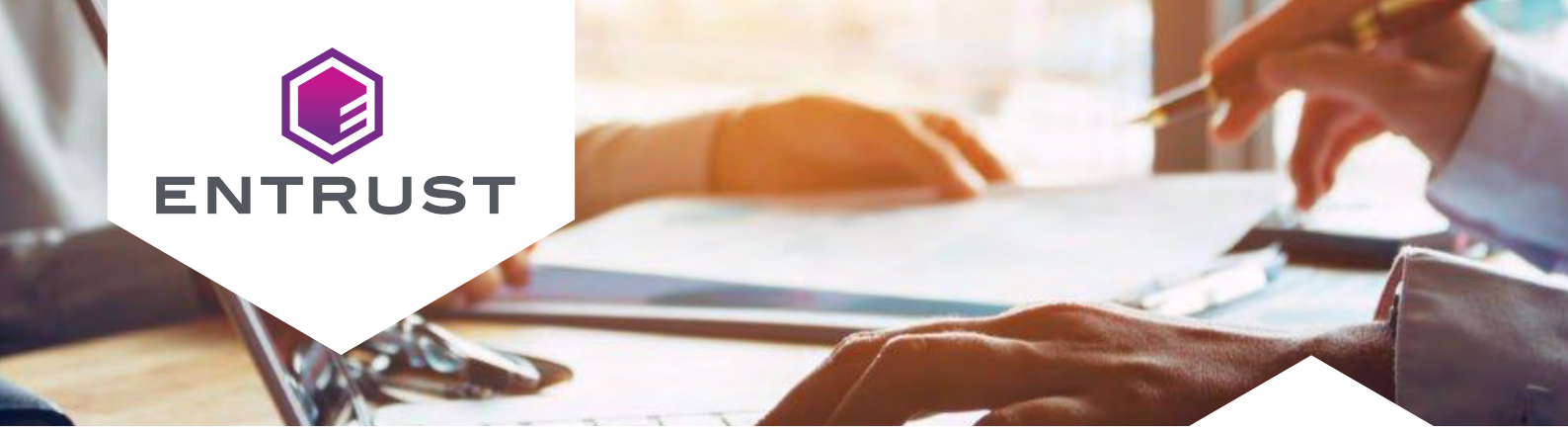


Sécuriser les infrastructures à clés publiques avec les HSM nShield de Entrust

STRATEGIC TECHNOLOGY PARTNER PROGRAM

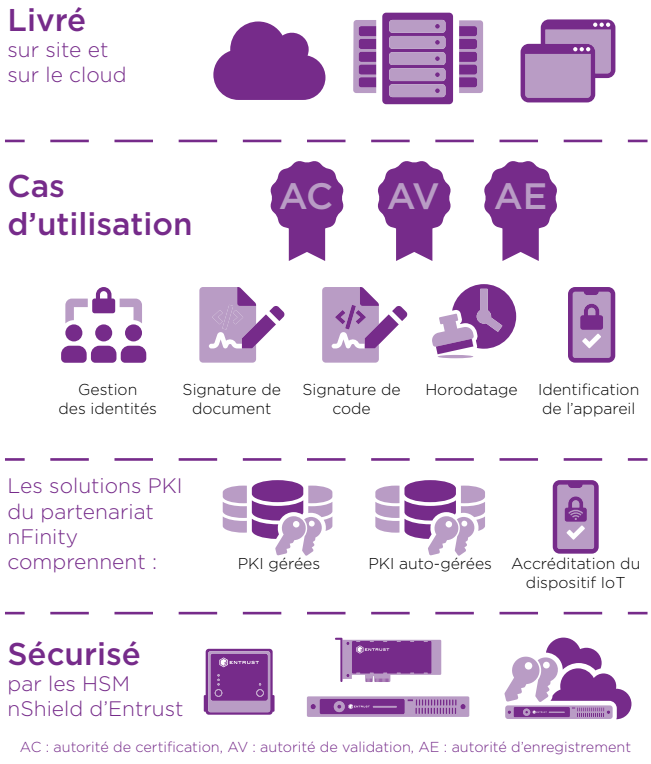
Une protection de haut niveau pour les clés renforçant les PKI

CARACTÉRISTIQUES

- Protéger la racine critique et les clés de la CA émettrice au sein d'un HSM inviolable certifié FIPS 140-2 de niveau 3
- Établir une authentification forte pour les appareils connectés
- Faciliter l'audit et le respect de la législation en vigueur sur la protection des données
- Bénéficier de meilleurs niveaux de fiabilité et de sécurité des données
- Conserver des niveaux élevés de service et de réactivité commerciale

Le défi :

La numérisation des entreprises et l'Internet des objets (IoT) en plein essor mettent clairement en évidence la nécessité d'établir des identités fiables pour les utilisateurs, les appareils et les applications qui accèdent aux systèmes et aux données. Des identités uniques et traçables pour les utilisateurs et les appareils permettent d'augmenter les revenus et de réduire les coûts grâce à de nouveaux produits, services et méthodes de travail.



