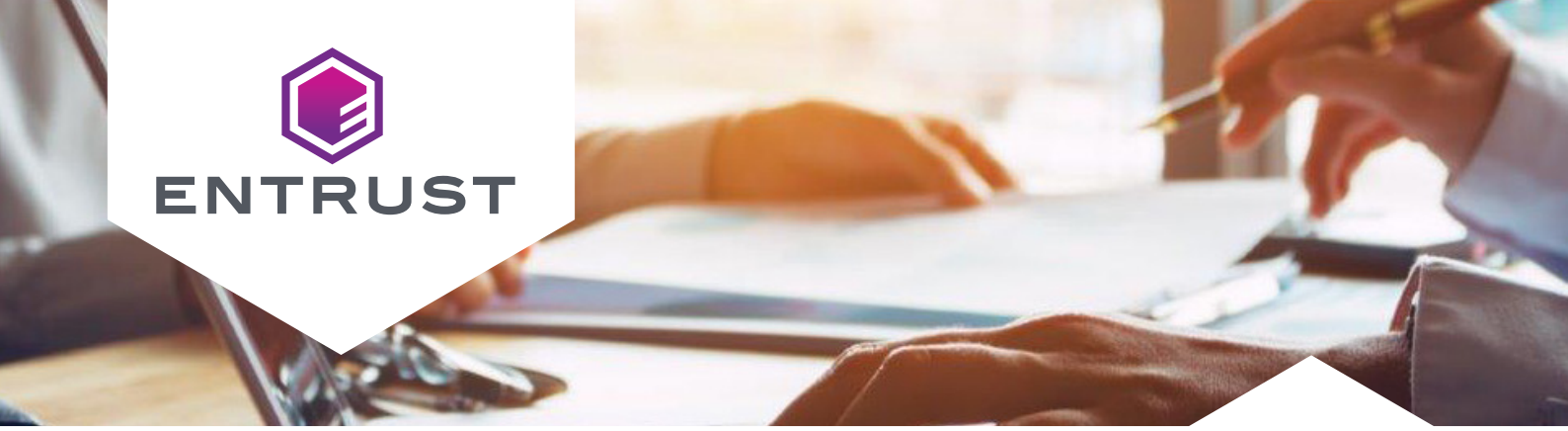

Les solutions de confiance d'Entrust permettent la transformation numérique des entreprises

Les solutions intégrées améliorent la sécurité des PKI déployées

CARACTÉRISTIQUES

- Sécurisation de l'identité des utilisateurs sur les applications de l'entreprise
- Contrôle des accès aux déploiements sur site et hébergés
- Gestion du cycle de vie du certificat, dont la sauvegarde et la récupération
- Racine de confiance pour la protection des clés privées sensibles
- Facilitation de la mise en conformité avec FIPS et les critères communs
- Prise en charge des déploiements sur site, dans le cloud et hybride

L'enjeu : augmentation du besoin d'identités de confiance dans un système en expansion rapide

L'Internet des Objets (IoT), la prolifération des appareils mobiles et la naissance de nouvelles exigences telles que la prise en charge de l'émission de certificats pour les appareils des programmes Bring Your Own Device (BYOD) et l'enrôlement des appareils IoT en réseau font de la solidité de la gestion des identités un facteur plus important que jamais. Les solutions d'infrastructure à clé publique (PKI) sont idéales pour établir des identités de confiance pour les utilisateurs, les appareils, les applications et les services afin de sécuriser l'accès aux systèmes et aux ressources critiques de l'entreprise, ce qui est un élément crucial de la sécurité d'un environnement.

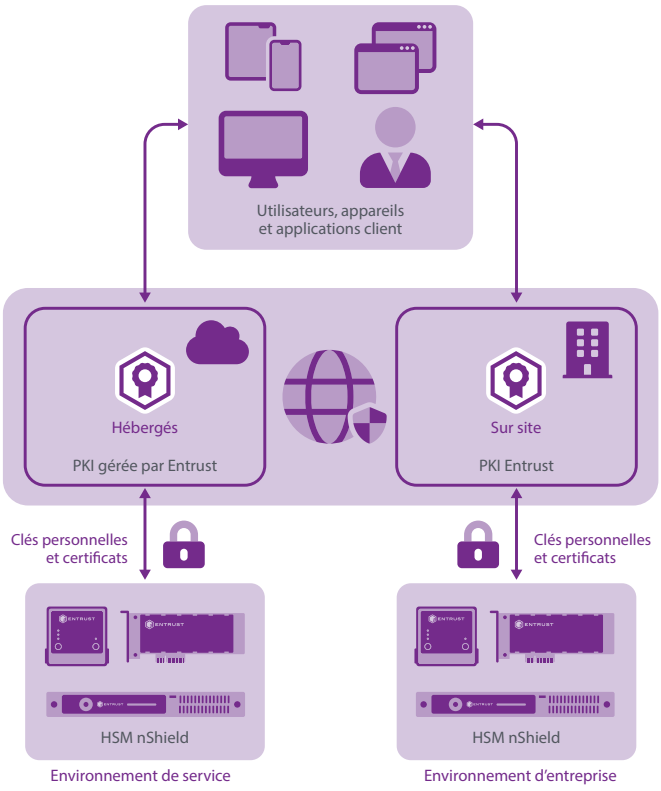

Illustration détaillée des composants utilisés dans un déploiement typique d'administration à distance

