Keystore à haute évolutivité

Manipulez des millions de clés tout en maintenant des performances élevées

CARACTÉRISTIQUES

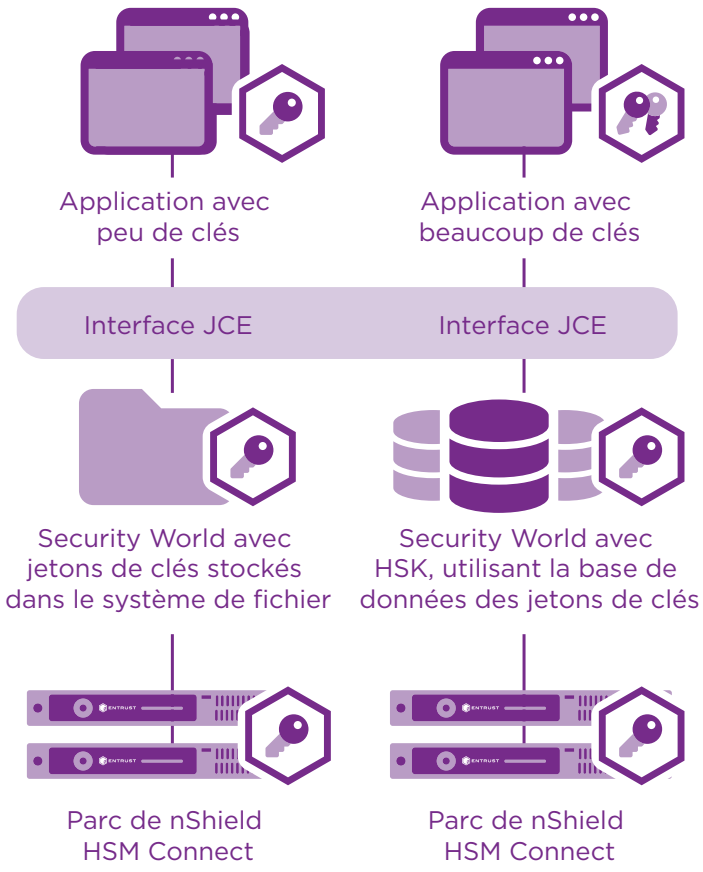
- Une solution hautement performante et évolutive pour les cas d'utilisation spécifiques des HSM nShield® de Entrust
- Un support d'un très grand nombre de clés de chiffrement actives simultanément
- Évite les goulots d'étranglement des systèmes d'exploitation

Certains cas d'utilisation de modules matériels de sécurité (HSM) doivent traiter simultanément un très grand nombre de clés de chiffrement. Cela peut entraîner des goulots d'étranglement dans le système de fichiers des ordinateurs connectés aux HSM. Le keystore à haute évolutivité (HSK) supporte un très grand nombre de clés tout en maintenant des performances élevées.

Fonctionnalités principales

La solution HSK fournit les fonctionnalités suivantes :

- Évolutivité jusqu'à des millions de clés RSA
- Des performances qui restent pratiquement inchangées à mesure que le nombre de clés augmente
- Prise en charge de la génération de clé RSA, de la génération de demande de signature de certificat (CSR), de la création et la vérification de signature numérique, du chiffrement et déchiffrement des données.
- Synchronisation automatique entre plusieurs ordinateurs appelants
- Solution extensible et personnalisable pour répondre à vos besoins



DÉCOUVREZ-EN PLUS SUR ENTRUST.COM/FR/HSM

Les HSM nShield Edge

Fonctionnement

Les HSM nShield de Entrust offrent une cadence de transactions hautement performante, prenant en charge des milliers de transactions par seconde. (Les performances dépendent du modèle de HSM et de l'opération de chiffrement spécifique. Voir les fiches techniques des modèles nShield spécifiques pour les dernières informations sur les performances des HSM).

L'architecture flexible et sécurisée du Security World de Entrust stocke les clés de chiffrement externes au HSM, sous forme de « jetons ». Les clés contenues dans les « jetons » sont fortement protégées par des clés principales de HSM, qui utilisent le chiffrement, les contraintes d'utilisation, les contrôles d'accès et la sécurité de l'authentification. Cette solution combine une sécurité renforcée avec les avantages de l'évolutivité, de la répartition des charges, du basculement, de l'expansion ou de la contraction facile du nombre de HSM dans un parc, de l'échange des HSM dans et hors du parc, et de la sauvegarde facile des jetons de clés sans avoir besoin de dispositifs de sauvegarde supplémentaires.

L'architecture standard de Security World stocke ces « jetons » dans les systèmes de fichiers des ordinateurs appelants (avec support de synchronisation), en utilisant un seul fichier par jeton. Cette approche convient à la plupart des cas d'utilisation qui ont généralement un nombre limité de clés actives par ordinateur client.

Dans certains cas d'utilisation, les performances du HSM nShield peuvent être limitées par les latences présentes dans le système de fichiers du système d'exploitation de l'ordinateur appelant. Le HSK offre des performances élevées lorsqu'il y a un très grand nombre de clés, en utilisant une base de données plutôt que le système de fichiers pour stocker les jetons de clés sur l'ordinateur client.

L'équipe des services professionnels (SP) Entrust vous aidera à évaluer si le HSK est adapté à vos besoins. Les conseillers SP vous fourniront également un soutien d'expert pour le développement, afin de vous aider à intégrer le HSK dans votre environnement, y compris en personnalisant le HSK pour répondre à vos besoins spécifiques si nécessaire.

Exemples de cas d'utilisation

- Sécurité des e-mails d'entreprise pour un grand nombre d'utilisateurs
- Signature des documents d'entreprise
- Internet des objets (IoT) avec un grand nombre d'appareils connectés
- Applications mobiles avec un grand nombre d'utilisateurs finaux
- Systèmes de porte-monnaie électronique pour les échanges de cryptomonnaies

Informations techniques

- Bibliothèque JCE (Java Cryptography Extension), utilisant les HSM nShield
- Pack d'options de services web RESTful JSON
- Stocke les « jetons » des clés HSM nShield dans une base de données plutôt que dans le système de fichiers
- Fonctionne avec les logiciels de bases de données relationnelles les plus répandus, notamment MSSQL, Oracle et Derby (des bases de données supplémentaires sont en cours d'ajout)
- Fonctionne avec un seul HSM ou plusieurs HSM dans un parc de répartition des charges

En savoir plus

Pour en savoir plus sur les HSM nShield® de Entrust, rendez-vous sur **entrust.com/fr/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**

Découvrez-en plus sur
entrust.com/fr/HSM

ENTRUST

Nous contacter :
HSMinfo@entrust.com