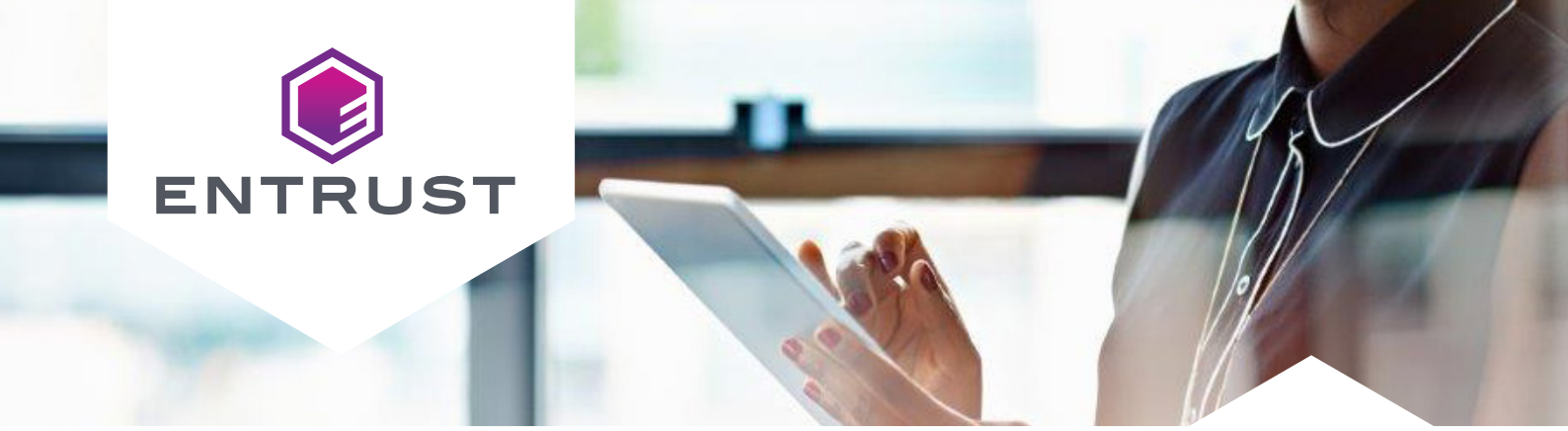

Pack d'options de sécurité nShield pour les bases de données

Intégration fluide des bases de données de Microsoft SQL Server grâce aux modules matériel de sécurité haute sécurité nShield

CARACTÉRISTIQUES

Une solide base de confiance pour les déploiements de bases de données Microsoft SQL Server

- Protège les clés de chiffrement des bases de données au sein de modules matériel de sécurité (HSM) certifiés FIPS et Critères Communs
- Sécurise à la fois le chiffrement au niveau cellule et le chiffrement transparent des données (TDE)
- Protège les données critiques d'une organisation contre les fuites de données

Dans la plupart des organisations, les bases de données constituent un important gisement d'informations sensibles. Les bases de données des entreprises contiennent les données des cartes de paiement des clients ainsi que des informations confidentielles sur la concurrence et la propriété intellectuelle. La fuite ou le vol de données sont des menaces considérables pour la réputation et la marque des entreprises, et peuvent entraîner de lourdes amendes. En protégeant les données critiques contre les risques internes et externes, les organisations peuvent limiter le risque de fuites de données et respecter les réglementations et les lois en vigueur, notamment la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS). De fait, le paragraphe 3.6 de la toute dernière norme PCI DSS (v3.2.1) stipule que « les clés de chiffrement doivent être stockées de manière sécurisée … au sein d'un appareil de chiffrement sécurisé de type HSM ». Ce paragraphe indique en outre des exemples de bonnes pratiques de gestion de clés, comme par exemple la double vérification par un HSM.

Protège vos bases de données avec le plus haut niveau de sécurité possible

Le chiffrement des données se trouvant dans vos bases de données protège les données, mais les clés de chiffrement qui déverrouillent les données doivent également être protégées. L'utilisation de modules matériel de sécurité (HSM) protège les clés de chiffrement en les stockant sur une plateforme sécurisée et fiable, qui est distincte de celle où se trouvent vos données. Les HSM nShield renforcent votre politique de sécurité interne en exigeant une autorisation basée sur le rôle et en séparant la gestion de la sécurité de celle des bases de données, ce qui simplifie la démonstration de la conformité auprès des auditeurs.

Disponible sous la forme d'une carte PCIe dédiée pour un seul serveur ou d'un appareil sur réseau partagé pour les environnements virtualisés.

Le pack d'options de sécurité nShield pour les bases de données (pour Microsoft SQL Server), aussi appelé le fournisseur SQLEKM, est une API de gestion des clés extensible (EKM) pour Microsoft SQL Server.

Pack d'options de sécurité nShield pour les bases de données

Microsoft SQL Server est livré avec deux mécanismes de chiffrement intégrés pour protéger vos données : TDE et chiffrement au niveau cellule. Ces fonctionnalités vous permettront de protéger l'ensemble de la base de données ou de ne sécuriser que les champs les plus sensibles de la base de données. Elles peuvent être activées sans que cela n'interrompe les applications, les structures de base de données et les processus en cours.

