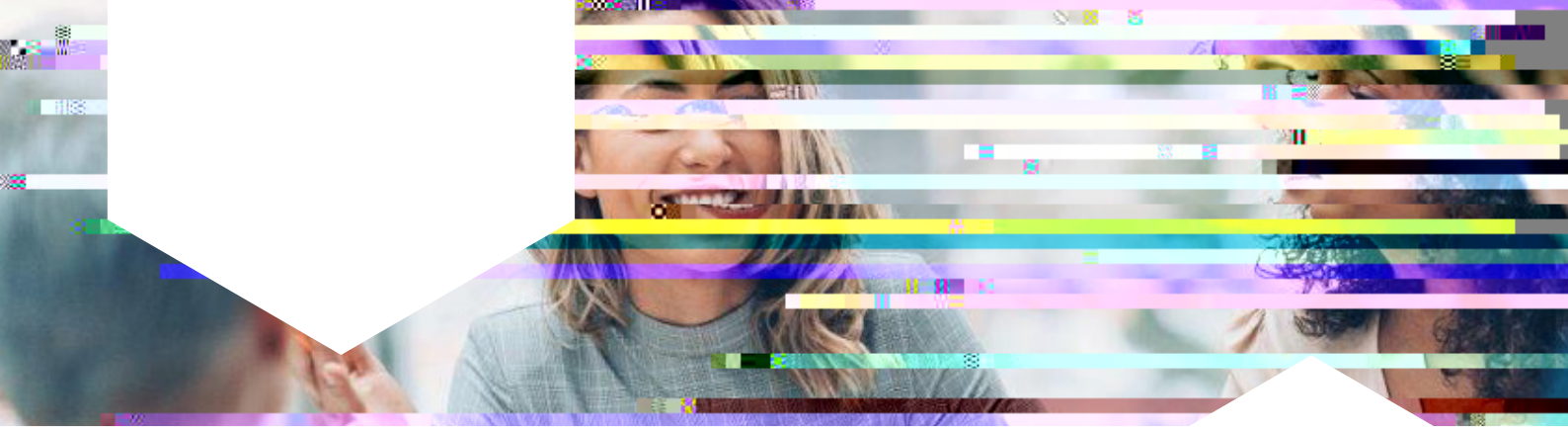


Microsoft et Entrust s'allient pour améliorer la sécurité et la confiance dans l'Internet des Objets

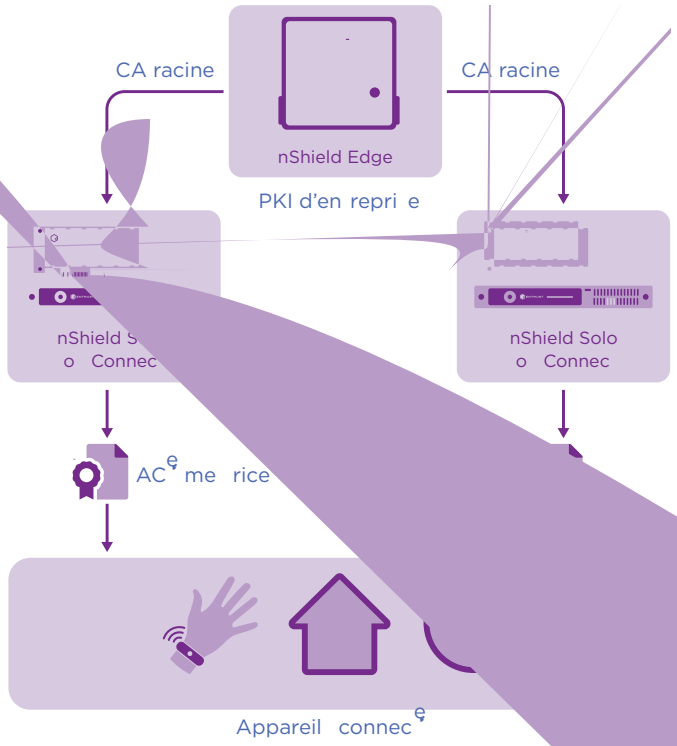
L[illegible] d'[illegible] d[illegible] a[illegible] d[illegible] a[illegible] c[illegible] (HSM) [illegible] c[illegible] d[illegible] a[illegible] l T

CARACTÉRISTIQUES

- Augmentation de l'int[illegible]é des certificats des appareils en réseau
- Prise en charge de l'enregistr[illegible]nt des appareils par les PKI existantes
- Possibilité de stockage et de gestion sécurisée des clés
- Protection des clés conforme à la norme FIPS 140-2 niveau 3
- Respect de la législation en vigueur sur la protection des données facilité

L'enjeu : un nombre croissant d'appareils en réseau qui se connectent à Internet à l'aide de certificats d'identifications et authentification doivent prendre en charge l'enrôlement des certificats.

