NCIPHER

www.ncipher.com

Oracle database and nCipher nShield HSMs protect sensitive data and securely manage underpinning encryption keys

- Support multiple database instances
- Deliver tablespace and column encryption
- Offload encryption and key management
- Provide FIPS 140-2 Level 3 and Common Criteria EAL4+ high assurance security
- Comply with regulatory requirements

ORACLE®

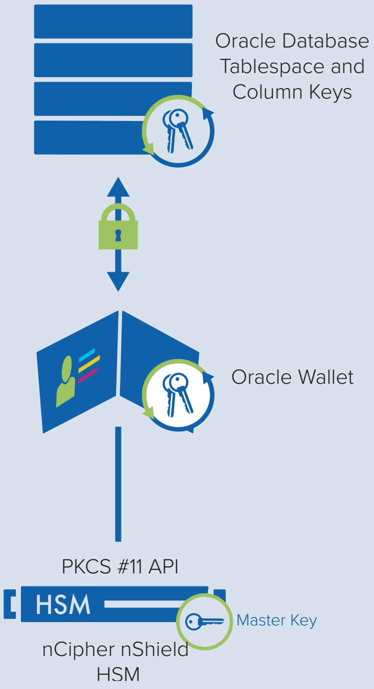
nCipher delivers enhanced security for Oracle transparent database encryption

THE PROBLEM: SENSITIVE DATA AT REST IN ENTERPRISE DATABASES IS AT RISK OF ATTACK.

Enterprise databases today contain increasing amounts of sensitive data including confidential personal information, intellectual property, and financial details that need be protected from unauthorized disclosure. The increasing incidence of data breaches brought about by advanced persistent threats puts at risk the reputational and brand image of enterprises. Data breach disclosure regulations, and potential fines and liabilities can have serious impacts on organizations. Encrypting data in enterprise databases has become a best practice, but the security of encrypted data is only as good as the protection afforded to the encryption keys.

THE CHALLENGE: PROTECTING AND MANAGING CRITICAL ENCRYPTION KEYS WITHOUT AFFECTING DATABASE PERFORMANCE.

Unauthorized access to encryption keys can compromise entire databases and the sensitive data that they hold. Protecting keys in a hardened environment, isolated from the data, the database application, and the database administrators, affords a greater level of protection from internal and external threats. This level of protection, however, must ensure that keys are always available when needed for optimum performance of the database and the applications that depend on the data it holds.



nCipher nShield hardware security modules (HSMs) safeguard and manage the Master Encryption Key (MEK) used by Oracle Database Wallet.

nCipher delivers enhanced security for Oracle transparent database encryption

THE SOLUTION: ORACLE DATABASE WITH TRANSPARENT DATABASE ENCRYPTION (TDE) AND NCIPHER NSHIELD HARDWARE SECURITY MODULES (HSMS).

Oracle Database provides organizations with access to fast, scalable, reliable, and secure database technology in a cost-effective cloud, on-premises, or hybrid environment. The database's TDE capability enables sensitive data stored in the tablespace, or in discrete columns, to be encrypted for security. Encrypted data is transparently decrypted for database users and applications with authorized access. TDE helps protect stored data in the event that the media or data files are compromised or stolen.

Combined with nCipher nShield Connect and nShield Solo HSMs, and the nCipher Security World key management architecture, the master keys used to protect the database encryption keys stored in the Oracle Wallet are given an additional layer of security. As FIPS 140-2 Level 3 and Common Criteria ELA 4+ certified devices, the nCipher nShield HSMs deliver a high grade of security assurance for the database applications and the data they process.

WHY USE NCIPHER NSHIELD HSMS WITH ORACLE DATABASE?

Encryption keys handled outside the cryptographic boundary of a certified HSM are significantly more vulnerable to attack, which can lead to compromise of critical keys. HSMs are the only proven and auditable way to secure valuable cryptographic material. nCipher nShield HSMs integrate with the Oracle Database to provide comprehensive logical and physical protection of cryptographic keys. The combination delivers a recognized auditable method for enforcing security policies. nCipher nShield HSMs enables Oracle Database customers to:

- Secure keys within a carefully designed cryptographic boundary that uses robust access control mechanisms, so keys are only used for their authorized purpose
- Ensure key availability by using sophisticated management, storage, and redundancy features to guarantee that the keys are always accessible when needed
- Deliver superior performance to support demanding applications

nCipher nShield HSMs provide a hardened, tamper-resistant environment for performing secure cryptographic processing, key protection, and key management. With nCipher HSMs:

- Provide a tightly controlled tamper resistant environment for safekeeping and managing encryption keys
- Enforce key use policies, separating security functions from administrative tasks
- Interface with applications using industry-standard APIs (PKCS#11, OpenSSL, JCE, CAPI, and CNG)

NCIPHER

Today's fast moving digital environment enhances customer satisfaction, gives competitive advantage and improves operational efficiency. It also multiplies the security risks.

nCipher Security empowers world-leading organizations by delivering trust, integrity and control to their business critical information and applications.

Our cryptographic solutions secure emerging technologies – cloud, IoT, blockchain, digital payments – and help meet new compliance mandates, using the same proven technology that global organizations depend on today to protect against threats to their sensitive data, network communications and enterprise infrastructure. We deliver trust for your business critical applications, ensuring the integrity of your data and putting you in complete control – today, tomorrow, at all times.

ORACLE

Oracle is a global provider of enterprise cloud computing. The company empowers businesses of all sizes on their journey of digital transformation. Oracle Cloud provides leading-edge capabilities in software as a service, platform as a service, infrastructure as a service, and data as a service. The purpose built Database solution:

- Enables compatible cloud and on-premises deployments
- Secures data at all layers - off-line, on-line, and in transit
- Provisions quickly to supports high-performance workloads

For more detailed technical specifications, please visit www.ncipher.com or www.oracle.com