THE KEY TO ENCRYPTION IS HOW YOU MANAGE IT™

nCipher Database Encryption Solution for Oracle 11g

Stop data breaches with integrated encryption

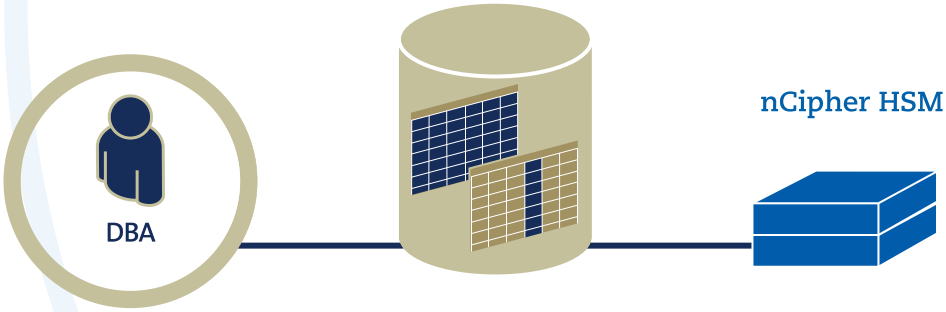
Databases are a treasure trove of sensitive information. Databases contain customers' personal data, confidential competitive information, and intellectual property. Lost or stolen data, especially customer data, can result in brand damage, competitive disadvantage, and serious fines. To help ensure companies protect customer data, the Payment Card Industry Data Security Standard (PCI DSS) defines strict security requirements for the processing, storage, and transmission of cardholder data.

As part of the Oracle 11g Advanced Security Option, Transparent Data Encryption enables you to encrypt customer, financial, and other sensitive data. Data is secured without changing existing applications or processes.

Safeguard your database with the highest level of assurance

To protect your data, nCipher hardware security modules (HSMs) secure the keys that safeguard Oracle Transparent Data Encryption. nCipher HSMs shelter encryption keys away from applications and the operating system with proven, trusted encryption. The use of encryption keys is enforced by policy, leaving your database safe from compromise.

nCipher HSMs secure the Oracle Transparent Data Encryption master key from compromise or misuse. To protect data and enable compliance, nCipher HSMs separate the roles of database and security administrators.



A seamless solution

nCipher HSMs integrate quickly and easily with the Oracle 11g Advance Security Option. Using standards-based interfaces you enjoy strong protection for your encryption keys and ensure the long-term usability of encrypted data. Supporting your disaster recovery and data retention needs, nCipher HSMs ease the burden of managing encryption with flexible deployment and management options. Available as a dedicated system for a single server or shared across the network for virtualized environments, nCipher HSMs are designed to meet the changing demands of your business.

ORACLE® PARTNER

Protect your brand and data

Validated to some of the highest security standards, such as FIPS, and under evaluation for Common Criteria, nCipher HSMs are ready to protect your data in even the most challenging and demanding security situations. nCipher HSMs are:

- Approved for high-security environments – Appropriate for public sector and security-conscious organizations.
- Reviewed by experts – Accepted by regulatory and compliance organizations.

Control access to database encryption

The nCipher HSM management system enables you to share keys across several HSMs. To enforce your policy, it separates the roles of security operators and administrators. For your Oracle database, nCipher HSMs deliver:

- Hardware key protection – Stores Transparent Data Encryption master keys in a secure, tamper-resistant environment to prevent copying.
- Tight control of keys – Smart card authentication firmly controls key access.
- Secure administration – Eliminates the need to rely on server administrators who can represent a single point of compromise.

Easy setup and integration

Using standards-based interfaces, nCipher HSMs integrate seamlessly with Oracle 11g. nCipher HSMs provide:

Smooth deployment – Fully tested and supported by nCipher and Oracle for quick deployment with Advance Security Option.

Integrates out of the box – Tested and fully documented configuration for Transparent Data Encryption.

Solution Specifications

Oracle 11g Advanced Security Option supports nCipher HSMs to secure the Transparent Data Encryption master key.

nCipher HSMs are available in two configurations:

- nCipher netHSM: Network-based module
- nCipher nShield: Single server PCI/PCIe interface card

nCipher HSMs provide encryption services for systems running Microsoft Windows, Sun Solaris, HP-UX, IBM AIX, and Linux.

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

Scale to meet your changing needs

nCipher HSMs integrate out of the box with leading enterprise applications, including web and application servers, databases, and public key infrastructures. Network-based HSMs can be shared by several servers to provide corporate security services. nCipher HSMs provide:

- Support for virtualized environments – For nCipher network-based HSMs, users have the option to add hardware-based key storage for virtualized servers.
- Performance – Hardware acceleration enables organizations to avoid bottlenecks.
- Failover capability – For nCipher network-based HSMs, users have the option to switch automatically to another HSM.
- Cost-effective resource – nCipher network-based HSMs enable the shared use of single modules across several servers, drastically reducing hardware, licensing, and operational costs.

ORACLE PARTNER

North America
nCipher, Inc.
1655 McCarthy Blvd
Milpitas, CA 95035 USA
92 Montvale Avenue #4500
Stoneham, MA 02180 USA
Tel: +1 800 nCIPHER

EMEA
nCipher Corporation
Jupiter House
Station Road
Cambridge CB1 2JD
UK
Tel: +44 (0) 1223-723600

Asia/Pacific
nCipher K.K.
15th Floor, Cerulean Tower
26-1 Sakuragaoka-cho
Shibuya-ku, Tokyo
Japan 150-8512
Tel: +81-3-5456-5486

www.ncipher.com
info@ncipher.com