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

Les solutions de confiance d'Entrust permettent la transformation numérique des entreprises

Le défi : sécuriser la gestion des clés de l'autorité de certification (AC)

La robustesse de la protection des clés privées utilisées par les PKI sur site ou hébergées est un aspect indispensable d'une bonne stratégie de sécurité. Le niveau de confiance d'une PKI dépend du niveau de protection des clés privées dans la hiérarchie de l'AC et des processus de vérification associés. Les clés de la CA stockées et gérées par des logiciels peuvent être vulnérables aux menaces sophistiquées qui peuvent compromettre la sécurité. Une gestion des clés matérielle dédiée améliore la sécurité et réduit le risque pour un écosystème commercial de confiance.

La solution : une solution intégrée avec une base de confiance solide

Les solutions de PKI d'Entrust prennent en charge la mise en place et la gestion de la sécurité basée sur les certificats pour les applications commerciales critiques. Le gestionnaire de sécurité d'Entrust permet aux clients de déployer et de gérer leurs propres certificats numériques. Le produit authentifie les utilisateurs, contrôle les accès et sécurise les applications de chiffrement. Pour les clients qui souhaitent une approche passive, la PKI gérée par Entrust propose une solution hébergée.

Les modules matériels de sécurité (HSM) nShield® d'Entrust s'intègrent aux solutions de PKI d'Entrust afin de protéger la confidentialité et l'intégrité de vos clés sensibles. Les organisations qui souhaitent développer la sécurité de leurs PKI sur site ou hébergées peuvent déployer les solutions Entrust avec les HSM nShield sur site ou en tant que service afin que leurs clés critiques ne soient jamais exposées à des entités non-autorisées. Les HSM nShield génèrent, stockent et gèrent de manière sécurisée les clés privées de l'AC.

Pourquoi utiliser nShield avec Entrust Security Manager et la gestion de PKI ?

Il est possible de déployer des PKI sans racine de confiance matérielle, mais les clés d'AC traitées hors du périmètre de chiffrement d'un HSM certifié sont beaucoup plus vulnérables aux attaques pouvant compromettre l'émission d'identifiants de PKI et les capacités de révocation de certificats.

L'utilisation de HSM est largement considérée comme la meilleure pratique pour les déploiements de PKI, car ils sont un moyen éprouvé et vérifiable de protéger les données de chiffrement cruciales. Les HSM permettent aux organisations de :

- sécuriser les clés de l'AC dans des limites de chiffrement rigoureusement définies utilisant des mécanismes de contrôle d'accès très performants et une séparation des responsabilités strictes, de sorte que les clés ne puissent être utilisées que par les entités autorisées
- veiller à la disponibilité en utilisant des fonctions très élaborées de gestion des clés, de stockage et de redondance qui garantissent que les clés soient toujours accessibles lorsque l'on en a besoin
- obtenir des performances supérieures afin de pouvoir prendre en charge un nombre croissant d'applications exigeantes

La certification Entrust Ready des HSM nShield assure l'interopérabilité, la facilité du déploiement et l'amélioration de la sécurité.

Les solutions de confiance d'Entrust permettent la transformation numérique des entreprises

Les HSM nShield d'Entrust sont des appareils de chiffrement à hautes performances conçus pour générer, protéger et gérer les clés sensibles. En plus de respecter des normes de sécurité très strictes, les HSM nShield d'Entrust :

- stockent les clés dans un environnement sécurisé et inviolable
- respectent les réglementations et normes en vigueur relatives au secteur public, aux services financiers et aux entreprises
- permettent d'appliquer des politiques d'utilisation des clés, dissociant les fonctions de sécurité des tâches administratives
- prennent en charge la cryptographie sur les courbes elliptiques (ECC)

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

- HSM nShield Edge : HSM portable USB pour une configuration AC racine hors ligne à faible volume
- HSM nShield Solo+ et Solo XC : HSM PCIe hautes performances intégré pour les serveurs et les applications de sécurité
- HSM nShield Connect+ et Connect XC : HSM hautes performances liés au réseau pour les environnements à disponibilité élevée
- nShield as a Service : option d'abonnement à hautes performances pour plus de flexibilité et un coût moindre

Les HSM d'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.

En savoir plus

Pour en savoir plus sur les HSM nShield d'Entrust, rendez-vous sur **entrust.com/fr/HSM**. Pour en savoir plus sur les solutions de protection numérique d'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