Sécurité renforcée : la protection de clés hautement sécurisée d´Entrust pour le Red Hat Certificate System

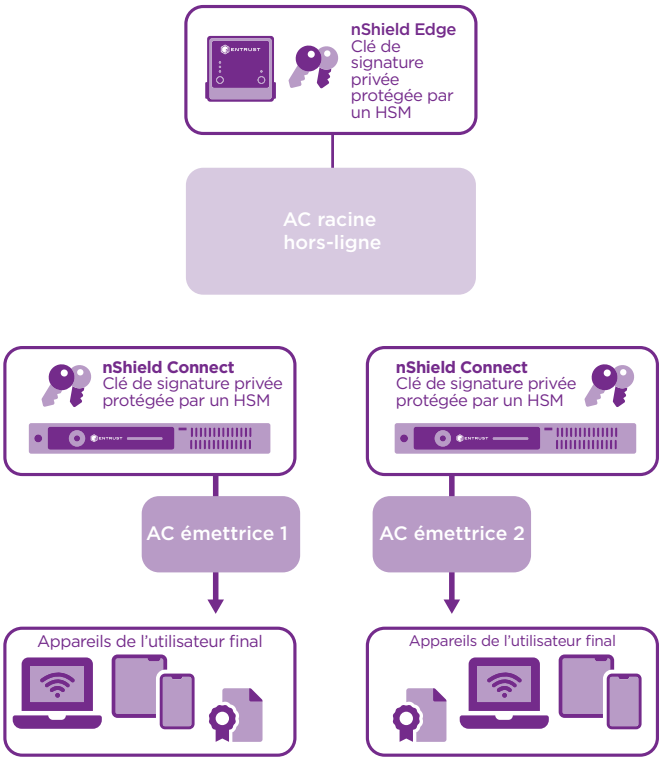
Établir une racine de confiance pour l'infrastructure à clés publiques (PKI)

CARACTÉRISTIQUES

- Étendre la sécurité de Red Hat Certificate System pour les solutions commerciales de la NSA pour les applications classifiées (CSfC)
- Renforcer le cadre de sécurité en gérant les identités des utilisateurs et en préservant la confidentialité des communications
- Protéger les transactions et les applications compatibles PKI
- Utilisez les modules matériels de sécurité (HSM) nShield® de Entrust certifiés NIST FIPS 140-2

L'enjeu : les PKI organisationnelles sont mises à rude épreuve pour répondre au nombre croissant d'applications commerciales

Les violations de données devenant de plus en plus sophistiquées, les organisations se sont tournées vers leurs PKI pour protéger et contrôler l'accès aux applications critiques et aux données sensibles. Dans le cadre d'une PKI, l'autorité de certification (AC) délivre des justificatifs électroniques pour valider les identités en ligne et faire respecter les contrôles d'accès. L'analyse du nombre de certificats numériques utilisés, de l'importance et de la valeur des applications qu'ils prennent en charge, et de la question de savoir si les applications sont soumises à un niveau d'examen plus élevé en raison de la conformité réglementaire du gouvernement ou du secteur ; tous sont des facteurs essentiels pour garantir que la PKI peut répondre aux demandes croissantes.



Les HSM nShield sécurisent les clés privées utilisées par le Red Hat Certificate System.

La protection de clés hautement sécurisée d´Entrust pour le Red Hat Certificate System

Le défi : établir une racine de confiance pour les contrôles d'identité et d'accès

La protection de l'intégrité et de la sécurité de l'AC qui dépend de la PKI est d'une importance capitale pour garantir la confiance dans les applications commerciales et les données qu'elles protègent. Étant donné que les PKI prennent de plus en plus en charge les topologies d'accès utilisateur changeantes, y compris l'accès mobile et le Bring Your Own Device (BYOD), les organisations doivent s'assurer que les clés de chiffrement privées sont protégées et gérées en toute confiance.

La solution : Red Hat et Entrust fournissent ensemble une protection robuste des identités numériques

Red Hat Certificate System émet, gère et valide les identités numériques utilisées pour lier des personnes, des appareils ou des services à leurs clés privées correspondantes. La validité de chaque certificat délivré dépend de la protection de la clé de l'AC qui délivre les identités. Lorsque le processus d'émission est exécuté sur un serveur à l'aide d'une clé stockée localement dans un fichier, cette clé peut être vulnérable à la duplication, à la modification et au remplacement. Aujourd'hui, la plupart des AC sont utilisées pour délivrer des certificats destinés à être utilisés au sein d'une organisation. En interne, les certificats sont généralement utilisés pour effectuer l'authentification avec et sans fil, les connexions SSL/TLS et l'authentification des réseaux privés virtuels (VPN). Comme les applications en expansion ont besoin des services d'une PKI, les exigences imposées aux AC et la nécessité de mettre en place une sécurité renforcée sont primordiales.

Les HSM nShield augmentent le niveau de sécurité de la PKI en protégeant la racine privée et en signant les clés de l'AC. Les HSM nShield protègent les processus d'émission, de gestion et de validation, permettant aux organisations de renforcer la solution d'identité et d'accès. Les HSM nShield s'intègrent facilement au Red Hat Certificate System en utilisant des interfaces de programmation d'applications de chiffrement (CAPI) standard. Lorsque les HSM nShield de Entrust sont utilisés, tous les processus de délivrance et de validation des certificats se déroulent dans les limites protégées des HSM. Les clés privées principales et de signature ne sont jamais accessibles ou dans un format lisible en dehors du HSM. Même pendant les processus de sauvegarde, d'archivage et de récupération, les HSM nShield garantissent que les clés privées ne sont pas susceptibles d'être manipulées et/ou compromises.

La protection de clés hautement sécurisée d´Entrust pour le Red Hat Certificate System

Pourquoi utiliser les HSM de Entrust avec le Red Hat Certificate System ?

L'identification des violations, la récupération et la planification d'urgence sont des mesures importantes qui peuvent être prises pour renforcer la sécurité d'une PKI. Une PKI renforcée et hautement sécurisée offre un environnement qui protège les clés essentielles à la sécurité contre le vol et l'utilisation abusive. Les failles de sécurité passées des AC nous ont appris une leçon importante, notamment le fait qu'il est important de relier l'émission des certificats à l'identité et à l'approbation à l'aide d'un HSM nShield d'Entrust.

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 les clés pour la signature et l'émission de certificats numériques dans un environnement sécurisé et inviolable
- 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

Les HSM de 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.

Red Hat

Red Hat est le premier éditeur mondial de solutions logicielles Open Source pour les entreprises. En plus du Red Hat Certificate System, les solutions comprennent les plateformes Red Hat Enterprise Linux, Red Hat OpenStack et Red Hat OpenShift, parmi une large gamme de gestion et de services. Les HSM nShield de Entrust sont certifiés avec le Red Hat Certificate System. **www.redhat.com**

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