Secure sensitive database data and address compliance requirements using Oracle TDE and Thales’ Luna HSM

Organizations use Oracle databases to store their most valuable data. With data breaches becoming more common, organizations are investing in security to protect their reputation and their bottom line. Oracle’s native encryption functionality – also known as transparent database encryption (TDE) – is a fundamental tool for protecting such sensitive data. Oracle TDE’s tablespace encryption keeps data safe and has very little impact on applications accessing encrypted data. Yet TDE alone is an incomplete protection strategy as it locally stores database encryption keys for management. This is especially problematic when regulatory compliance is a consideration, because TDE keys stored locally, in software, on the same server as the database, is a violation of best security practice and many compliance frameworks.

Fortunately, Thales solves this problem for Oracle TDE customers with its Luna HSM platform by storing high value keys in a high assurance hardware root of trust.

Separating encryption keys from the data they are protecting is a best practice and the foundation of an effective security strategy. Organizations that choose Oracle TDE can secure those keys with Luna HSM – a purpose-built hardware appliance – so that the encrypted database cannot be accessed without appropriate authentication. The additional barriers of separated key storage and authorization controls both secure data and deter would-be attackers.

Luna Hardware Security Modules (HSM)

Luna HSMs are purpose built hardware appliances that secure cryptographic materials in a trusted manner. Luna HSMs protect the entire encryption key lifecycle within the tamper-resistant, FIPS 140-2 Level 3 validated confines of the appliance. Thales’ unique approach to protecting cryptographic keys in hardware makes these appliances the most trusted general purpose HSMs on the market, and ensures that encryption keys always benefit from both physical and logical protections.
Oracle TDE/ Luna HSM Benefits

High-Assurance Root Key Protection
All encryption and decryption, digital signing and verification operations are performed within the tamper-proof, FIPS 140-2-validated Luna HSM to deliver the highest levels of performance, availability and security to ensure business processes and systems are running efficiently.

Ease of Management & Integration
Storing master encryption keys in Luna HSMs adds centralized, network-based physical storage of master encryption keys used by Oracle TDE, never letting them leave the secure confines of the HSM. The TDE master encryption key is part of a two-tiered key architecture that protects the encryption keys used to encrypt the data. The TDE master key can be stored with minimal security, in software only in an Oracle Wallet (a PKCS#12 formatted file), or in a highly secure and auditable format in the Luna HSM. This two-tiered key architecture allows for easy re-keying and high performance. As a centralized, hardened device, Luna HSMs are also ideal for securely storing a backup private key copy.

Persistent Data Protection
With Oracle TDE and Luna HSM, customers ensure encrypted database data stays safe throughout its lifecycle, wherever it is backed-up, transferred or copied. With access controls, authorized users and processes still have appropriate levels of access to the secured data they need for their responsibilities when they need it. Protection for the data’s full lifecycle improves overall security and facilitates collaboration by eliminating vulnerabilities outside the database.

Ensure Compliance
Oracle databases’ ability to store large quantities of sensitive data make it a central compliance issue for many customers as regulatory compliance is an important concern. Requirements such as Payment Card Industry Data Security Standard (PCI-DSS), Health Insurance Portability and Accountability Act (HIPAA), electronic IDentification, Authentication and Trust Services (eIDAS), and General Data Protection Regulation (GDPR), state that keys should be secured in separate hardware devices such as the Luna HSM.

Oracle TDE secures data per compliance requirements while Luna HSM as a root of trust, allows administrators to demonstrate control over their data to regulators to aid compliance efforts. With Luna HSM, organizations can also effectively address their internal policies and relevant regulatory mandates, and provide a verifiable audit trail, proving that keys have been properly secured throughout their entire life cycle.

Highlights

Transparent and Efficient Encryption
- Transparently encrypt sensitive database data
- No need to make application changes

Achieve Compliance
- Meet compliance and audit mandates that require encryption of data and separation of duties

Risk Mitigation with Maximum Key Security
- Tamper-proof hardware options supporting a hardware root of trust with Luna HSM

Security Certifications
- FIPS 140-2 Level 3 – Password and Multi-Factor (PED)
- eIDAS CC EAL4+ (AVA_VAN.5 and ALC_FLR.2) against the Protection Profile 419221-5 *

Separation of Duties
- Multiple roles for strong separation of duties
- Multi-person MolN with multi-factor authentication for increased security

Hardware Key Storage
- Master keys never leave the confines of the hardware appliance for robust, persistent security

About Thales
The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.