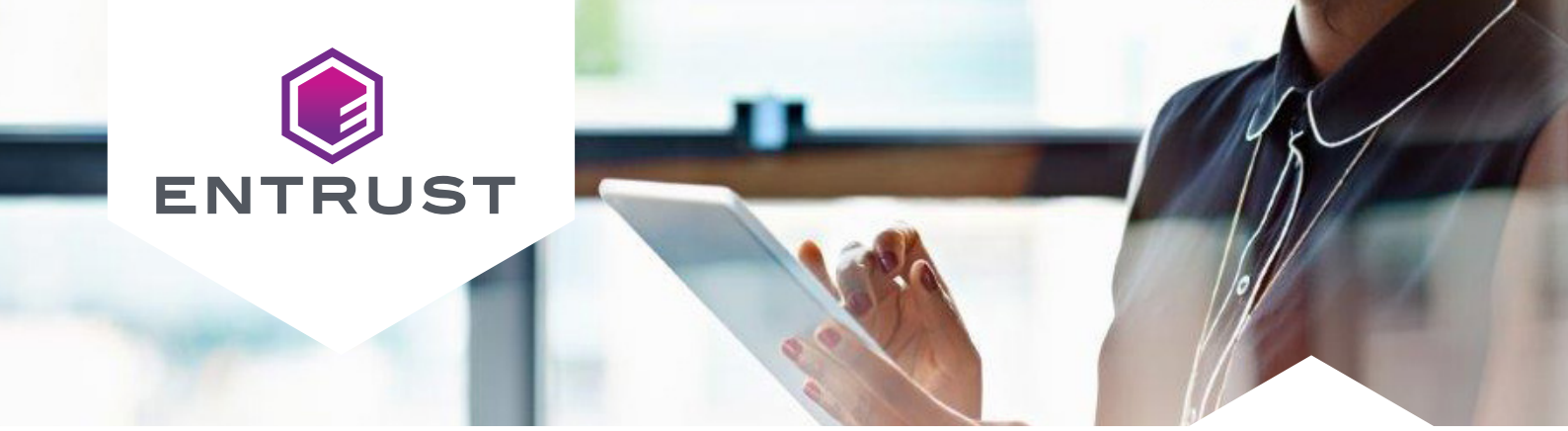

nShield Database Security Option Pack

Nahtlose Integration von Microsoft-SQL-Server-Datenbanken mit hochsicheren Hardware-Sicherheitsmodulen von nShield

HIGHLIGHTS

Leistungsstarker Vertrauensanker für Microsoft-SQL-Server-Datenbanken

- Schützt die kryptographischen Schlüssel von Datenbanken mithilfe bewährter, gemäß FIPS und Common Criteria zertifizierter Hardware-Sicherheitsmodule (HSM)
- Sichert Verschlüsselung auf Zellebene sowie transparente Datenverschlüsselung (Transparent Data Encryption, TDE)
- Schützt kritische Unternehmensdaten vor Datenschutzverletzungen

Datenbanken speichern in den meisten Unternehmen große Mengen sensibler Daten. Unternehmensdatenbanken enthalten Kreditkartendaten der Kunden, vertrauliche Wettbewerbsinformationen sowie geistiges Eigentum. Verlorene oder gestohlene Daten bergen beachtliche Risiken für den Ruf und das Markenimage von Unternehmen. Außerdem können drastische Bußgelder fällig werden. Indem Unternehmen kritische Daten vor internen und externen Bedrohungen schützen, können sie das Risiko von Datenschutzverletzungen senken und regulatorische und gesetzliche Vorschriften wie den Payment Card Industry Data Security Standard (PCI DSS) einhalten. In der Tat heißt es im Abschnitt 3.6 der neusten PCI DSS-Norm (v3.2.1), dass „kryptographische Schlüssel sicher … in einem sicheren kryptographischen Gerät wie einem HSM gespeichert werden müssen“. Ferner beschreibt Abschnitt 3.6 bewährte Schlüsselverwaltungsverfahren, die als Funktion eines HSM bereitgestellt werden, wie z. B. doppelte Kontrolle.

Schützen Sie Ihre Schlüssel in der Cloud durch höchste Sicherheit

Für optimalen Schutz sollten Sie in Ihrer Datenbank neben den Daten auch die Schlüssel verschlüsseln, die zur Entschlüsselung dieser Daten verwendet werden. Hardware-Sicherheitsmodule (HSM) schützen kryptographische Schlüssel, indem Sie diese getrennt von den Daten auf einer sicheren, vertrauenswürdigen Plattform speichern. nShield HSM setzen Ihre internen Sicherheitsrichtlinien mittels rollenbasierter Berechtigungen und der Trennung von Sicherheits- und Datenbankverwaltung durch. Somit ist es viel einfacher, Prüfern nachzuweisen, dass Vorgaben eingehalten werden.

Sie sind als spezielle PCIe-Card für einen einzelnen Server oder als Appliance für gemeinsame Netzwerke in virtuellen Umgebungen erhältlich.

Das nShield Database Security Option Pack (für Microsoft-SQL-Server), auch bekannt als SQLEKM-Anbieter, ist die Extensible Key Management (EKM) API für Microsoft-SQL-Server.

nShield Database Security Option Pack

Microsoft-SQL-Server schützt Ihre Daten mithilfe zweier eingebauter Verschlüsselungsfunktionen: TDE und Verschlüsselung auf Zellebene. Mit diesen Funktionen können Sie die gesamte Datenbank oder ausschließlich sensible Datenbankfelder schützen. Sie können aktiviert werden, ohne Ihre laufenden Anwendungen, Datenbankstrukturen oder Prozesse zu stören.

