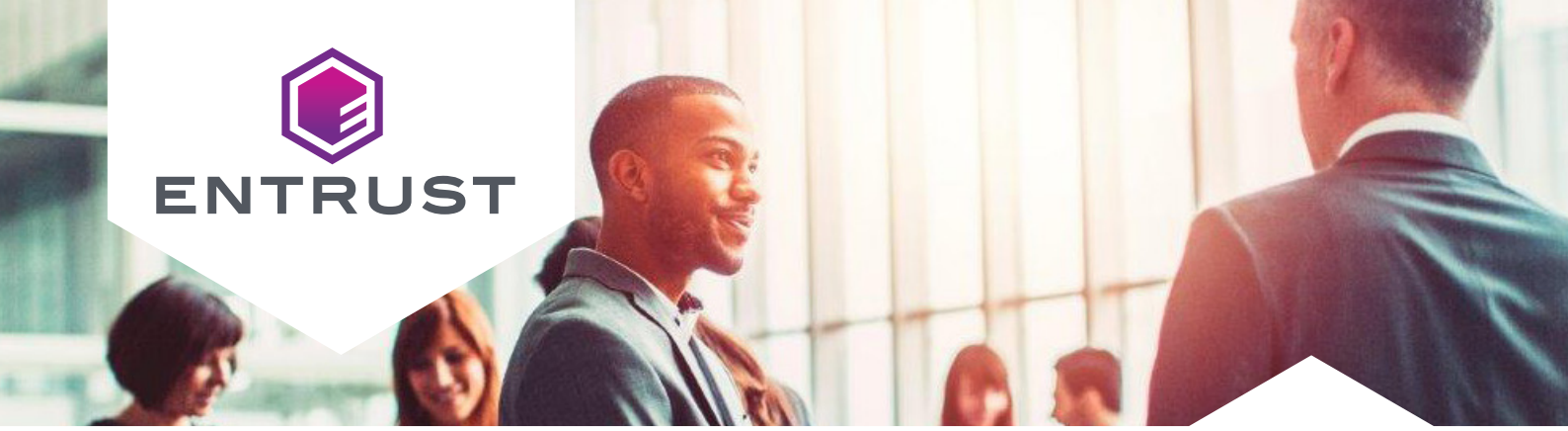


Entrust fournit des solutions PKI auto-gérées pour répondre aux besoins de sécurité spécifiques des entreprises

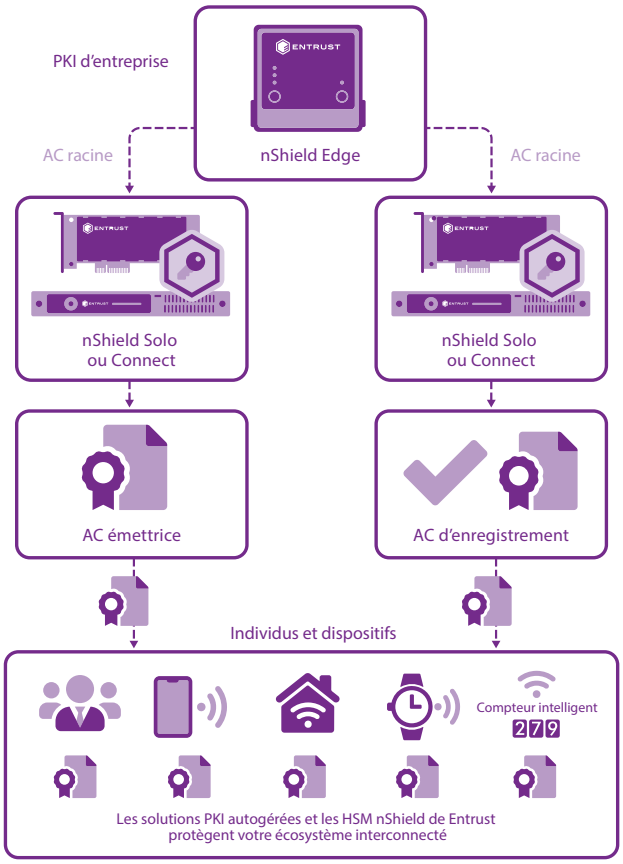
Déployer et maintenir des solutions de gestion d'identité sécurisées avec les services Entrust et les modules matériels de sécurité (HSM)

CARACTÉRISTIQUES

- Protéger l'identité des personnes et du dispositif
- Développer le processus et les procédures appropriés
- Évaluer l'état d'intégrité des déploiements PKI existants
- Migrer les PKI pour répondre à la demande croissante
- Faciliter l'audit et le respect de la conformité en matière de sécurité

L'enjeu : le recours grandissant aux technologies interconnectées met à rude épreuve les capacités des infrastructures à clé publique (PKI) existantes et entraîne la nécessité d'en créer de nouvelles.

L'utilisation croissante des applications de chiffrement et l'impact de l'Internet des objets (IoT) créent de nouvelles demandes sans précédent pour les PKI. La hausse des exigences en matière d'accréditation et la nécessité de gérer la manière dont les dispositifs et les capteurs se connectent en toute sécurité à des écosystèmes de réseau proches poussent les entreprises à réévaluer l'intégrité de leurs PKI existantes. Parallèlement à l'évolution des normes de sécurité, les entreprises repensent leurs stratégies de mise en œuvre de PKI et, dans certains cas, reconçoivent et migrent vers de nouveaux déploiements plus robustes.



