nShield Database Security Option Pack

Seamless integration of Microsoft SQL server databases with high-assurance nShield hardware security modules

HIGHLIGHTS

Strong root of trust for Microsoft SQL server database deployments

- Protect database cryptographic keys in best practice FIPS and Common Criteria certified hardware security modules (HSMs)
- Secures both cell level encryption and transparent data encryption (TDE)
- Safeguard an organization's critical data from breaches

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). In fact Section 3.6 of the latest PCI DSS standard (v3.2.1) specifies that "cryptographic keys must be stored securely …within a secure cryptographic device such a an HSM." Furthermore Section 3.6 outlines key management good practice delivered as a function of an HSM such as dual control.

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. nShield HSMs enforce your internal security policy by requiring role-based authorization and separating security and database administration, making it easier to demonstrate compliance to auditors.

Available as a dedicated PCIe card for a single server or as a shared network appliance for virtualized environments.

The nShield Database Security Option Pack (for Microsoft SQL Server) also known as the SQLEKM provider is the Extensible Key Management (EKM) API provided for Microsoft SQL Server.

nShield Database Security Option Pack

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

Protect your brand and data

Validated to some of the highest security standards, such as FIPS and Common Criteria, Entrust nShield HSMs are ready to protect your data in even the most challenging and demanding security situations. nShield HSM's fine grained access controls enable you to manage encryption keys for Microsoft SQL Server. To enforce your policies, security capabilities are separate from administrative functions.

Entrust nShield HSMs deliver:

- **Hardware key protection** – Stores database encryption keys in a secure, tamper-resistant environment to prevent copying or compromise
- **Enforcement of users and roles** – Provides stronger control for accessing encrypted data in Microsoft SQL Server
- **Tight control of keys** – Uses smart card authentication of administrators to provide robust control to database encryption keys
- **Separation of roles** – Splits responsibility for important tasks and procedures across multiple administrators
- **Easy setup and integration** – Entrust nShield HSMs integrate seamlessly with Microsoft SQL Server to provide:
  - TDE and cell-level encryption modes with the protection of applicable encryption keys

Scale to meet your changing needs, nShield HSMs integrate out of the box with other leading enterprise applications, including web and application servers and public key infrastructures (PKIs).

Network-based nShield Connect HSMs can be shared by several servers providing:

- **Support for virtualized environments** – Hardware based key storage for virtualized servers, including Hyper-V and VMware
- **Failover cluster support** including AlwaysOn availability group
- **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

nShield Database Security Option Pack

TECHNICAL SPECIFICATIONS

Supported configurations

- Requires nShield Security World Software v12.40.2 or v12.60.x or greater.
- Microsoft SQL server version (enterprise edition) 2019 x64, 2017 x64
- Windows server operating system support 2019 R2 x64, 2016 R2 x64
- Supported HSMs
  - Compatible with all nShield Solo and Connect HSM models

Supported cryptographic algorithms

- Asymmetric - including RSA 2048, 3072 and 4096 bit key lengths
- Symmetric - including AES 128, 192 and 256 bit key lengths

SUPPORTED NSHIELD FUNCTIONALITY

Access the following functionality when you integrate an nShield HSM with Microsoft SQL server:

Functionality	Support
1 of N Card Set	Yes
K of N Card Set	No
Softcards	Yes
Module Only Key	No
Key Recovery	Yes
Key Import	Partial[1]
Load Balancing	Yes
Fail Over	Yes
Strict FIPS (FIPS 140-2 Level 3) support	Yes[2]

1. Key import is supported for nCore keys only. The nCore API is the native application programming interface for nShield modules
2. Check release notes and user guide for details.

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