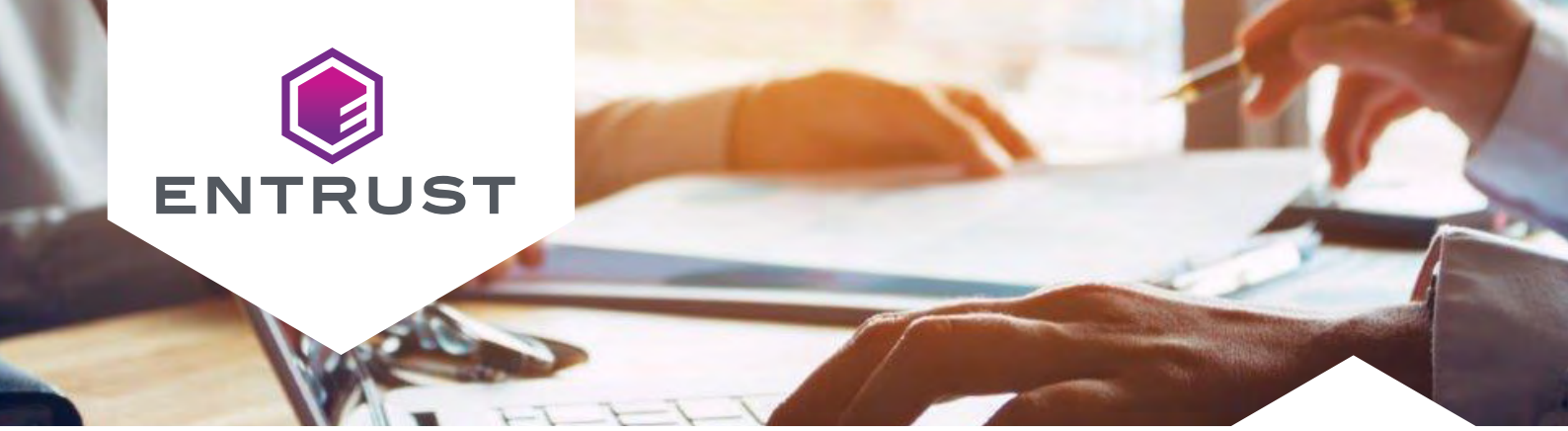


Entrust et les fournisseurs de tokénisation renforcent la sécurité des données et la conformité

NFINITY STRATEGIC TECHNOLOGY PARTNER PROGRAM

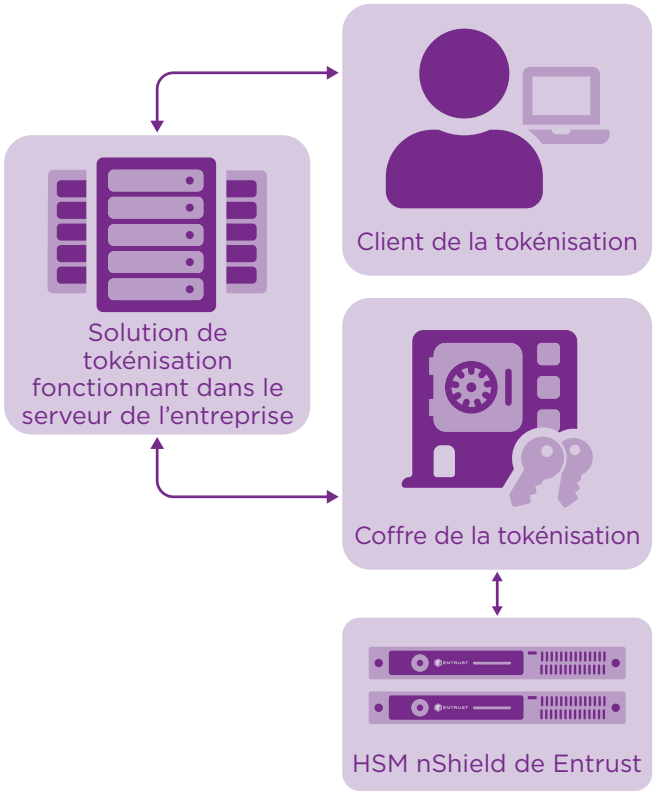
Une tokénisation et une conformité renforcées avec les modules matériels de sécurité (HSM) nShield de Entrust

CARACTÉRISTIQUES

- Protéger les données sensibles inactives, utilisées et en mouvement
- Réduire l'étendue et les coûts des audits de conformité
- Éviter de perturber les applications en utilisant une tokénisation qui préserve le format
- Sécuriser les clés de chiffrement dans un module matériel de sécurité certifié FIPS 140-2 niveau 3 inviolable
- Générer des nombres aléatoires avec une source d'entropie certifiée et conforme

Le défi :

Dans tous les secteurs, les entreprises accumulent et transmettent des données plus sensibles que jamais auparavant, ce qui augmente le risque d'attaque par des cybercriminels cherchant à monétiser les données privées. L'existence de marchés secondaires pour ces données rend les données à caractère personnel, les numéros de cartes de paiement et les dossiers médicaux particulièrement vulnérables.



