DATASHEET

Entrust Cryptographic Security Platform Key Management Vault for Databases

Securing Microsoft SQL Database TDE Encryption Keys

The Challenge

Databases represent a critical security risk for many organizations. Often in security breaches, the main goal of the attackers is to gain access to databases to steal a large volume of sensitive information.

An in-depth security protocol should be put in place to protect the network, control database access, harden the database, and encrypt the data.

Security solutions designed for Microsoft SQL servers include native encryption capabilities known as TDE (transparent data encryption), which enables encryption for entire databases and associated log files. Data gets encrypted or decrypted as information is inserted, updated, and retrieved from the database by users or applications.

Managing the keys for encrypted databases is not an easy task. To ensure strong data security, keys must be rotated frequently, and transported and stored securely. In addition to the high demand for strong data security, there's an ever-increasing business need to meet requirements for regulations such as:

- Payment Card Industry Data Security Standard (PCI DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- National Institute of Standards and Technology (NIST) 800-53
- General Data Protection Regulation (GDPR)

Key Features

- Supports Transparent-Level Encryption Mode (TDE)
- Supports Cell-Level Encryption Mode (CLE)
- On-demand key rotation
- Deployed as a virtual appliance
- High availability, load balancing, and failover capabilities
- Easy setup and integration
- Separation of roles and multitenancy
- Optional hardware key protection
- Optional automated compliance engine for PCI DSS, DISA STIGs, NIST 800-130, HIPAA, and other standards

ENTRUST
SECURING A WORLD IN MOTION

Solution

With Entrust Cryptographic Security Platform Key Management Vault for Databases, you can easily manage encryption keys at scale. It simplifies the management of encrypted databases by automating the lifecycle of encryption keys – including key storage, backup, distribution, rotation, and revocation.

Safeguards your Database with the Highest Level of Assurance

Encrypting the data in your database protects the data, but the encryption keys that unlock the data must also be protected. The Key Management Vault for Databases secures encryption keys by storing the keys separately from the data on a secure, trusted platform. Moreover, it enforces your internal security policy by requiring role-based authorization and separating security and database administration, making it easier to demonstrate compliance to auditors.

Simplifies Key Lifecycle Management at Scale

While database vendors offer key management functionality, it only works with the vendor's specific databases. With the growing number of databases, administrators are often faced with the complex and costly task of managing disparate encryption keys for many different databases provided by multiple vendors. Having one unified key management solution for all databases across on-premises and cloud environments streamlines key management processes and reduces the risk of errors and fraud. Plus, with the platform you can automate key rotation, further simplifying the management of keys.

Facilitates Compliance with Regulatory Requirements using Entrust Cryptographic Security Platform Compliance Manager

