



ENTRUST

Un fournisseur d'énergie du service public figurant au classement du Fortune 500 met en place une infrastructure à clé publique hautement disponible dans un environnement géographiquement distribué.

Découvrez comment les conseils de Entrust et l'utilisation de ses modules matériels de sécurité (HSM) hautement sécurisés ont permis à l'un des plus importants fournisseurs d'énergie des États-Unis de renforcer sa protection et d'offrir de nouveaux services.

L'OBJECTIF : ANTICIPER L'AVENIR

L'équipe informatique de l'un des principaux fournisseurs d'énergie des États-Unis s'était fixée un objectif ambitieux pour elle-même et pour son infrastructure de sécurité.

Alors que les technologies utilisées dans le secteur de l'énergie étaient en pleine évolution, elle était résolue à demeurer à la pointe du progrès. Ces professionnels souhaitaient pouvoir assurer un service continu à leurs clients tout en préparant l'équipe informatique à des nouvelles technologies exigeantes comme les compteurs et les réseaux électriques intelligents. Ils étaient soucieux de satisfaire et de dépasser les exigences de sécurité élevées que leurs auditeurs et le département de la Sécurité intérieure des États-Unis avaient établies. Ils envisageaient en outre de lancer de nouveaux services, comme la possibilité pour leurs collaborateurs comme pour leurs clients de pouvoir accéder au réseau à partir de tablettes et de smartphones.



Nous savions que nous aurions besoin d'une solution matérielle certifiée. Il fallait que nous puissions nous assurer que toutes nos clés privées bénéficieraient de la meilleure protection possible. Nous avons lu bien trop d'articles sur des cas de vol de clés privées qui avaient compromis des PKI entières. Notre principale mission est de fournir des services au public, c'est pour cela qu'il fallait que nous nous assurions de pouvoir bénéficier du plus haut degré de sécurité possible. >>>

- Chef de la sécurité informatique du fournisseur d'énergie classé au Fortune 500

DÉCOUVREZ-EN PLUS SUR [ENTRUST.COM/FR/HSM](https://www.entrust.com/fr/hsm)

Fournisseur d'énergie du Fortune 500

Pour atteindre ces objectifs, l'équipe de sécurité de ce fournisseur d'énergie prévoyait de procéder à une migration vers une version mise à jour de son logiciel d'infrastructure à clé publique (PKI) et de ses principaux serveurs. Leur PKI en place, depuis près de dix ans, avait jusque-là bien fonctionné pour l'authentification des serveurs internes et des ordinateurs portables. Mais pour pouvoir émettre des certificats pour ces appareils mobiles et intégrer de nouvelles technologies tout en bénéficiant du niveau optimal de sécurité, il leur fallait opter pour une nouvelle solution.

Une nouvelle PKI permettrait de déployer de nouveaux services tels que la signature de code et l'horodatage afin de garantir l'intégrité et la bonne gestion de leurs processus internes de développement de logiciels, ou encore de bénéficier de solutions BYOD (« Bring Your Own Device », ou en français AVEC pour « Apportez Votre Équipement personnel de Communication ») qui permettraient aux appareils mobiles et aux tablettes d'accéder au réseau de manière contrôlée et sécurisée.

LE DÉFI : UN ENVIRONNEMENT AUSSI COMPLEXE QU'ÉTENDU

Le véritable défi de ce déploiement réside dans sa capacité à fonctionner au sein de l'environnement singulier de ce fournisseur d'énergie. Pour obtenir la haute disponibilité, la redondance et la fonctionnalité de restauration en cas de défaillance dont l'équipe avait besoin, celle-ci devait déployer la PKI en tenant compte d'une infrastructure complexe de clusters de serveurs répartis sur plusieurs sites. En cas de succès, l'infrastructure du fournisseur d'énergie serait en mesure de répondre facilement à la demande de la prochaine décennie. Il y avait toutefois peu d'informations sur la manière de configurer une PKI au sein d'un tel environnement. Si quelques experts laissaient effectivement entendre que cela était possible, il s'agissait d'une tâche ardue.

Compte tenu de leurs exigences en matière de sécurité, l'équipe était consciente que la solution nécessiterait l'utilisation de modules matériels

de sécurité (HSMs). « Nous savions que nous aurions besoin d'une solution matérielle certifiée » indique le chef de la sécurité informatique du fournisseur d'énergie. « Il fallait que nous puissions nous assurer que toutes nos clés privées bénéficieraient de la meilleure protection possible. Nous avons lu bien trop d'articles sur des cas de vol de clés privées qui avaient compromis des PKI entières. Notre principale mission est de fournir des services au public, c'est pour cela qu'il fallait que nous nous assurions de pouvoir bénéficier du plus haut degré de sécurité possible. »

LA SOLUTION : L'EXPERTISE DE ENTRUST ET L'UTILISATION DE SES HSM NSHIELD

Afin de pouvoir déployer leur solution innovante, l'entreprise a choisi d'utiliser une gamme de produits de Entrust : les HSM nShield® Connect et nShield Edge, et le pack d'options d'horodatage nShield. L'équipe de sécurité savait que ces produits fourniraient les niveaux de paramétrage et d'évolutivité nécessaires pour faire fonctionner cet environnement exigeant. Cela fait en effet longtemps que ce fournisseur d'énergie utilisait les solutions de Entrust pour l'efficacité opérationnelle et le haut niveau de sécurité qu'ils procurent.

