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-certified hardware and software solutions

Thales eSecurity

Encryption Key Management Solutions
for Microsoft® SQL Server® and Oracle® Database

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.
Thales offers two complementary solutions to support your TDE applications:

- Vormetric™ Key Management in concert with the Vormetric Data Security Manager (DSM)
- Key management using nShield™ Hardware Security Modules (HSMs)

Both options offer the opportunity to expand your solutions to a wide set of applications; the option you choose to manage your TDE keys will depend largely on other functions you want to support with your Thales eSecurity solution. For example, if you also plan to support a public key infrastructure (PKI) or need an environment for secure code execution, you will likely choose an nShield solution, while if your requirements include more comprehensive encryption such as database or files, Vormetric products will be the more suitable choice. More information can be found in the section below, Vormetric DSM and nShield HSM Key Management Solutions. Also, your Thales representative or certified channel partner can help you decide between Vormetric and nShield-based TDE key management solutions.

**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-certified Vormetric DSM or nShield HSM.

**Oracle Database Transparent Data Encryption**

The Vormetric DSM and nShield HSMs complement 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.

**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.
Vormetric DSM and nShield HSM Key Management Solutions

Whichever Thales key management solution suits your needs, 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 from Thales eSecurity.

<table>
<thead>
<tr>
<th>Key Management Solution</th>
<th>Vormetric DSM</th>
<th>nShield HSM</th>
</tr>
</thead>
<tbody>
<tr>
<td>TDE key management</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Database encryption, file encryption,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>comprehensive data encryption</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>KMIP-compliant applications</td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>Tokenization</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>PKI support</td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>Digital signing, code signing</td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>Secure code execution inside FIPS boundary</td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>(CodeSafe)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud key management (CipherTrust</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Cloud Key Manager)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>nShield Bring Your Own Key (BYOK)</td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>Key management through APIs</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Key storage</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>

LEARN MORE

Visit us at [www.thalesesecurity.com](http://www.thalesesecurity.com) to learn more about how Thales eSecurity can help you simplify and strengthen key management for your enterprise database encryption solution.

Vormetric Data Security Manager

The Vormetric Data Security Manager (DSM) 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 Vormetric and third-party encryption solutions. The DSM manages key life-cycle tasks including generation, back-ups, destruction, import and export.

The Vormetric DSM is available as either hardware or a virtual appliance:

- The V6000 DSM hardware appliance, certified to FIPS 140-2 Level 2, and the V6100 DSM hardware appliance, underpinned by nShield HSM certified to FIPS 140-2 Level 3
- The vDSM, a virtual appliance certified to FIPS 140-2 Level 1

nShield General Purpose Hardware Security Modules (HSMs)

nShield HSMs are hardened, tamper-resistant devices that provide a secure environment for generation, protection and storage of your Oracle Database and Microsoft SQL Server TDE database encryption keys, as well as a variety of other applications.

nShield HSMs are available in three form factors:

- nShield Connect, an appliance serving multiple applications across a network
- nShield Solo, a PCIe card serving applications on a single server
- nShield Edge, a USB-attached desktop device for lower volume transactions

nShield HSMs are certified to FIPS 140-2 Level 2 and Level 3.
About Thales eSecurity

Thales eSecurity is the leader in advanced data security solutions and services that deliver trust wherever information is created, shared or stored. We ensure that the data belonging to companies and government entities is both secure and trusted in any environment – on-premises, in the cloud, in data centers or big data environments – without sacrificing business agility. Security doesn’t just reduce risk, it’s an enabler of the digital initiatives that now permeate our daily lives – digital money, e-identities, healthcare, connected cars and with the internet of things (IoT) even household devices. Thales provides everything an organization needs to protect and manage its data, identities and intellectual property and meet regulatory compliance – through encryption, advanced key management, tokenization, privileged user control and high assurance solutions. Security professionals around the globe rely on Thales to confidently accelerate their organization’s digital transformation. Thales eSecurity is part of Thales Group.