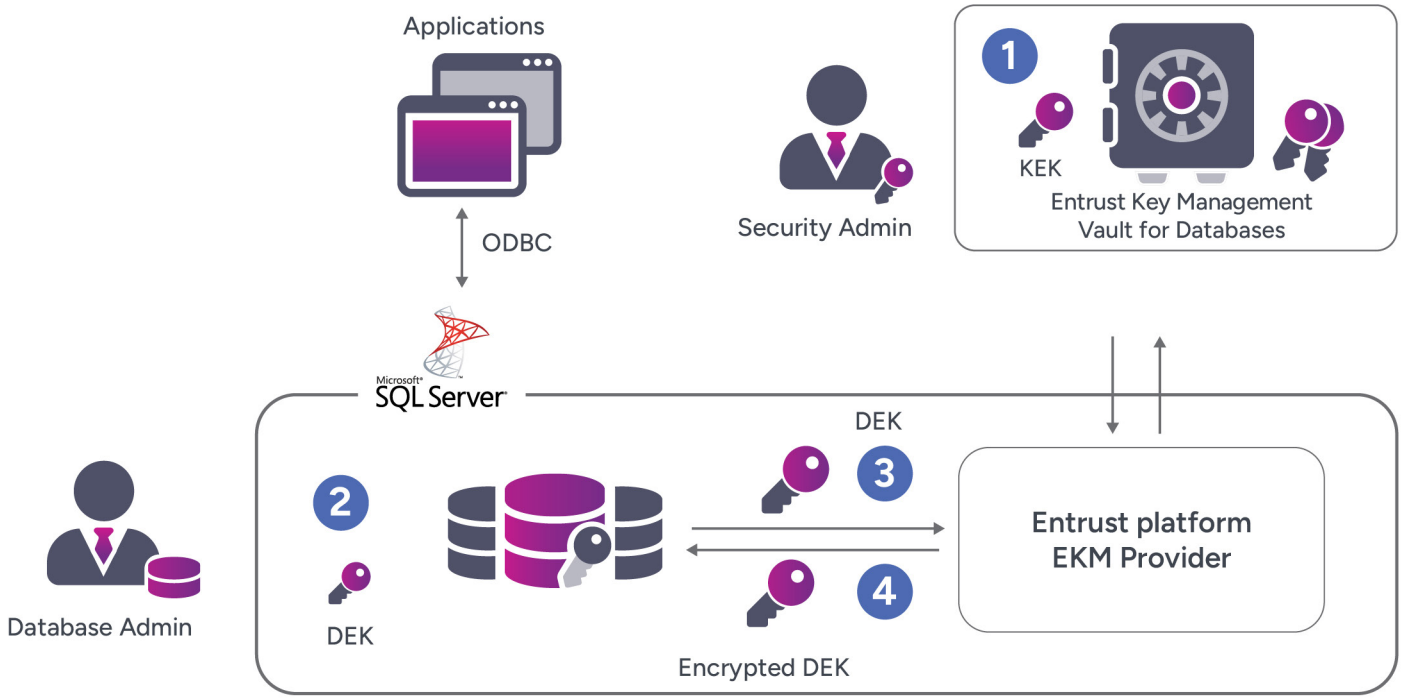
Beyond the cyber threat, an increasingly complex regulatory environment brings its own risks to businesses. Ensuring compliance with legal requirements and standards is often impractical using only database encryption management tools. Entrust Cryptographic Security Platform Compliance Manager extends the Key Management Vault for Databases cryptographic capabilities by providing an automatic approach to help support compliance with PCI DSS, HIPAA, GDPR, and other standards.

Wherever you operate and whatever the regulation, the platform Compliance Manager can help you achieve and maintain compliance, improving your security and managing your risk.

How It Works

Microsoft SQL Server databases implement a provider interface for encryption and key management. The “Extensible Key Management” provider interface, or “EKM provider” complements the encryption capabilities of the database server architecture, allowing an external key management system.

The platform Key Management Vault for Databases centrally manages and enforces access control to TDE keys. It requires the Entrust platform EKM Provider software to be installed on the Microsoft SQL server.



ENTRUST
SECURING A WORLD IN MOTION

From a high-level point of view, two types of keys are generated for encrypting the database files. The two key types are created as follows:

1. The security administrator generates a new asymmetric key encryption key (KEK), which will reside in the Key Management Vault for Databases, outside of the Microsoft SQL database. This key will be used to encrypt a second key, called the database encryption key (DEK).
   Note: RSA 2048 bit key length or higher is the recommended algorithm for the KEK.

2. The database administrator generates the symmetric DEK to encrypt the data. TDE is then enabled on the database to activate the encryption of the database files and log files.

3. The database engine requests the encryption of the DEK with the previously generated KEK to the Key Management Vault for Databases through the EKM Provider.

