Hold Your Own Key pour une gestion de clés hautement sécurisée

Microsoft

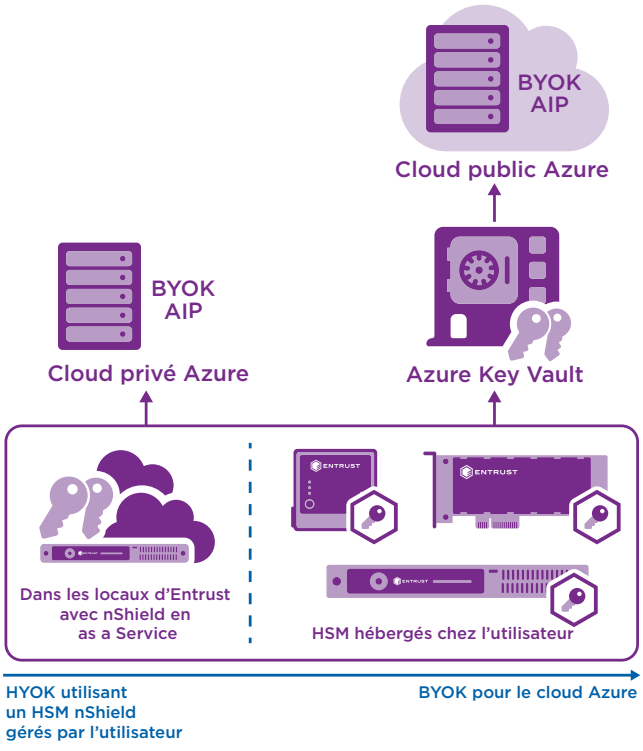
Microsoft et Entrust s´associent pour une protection permanente des informations et une gestion des clés qui vous donne le contrôle dans le cloud

CARACTÉRISTIQUES

- Met en place des mécanismes de contrôle d'accès et d'utilisation des données que vous échangez
- Conserve et protège vos clés grâce à des HSM dont vous avez le contrôle
- Assure une gestion du cycle de vie des clés certifiée FIPS 140-2
- Veille à ce que les clés ne soient jamais visibles pour Microsoft

Microsoft Azure Information Protection (AIP) protège les données échangées au sein de votre environnement de travail collaboratif en intégrant des procédures de sécurité applicables aux actifs de données, et ce, quel que soit leur type. Ce service cloud vous permet d'utiliser AIP à la demande sans avoir besoin d'une infrastructure informatique et s'assure que vos données sont protégées au-delà du cadre de votre organisation.

AIP utilise le chiffrement afin de garantir un accès sécurisé et une protection permanente de vos données. Le niveau de sécurité de AIP dépend du degré de protection des clés de chiffrement. Lorsque les clés de chiffrement sont vulnérables, vos données sensibles sont compromises.



Que vous utilisiez AIP sur site, dans une configuration hybride ou bien intégralement sur cloud, les HSM nShield® de Entrust vous assure le contrôle total sur vos clés.

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

Hold Your Own Key pour une gestion de clés hautement sécurisée

Le défi : les données les plus sensibles nécessitent que les clés de chiffrement restent sur site

Si les clés stockées de manière sécurisée dans Azure conviennent à la plupart des contenus, d'autres contenus plus sensibles ne doivent jamais être partagés ou transmis en dehors de votre propre environnement sécurisé. La sécurité de ces contenus sensibles doit se faire exclusivement sur site, et leur accès et partage doivent être considérablement restreints.

Afin de pouvoir gérer vos données les plus sensibles au sein de votre propre environnement sécurisé avec AIP, vous pouvez conserver les informations de votre propre clé (Hold Your Own Key, HYOK) grâce à un module matériel de sécurité (HSM) de Entrust, dispositif sur site qui assure la gestion des clés, lesquelles peuvent être localisées sur site ou au sein de l'environnement en tant que Service.

Les HSM nShield® de Entrust forment un environnement verrouillé qui protège vos clés et renforce la sécurité de vos données sensibles.

La solution : déploiements HYOK avec contrôle des clés renforcé de Entrust

Les HSM nShield de Entrust établissent des mécanismes de protection rigoureux pour la gestion et l'utilisation des clés de chiffrement utilisées dans les déploiements AIP.

Les HSM nShield de Entrust constituent une solution matérielle pour la protection de vos clés. Ils permettent de protéger et de gérer les clés indépendamment de l'environnement logiciel, ce qui vous permet de conserver le contrôle total sur vos clés.

Vos clés seront générées et gérées au sein de l'environnement sécurisé de vos HSM nShield, ce qui vous permettra de protéger vos données les plus sensibles.

Pourquoi associer les HSM de Entrust à AIP et HYOK

Les HSM de Entrust vous offrent la souplesse d'utiliser AIP comme bon vous semble pour répondre à vos besoins en matière de sécurité des données, et ce, que votre configuration soit sur site, dans le cloud ou hybride. Les HSM nShield :

- Protègent les clés au sein d'un dispositif de chiffrement certifié FIPS 140-2
- Utilisent des mécanismes de contrôle d'accès très performants avec une stricte séparation des tâches, de sorte que les clés ne puissent être utilisées qu'à leur fin autorisée
- Veillent à la disponibilité des clés en utilisant des mécanismes de gestion, de stockage et de redondance

Si vous souhaitez utiliser Azure Key Vault pour stocker vos clés et les utiliser avec AIP, Entrust vous permettra de renforcer la sécurité de vos clés. Vous pouvez générer vos clés grâce à vos HSM nShield, pour ensuite les transférer en toute sécurité à Azure Key Vault. La fonctionnalité Bring Your Own Key (BYOK) vous permet de bénéficier d'un contrôle total sur vos clés et de protéger vos données dans le cloud.

Hold Your Own Key pour une gestion de clés hautement sécurisée

Les HSM nShield d'Entrust :

- Protègent les clés au sein d'un environnement renforcé et inviolable
- Permettent d'appliquer des politiques d'utilisation des clés, dissociant les fonctions de sécurité des tâches administratives
- Respectent les réglementations et normes en vigueur relatives au secteur public, aux services financiers et aux entreprises
- Sont certifiés aux normes FIPS 140-2 et Critères Communs

Les HSM nShield d'Entrust sont le compromis idéal entre valeur et performance :

- Pour la génération et la gestion de clés en grand volume (ou dans le cadre d'un déploiement hybride), les cartes PCIe intégrées des HSM nShield Solo et les dispositifs connectés en réseau des HSM nShield Connect garantissent une protection matérielle très performante
- Les HSM nShield Connect peuvent être déployés sur les sites des utilisateurs ou bien au sein de l'environnement de nShield as a Service
- Pour la génération de clés sur site à faible volume dans le cadre de la fonctionnalité BYOK, le HSM nShield Edge procure une sécurité matérielle pratique par connexion USB

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.

Microsoft

Microsoft a révolutionné la manière dont les entreprises créent et partagent des contenus et mettent en place des mécanismes de collaboration. Les systèmes basés sur les solutions Microsoft maximisent les performances. Afin de protéger les données, Microsoft AIP utilise le chiffrement pour élaborer des environnements opérationnels fiables permettant de :

- Gérer les identifications au sein des organisations
- Distribuer des certificats d'authentification
- Contrôler les droits d'accès des utilisateurs aux ressources de données
- Assurer une protection totale des données

www.microsoft.com

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/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/HSM

ENTRUST

Nous contacter :
HSMinfo@entrust.com