Les HSM nShield hébergent la clé racine principale de la fonction de tokénisation et peuvent également exécuter des fonctions critiques à l'intérieur de leur dispositif sécurisé en utilisant l'exécution de code sécurisé CodeSafe.

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

Amélioration de la sécurité des données et de la conformité

En réponse, les organisations se sont tournées vers la tokénisation pour réduire le risque d'exposition des données. La tokénisation remplace une valeur réelle par un jeton aléatoire qui conserve le même format et le même type que les données d'origine. Cela permet aux applications et bases de données existantes de reconnaître et de traiter le jeton de la même manière que les données d'origine. Par exemple, lorsqu'un représentant du service clientèle ajoute des informations au dossier d'un client, des champs spécifiques peuvent être immédiatement tokénisés afin de les protéger contre tout accès non autorisé. Selon l'architecture, les valeurs réelles sont chiffrées et stockées dans un coffre séparé ou, dans une approche sans coffre, le jeton est généré par un algorithme, ce qui évite de devoir stocker les données réelles.

Parce que les données sont dévaluées, la tokénisation améliore leur sécurité tout en réduisant le risque de vol. Cela peut également renforcer la conformité aux mandats tels que le Standard de Sécurité des Données PCI, qui indique que les organisations peuvent efficacement réduire leur portée PCI DSS par l'utilisation d'un système de tokénisation conforme.

Lorsqu'elle met en œuvre un système de tokenisation, une entreprise doit s'assurer qu'il est conçu pour empêcher l'inversion des jetons qui révélerait les données d'origine. Cela est essentiel pour garantir que les données sensibles restent sécurisées et que l'organisation respecte les mandats relatifs à la protection des données.

La solution : une tokénisation intégrée aux HSM nShield de Entrust

Une solution de tokénisation robuste commence par le processus de génération de jetons. Les meilleures pratiques reconnues en matière de génération de jetons préconisent soit la tokénisation aléatoire, soit la tokénisation par chiffrement, associée à un stockage sécurisé des clés de chiffrement. Les directives de la PCI relatives aux jetons précisent que « les clés de chiffrement doivent être gérées et protégées conformément aux exigences de la PCI DSS… Les clés de chiffrement utilisées pour la génération des jetons et la détokénisation ne doivent donc être accessibles à aucune application, aucun système, utilisateur ou processus en dehors du système de jetons sécurisé ».[1]

Les HSM nShield® de Entrust sont intégrés aux solutions de tokénisation de premier plan. Ils établissent des tableaux de référence de clés de chiffrement aléatoires et hautement sécurisées qui sont utilisées dans le processus de génération des jetons. Le générateur de nombres aléatoires du HSM nShield a été certifié comme une source d'entropie conforme à la norme FIPS. Cela permet aux organisations de créer des jetons hautement sécurisés qui ne peuvent être inversés par des utilisateurs non autorisés. Le HSM nShield génère et protège également les clés utilisées pour chiffrer les tableaux de référence.

Lorsque l'architecture de tokénisation intègre un coffre séparé de données originales, les clés de chiffrement qui aident à protéger les données du coffre sont générées par un HSM nShield et sécurisées dans celui-ci.

1. https://www.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf

Amélioration de la sécurité des données et de la conformité

La différence nShield de Entrust

Les HSM nShield de Entrust protègent les clés de chiffrement dans un environnement certifié et inviolable. Les clés de chiffrement traitées en dehors des limites de chiffrement d'un HSM nShield sont nettement plus vulnérables aux attaques, ce qui peut mener à la divulgation d'informations confidentielles. Les HSM représentent le seul moyen éprouvé et vérifiable de protéger ses documents chiffrés importants. Les HSM nShield permettent de :

- Sécuriser les clés et les certificats au sein d'un dispositif de chiffrement soigneusement conçu
- Utiliser des mécanismes de contrôle d'accès robustes afin que les clés ne soient utilisées que pour leur usage autorisé
- Veiller à la disponibilité en utilisant des fonctions très élaborées de gestion des clés, de stockage et de redondance qui garantissent que les clés sont toujours accessibles lorsque l'on en a besoin
- Fournir des performances élevées pour supporter des volumes importants de tokénisation
- Être conforme aux exigences réglementaires pour les services financiers, le commerce de détail et les autres secteurs

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**

MICRO FOCUS Voltage

PrimeFactors™ — Applied Data Protection —

Pour en savoir plus sur les HSM nShield d'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