L'équipe s'est également appuyée sur l'expertise des professionnels des services techniques de Entrust pour aider à structurer le déploiement. « L'équipe technique de Entrust a été formidable, » explique le chef de la sécurité informatique. « Il faut rappeler que cela n'avait jamais été fait auparavant. Des livres blancs mentionnaient le fait que c'était possible, mais certaines des technologies les plus avancées et les plus complexes n'avaient pas encore été utilisées dans le cadre d'un véritable déploiement. Entrust nous a fourni les HSM, nous a appris à les configurer, à les utiliser correctement au sein de notre environnement et nous a permis d'y voir plus clair avec une formation. Leurs experts étaient également très qualifiés et expérimentés en technologies PKI et leur engagement pour assurer la réussite du projet était sans pareille. »

Fournisseur d'énergie du Fortune 500

Qu'est-ce que cela a donné ? « Notre solution Entrust a eu un impact considérable sur nos activités. Notre infrastructure peut désormais se consacrer à de nombreux autres projets qui étaient en attente. Et notre PKI fait ce pour quoi elle a été créée : elle ne se contente pas d'émettre des certificats pour le serveur, mais elle permet en outre de fournir un grand nombre de services différents. Nous nous reposons sur la PKI pour tellement de choses. Et plus vous en dépendez, plus il vous faut disposer d'une solution matérielle de sécurité. »

LES PRODUITS DE ENTRUST

Les éléments déployés dans le cadre de cette solution sont les suivants :

Les HSM nShield Connect de Entrust

Ce HSM à hautes performances en réseau fournit des services cryptographiques en tant que ressources partagées pour des instances d'applications distribuées et des machines virtuelles. Les HSM nShield Connect sont des solutions rentables permettant de définir les niveaux appropriés de contrôles physiques et logiques pour les systèmes basés sur des serveurs. Les HSM nShield Connect permettent aux organisations de :

- Limiter leurs coûts opérationnels grâce à une puissante architecture de gestion des clés
- Optimiser l'utilisation et l'évolutivité grâce à une plateforme partagée centralisée
- Protéger par chiffrement l'architecture des réseaux dans le cadre de déploiements classiques, virtualisés et sur cloud
- Pallier aux vulnérabilités inhérentes au chiffrement logiciel

Les HSM nShield Edge d'Entrust

Ce HSM à interface USB représente un moyen rentable pour les organisations de se doter d'une technologie de chiffrement hautement sécurisée. Grâce à leur grande portabilité et à la connexion USB, les HSM nShield Edge conviennent parfaitement aux ordinateurs portables comme aux environnements de postes de travail. Leur forme compacte et leur lecteur de carte à puce intégré en font les solutions idéales pour les déploiements dans les espaces restreints ou lorsque les HSM ne sont utilisés que de temps en temps.

Le pack d'options d'horodatage nShield de Entrust

Cette solution d'horodatage clé en main hautement sécurisée donne l'heure exacte et fournit un horodatage sécurisé lors de la création de données, le dépôt de données et l'enregistrement d'autres événements en lien avec les documents électroniques et les applications. Le pack d'options d'horodatage nShield de Entrust protège les opérations d'horodatage au sein d'un environnement matériel inviolable certifié de manière indépendante qui offre ainsi une précision du temps et une vérifiabilité supérieures.

Fournisseur d'énergie du Fortune 500

AVANTAGES : DISPONIBILITÉ, SÉCURITÉ ET PLUS GRANDE GAMME DE SERVICES

Les solutions de Entrust fournissent de nombreux avantages :

Haute disponibilité

La configuration groupée et les capacités de résilience des HSM nShield permettent une plus grande redondance, notamment un basculement automatisé assurant une restauration en cas de défaillance plus fiable et une disponibilité continue.

Une meilleure sécurité

À mesure que l'entreprise ouvre le réseau à d'autres appareils, les HSM nShield de Entrust permettent de renforcer l'authentification par la délivrance de certificats pour les appareils. La PKI peut émettre des certificats pour tous les dispositifs, les appareils personnels n'ayant qu'un accès limité au réseau.

Un grand choix de HSM.

L'utilisation des HSM de Entrust a permis d'investir dans du matériel adéquat pour les ordinateurs portables et les serveurs, sans surplus d'achat.

Prise en charge de compteur intelligent.

Parallèlement au déploiement de la technologie de comptage intelligent, la solution garantira l'intégrité et la confidentialité des données transmises.

À PROPOS DE 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 portefeuille unique de solutions pour la sécurité numérique et l'émission de titres sécurisés permet de répondre précisément à ces souhaits. Grâce à nos 2500 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

