THALES

Thales Key Management Solution for Oracle Database 11g Release 2

KEY BENEFITS

What

- Centralized key management for Oracle Database 11g Release 2

How

- Thales HSMs protects Oracle TDE master encryption keys with FIPS 140-2 Level 3 and Common Criteria EAL4+ – the highest hardware-based levels of security
- Protect and manage encryption keys in hardware-based appliance
- Consolidate key management across multiple databases

Why

- Reduce the cost of compliance with network-based HSMs
- Simplify PCI compliance for key management and avoid costly fines
- Ensure the secure creation, storage, and use of keys
- Consolidate key management across multiple databases and facilitate the security auditing process
- Protect your data, brand and competitive advantage

Easier PCI DSS Compliance. Stronger Data Protection.

The Payment Card Industry Data Security Standard (PCI DSS) defines strict security requirements for the processing, storage, and transmission of cardholder data. And for good reason. Databases are a treasure trove of sensitive information – customers' personal data, confidential corporate information, and intellectual property that are the prime targets of cyber thieves or rogue employees.

How can you prevent the loss or theft of sensitive data and avoid brand damage, competitive disadvantage, and serious fines for non-compliance? Thales and Oracle have partnered to deliver the next-generation of integrated, highly secure database encryption and key management – Thales nShield hardware security modules (HSMs) integrated with Oracle Database 11g Release 2 Transparent Data Encryption (TDE).

Transparent Data Encryption, part of the Advanced Security option to the Oracle Enterprise Edition, enables you to efficiently and securely encrypt all types of sensitive data. With TDE, compatibility is ensured without affecting the performance of existing applications. Most importantly, Oracle Database 11g

>> Thales Key Management Solution for Oracle Database 11g Release 2

Release 2 supports HSMs – which provides a significantly higher level of security than software-based key management – as an industry best practice for key management.

Reduce the risk to data at rest

Thales and Oracle understand that data at rest is data at risk. That's why we've partnered to take TDE database encryption to a new level of security and performance with HSMs that provide centralized key management. Why? Because this best practice can help you:

- Reduce operational costs by consolidating key management across multiple databases.
- Ensure the secure creation, storage and use of keys.
- Simplify key management while providing the highest level of security.
- Reduce the effort to ensure compliance and avoid costly fines.
- Deliver a higher level of security – that only hardware can provide – FIPS 140-2 Level 3 and Common Criteria EAL4+.

Data encryption is only as strong as your encryption key management process. That's why it makes sense to strengthen and simplify key management with the Thales integrated HSM solution – a proven secure and compliant way to protect your Oracle 11g Release 2 databases.

Protect your data. Simplify key management.

Superior key management for superior data protection – Thales HSMs are validated to the highest security standards, including FIPS 140-2 Level 3 and Common Criteria EAL4+. Approved for high-security environments in the public and private sectors, our HSMs protect root keys from exposure so your Oracle 11g Release 2 databases are protected in even the most challenging and demanding security situations.

Efficient key management and key administration – Thales HSMs store Oracle's TDE master encryption keys in a highly secure environment. Smart card authentication firmly controls key access. To enforce your security policy, our centralized key management approach lets you split important tasks and procedures across multiple security operators, and separate them from database administrators.

Simplify key management across multiple databases – Thales HSMs support centralized key management for all of your Oracle 11g Release 2 databases, thus reducing the time, effort, and cost of enterprise-wide key management and facilitating the security auditing process. Meet PCI compliance requirements more easily and efficiently since keys are stored in as few places as possible.

Recover keys with Thales exclusive disaster recovery – Only Thales provides a simple and secure process for archiving and recovering keys that features automatic failover and load balancing of Thales HSMs.

Easy setup and integration – Using standards-based interfaces, Thales HSMs integrate seamlessly with Oracle Database 11g Release 2 Advance Security. We ensure a quick deployment because all HSMs are fully tested and supported by Thales and Oracle.

Scale to meet your changing needs – Thales HSMs integrate out of the box with leading enterprise applications, including identity services and public key infrastructures (PKIs). Network-attached HSMs can be shared by several servers, including support for virtualized environments. You can add HSMs easily as your traffic needs expand, and hardware acceleration ensures performance without bottlenecks.

For more Information

For more information, visit **www.thalesesec.com/oracle** or contact **oracle@thalesesec.com**.

THALES

Americas: 2200 North Commerce Parkway, Suite 200 • Weston • Florida 33326 • Tel: +1 888 744 4976 or +1 954 888 6200 • Fax: +1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific: Units 2205-06, 22/F Vicwood Plaza, 199 Des Voeux Road Central • Hong Kong, PRC • Tel: +852 2815 8633 • Fax: +852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa: Meadow View House, Long Crendon, Aylesbury • Buckinghamshire • HP18 9EQ • Tel: +44 (0)1844 201800 Fax: +44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com