DATA SHEET

Entrust KeyControl Vault for Databases

Secure your data with Oracle Database TDE Encryption Keys

Overview

During security breaches, the main goal of the attackers is to steal large volumes of information by gaining access to seemingly protected databases. An in-depth defense is required to protect the network, secure database access control, and encrypt the data stored in the table.

Oracle database solutions provide a native encryption capability known as transparent data encryption (TDE), which enables encryption for entire databases and log files. TDE encrypts entire database backups and data pump exports, integrating with Oracle Recovery Manager (RMAN) and Data Pump Export/Import.

To ensure strong data security, keys must be rotated frequently and stored securely to meet compliance requirements such as the Payment Card Industry Data Security Standard (PCI DSS). The combination of TDE and external encryption key management contributes to the "separation of duties" requirement of PCI DSS and other compliance standards.

With Entrust KeyControl Vault for Databases, businesses can easily manage encryption keys at scale. The vault simplifies the encryption of Oracle databases by automating the lifecycle of encryption keys; including key storage, backup, distribution, rotation, and key revocation.

Key Features

- Supports both tablespace and column-level encryption
- Supports auto-login wallets
- Supports Oracle Real Application Clusters (Oracle RAC)
- On-demand key rotation
- Deployed as a virtual appliance
- High-availability (HA) support with active-active cluster
- Easy setup and integration
- Supports separation of duties, least privilege, and multi-tenancy
- (Optional) FIPS 140-3 Level 3 Hardware key protection
- (Optional) Automated compliance engine for NIST 800-130 and other standards

ENTRUST

SECURING A WORLD IN MOTION

BENEFITS

Safeguard your database with the highest level of assurance

Oracle 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 KeyControl Vault for Databases secures encryption keys by storing the keys separately from the data on a secure platform.

Moreover, KeyControl 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.

Entrust KeyControl can automate key rotation, further simplifying the management of keys. Having one unified key management solution for all databases across on-premises and cloud environments enables you to streamline key management processes and reduce the risk of errors and fraud.

Facilitates compliance with regulatory requirements using KeyControl Compliance Manager and HSM

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 KeyControl Compliance Manager extends the vault key management capabilities by providing an automatic approach to help support compliance with standards such as NIST 800-57. Furthermore, Entrust KeyControl offers high assurance safeguarding of encryption keys with a FIPS 140-3 Level 3 nShield HSM, making compliance with standards and regulations such as PCI DSS and the Health Insurance Portability and Accountability Act (HIPAA) easier. Wherever you operate and whatever the regulation, KeyControl can help you achieve and maintain compliance, improving your security and managing your risk.

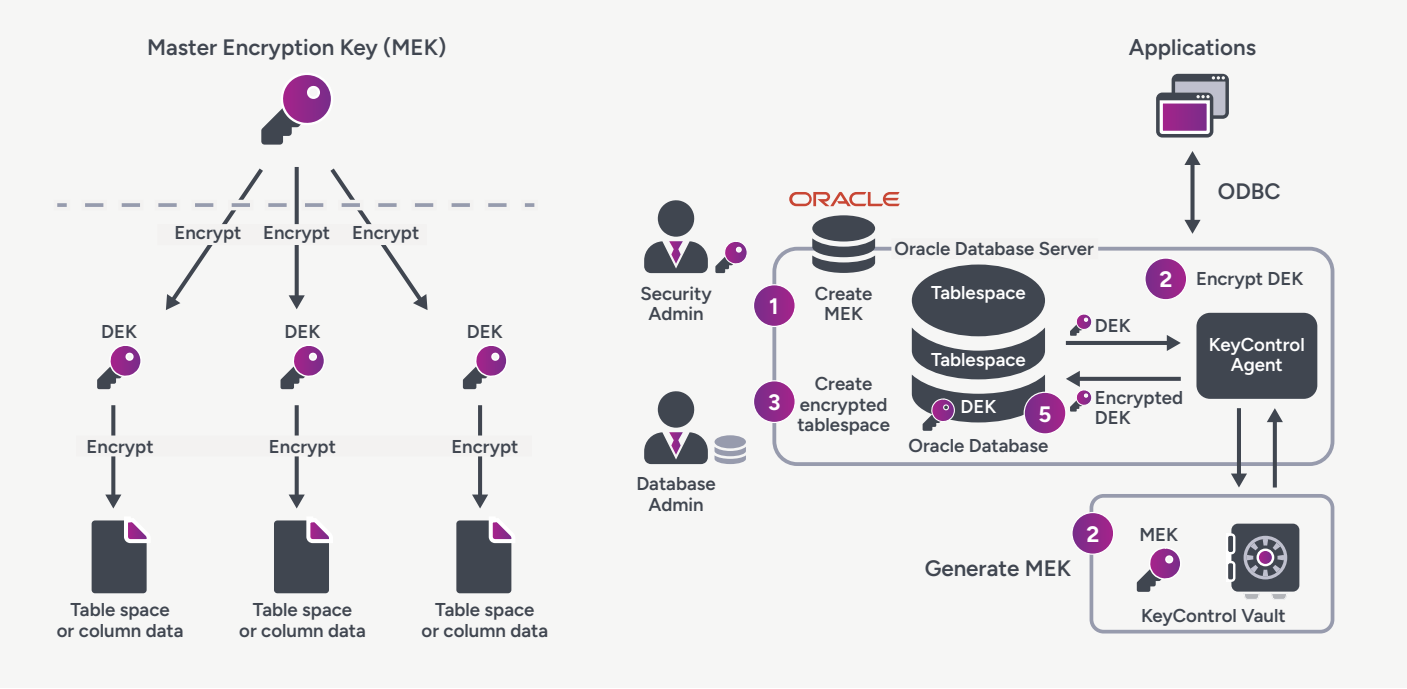
How does it work?