AC : autorité de certification, AV : autorité de validation, AE : autorité d'enregistrement

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

Sécuriser les infrastructures à clés publiques avec les HSM nShield de Entrust

Pour tirer parti de ces possibilités et sécuriser les systèmes et les données, il est essentiel de s'assurer que :

- Les utilisateurs qui gèrent l'appareil ou le système sont autorisés à le faire
- Le code fonctionnant sur les appareils connectés, y compris les micrologiciels, le système d'exploitation et les applications, est fiable et n'a pas été altéré
- Les données qui circulent entre les appareils, les personnes et les applications sont valides et protégées contre les modifications non autorisées
- Les transactions financières peuvent être sécurisées et authentifiées

Une infrastructure à clé publique (PKI) fournit un mécanisme par lequel il est possible d'établir et de gérer des identités authentiques pour les utilisateurs et les dispositifs, également appelés entités. Une fois authentifiées, ces entités peuvent accéder aux systèmes et ressources critiques de l'entreprise, ainsi qu'à des opérations complètes de signature numérique. Une PKI repose sur des certificats numériques, signés par une autorité de certification (CA), qui lient une clé publique à un utilisateur ou à un dispositif spécifique. En partant de là, la racine et les clés privées de la CA émettrice sont des cibles de choix qui nécessitent une protection de haut niveau, car elles représentent les clés virtuelles du royaume.

La solution : des solutions de PKI intégrées aux HSM nShield de Entrust

Il est possible de déployer une PKI sans base de confiance matérielle, mais les clés de CA traitées hors du périmètre de chiffrement d'un module matériel de sécurité (HSM) certifié peuvent être vulnérables aux attaques qui compromettent l'émission d'identifiants de PKI et les capacités de révocation de certificats.

L'utilisation de HSM est une meilleure pratique reconnue pour protéger la racine et les clés privées de la CA émettrice qui soutiennent les déploiements de la PKI.

Les HSM nShield® de Entrust sont intégrés aux principaux fournisseurs de PKI pour offrir une protection FIPS 140-2 niveau 3 et Critères communs EAL 4+ pour la racine et les clés privées de la CA émettrice. Les clients bénéficient d'un niveau de sécurité renforcé et sont en mesure de démontrer leur conformité à des exigences telles que la norme de sécurité des données de l'industrie des cartes de paiement.

Pourquoi choisir nShield

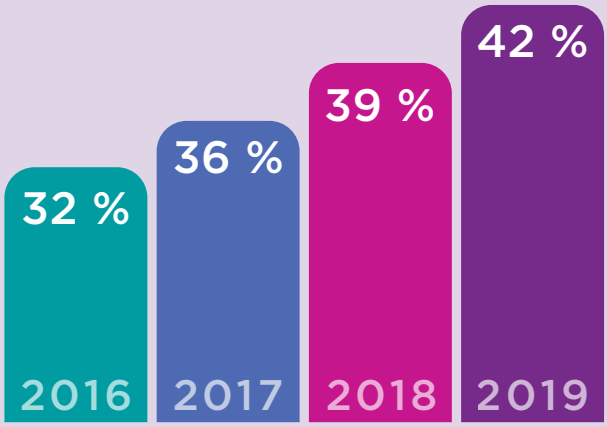
Les HSM nShield de Entrust sont un moyen éprouvé et vérifiable de protéger ses clés et documents chiffrés importants. Les HSM nShield certifiés FIPS et Critères Communs permettent de :

- Sécuriser les clés au sein d'un dispositif de chiffrement soigneusement conçu
- Utiliser des mécanismes de contrôle d'accès très performants avec une stricte séparation des tâches, pour garantir que les clés ne sont utilisées que par les entités autorisées
- Veiller à la disponibilité des clés en utilisant des mécanismes de gestion, de stockage et de redondance avancés
- Obtenir des performances supérieures afin de pouvoir prendre en charge un nombre croissant d'applications exigeantes
- Disposer d'une évolutivité permettant de répondre à l'évolution de la demande grâce à une meilleure gestion

Les HSM nShield de Entrust sont disponibles sous de multiples formes, tandis que nShield en tant que Service fournit un accès par abonnement aux HSM nShield Connect.

Sécuriser les infrastructures à clés publiques avec les HSM nShield de Entrust

Comment gérez-vous les clés privées de votre base/politique/CA émettrice ?



Les modules matériels de sécurité (HSM)

Source : Étude mondiale 2019 sur les tendances des PKI, Ponemon Institute et Entrust

« Les PKI des organisations soutiennent en moyenne 8,5 applications différentes. Cela indique que la PKI est au cœur de l'ossature informatique de l'entreprise. »

Étude mondiale 2019 sur les tendances des PKI, Ponemon Institute et Entrust

Partenariat nFinity

Les HSM nShield de Entrust sont intégrés avec les fournisseurs de PKI suivants par le biais de notre Programme de partenariat technologique nFinity. Veuillez vous rendre sur notre site web pour la liste complète des partenaires.

axway
KEYFACTOR
cybertronixx
Microsoft
nexus
DEVICE AUTHORITY
IoT Security Simplified
PrimeKey
digicert®
Red Hat
Entrust Datacard
RSA SECURITY™
HID
HID CORPORATION
SAFELAYER
INSTA
TRUSTONIC
Information Security CORPORATION

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 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