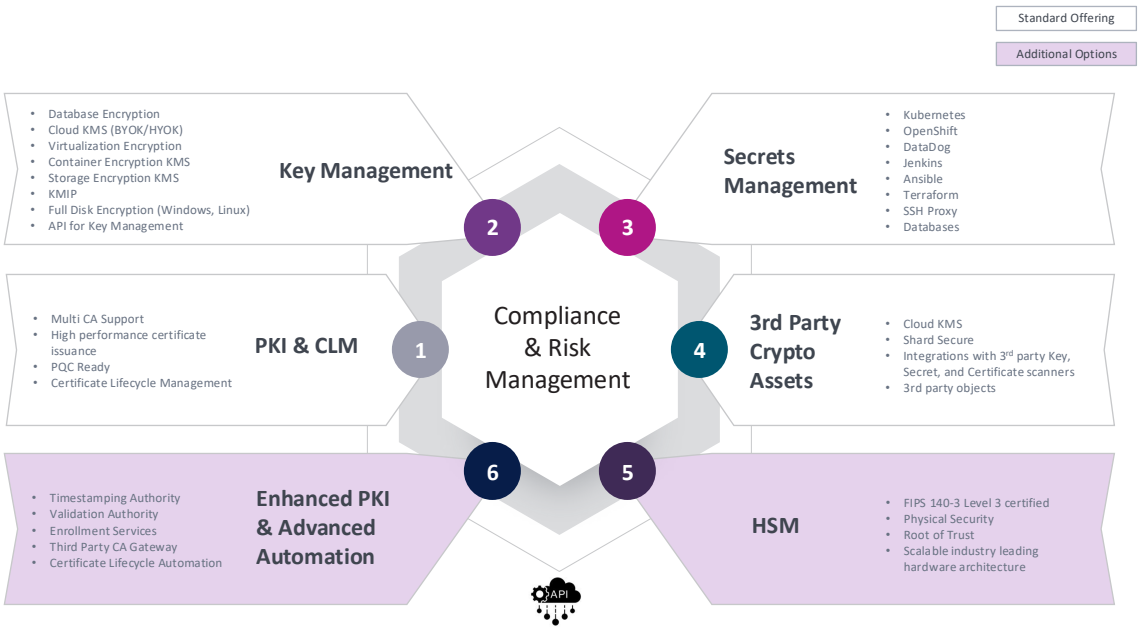
### Vault for Secrets Management

Enables organizations to securely store and strictly control access to passwords, token certificates, and cryptographic keys for protecting resources such as cloud services, databases, servers, or containers.

### Vault for VM Encryption

Provides agent-based virtual machine (VM) workload encryption, offering zero downtime encryption per VM. Unique keys can be assigned to encrypt each partition, including the boot (OS) disk and swap partitions.

The Entrust Cryptographic Security Platform (CSP), provides a comprehensive solution for discovering and managing the lifecycle of certificates, cryptographic keys, secrets, tokens, libraries, protocols, and configurations. By centralizing cryptographic asset management, it enhances security, ensures compliance, and streamlines operations, enabling seamless integration across both on-premises and cloud environments



# Redefining Key and Secrets Management

## Key lifecycle management

Simplifies management of encrypted workloads by automating the lifecycle of encryption keys; including key storage, backup, distribution, rotation, and revocation.

## Decentralized architecture

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

## Unified dashboard

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

## Wide range of vault use cases

The flexible vault architecture provides support for a wide range of features and services including KMIP, cloud key management (including BYOK and HYOK deployments).

## Enterprise-wide cryptographic security

Rich capabilities to operate PKI, HSMs, key, certificates and secrets management in a complex enterprise environment.



entrust.com Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST
SECURING A WORLD IN MOTION