Garantit la protection de votre marque et de vos données

Certifiés conformes à des normes de sécurité parmi les plus rigoureuses telles que les FIPS et les Critères communs, les HSM nShield de Entrust garantissent la protection de vos données, même dans les conditions de sécurité les plus complexes et les plus exigeantes. Les contrôles d'accès perfectionnés des HSM nShield permettent de gérer les clés de chiffrement pour Microsoft SQL Server. Pour garantir l'application de vos politiques, les fonctionnalités de sécurité sont indépendantes des fonctionnalités de gestion.

Avantages des HSM nShield de Entrust :

- **Protection matérielle des clés** – permet de stocker les clés de chiffrement des bases de données au sein d'un environnement sécurisé inviolable afin d'éviter toute copie ou menace
- **Application de règles pour les utilisateurs et les rôles** – Permet de renforcer le contrôle de l'accès aux données chiffrées dans Microsoft SQL Server
- **Contrôle rigoureux des clés** – Utilisation de l'authentification des administrateurs par carte à puce afin que les clés de chiffrement des bases de données soient bien protégées
- **Séparation des rôles** – Répartition de la responsabilité des tâches et procédures importantes entre plusieurs administrateurs
- **Installation et intégration très simples** – Les HSM nShield de Entrust s'intègrent parfaitement à Microsoft SQL Server pour fournir :
  - des méthodes de chiffrement TDE et au niveau cellule avec protection des clés de chiffrement correspondantes

Évolutifs pour s'adapter à vos besoins, les HSM nShield s'intègrent immédiatement à des applications d'entreprise de premier plan, notamment les serveurs web et d'applications et les infrastructures à clé publique (PKI).

Les HSM en réseau nShield Connect peuvent être répartis sur plusieurs serveurs, permettant :

- **La prise en charge d'environnements virtualisés** – Stockage matériel des clés pour serveurs virtualisés, notamment Hyper-V et VMware
- **La prise en charge du basculement regroupé** dont les groupes de disponibilité AlwaysOn
- **Une gestion simplifiée** – Gère les clés de chiffrement de nombreuses bases de données ainsi que les clés utilisées par d'autres applications
- **La capacité de basculement** – Lorsqu'il est nécessaire de disposer d'une haute disponibilité, les utilisateurs peuvent passer automatiquement à un autre HSM si un HSM devient indisponible
- **La restauration en cas de défaillance.** – Des processus simples et sécurisés d'archivage et de récupération des clés
- **Une solution rentable** – l'utilisation partagée du module sur plusieurs serveurs réduit les dépenses liées au matériel, aux licences et au fonctionnement

Pack d'options de sécurité nShield pour les bases de données

INDICATIONS TECHNIQUES

Configurations prises en charge

- Nécessite le logiciel nShield Security World v12.40.2, v12.60.x ou version plus récente.
- Version serveur de Microsoft SQL (édition entreprise) 2019 x64, 2017 x64
- Prise en charge du système d'exploitation de Windows Server 2019 R2 x64, 2016 R2 x64
- HSM pris en charge
  - Compatible avec les modèles nShield Solo et Connect

Algorithmes de chiffrement pris en charge

- Asymétrique - incluant notamment les longueurs de clé RSA 2048, 3072 et 4096 bits
- Symétrique - incluant notamment les longueurs de clé AES 128, 192 et 256 bits

FONCTIONNALITÉS NSHIELD PRISES EN CHARGE

Vous pouvez bénéficier des fonctionnalités suivantes lorsque vous intégrez un HSM nShield à Microsoft SQL Server :

Fonctionnalité	Prise en charge
1 sur N du set de Cartes	Oui
K sur N du set de Cartes	Non
Cartes électroniques	Oui
Clés de module seulement	Non
Récupération des clés	Oui
Importation des clés	Partielle [1]
Répartition de la charge	Oui
Basculement	Oui
Prise en charge stricte de la norme FIPS (FIPS 140-2 niveau 3)	Oui [2]

1. L'importation de clés n'est prise en charge que pour les clés nCore. L'API nCore est l'interface de programmation d'application native pour les modules nShield
2. Consultez les notes de version et le guide de l'utilisateur pour plus de précisions.

En savoir plus

Pour en savoir plus sur les HSM nShield de Entrust, rendez-vous sur **entrust.com/fr/digital-security/hsm** Pour en savoir plus sur les solutions de protection numérique de Entrust pour les identités, l'accès, les communications et les données, rendez-vous sur **entrust.com/fr**

Pour en savoir plus sur les HSM nShield de Entrust

HSMinfo@entrust.com
entrust.com/fr/digital-security/hsm

À PROPOS DE LA SOCIÉTÉ ENTRUST

Entrust sécurise un monde en évolution permanente avec des solutions qui protégent les identités, les paiements et les données, dans tous les pays. Aujourd'hui, les gens s›attendent à des parcours plus fluides et plus sûrs quand ils traversent les frontières, font des achats, utilisent des services administratifs en ligne ou des réseaux d'entreprises. Notre portefeuille unique de solutions pour la sécurité numérique et l'émission de titres sécurisés permet de répondre exactement à cette demande. Grâce à nos 2500 collaborateurs, notre réseau international de partenaires et des clients dans plus de 150 pays, les organisations les plus fiables au monde nous font confiance.

Découvrez-en plus sur
entrust.com/HSM

ENTRUST

Nous contacter :
HSMinfo@entrust.com