DATA SHEET

Entrust Cryptographic Security Platform Key Management Vault for TDE Databases - MariaDB

Securing MariaDB TDE Encryption Keys

Overview

Databases, as central repositories of valuable information, pose a substantial security risk. In numerous security breaches, attackers primarily target databases to extract a vast amount of sensitive data.

Therefore, encrypting databases is crucial for protecting sensitive information such as personal data and financial records. It also helps ensure compliance with legal and regulatory standards like the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). Additionally, encryption significantly mitigates the risks and potential impacts associated with data breaches, making it a fundamental aspect of data security strategies.

Like most modern database vendors, MariaDB provides a built-in encryption capability known by the acronym TDE (Transparent Data Encryption), which enables encryption of the database files. Once encrypted, the data is transparently decrypted for authorized users or applications that need to access the database.

Managing the keys for encrypted databases is not a trivial task. To ensure strong data security, keys must be rotated frequently, and transported and stored securely.

Key Features

- Supports InnoDB storage engine
- On-demand and automatic key rotation
- Deployed as a virtual appliance
- High Availability (HA) support with active-active cluster
- Easy setup and integration
- Support separation of duties, least privilege, and multi-tenancy
- (Optional) FIPS 140-2 Level 3 Hardware key protection
- (Optional) Automated compliance engine for NIST 800-57, NIST 800- 130, and other standards

ENTRUST
SECURING A WORLD IN MOTION

Furthermore, along with the high demand for strong data security, there is an ever-increasing business need to meet regulatory requirements such as the Payment Card Industry Data Security Standard (PCI DSS) or HIPAA. The combination of TDE and external encryption key management contributes to the principle of "Separation of Duties" as required by PCI DSS and other compliance regulations.

With Entrust Cryptographic Security Platform Key Management Vault for Databases, you can easily manage encryption keys at scale. The vault simplifies the task of securing your data in MariaDB databases by automating the lifecycle of encryption keys; including key storage, backup, distribution, rotation, and revocation.

Benefits

Safeguard your Database With the Highest Level of Assurance

MariaDB TDE prevents operating system administrators from directly accessing sensitive database information by reading the contents of database files, but as with any encryption solution, a crucial element of overall system security is that the keys that encrypt the data are adequately safeguarded.

The Entrust Cryptographic Security Platform Key Management Vault for Databases secures encryption keys by storing the keys separately from the data on a secure platform. Moreover, the Cryptographic Security Platform enforces your internal security policy by requiring role-based authorization and separating security and database administration, making it easier to demonstrate compliance to auditors.

Simplify Key Lifecycle Management at Scale

While database vendors offer key management, this functionality only works with the vendor's specific databases. Key management becomes more complex with the growing number of databases and the diversification of database vendors.

Administrators are faced with the complex and costly task of managing disparate encryption keys for many different databases provided by multiple vendors.

The Entrust platform Key Management Vault for Databases provides a unified key management solution for all databases across on-premises and cloud environments, enabling you to streamline key management processes such as automating key rotation, thus reducing the risk of errors and fraud.

Facilitate Compliance With Regulatory Requirements Using Our Cryptographic Security Platform Compliance Manager and HSMs

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. The Entrust Cryptographic Security Platform Compliance Manager extends the Vault's key management capabilities by providing an automatic approach to supporting compliance with standards such as NIST 800-57. Furthermore, Entrust platform offers high assurance safeguarding of encryption keys with a FIPS 140 Level 3 nShield HSM, making compliance with regulations such as PCI DSS and HIPAA easier.

Wherever you operate and whatever the regulations you are required to meet, the Entrust platform can help you achieve and maintain compliance, improving your security and managing your risk.

How It Works

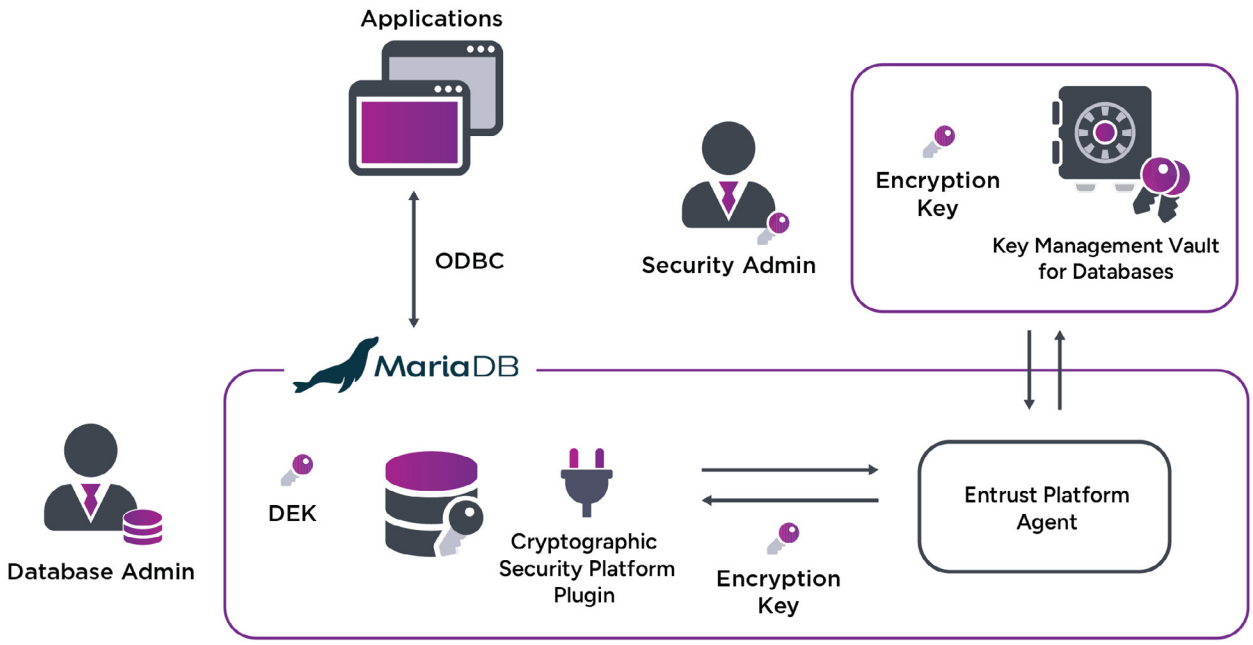
MariaDB's TDE requires the use of a key management and encryption plugin. This plugin is used both for the management of encryption keys and for the actual encryption and decryption of data.

