THALES

Encryption key management solutions for Microsoft® SQL Server® and Oracle® Database

Simplified and protected management for database encryption keys

- Streamlined operations through centralized key management
- Stronger security by separating keys from databases
- Comprehensive key security based on FIPS 140-2 compliant hardware and software solutions

Microsoft SQL and Oracle Database key management challenges

Microsoft SQL Server and Oracle Database solutions provide native transparent database encryption (TDE) that protects the data stored in their customers' enterprise and cloud-hosted databases. And, as with any encryption-based security scheme, securing and managing the encryption keys is critically important for robust data security.

Managing encryption keys presents challenges such as isolating them from the assets they protect and storing them securely—not only a best practice for key management, but a common industry data protection mandate. Encryption key management challenges multiply as organizations use multiple databases for different purposes, each requiring dedicated key management to ensure that keys are securely stored, backed up and available when needed.

## Thales key management solutions for transparent database encryption

Thales key management solutions centralize key management for your enterprise and cloud-hosted Microsoft SQL Server and Oracle Database, giving you greater command over the keys while increasing your data security.

CipherTrust key management using the CipherTrust Manager

The CipherTrust Manager centrally manages keys for Microsoft SQL and Oracle TDE keys and Thales Data Protection portfolio.

Microsoft SQL Transparent Data Encryption
Thales key management solutions complement Microsoft native TDE by providing secure storage and management of the keys used in Microsoft's database encryption scheme. Microsoft TDE encrypts the sensitive data in the SQL database using a database encryption key (DEK), and Thales interfaces with Microsoft Extensible Key Management (EKM) to store and manage the DEKs in the FIPS 140-2 compliant CipherTrust Manager.

Microsoft SQL Server TDE — Database Encryption Keys (DEKs)

Microsoft Extensible Key Management (EKM)

CipherTrust Manager
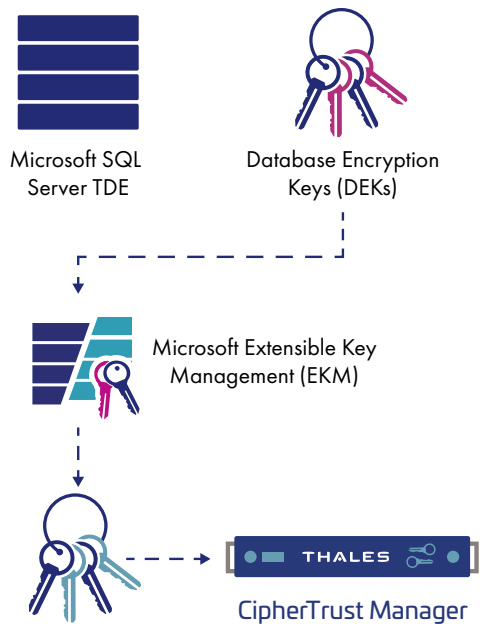
Oracle Database Transparent Data Encryption

The CipherTrust Manager complements Oracle Database native TDE by centrally storing and managing Oracle Database encryption keys. As a part of the Oracle Advanced Security TDE two-tier key architecture, Oracle Database uses master encryption key (MEKs) to encrypt the database encryption keys (DEKs), which are used to encrypt columns and tablespaces within the databases. Thales key management solutions interface with the Oracle Wallet to protect and manage these MEKs within a secure FIPS-certified boundary.

Oracle Database TDE — Master Encryption Keys (MEKs)

Oracle Wallet

CipherTrust Manager
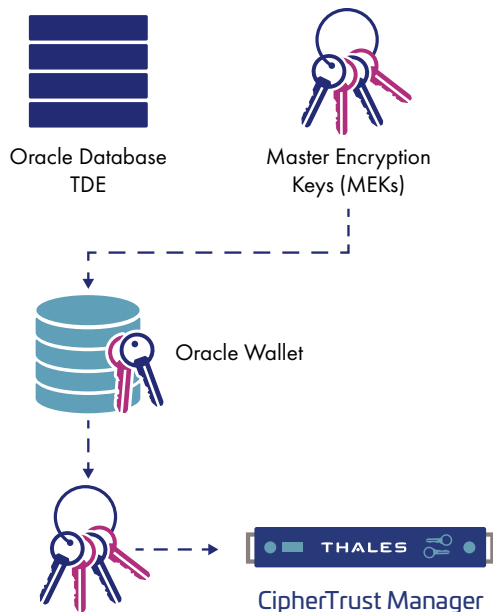
Enterprise and Cloud Support

Whether your database resides on-premises or in the cloud, Thales solutions provide secure and efficient management of your database encryption keys.

CipherTrust Manager: the foundation for Thales key management solutions

The CipherTrust Manager is a high-availability appliance that centralizes encryption key management for Oracle Database and Microsoft SQL Server TDE as well as a variety of additional Thales and third-party encryption solutions. CipherTrust Manager helps direct key life-cycle tasks including generation, rotation, destruction, import and export as well as provide abilities to manage certificates and secrets.

The CipherTrust Manager is available as either hardware or a virtual appliance.Either appliance is hardened to ensure protection of its contents and prevents any modification to the underlying operating system. In addition, non-HSM enabled appliances can utilize an external HSM as a root of trust for better security as well as utilize its random number generator for better key entropy.

CipherTrust key management solutions

Centrally managing your keys independently from your database applications will help you streamline operations, fulfill compliance mandates and better protect your sensitive data. And as your needs expand, Thales solutions can grow with you. Below is a summary of key management offerings and related products.

- TDE key management
- Database encryption, file encryption, comprehensive data encryption
- KMIP-compliant applications
- Tokenization
- Cloud key management (CipherTrust Cloud Key Manager)
- Key management through APIs
- Key storage

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled. For more information, visit www.thalestct. com