nShield Bring Your Own Key permet aux clients du cloud de mieux contrôler la sécurité des données

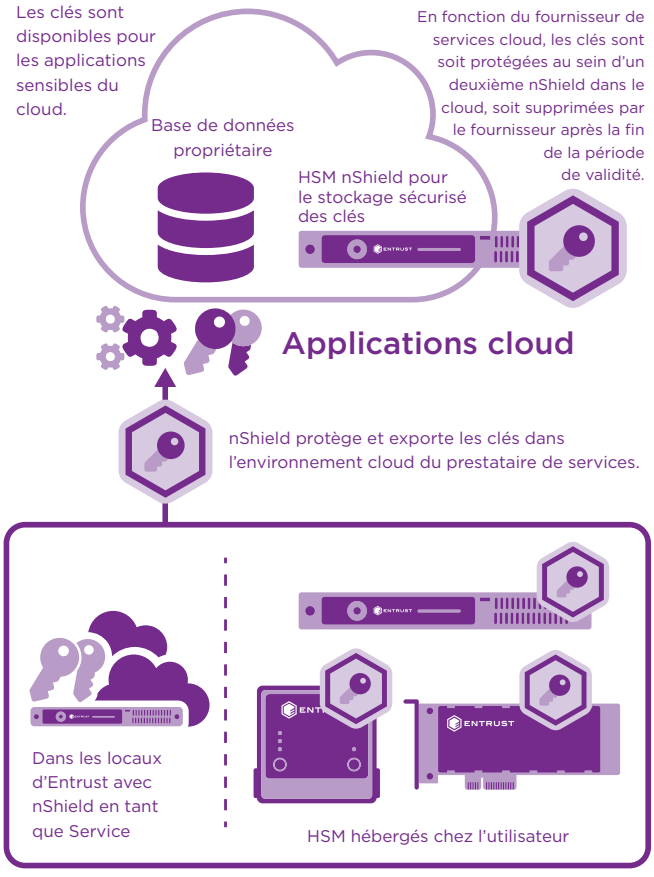
Quand simplicité du cloud rime avec sécurité

CARACTÉRISTIQUES

- Des pratiques de gestion des clés plus sécurisées qui renforcent la sécurité de vos données sensibles au sein du cloud
- Génération de clés plus performantes grâce au générateur de nombres aléatoires à haute entropie nShield® de Entrust, protégé au sein d'un appareil certifié FIPS
- Un meilleur contrôle des clés : vous utilisez vos propres modules matériels de sécurité (HSM) nShield au sein de votre environnement pour créer et exporter vos clés en toute sécurité dans le cloud
- Des opérations de gestion des clés plus homogènes, que vos clés soient utilisées dans le cloud ou sur site

Grâce aux HSM nShield, vous pourrez utiliser Bring Your Own Key (BYOK) dans vos applications cloud si vous utilisez Amazon Web Services (AWS), Google Cloud Platform (GCP) ou Microsoft Azure.

Les HSM nShield à haute protection vous permettent de bénéficier de la même souplesse et des mêmes avantages que les services cloud, tout en renforçant le contrôle et la protection de vos clés.



L'architecture unique Security World de Entrust permet de sécuriser le stockage à long terme et de récupérer les clés principales en cas d'incident

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

Permet aux utilisateurs du cloud de mieux maîtriser la sécurité de leurs données

Le rôle de nShield BYOK

Grâce à nShield BYOK, vous pourrez utiliser vos HSM nShield pour générer, stocker et gérer les clés sur lesquelles repose la protection de vos applications sensibles hébergées sur cloud, de vos bases de données et du stockage de vos données. nShield BYOK vous permet de :

- Bénéficier de la racine de confiance des HSM. Les HSM nShield sont des dispositifs hautement sécurisés, inviolables et certifiés FIPS 140-2 de niveau 3. Ils établissent la racine de confiance pour vos services cloud, vous permettant de générer et de garantir la sécurité de vos clés de chiffrement et de signature.
- Utiliser nShield pour la gestion de vos clés. Lorsque vos applications cloud contiennent des données personnelles, vous pourrez compter sur vos HSM nShield pour générer et protéger vos clés en vue de les transmettre en toute sécurité à vos applications.
- Vérifier la disponibilité de vos clés. Vous exercez un contrôle total sur vos HSM nShield, qu'ils soient sur site ou dans l'environnement nShield as a Service (en tant que service), et c'est vous qui déterminez à quel moment les clés sont générées et exportées. La vérification des clés vous permet aussi de surveiller si des exportations supplémentaires vers votre fournisseur de services cloud ont lieu et à quel moment.
- Choisir votre fournisseur de service cloud. Avec nShield BYOK, vous déterminez le fournisseur de services cloud à utiliser pour chaque clé. Cela vous laisse la liberté de choisir le bon cloud à partir de vos environnements sur site ou nShield as a Service pour vos applications, vous permettant ainsi de profiter de la fiabilité optimale de nShield pour la génération et la protection des clés.