Avec l'augmentation du nombre d'appareils connectés à Internet et aux réseaux d'entreprise, leur identification et leur authentification deviennent cruciales. Les appareils non-autorisés sont des vecteurs d'attaque des domaines fermés pour les virus et autres programmes malveillants, ce qui est un risque non-négligeable. Les infrastructures à clés publiques (PKI) servent à émettre et à gérer les identifiants des appareils, permettant ainsi leur identification et leur authentification, mais il est également nécessaire d'avoir mis en place un processus d'enregistrement de confiance.



Les HSM nShield d'Entrust nShield HSMs protègent la raci[illegible] de l'entreprise et les clés de la CA émettrice, mais aussi les c[illegible] privées qui servent à lier les certificats des appareils à la racine d[illegible] confiance de la CA afin de certifier l'intégrité et la validation.

Microsoft et Entrust s'allient pour améliorer la sécurité et la confiance dans l'Internet des Objets

Le défi : permettre à un nombre croissant d'appareils connectés d'enrôler des certificats en toute sécurité à l'aide d'identifiants de confiance basés sur les domaines.

Émettre des certificats pour les appareils n'est que la première étape de la mise en place d'un environnement réseau sécurisé où de plus en plus d'appareils autorisés se connectent à des domaines protégés. Il est nécessaire que ces certificats délivrés par une autorité de certification (AC) soient enrôlés pour valider et contrôler les connexions des appareils. Protéger et gérer les clés de chiffrement qui sous-tendent le processus d'enregistrement est indispensable à la confiance dans l'ensemble du système.

La solution : combiner les solutions de Microsoft et d'Entrust pour permettre l'enrôlement sécurisé des certificats des appareils connectés.

Network Device Enrollment Service (NDES), l'une des fonctions de Microsoft Active Directory Certificate Services (AD CS), met en place le Simple Certificate Enrollment Protocol (SCEP) pour définir les communications entre les appareils connectés et une autorité d'enregistrement (AR) pour l'enrôlement des certificats. Les solutions basées sur le cloud et sur site telles que Microsoft Intune et System Configuration Manager utilisent NDES pour provisionner et enrôler les appareils. NDES permet l'enrôlement et la validation des identités numériques des appareils connectés à Windows Server en les liant à une clé privée correspondante. En utilisant l'AC comme base de confiance, le service permet l'enrôlement des certificats et la validation de leur authenticité et de leur intégrité.

Lorsque le processus d'émission est exécuté sur un serveur à l'aide d'une clé stockée localement dans un fichier, la clé peut faire l'objet d'attaques qui la rendent vulnérable à la duplication, à la modification et au remplacement. Les modules matériels de sécurité (HSM) nShield d'Entrust améliorent le niveau d'assurance du processus d'enrôlement du certificat en protégeant la clé NDES privée. Les HSM nShield® d'Entrust s'intègrent avec Microsoft NDES à l'aide des interfaces de programmation d'applications de chiffrement standard de Microsoft (CAPI).

Pourquoi utiliser les HSM avec Microsoft NDES ?

Étant donné que de plus en plus d'appareils sont déployés pour supporter la croissance de l'Internet des Objets (IoT), les PKI doivent non seulement protéger la clé privée de l'AC racine qui garantit la sécurité des certificats émis dans l'ensemble du domaine, mais également l'enregistrement du nombre croissant de certificats. Les PKI organisationnelles qui n'utilisent pas de HSM pour protéger leurs clés privés et qui n'emploient pas de mécanisme pour enrôler et valider les certificats 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. Ils permettent également la gestion du cycle de vie complet, avec basculement si plusieurs HSM sont utilisés de concert pour favoriser la disponibilité. Les failles de sécurité des AC nous ont appris des leçons importantes. Entre autres, 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 et de contrôler l'enrôlement et la validation des certificats.

En plus de respecter des normes de sécurité très strictes comme FIPS 140-2 niveau 3, 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
-