The Entrust platform provides a plugin for MariaDB that communicates with the key management vault to access encryption keys for data-at-rest encryption.

The solution supports multiple encryption keys and logs all key-related activities for audit trails.

Initially, an encryption key is generated in the Key Management Vault for Databases. When MariaDB starts, the platform plugin retrieves this encryption key from the vault.

Every time MariaDB restarts, the plugin fetches this encryption key again and stores it in memory while the MariaDB server is running. This in-memory encryption key is then used for encrypting and decrypting database data.



ENTRUST
SECURING A WORLD IN MOTION

Technical Specifications

Supported Databases:

- MariaDB version 10.1 and subsequent releases above

Supported Storage Engines:

- InnoDB

Platforms Supported:

- Private cloud platforms: vSphere, VCE, VxRail, Nutanix, vCloud Air (OVH)
- Public cloud platforms: AWS, IBM Cloud, Microsoft Azure, VMware Cloud (VMC) on AWS, Google Cloud Platform (GCP)
- Hypervisor support: ESXi, KVM, Hyper-V, AHV

Deployment Media:

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

Supported Cryptographic Algorithms:

- AES 256-bit key lengths

Management and Monitoring:

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

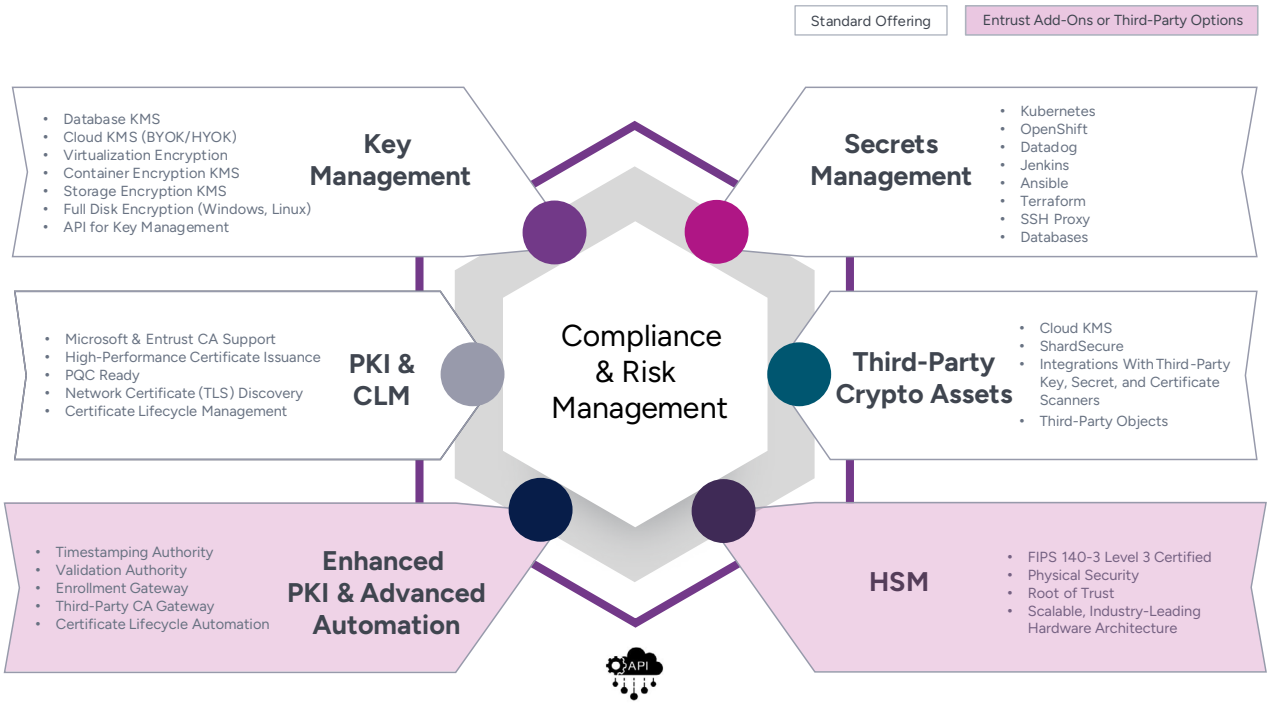
Certifications:

- FIPS 140 Level 3 or eIDAS CC EAL4+ 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