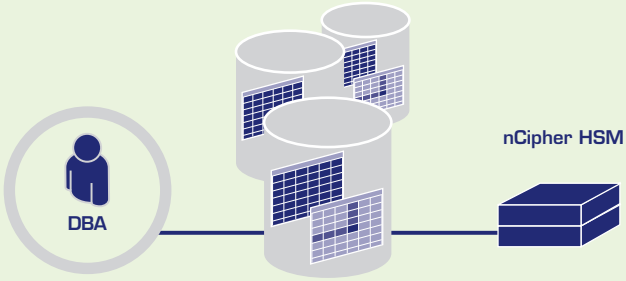
THALES

Database Security for Microsoft SQL Server 2008



Thales nCipher HSMs help demonstrate compliance by enforcing security policies and separating the roles of database and security administrators.

Thales nCipher hardware security modules increase security, simplify IT operations and help demonstrating compliance

Databases are a significant repository of sensitive information in most organizations. Corporate databases contain customers' credit card data, confidential competitive information, and intellectual property. Lost or stolen data puts organizations at significant risk of reputation and brand damage as well as serious fines. By protecting critical data from both internal and external threats, organizations mitigate the risk of data breaches and comply with regulatory and legislative mandates, including the Payment Card Industry Data Security Standard (PCI DSS).

Microsoft SQL Server 2008 ships with two built-in encryption features to protect your data: transparent data encryption (TDE) and cell-level encryption. These functions enable you to either protect the entire database or to secure only sensitive database fields and can be activated without disrupting your current applications, database structures, and processes.

>> Database Security for Microsoft SQL Server 2008

Safeguard your database with the highest level of assurance

Encrypting the data in your database protects the data, but the encryption keys that unlock the data must also be protected. The use of hardware security modules (HSMs) safeguards encryption keys by storing the keys separately from the data on a secure, trusted platform. Thales nCipher HSMs can enforce your internal security policy by requiring role-based authorization and separating security and database administration, making it easier to demonstrate compliance to auditors.

Seamless integration with Microsoft SQL Server 2008

Thales nCipher HSMs integrate with Microsoft SQL Server 2008 using Microsoft's Extensible Key Management (EKM). If your organization needs to protect an entire database farm, you can use the HSMs to consolidate all encryption keys in one place. This also simplifies the archiving of keys for long-term access to the data and facilitates the periodic rotation of encryption keys as required by several regulations such as PCI DSS.

Available as a dedicated appliance for a single server or as a shared network appliance for virtualized environments, nCipher HSMs are designed to meet the changing demands of your business.

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.

Control access to database encryption

Thales nCipher HSMs enable you to manage encryption keys for Microsoft SQL Server 2008 and other databases. To enforce your policies, security functions are separate from administrative functions. Thales nCipher HSMs deliver:

- **Hardware key protection** – Stores database encryption keys in a secure, tamper-resistant environment to prevent copying or tampering.
- **Enforcement of users and roles** – Stronger control for accessing encrypted data in Microsoft SQL Server 2008.
- **Tight control of keys** – Smart card authentication of administrators firmly controls access to database encryption keys.
- **Separation of roles** – Responsibility for important tasks and procedures can be split across multiple administrators.

Easy setup and integration

Thales nCipher HSMs integrate seamlessly with Microsoft SQL Server 2008 and provide:

- **Extensible Key Management (EMK) configuration** – Easily configures TDE and cell-level encryption modes and the protection of applicable encryption keys.
- **Smooth deployment** – Fully tested and supported by Thales and Microsoft for quick deployment.

Scale to meet your changing needs

Thales nCipher HSMs integrate out of the box with other leading enterprise applications, including web and application servers and public key infrastructures. Network-based HSMs can be shared by several servers providing:

- **Support for virtualized environments** – Hardware-based key storage for virtualized servers, including Hyper-V and VMware.
- **Simplified administration** – Manages the encryption keys for many databases as well keys used by other applications.
- **Failover capability** – When high availability is critical, users have the option to automatically switch to another HSM when an HSM becomes unavailable.
- **Disaster recovery** – Simple and secure processes for archiving and recovering keys.
- **Cost-effective resource** – Shared use of the module across several servers reduces hardware, licensing, and operational costs.

For more detailed technical specifications, please visit www.thalesgroup.com/InfoSysSecurity

© 2009 Thales — 0414

Thales
Information Systems Security

Americas: 2200 North Commerce Parkway, Suite 200 • Weston • Florida 33326 • Tel: +1 888 744 4976 or +1 954 888 6200 • Fax: +1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific: Units 2205-06, 22/F Vicwood Plaza, 199 Des Voeux Road Central • Hong Kong, PRC • Tel: +852 2815 8633 • Fax: +852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa: Meadow View House, Long Crendon, Aylesbury • Buckinghamshire • HP18 9EQ • Tel: +44 (0)1844 201800 Fax: +44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com