4. The database engine receives the encrypted DEK and stores it in the master database.

Technical Specifications

Supported Databases

- Microsoft SQL Server Version (Enterprise Edition) 2016 SP2
- Microsoft SQL Server Version (Enterprise Edition) 2016 SP3
- Microsoft SQL Server Version 2019
- Microsoft SQL Server Version 2022

Supported Cryptographic Algorithms

- Asymmetric, including RSA 2048-, 3072-, and 4096-bit key lengths
- Symmetric, including AES 128-, 192-, and 256-bit key lengths

Management and Monitoring:

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

Supported Hypervisors for the Key Management Vault

- VMware ESXi 7.0 (HW version 17) and above
- Red Hat KVM 7.8 and above
- AWS, Azure, and GCP (latest Entrust version available in the marketplace)

Deployment Media

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

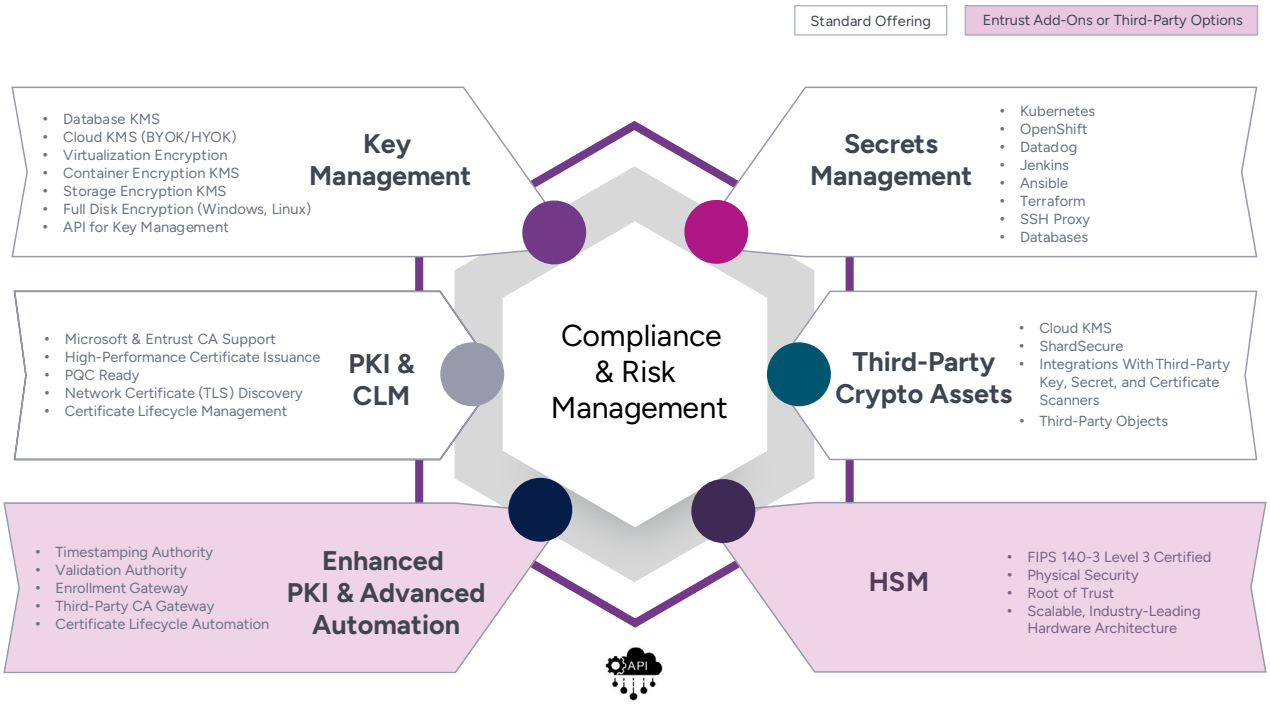
Certifications

- FIPS 140-3 Level 3 compliance via Entrust nShield HSM on premises or as a service

Entrust Cryptographic Security Platform

The Entrust Cryptographic Security Platform provides a comprehensive solution for discovering and managing the lifecycles of certificates, cryptographic keys, secrets, tokens, libraries, protocols, and configurations.

By centralizing cryptographic asset management, it enhances security, helps ensure compliance, and streamlines operations, enabling seamless integration across both on-premises and cloud environments.



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

ENTRUST
SECURING A WORLD IN MOTION