La solution Entrust Double Key Encryption pour Microsoft Azure Information Protection

AVANTAGES

Renforcez le contrôle et la sécurité des données sensibles dans les environnements cloud et hybrides

- Protégez votre contenu le plus sensible avec deux niveaux de sécurité dans le cloud Azur
- Cryptez vos données de sorte que même Microsoft ne puisse pas accéder à votre contenu
- Gérez et contrôlez entièrement votre clé et le logiciel qui la génère
- Hébergez votre clé et stockez vos données sensibles à l'emplacement de votre choix
- Gérez l'accès des utilisateurs à votre clé ainsi que le contenu qu'elle protège

FONCTIONNALITÉS

Dévelopée par Entrust Professional Services, la solution Entrust Double Key Encryption pour Microsoft Azure Information Protection (AIP) permet d'aider les entreprises à protéger leur contenu sensible au sein de Microsoft 365.

- Intégration des HSM Entrust nShield® pour fournir une racine de confiance et protéger les clés client sensibles.
- Les outils et les composants laissent aux entreprises la propriété et le contrôle complet du logiciel permettant le processus de chiffrement à double clé, sans aucune infrastructure Microsoft chez les clients.

La solution de chiffrement à double clé Double Key Encryption (DKE) permet aux organisations d'utiliser des environnements hybrides avec des niveaux supplémentaires de protection, de contrôle et d'assurance. Dans le cadre de l'offre Microsoft AIP, la solution permet aux entreprises de choisir qui peut accéder aux clés associées au contenu et le déchiffrer. Les entreprises peuvent stocker les données chiffrées sur site ou dans le cloud, celles-ci restant illisibles pour Microsoft.

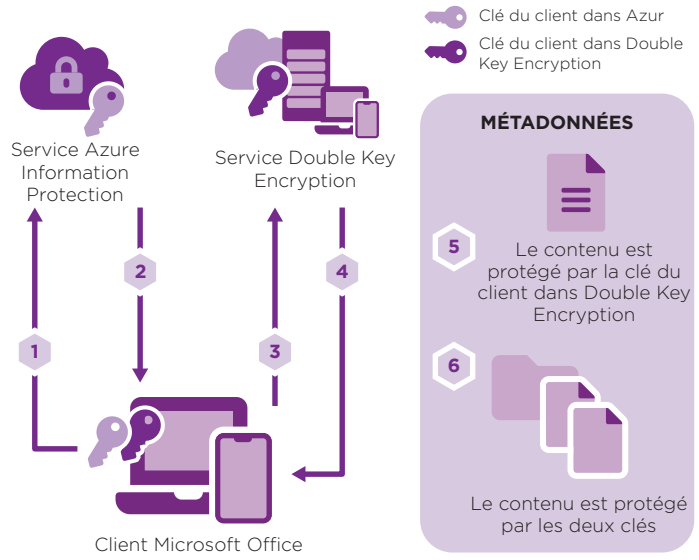
La solution Double Key Encryption remplace Microsoft HYOK (Hold Your Own Key) et n'impose pas aux entreprises d'utiliser leurs propres serveurs Active Directory et Rights Management. Au contraire, les clients sont incités à fournir leurs propres clés de chiffrement en temps réel.

Solution Double Key Encryption pour Microsoft Azure

FONCTIONNEMENT

La solution Double Key Encryption utilise deux clés de chiffrement pour protéger les données sensibles au sein de toute l'entreprise : une clé Microsoft et une clé client.

- La clé Microsoft est d'abord utilisée pour chiffrer le contenu client dans Azure.
- La clé Microsoft est chiffrée à l'aide de la clé client, qui est protégée par un HSM nShield sur site.
- Ce processus empêche Microsoft d'accéder à la clé et au contenu client dans Azure.

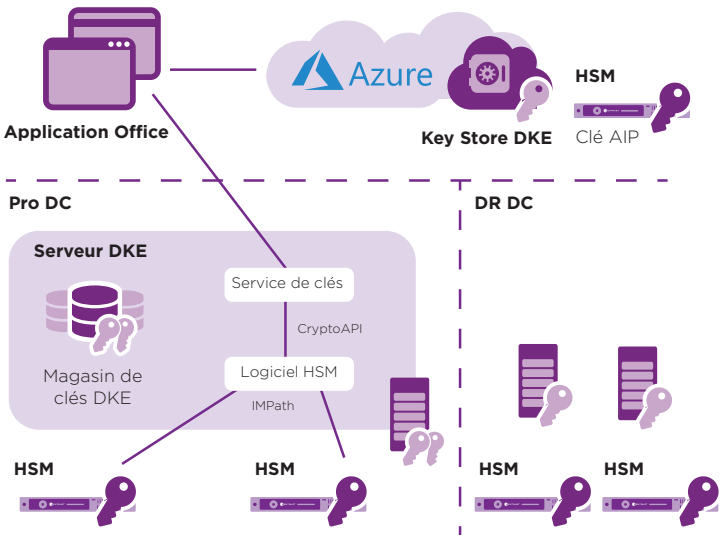


CARACTÉRISTIQUES TECHNIQUES

Intégration des HSM Entrust nShield

Les HSM Entrust nShield détiennent la clé maîtresse qui protège le serveur Double Key Encryption et le magasin de clés. Quatre HSM nShield sont généralement déployés pour assurer la redondance des environnements de production et de reprise après incident.

La solution Entrust Double Key Encryption repose sur les HSM nShield Solo XC (PCIe) et nShield Connect XC (connecté au réseau) conformes à la FIPS 140-2 Niveau 3 et certifiés Critères Communs EAL4+.



La solution Double Key Encryption pour Microsoft Azure

Démarrer

Si vous souhaitez utiliser Entrust Double Key Encryption pour Microsoft AIP, vous avez besoin des solutions suivantes :

- Entrust Double Key Encryption
- Entrust nShield Solo ou HSM nShield Connect

HSM Entrust

Les HSM Entrust nShield comptent parmi les solutions HSM les plus performantes, sûres et simples à intégrer. Ils facilitent la conformité réglementaire et offrent les plus hauts niveaux de sécurité pour les données et applications des entreprises ainsi que des organismes financiers et gouvernementaux. Notre architecture unique de gestion de clés Security World garantit des contrôles granulaires solides sur l'accès et l'utilisation des clés.

En savoir plus

Pour en savoir plus sur les HSM Entrust nShield, rendez-vous sur **entrust.com/fr/HSM.** Pour en savoir plus sur nos solutions de sécurité numérique des identités, accès, communications et données, rendez-vous sur **entrust.com.**

Pour en savoir plus sur les HSM Entrust nShield :

HSMinfo@entrust.com

www.entrust.com/fr/HSM

À PROPOS D'ENTRUST CORPORATION

Entrust permet au monde d'avancer sûrement en sécurisant les identités, les paiements et les données dans le monde entier. Aujourd'hui, les personnes exigent des expériences plus fluides et plus sûres quand elles traversent les frontières, font un achat et utilisent des services gouvernementaux en ligne ou des réseaux d'entreprise. Notre portefeuille unique de solutions pour la sécurité numérique et l'émission de titres sécurisés permet de répondre exactement à cette demande. Avec plus de 2 500 collaborateurs, un réseau de partenaires international et des clients dans plus de 150 pays, nous avons gagné la confiance des organisations les plus fiables au monde.

Pour en savoir plus, rendez-vous sur :
entrust.com

ENTRUST
Siège social
One Station Square
Cambridge CB1 2GA
Royaume-Uni
Appel international : +44 1223 723600
Appel ventes : +44 1223 723711
hsminfo@entrust.com entrust.com/contact