

Luna Key Broker for Microsoft Double Key Encryption (DKE)

Contrôle et sécurité avancés pour les données sensibles dans Microsoft Azure



Aperçu

L'environnement de télétravail actuel s'appuie fortement sur le partage collaboratif d'informations, compliquant la tâche de maintien de la sécurité des données confidentielles et de la conformité pour les organisations, tout en encourageant la productivité des employés. Pour les organisations dans des industries hautement réglementées telles que les services financiers, gouvernementaux et de santé, les données sensibles requièrent le plus haut niveau de contrôle et de sécurité.

Les HSM Luna de Thales et Double Key Encryption for Microsoft 365 s'associent pour permettre aux organisations de protéger leurs données les plus sensibles tout en conservant un contrôle total sur leurs clés de chiffrement. La solution utilise deux clés pour la protection des données. Une clé est sous le contrôle du client dans un HSM Luna certifié FIPS 140-2 niveau 3, tandis que l'autre clé est stockée en sécurité dans Microsoft Azure. Les deux clés sont requises pour accéder aux données protégées, garantissant que Microsoft et d'autres organisations tierces n'ont jamais directement accès aux données protégées.

Grâce à cette capacité de protection des données avancée, les organisations bénéficient de l'intégralité des fonctionnalités des outils de collaboration et de productivité Microsoft 365 tout en protégeant leurs données sensibles et en satisfaisant les réglementations et les exigences de confidentialité des données.

Luna Key Broker for Microsoft DKE

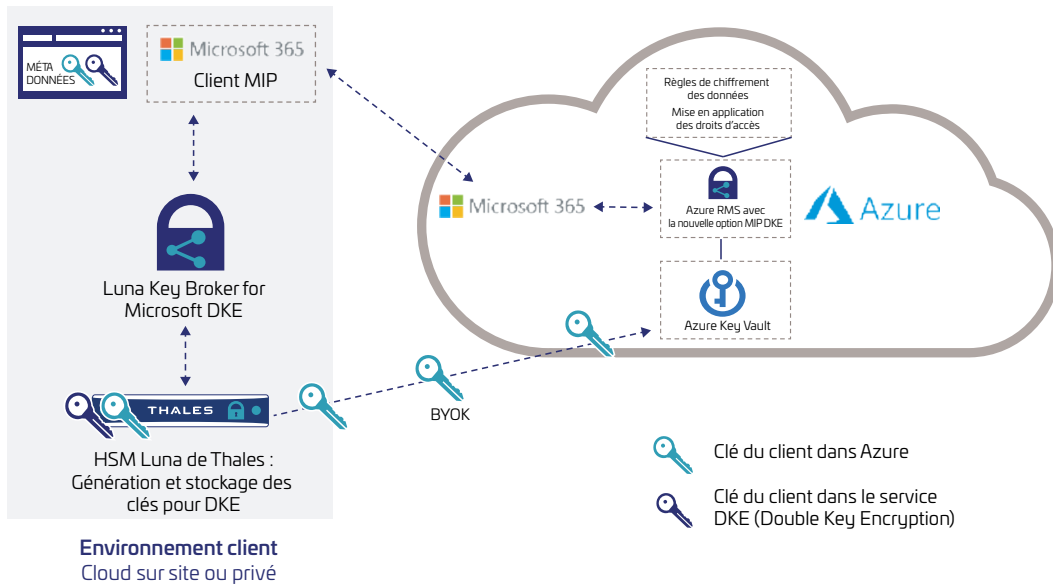
Les organisations peuvent protéger leurs données les plus sensibles en toute confiance tout en conservant le contrôle total et la pleine propriété de leur chiffrement.

Fonctionnalités et avantages de la solution :

- Contrôle avancé sur les données et les clés : Luna Key Broker for Microsoft DKE fournit une base de confiance sécurisée pour le processus de chiffrement à double clés. Seules les organisations bénéficient d'un contrôle total sur les personnes ayant l'autorisation d'accéder aux clés pour déchiffrer les données protégées.
- Gestion du cycle de vie des clés : génération sécurisée, stockage et protection des clés de chiffrement dans un HSM Luna certifié FIPS 140-2 niveau 3 en dehors de Microsoft Azure.
- Sécurité et conformité : aide à satisfaire les exigences des politiques internes et de conformité, y compris les réglementations telles que le RGPD, HIPAA et Schrems II. Les clés de chiffrement principales sont conservées dans un HSM Luna séparé de l'emplacement où les données sensibles résident. Cette configuration garantit une racine de confiance FIPS 140-2 niveau 3 ainsi qu'une séparation entre les données sensibles et les clés de chiffrement.
- Déploiement flexible : Luna Key Broker for Microsoft DKE peut se déployer dans le Cloud, sur site ou dans des environnements hybrides. La solution fonctionne avec les modules Luna Network HSM et Luna Cloud HSM.