Premiers pas avec nShield BYOK

Il vous faut un HSM nShield avant de pouvoir commencer à utiliser nShield BYOK avec AWS, GCP ou Azure. Nous vous proposons plusieurs solutions :

- nShield Connect, un appareil en réseau.
- nShield Solo, une carte PCIe intégrée au serveur.
- nShield Edge, un périphérique USB pour les applications à faible volume.
- nShield as a Service, une solution sur abonnement permettant de bénéficier des HSM nShield Connect

Pour la plus grande sécurité d'utilisation de Microsoft Azure, choisissez Entrust BYOK. Voir : **docs.microsoft.com/en-us/azure/key-vault/keys/hsm-protected-keys-Entrust** Si vous avez besoin d'aide pour le déploiement, vous pouvez acheter le pack optionnel suivant :

Bring Your Own Key,
Services professionnels Azure
Ce pack comprend un nShield Edge, l'intégration assurée par l'équipe des services professionnels de Entrust, et un an de maintenance.

Il est également possible de commander les HSM nShield Connect, Solo, ou Edge et les services professionnels séparément.

Pour utiliser nShield BYOK avec AWS, GCP ou Microsoft Azure en utilisant la méthode des normes ouvertes de Microsoft, vous aurez besoin du pack Entrust suivant :

Pack d'intégration Cloud
Ce pack d'options contient tout ce dont vous avez besoin pour utiliser vos HSM nShield sur site pour protéger, transporter de manière sécurisée et louer vos clés à AWS ou à GCP, ou à Microsoft Azure en utilisant Azure BYOK.

Vous pouvez intégrer nShield BYOK avec AWS, GCP ou Azure par vous-même, ou bien faire appel à l'équipe des services professionnels de Entrust pour vous aider à établir une connexion continue et performante.

Permet aux utilisateurs du cloud de mieux maîtriser la sécurité de leurs données

Fonctionnement de nShield BYOK

Entrust fournit la technologie qui vous permet d'utiliser vos HSM nShield afin de générer des clés, de protéger le stockage à long terme et d'exporter vos clés dans le cloud. Une fois que vos clés sont exportées dans le cloud depuis votre site ou nShield as a Service, vous gérerez les clés selon l'une des approches suivantes :

Si vous utilisez Microsoft Azure…
Pour la plus grande sécurité d'utilisation de Microsoft Azure, choisissez Entrust BYOK. Il contrôle les conditions qui doivent être remplies pour permettre le téléchargement d'une clé vers Azure et restreint étroitement ce que Microsoft peut en faire une fois qu'elle y est.

Vous transférerez vos clés en toute sécurité aux HSM nShield opérant au sein de l'infrastructure Azure, ce qui vous permettra de bénéficier d'une double protection des HSM.

Si vous utilisez AWS ou GCP…
Vous louerez vos clés à AWS ou GCP pour une utilisation temporaire dans le cloud. Après une période prédéterminée, vos clés installées dans le cloud seront détruites. Au besoin, vous pouvez à nouveau louer les clés stockées dans votre HSM.

Quel que soit votre choix de service cloud, générez votre propre clé et contrôlez son exportation vous permettra d'établir des mécanismes de protection robustes autour de vos données et applications sensibles dans le cloud.

Les HSM de Entrust

Les HSM nShield d'Entrust représentent l'une des solutions HSM les plus performantes, les plus sécurisées et les plus faciles à intégrer, permettant de respecter les réglementations et de fournir les plus hauts niveaux de sécurité pour les données et les applications des entreprises, des organismes financiers et des administrations publiques. Notre architecture de gestion de clés Security World permet un contrôle granulaire et très robuste de l'accès aux clés et de leur usage.

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**

Pour en savoir plus sur les HSM nShield de Entrust

HSMinfo@entrust.com

entrust.com/fr/HSM

À PROPOS DE LA SOCIÉTÉ ENTRUST

Entrust sécurise un monde en mouvement avec des solutions qui protègent les identités, les paiements et les données, dans tous les pays. Aujourd'hui, les gens souhaitent 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 gamme unique de solutions pour la sécurité numérique et l'émission de titres sécurisés permet de répondre précisément à ces souhaits. Grâce à nos 2 500 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/fr/HSM

ENTRUST

Nous contacter :
HSMinfo@entrust.com