HSM & Oracle Transparent Database Encryption

SOLUTION BRIEF

Features and Benefits:

Peace of Mind

- All encryption and decryption, digital signing and verification operations are performed within the HSM to deliver the highest levels of performance, availability and security to ensure business processes and systems are running efficiently

Ease of Management & Integration

- Centralized network appliance performs all key management functions in a secure location
- Also offers local and remote key management control for flexibility

High Assurance Protection

- Stored on hardened and FIPS 140-2 Level 3 and Common Criteria EAL 4+ certified cryptographic modules, cryptographic keys never leave the confines of the HSM.
- Prevention of database and key theft which is easy to do without hardware
- Auditing of cryptographic keys and tracking changes
- Separation of duties between DBA and System Administrator

Cryptographic Offload

- Secure computational storage
- Storage of SSL Cert keys in the HSM
- Eliminate key limit size constraints

ORACLE PARTNERNETWORK

SafeNet hardware security modules (HSMs) combine the strongest cryptographic security with the highest performance, reliability and ease of integration for rapid and affordable application protection using Oracle Advanced Security with Oracle Database 11g.

Overview

Oracle Advanced Security, an option to Oracle Database 11g helps address privacy and regulatory requirements including the Payment Card Industry Data Security Standard (PCI-DSS), Health Insurance Portability and Accountability Act (HIPAA), and numerous breach notification laws. Oracle Advanced Security provides data encryption and strong authentication services to the Oracle database, safeguarding sensitive data against unauthorized access to the network, operating system or through theft of hardware or backup media. Oracle Advanced Security benefits include:

- No application changes
- Built-in key management
- High performance

The secure storage of master encryption keys is the foundation of any robust security solution. Integration of SafeNet Luna SA hardware security modules (HSMs) with Oracle Advanced Security transparent data encryption (TDE) allows for the Oracle master encryption keys to be stored in the HSM, offering greater database security and centralized key management for Oracle Advanced Security with Oracle Database 11g. The master encryption key never leaves the secure confines of the HSM.

Centralized, Network Storage of Keys with HSMs

Oracle Advanced Security provides built-in key management, eliminating the complex issues associated with traditional encryption solutions. Optionally storing master encryption keys in SafeNet Luna SA HSM adds centralized, network-based physical storage of master encryption keys used by Oracle TDE.

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 SafeNet Luna SA HSM. This two-tiered key architecture allows for easy re-keying and high performance.

As a centralized, hardened device, HSMs are ideal for securely storing a backup private key copy. The high assurance Luna SA HSM also provides a verifiable audit trail, proving that keys have been properly secured throughout their entire life cycle. The Oracle and SafeNet integration solves the security issue of storing master encryption keys and security cryptographic operations such as key creation, deletion, encryption, and decryption for complying with security best practices and industry regulations.

Solution offers:

- Eliminates costs associated with:
  - Company brand damage by security breach and information leaking
  - Loss of customer loyalty and confidence
  - Fines by not complying with industry mandates
- Key lifecycle management
- Master encryption key never leaves the HSM
- Restricted access control
- Network-based physical storage of master encryption keys (high assurance)
- Storage of backup private key copy
- Verifiable audit trail
- Compliance with security best practices and industry regulations
- Secures cryptographic operations
- Transparency: No changes to applications required
  - Numbers and Text
  - Scanned documents (medical, financial, personnel records)

How the Solution Works

HSMs are dedicated systems that physically and logically secure the cryptographic keys and cryptographic processing that are at the heart of any digital signature and data protection solution. Besides physically securing the master keys used by Oracle Database 11g HSMs assure restricted access by authorized users.

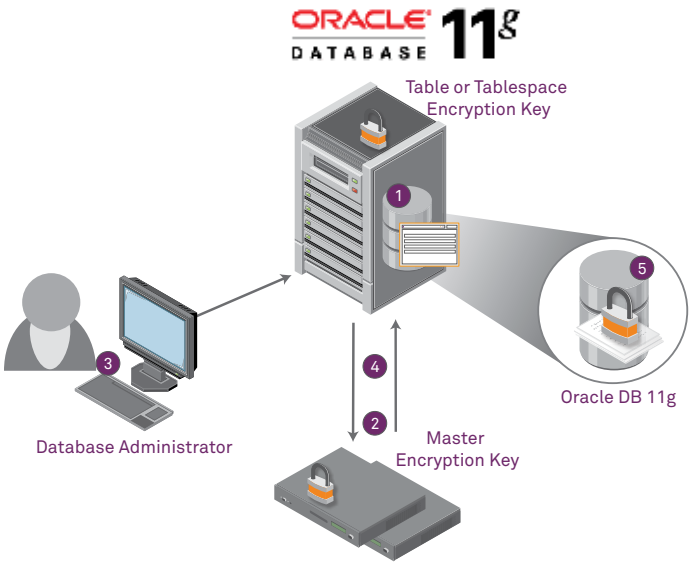
1. Sensitive data is encrypted either with Oracle Advanced Security TDE column or with tablespace encryption (no change to application required). The former encrypts application table columns containing sensitive information like credit card or social security numbers. The latter encrypts entire application tablespaces, eliminating the need to identify sensitive columns. Encrypted data remains encrypted when exported via Oracle Data Pump, or in database backups. (Unstructured data, like scanned financial documents or X-ray images (DICOM), can be stored encrypted in Oracle SecureFiles.)

2. The TDE table keys used for column encryption are stored inside the database. The TDE tablespace keys are stored in the header of the operating system file(s) that contain the tablespaces. Both are encrypted with the Oracle Advanced Security TDE master encryption key that is stored externally, either in the Oracle Wallet or the SafeNet Luna SA HSM.

3. With a single command, the Oracle database security administrator interfaces with the external security module of choice to make the master encryption key available to the Database.

4. When using the Oracle Wallet, the TDE master encryption key is loaded into database memory in order to decrypt table or tablespace keys. When using the HSM, table and tablespace keys are sent to the HSM and returned decrypted over a secure connection so they can be used to decrypt or encrypt data in the database.

5. Table & tablespace keys encrypt/decrypt data



Contact Us: For all office locations and contact information, please visit **www.safenet-inc.com**
Follow Us: www.safenet-inc.com/connected