Entrust delivers enhanced security for Oracle transparent database encryption

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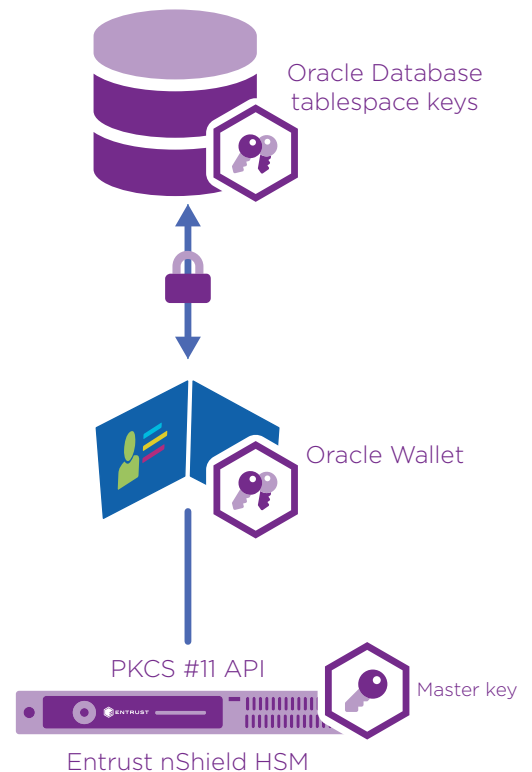
HIGHLIGHTS

- Support multiple database instances

- Deliver high availability root of trust

- Offload encryption and key management

- Provide FIPS 140-2 Level 3 and Common Criteria EAL4+ high assurance security

- Comply with regulatory requirements

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.

Oracle Database tablespace keys

Oracle Wallet

PKCS #11 API

Master key

Entrust nShield HSM

Entrust nShield hardware security modules (HSMs) safeguard and manage the master encryption key (MEK) used by Oracle Database Wallet.

LEARN MORE AT ENTRUST.COM/HSM

Enhanced security for Oracle transparent database encryption

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.

The solution: Oracle Database with transparent database encryption (TDE) and Entrust nShield 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 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 Entrust nShield Connect and nShield Solo HSMs, and the Entrust 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 Entrust nShield HSMs deliver a high grade of security assurance for the database applications and the data they process.

Why use Entrust 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. Entrust 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. Entrust 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

Enhanced security for Oracle transparent database encryption

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

Entrust HSMs

Entrust nShield HSMs are among the highest-performing, most secure and easy-to-integrate HSM solutions available, facilitating regulatory compliance and delivering the highest levels of data and application security for enterprise, financial and government organizations.

Our unique Security World key management architecture provides strong, granular controls over access and usage of keys.

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

www.oracle.com

Learn more

To find out more about Entrust nShield HSMs visit **entrust.com/HSM**. To learn more about Entrust's digital security solutions for identities, access, communications and data visit **entrust.com**

To find out more about Entrust nShield HSMs

HSMinfo@entrust.com

entrust.com/HSM

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com/HSM

ENTRUST

Contact us:
HSMinfo@entrust.com