cpl.thalesgroup.com

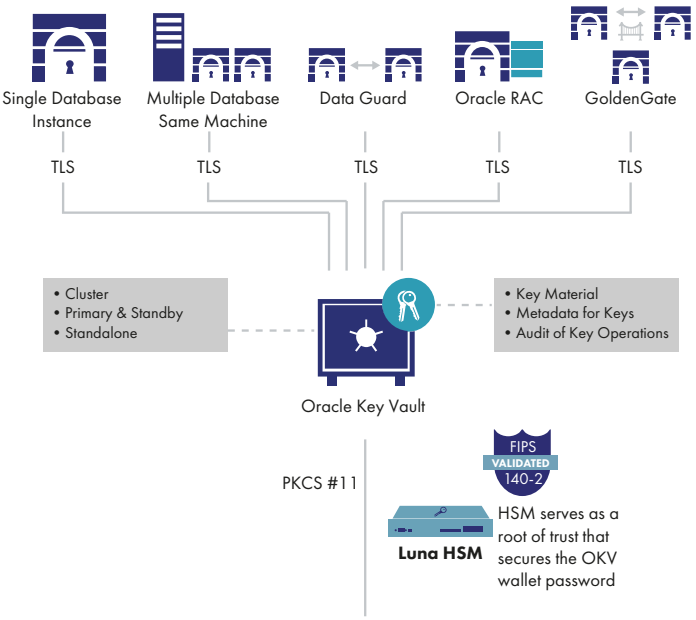
THALES

Securing Oracle Key Vault Keys in Thales Luna Network HSMs

When customers opt for Oracle's Transparent Data Encryption (TDE) to secure their databases and address their compliance obligations they also have the option to use Oracle Key Vault (OKV) for the associated key management. As a purpose-built solution, OKV simplifies an organization's on-going encryption administration at the scale needed to support the large database installations across geographies that are typical of Oracle deployments. While these are important tools in protecting sensitive customer data, regulations and best practices often stipulate that organizations should store their encryption keys externally in a hardware appliance. In these scenarios, Oracle and Thales work together to integrate Thales' Luna Network Hardware Security Module (HSM) with Oracle Key Vault for secure encryption key storage.

Oracle Key Vault integrates with Luna Network HSMs to provide additional security for keys, certificates, and other Oracle security artifacts. Luna HSMs serve as a root of trust that protects the wallet password which, in turn, protects the Oracle TDE master key securing all of the encryption keys, certificates, and security artifacts managed by OKV. Thales HSMs mitigate the risk of administrators extracting keys, credentials and sensitive data using their privileges and system access.

Oracle Key Vault with Luna HSM



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

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 *

* pending

Separation of Duties

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

Luna Hardware Security Modules

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 Key Vault (OKV)/ Thales Luna Networks 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.

Protect Against Stolen OKV Servers

Luna Network HSMs prevent individuals from taking keys from Oracle Key Vault servers started in unauthorized environments. Should an OKV server be physically moved from a datacenter, unauthorized users would not be able to run it without authorized access to the HSM. Without HSM authorization, unauthorized users would be prevented from accessing any encryption key located on the appliance.

Ensure Compliance

Oracle's ability to store large quantities of sensitive data make it a central compliance focus for many customers. Requirements from the Payment Card Industry Data Security Standard (PCI-DSS), Health Insurance Portability and Accountability Act (HIPAA), Electronic Identification (eID), Authentication and trust Services (eIDAS), and General Data Protection Regulation (GDPR), specifically mandate that organizations should secure encryption keys separately from software key managers in hardware devices such as the Luna HSM.

Oracle Key Vault secures data per regulation while Luna HSM, as a foundation of trust, allows administrators to demonstrate to regulators that they maintain sole control over their data. 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.

Persistent Data Protection

With OKV and Luna HSM, customers ensure TDE encrypted 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.

Thales can help

Contact us for more information on how you can meet your security, compliance and audit needs by securing your Oracle TDE master encryption key in a FIPS 140-2 Level 3 hardware root of trust, and demonstrating control over your data by restricting access, protecting against stolen servers and using persistent data protection.

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.

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us