Oracle TDE enables the encryption at the column level or the tablespace level. Oracle implements a two-tier key architecture with:

- A single master encryption key (MEK) stored in the KeyControl Vault for Databases
- Multiple data encryption keys (DEKs) stored within the Oracle database

The separation between the MEK and the DEKs increases the level of security and facilitates the rotation of the master key.

The MEK encrypts the database-generated DEKs, which encrypt columns or tablespace data. These MEKs are centrally managed in the KeyControl Vault, which enforces access control to the keys.



From a high-level point of view, tablespace encryption is carried out in the following manner:

1. The security administrator enables TDE with external key management by modifying the Oracle Database Server Configuration. Once TDE is enabled, the administrator runs a command to generate a TDE MEK.
2. The database engine requests the generation of a MEK from the KeyControl vault. This key is used to encrypt the DEK and resides in the vault, outside of the Oracle database.
3. A database administrator creates an encrypted tablespace in the database. The database engine generates a symmetric DEK to encrypt the tablespace.
4. The database engine requests the encryption of the DEK with the previously generated MEK, located in the KeyControl Vault.
5. The database engine receives the encrypted DEK and stores it in the database.

When the MEK is rotated, there is no need to re-encrypt all data. Only DEKs are re-encrypted by the MEK.

Technical Specifications

Supported databases

- Oracle 11g R2, Oracle 12c, Oracle 18c, Oracle 19c

Supported cryptographic algorithms

- 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

Platforms supported

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

Deployment media

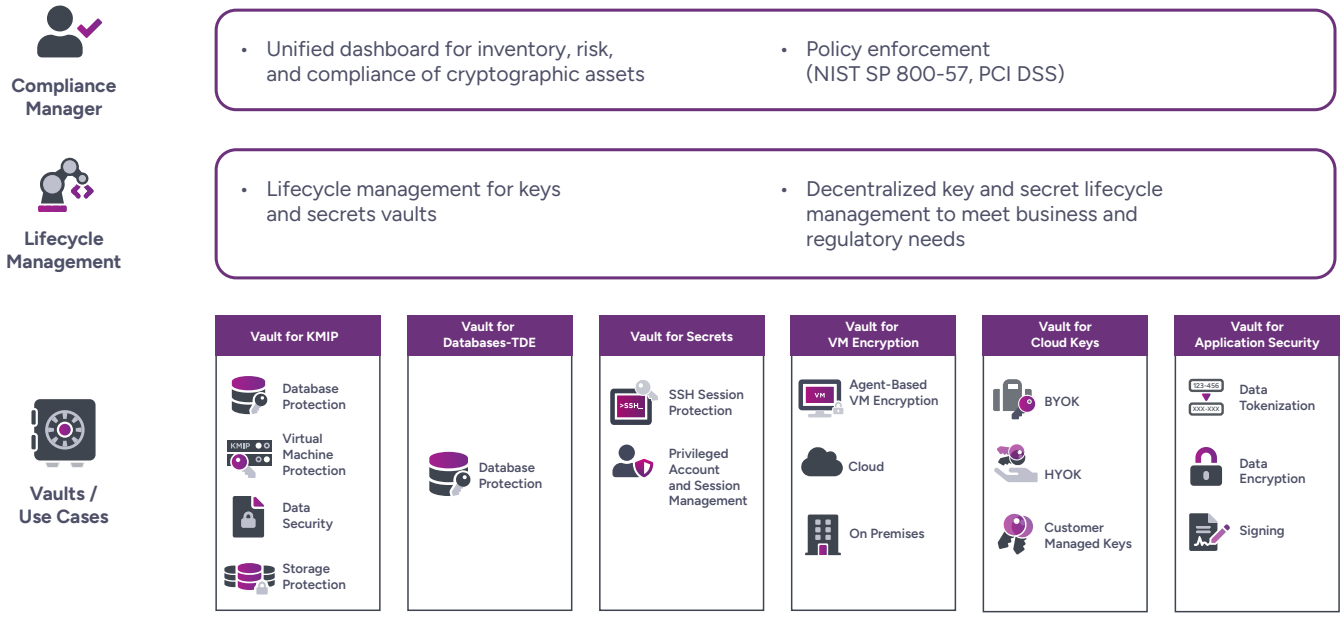
- ISO, OVA (Open Virtual Appliance), AMI (Amazon Web Services Marketplace), or VHD (Microsoft Azure Marketplace)

Certifications

- FIPS 140-2 Level 3 or eIDAS CC EAL4+ compliance via Entrust nShield HSM on premises or as a service

Entrust KeyControl Platform

Entrust KeyControl Vault for Databases is part of a suite of products designed to manage key lifecycles at scale for encrypted workloads in virtualized environments across on-premises, multi-cloud, and hybrid deployments.



For more details on the KeyControl platform, KeyControl Compliance Manager, and the range of vaults, download the Entrust KeyControl Solution Brochure.

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

ENTRUST
SECURING A WORLD IN MOTION