Chiffrement de Microsoft 365 avec Luna Key Broker for Microsoft DKE

Les organisations contrôlent la clé du client dans un HSM Luna de Thales. Cette configuration garantit une racine de confiance certifiée FIPS 140-2 niveau 3 ainsi qu'une séparation entre les données sensibles et les clés de chiffrement, permettant de respecter les exigences en matière de conformité et de sécurité.



Comment ça marche ?

Double Key Encryption (DKE) utilise deux clés simultanément pour accéder aux données protégées, une clé client et une clé locataire.

Clé locataire : cette clé est stockée dans Microsoft Azure et sert à chiffrer et protéger les données sensibles d'une organisation.

Clé client : cette clé reste sous le contrôle du client et sert également à chiffrer les données, ajoutant une couche de sécurité supplémentaire. La clé client reste protégée par un HSM Luna (sur site ou dans le Cloud).

Tout utilisateur souhaitant déchiffrer et consulter les données doit avoir accès aux deux clés. Microsoft n'a accès qu'à une clé et, par conséquent, ne peut pas accéder aux données du client.

Thales est là pour vous

Thales peut aider les organisations à évaluer et définir leur stratégie et leur prise en charge DKE, y compris l'intégration et le déploiement. Pour cette solution, les organisations devront s'équiper d'un HSM Luna (sur site ou service HSM Luna Cloud) et de Luna Key Broker for Microsoft DKE.

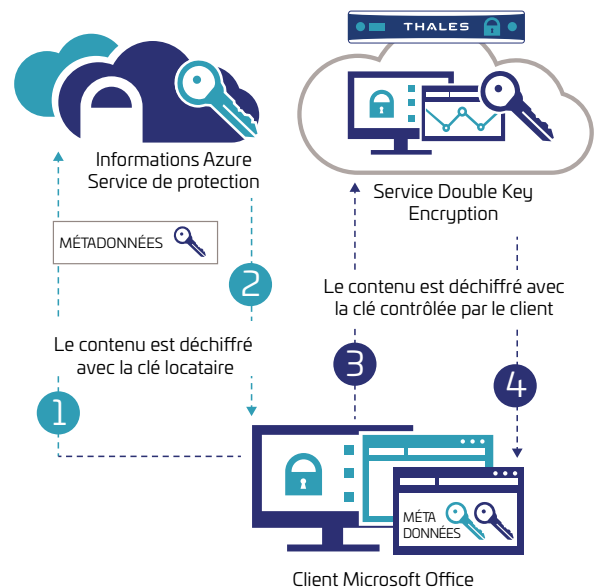
HSM Luna de Thales

Les HSM Luna de Thales ont occupé une place de leader sur le marché pendant plus de 25 ans ; ils sont la base de la sécurité numérique pour les technologies traditionnelles et émergentes dans tous les environnements, y compris hybrides et de Cloud multiple. Pour vous offrir la flexibilité nécessaire pour satisfaire vos exigences d'entreprise et de conformité avec sécurité et efficacité, Thales fournit un HSM certifié FIPS 140-2 niveau 3 à niveau d'assurance élevé pour tous les cas d'utilisation, les applications, les secteurs et les environnements.

> cpl.thalesgroup.com/fr <

Nous consulter - Pour consulter les emplacements de tous nos bureaux et nos coordonnées, veuillez vous rendre à la page cpl.thalesgroup.com/fr/contact-us

Flux de déchiffrement



Clés de chiffrement

- Clé du client dans Azure
- Clé du client dans le service DKE (Double Key Encryption)

À propos de Thales

Les personnes à qui vous faites confiance pour protéger votre vie privée font confiance à Thales pour protéger leurs données. En matière de sécurité des données, les entreprises sont confrontées à un nombre croissant de moments décisifs. Qu'il s'agisse de mettre en place une stratégie de chiffrement, de passer au Cloud ou de respecter les obligations de conformité, vous pouvez compter sur Thales pour sécuriser votre transformation numérique.

Une technologie décisive pour des moments décisifs.