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

Des solutions PKI auto-gérées pour répondre aux besoins de sécurité spécifiques des entreprises

Le défi : maintenir une base de confiance solide dans la PKI d'entreprise qui répond aux exigences opérationnelles des applications plus sensibles en matière de sécurité

Avec de plus en plus d'applications sensibles en termes de sécurité ayant recours à des PKI, la sécurité des clés privées fondamentales est essentielle. Selon l'étude des tendances en matière de PKI 2020 du Ponemon Institute, les trois principales applications utilisant des certificats numériques comprennent le SSL/TLS pour les sites web publics, les applications publiques dans le cloud et l'authentification des utilisateurs en entreprise. Les certificats numériques permettent l'identification des applications et des dispositifs et l'authentification dans des écosystèmes de confiance. Cela nécessite de protéger et de gérer un nombre croissant de clés privées de manière automatisée et fiable.

La solution : les offres de PKI autogérées d´Entrust combinent des services de conseil avec le matériel de sécurité adéquat pour aider le client à définir ses besoins, à déployer la solution et à former son personnel

Les exigences des entreprises en matière de PKI sont généralement uniques et dépendent de leur activité, de leurs clients et des applications qu'elles prennent en charge. Les offres de PKI autogérées d´Entrust combinent l'expertise technique dans la conception et la mise en œuvre de PKI organisationnelles, avec le matériel de sécurité nécessaire pour fournir une racine de confiance solide pour le système.

Les services comprennent l'évaluation initiale des besoins et le développement de processus et de procédures, ainsi que la conception et la mise en œuvre de l'infrastructure nécessaire pour que les clients puissent déployer des PKI qui répondent aux exigences actuelles et futures. Les conseillers peuvent soutenir les paramètres opérationnels nécessitant une haute disponibilité et une redondance, ou les environnements de laboratoire pour aider les clients à développer leurs propres ensembles de compétences en matière de PKI. Pour les clients qui déploient des PKI pour la première fois, les offres comprennent des services de documentation et de déploiement combinés à du matériel de sécurité. Pour les clients dont les déploiements de PKI sont déjà en cours ou en expansion, les offres comprennent des diagnostics et des services de migration, y compris le service de migration SHA avec le matériel de sécurité.

Les modules matériels de sécurité (HSM) nShield® de Entrust augmentent le niveau de sécurité des déploiements PKI. Conçus pour protéger et gérer la clé privée fondamentale dans un environnement isolé certifié, les HSM nShield de Entrust prennent en charge les PKI de Microsoft, Red Hat, Entrust, RSA et Insta en utilisant des interfaces de programmation d'applications de chiffrement (CAPI) standard.

Des solutions PKI auto-gérées pour répondre aux besoins de sécurité spécifiques des entreprises

Pourquoi utiliser les HSM de Entrust avec des PKI auto-gérées ?

Le déploiement de davantage d'applications sensibles en matière de sécurité et de dispositifs connectés impose une demande accrue vis-à-vis des PKI, qui doivent non seulement protéger les clés privées de l'autorité de certification racine (AC) des certificats individuels et de dispositifs délivrés dans les différents domaines, mais aussi leur enregistrement. Les PKI organisationnelles qui n'utilisent pas de HSM pour protéger leurs clés privées sont vulnérables et peuvent subir des perturbations dont les conséquences peuvent être graves. Les HSM créent un environnement plus robuste qui protège les clés cruciales pour la sécurité contre le vol et les usages non-autorisés, et permettent également la gestion du cycle de vie complet avec une prise en charge du basculement. Les failles de sécurité des AC nous ont appris une leçon importante, notamment le fait qu'il est essentiel de relier l'émission des certificats à l'identité et à l'approbation à l'aide d'un HSM. En plus de respecter des normes de sécurité très strictes comme FIPS 140-2 niveau 3 et Critères Communs EAL4+, les HSM nShield d'Entrust :

- Stockent l'AC racine et les clés d'enrôlement dans un environnement inviolable et sécurisé
- Gèrent les accès administrateurs avec une politique basée sur des cartes intelligentes et une authentification à deux facteurs
- Respectent les réglementations et normes en vigueur relatives au secteur public, aux services financiers et aux entreprises

Entrust

Simplifiant la gestion des justificatifs d'identité dans toute l'entreprise, y compris les environnements virtualisés, les HSM nShield d'Entrust aident les organisations à répondre aux exigences d'audit et de conformité telles que la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) et la Directive sur les Services de Paiement (DSP2). Les HSM nShield sont disponibles dans les modèles suivants pour répondre aux besoins spécifiques des clients :

- HSM nShield Edge : HSM portable USB pour une configuration AC racine hors ligne et pour les applications de développeur
- HSM nShield Solo/Solo+/Solo XC : hautes performances PCI Express intégrées pour les serveurs
- HSM nShield Connect/Connect+/Connect XC : hautes performances liées au réseau pour les centres de données

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 de 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