VINCI Autoroutes fait avancer les routes de France avec un système de paiement rapide, fluide et sécurisé

PROFIL CLIENT

VINCI Autoroutes est un leader mondial des infrastructures de mobilité et s'engage pour une croissance durable et partagée avec les territoires et les collectivités. VINCI Autoroutes exploite des autoroutes à péage en tant que concessionnaire de l'État français et partenaire des autorités locales. VINCI Autoroutes dessert 10 régions de France, 45 départements administratifs, 14 grandes villes, plus de 100 villes de plus de 10 000 habitants et des milliers de communes rurales situées à proximité de son réseau autoroutier concédé, qui s'étend sur 4 443 km. En reliant les territoires et en favorisant les nouveaux usages des autoroutes, VINCI Autoroutes contribue au développement d'une mobilité propre, connectée et sûre, elle-même catalyseur de cohésion économique et sociale.

Besoin d'entreprise

- Protéger les données personnelles et de paiement des autoroutes à péage
- Maintenir la confiance dans le système de paiement de VINCI Autoroutes

Besoin technologique

- Mettre à niveau l'ancienne PKI pour répondre aux exigences de la certification PCI DSS

Solution

- Les HSM nShield d´Entrust
- L´architecture nShield Security World d´Entrust
- Microsoft Active Directory Certificate Services

Résultats

- Transition fluide de l'ancienne à la nouvelle PKI
- Sécurité numérique accrue
- Certification PCI DSS

En entrust.com/fr/HSM

Étude de cas sur VINCI Autoroutes

Défi d'entreprise

Lors du passage aux péages routiers, nous cherchons tous à éviter les embouteillages. Il est donc essentiel de relever les défis inhérents à la gestion de transactions à grand volume, à la collecte fluide des redevances et à un service client réactif, le tout en même temps. S'arrêter aux postes de péage et chercher de la monnaie ou une carte de débit ou de crédit peut être pénible. Le télépéage permet d'éviter cela. Il est possible d'acheter un badge de télépéage et de l'installer sur une voiture, ce qui permet aux automobilistes de circuler sur les routes à péage françaises sans avoir besoin de s'arrêter physiquement et de payer à la barrière. Votre véhicule peut automatiquement emprunter les voies désignées et le badge sert de moyen de paiement aux péages, de sorte que tout montant dû est débité sur une carte via celui-ci. Mais qu'en est-il de la sécurité ? Les terminaux de télépéage sont associés à des comptes bancaires et à des informations personnelles identifiables (PII). Par conséquent, afin d'assurer la sécurité numérique et de gagner la confiance des utilisateurs dans l'ensemble du système, ces informations sensibles doivent être protégées.

Défi technique

VINCI Autoroutes avait besoin de faire évoluer ses systèmes pour rester en conformité avec la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS V2 et bientôt V3), le règlement général sur la protection des données (RGPD) et d'autres réglementations européennes. Le personnel informatique souhaitait également mettre en place un système robuste qui permettrait non seulement de répondre aux menaces de cybersécurité actuelles, mais également de les protéger des futures menaces en évolution. Dans ce cas précis, le défi technique consistait à mettre à niveau son infrastructure à clé publique (PKI) et son parc modules matériels de sécurité (HSM) existant pour se conformer aux meilleures pratiques de sécurité et aux nouvelles exigences réglementaires.

Solution

VINCI Autoroutes utilise les HSM nShield d´Entrust comme racine de confiance à assurance élevée pour sa PKI et obtient d'excellents résultats depuis plus de 10 ans. Il n'y avait donc aucun doute dans leur esprit quant au choix du HSM pour la mise à niveau.

Les HSM nShield d´Entrust comptent parmi les solutions HSM les plus performantes, les plus sécurisées et les plus faciles à intégrer disponibles, facilitant la conformité réglementaire et offrant les plus hauts niveaux de sécurité des données et des applications pour les entreprises, les finances et les organisations gouvernementales. L'architecture unique de gestion des clés de Security World fournit des contrôles puissants et granulaires sur l'accès aux clés et leur utilisation.

Le nouveau système utilise Microsoft Active Directory Certificate Services pour émettre, gérer et valider les identités numériques utilisées pour lier les badges de télépéage, les coordonnées bancaires et les PII à leurs clés privées correspondantes. Toutes les informations sont stockées dans une base de données Oracle. La validité de chaque certificat émis dépend de la protection de la clé de l'autorité de certification émettant les identités. Les HSM nShield protègent ces clés d'autorité de certification, ainsi que la clé principale utilisée pour protéger la clé de chiffrement de la base de données stockée dans Oracle Wallet.

Étude de cas sur VINCI Autoroutes

L'architecture de Security World

L'architecture Security World de nShield prend en charge un cadre de gestion des clés spécialisé qui couvre toute la famille de modules matériels de sécurité (HSM) polyvalents de nShield. Que vous déployiez des dispositifs HSM aux performances élevées, partageables et attachés au réseau, des cartes HSM host-embedded ou des HSM portables USB, l'architecture Security World offre une expérience administrateur et utilisateur unifiée et garantit l'interopérabilité, que le client déploie un appareil ou des centaines.

Grâce à Security World de nShield, les utilisateurs peuvent facilement établir une limite de sécurité logique pour la gestion des groupes d'HSM. En tirant parti de cette architecture, les équipes de sécurité peuvent bénéficier des avantages suivants :

- Sécurité renforcée
- Efficacité opérationnelle accrue
- Résilience accrue
- Flexibilité et évolutivité du système

Résultats

VINCI Autoroutes a su faire évoluer son ancien système, en augmentant sa robustesse et son niveau de sécurité numérique, en faisant avancer sans cesse les autoroutes de France en toute sécurité. De plus, la mise à niveau de la technologie fournie par Entrust a permis à VINCI Autoroutes d'obtenir sa certification PCI DSS, l'ensemble d'exigences visant à garantir que toutes les entreprises qui traitent, stockent ou transmettent des informations de carte de crédit maintiennent un environnement sécurisé.

Pour en savoir plus, consultez le site
entrust.com

ENTRUST

Siège social mondial
1187 Park Place, Minneapolis, MN 55379

É.-U. Téléphone gratuit : 888 690 2424
Téléphone international : +1 952 933 1223