Schützen Sie Ihre Marke und Ihre Daten

Die nShield-HSM von Entrust sind nach höchsten Sicherheitsstandards wie FIPS und Common Criteria validiert und schützen Ihre Daten auch in den schwierigsten und anspruchsvollsten Situationen. Dank ihrer granularen Zugriffskontrolle können Sie kryptographische Schlüssel für Microsoft-SQL-Server verwalten. Damit Ihre Richtlinien durchgesetzt werden, sind die Sicherheitsfunktionen von den administrativen Funktionen getrennt.

nShield-HSM von Entrust bieten:

- **Schutz der Hardwareschlüssel**: Die kryptographischen Schlüssel für Datenbanken werden in einer sicheren, manipulationssicheren Umgebung gespeichert, damit sie nicht kopiert werden können oder anderweitig gefährdet sind.
- **Durchsetzung von Benutzern und Rollen:** Der Zugriff auf verschlüsselte Daten in Microsoft-SQL-Server wird schärfer kontrolliert.
- **Engmaschige Schlüsselkontrolle:** Administratoren werden mittels Smartcards authentifiziert und die kryptographischen Schlüssel von Datenbanken somit streng kontrolliert.
- **Aufgabentrennung:** Die Verantwortung für wichtige Aufgaben und Verfahren wird auf mehrere Administratoren verteilt.
- **Einfache Einrichtung und Integration:** Die nShield-HSM von Entrust lassen sich nahtlos in Microsoft-SQL-Server integrieren und stellen Folgendes bereit:
  - TDE und Verschlüsselung auf Zellebene mit dem Schutz der entsprechenden kryptographischen Schlüssel.

nShield-HSM sind je nach Bedarf skalierbar. Sie sind sofort einsatzbereit und können mit anderen führenden Unternehmensanwendungen integriert werden, wie z. B. Web- und Anwendungsserver und Public Key Infrastructure (PKI).

Die netzwerkbasierten nShield-Connect-HSM können für mehrere Server eingesetzt werden und unterstützen:

- **Virtuelle Umgebungen:** Hardware-basierte Schlüsselspeicherung für virtuelle Server wie Hyper-V und VMware.
- **Failover Cluster** einschließlich AlwaysOn-Verfügbarkeitsgruppe.
- **Einfache Administration:** Schlüsselverwaltung für viele Datenbanken sowie für Schlüssel, die von anderen Anwendungen verwendet werden.
- **Failover-Funktion:** Wenn eine hohe Verfügbarkeit gefordert ist, können Benutzer automatisch auf ein anderes HSM wechseln, falls ein bestimmtes HSM nicht verfügbar ist.
- **Notfallwiederherstellung:** einfache und sichere Verfahren für die Archivierung und Wiederherstellung von Schlüsseln.
- **Kosteneinsparungen:** Gemeinsame Nutzung des Moduls über mehrere Server hinweg senkt die Hardware-, Lizenz- und Betriebskosten.

nShield Database Security Option Pack

TECHNISCHE DATEN

Unterstützte Konfigurationen

- Erfordert nShield Security World Software v12.40.2 oder v12.60.x oder höher.
- Microsoft-SQL-Server Version (Enterprise Edition) 2019 x64, 2017 x64
- Windows-Server-Betriebssystem-Support 2019 R2 x64, 2016 R2 x64
- Unterstützte HSM
  - Mit allen nShield Solo und Connect HSM-Modellen kompatibel

Unterstützte kryptographische Algorithmen

- Asymmetrisch: einschließlich RSA 2048-, 3072- und 4096-Bit-Schlüssellängen
- Symmetrisch: einschließlich AES 128-, 192- und 256-bit-Schlüssellängen

UNTERSTÜTZTE NSHIELD-FUNKTIONEN

Greifen Sie auf die folgenden Funktionen zu, wenn Sie einen nShield-HSM mit Microsoft-SQL-Server integrieren:

Funktion	Support
1-von-N-Cardset	Ja
K-von-N-Cardset	Nein
Softcards	Ja
Module Only Key	Nein
Schlüsselwiederherstellung	Ja
Schlüsselimport	Teilweise[1]
Load Balancing	Ja
Failover	Ja
Strikte FIPS-Unterstützung (FIPS 140-2 Level 3)	Ja[2]

1. Schlüsselimport wird nur für nCore-Schlüssel unterstützt. Die nCore API ist die native Programmierschnittstelle für nShield-Module
2. Weitere Informationen finden Sie in den Versionshinweisen und im Benutzerhandbuch.

Weitere Informationen

Mehr Informationen zu den nShield HSM von Entrust finden Sie auf **entrust.com/HSM**. Auf **entrust.com** erfahren Sie zudem mehr über die digitalen Sicherheitslösungen für Identitäten, Zugriff, Kommunikation und Daten von Entrust.

Mehr Informationen zu Entrust nShield HSM

HSMinfo@entrust.com
entrust.com/HSM

ÜBER ENTRUST CORPORATION

Entrust ermöglicht vertrauenswürdige Identitäten und Zahlungen sowie verlässlichen Datenschutz und hält damit die Welt sicher in Bewegung. Ein nahtloses und sicheres Umfeld ist heute mehr denn je unerlässlich, sei es bei Grenzübertritten, beim Einkaufen, beim Zugriff auf E-Government-Dienste oder beim Einloggen in Unternehmensnetzwerke. Entrust bietet für genau diese Interaktionen eine unübertroffene Bandbreite an Lösungen für digitale Sicherheit und die Ausstellung von Berechtigungsnachweisen. Mit 2.500 Mitarbeitern und einem weltweiten Partnernetzwerk ist Entrust für Kunden in über 150 Ländern tätig, die sich bei ihren sensibelsten Operationen auf uns verlassen.

Weitere Informationen auf
entrust.com/HSM

ENTRUST

Kontakt:
HSMinfo@entrust.com