Entrust permet à Xumi de créer et de protéger de nouvelles technologies de paiement mobile

DÉFI COMMERCIAL

La technologie de communication en champ proche (NFC) permet à deux appareils placés à proximité d'échanger des données. Ces dernières années, la technologie NFC a permis le paiement sans contact par le bais de portefeuilles mobiles et de cartes sans contact.

Les paiements NFC introduisent un autre niveau de confort pour les consommateurs et les vendeurs, mais ils sont également de nouveaux canaux de fraude. D'après Juliana Cafik, fondatrice de Xumi, avec la démocratisation des portefeuilles mobiles et du paiement sans contact, les fraudes aux NFC vont se développer. Chaque achat frauduleux implique des produits perdus et des frais de remboursement couteux pour les vendeurs.

Xumi est un fournisseur de paiement sécurisé dont l'objectif est de prévenir les transactions frauduleuses avant leur apparition, au lieu de les détecter après coup. Pour cela, l'entreprise s'appuie sur des couches de protection uniques contre les fraudes dans le but d'améliorer la sécurité pour les détenteurs de cartes et les vendeurs.

> **« Pour nous, le défi technique était de créer un environnement sécurisé sur le téléphone mobile d'un consommateur afin de pouvoir y accueillir une carte bancaire sans devoir s'en remettre à un environnement d'exécution de confiance (TEE) ou concevoir de nouveaux algorithmes et méthodologies de chiffrement. C'est là que les HSM nShield d'Entrust entrent en jeu. »**
>
> – Juliana Cafik, fondatrice de Xumi

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

Xumi

Pour que les paiements mobiles soient possibles, les consommateurs ont besoin d'un portefeuille pour rassembler leurs cartes bancaires et les vendeurs ont besoin d'un point de vente pour les appareils mobiles ainsi que pour les transactions en ligne et physiques. La technologie sous-jacente doit être homogène pour les deux parties, et surtout, elle doit être sûre.

DÉFI TECHNIQUE

« L'industrie des paiements est fracturée, » déclare Cafik. Il y a un fossé systémique entre le produit client, donc une carte ou un compte, et les applications des vendeurs qui reçoivent des transactions permises par d'autres parties qui fonctionnent à l'aide d'un ensemble de technologies totalement différent.

Ce décalage empêche de mettre en place une relation de confiance systématique entre deux parties qui ne se connaissent pas : le consommateur et le vendeur. C'est pour cela que la fraude est si généralisée. Le seul moyen de corriger ce problème est de créer une technologie qui prend en charge de manière sécurisée les deux parties de la transaction.

« Pour nous, le défi technique était de créer un environnement sécurisé sur le téléphone mobile d'un consommateur afin de pouvoir y accueillir une carte bancaire sans devoir s'en remettre à un environnement d'exécution de confiance (TEE) ou concevoir de nouveaux algorithmes et méthodologies de chiffrement. C'est là que les modules matériels de sécurité (HSM) nShield® d'Entrust entrent en jeu. »

SOLUTION

Les HSM nShield Connect sont des dispositifs matériels renforcés et inviolables qui renforcent les processus de chiffrement et générant et en protégeant les clés qui servent à chiffrer et à déchiffrer les données et en créant des signatures et des certificats numériques. Les HSM nShield d'Entrust permettent aux utilisateurs de :

- Respecter et dépasser les normes réglementaires établies et émergentes en matière de cybersécurité
- Atteindre de meilleurs niveaux de sécurité des données et de confiance
- Maintenir des niveaux élevés de service et de réactivité commerciale

« Nous employons plusieurs méthodologies de protection, dont le chiffrement, l'authentification et l'obfuscation du code, entre autres », remarque Cafik. « Cependant, les HSM nShield d'Entrust nous permettent de construire une architecture de transaction adaptée au consommateur et au vendeur et ainsi de créer une nouvelle norme de sécurité pour les portefeuilles et les points de vente mobiles sans devoir avoir accès au TEE du téléphone. »

« Le système est sécurisé à la fois au niveau de l'appli mobile et du serveur. » « Le HSM nous aide à créer des structures pouvant vérifier la confiance des deux côtés et être indépendantes des appareils mobiles des consommateurs. C'est particulièrement utile au niveau du serveur. Notre objectif principal est de lutter contre les paiements frauduleux, c'est pourquoi le serveur doit pouvoir respecter toutes les exigences de sécurité de la Payment Card Industry Data Security Standard (PCI DSS) en ce qui concerne le chiffrement des informations de paiement et personnelles stockées, et configurer les transactions dans un environnement hautement sécurisé. Dans ce cadre, le HSM est indispensable. Nous utilisons également les HSM pour sécuriser d'une part les communications entre le serveur et le client et d'autre part les informations de configuration. »

Xumi

> **L'équipe de ventes d'Entrust a été très présente et nous a beaucoup aidés lors de la mise en place de ce projet. Ils connaissaient bien leur sujet et nous ont accompagnés à chaque étape**
>
> – Juliana Cafik, fondatrice de Xumi

D'après Cafik, les HSM nShield Connect d'Entrust étaient une intégrés au modèle dès le départ et sont indispensables à la sécurité de l'environnement opérationnel global, car ils assurent la racine de confiance.

RÉSULTATS

Avec ses partenaires CyberSource et Global Payments, Xumi se prépare à passer au stade de la démonstration de faisabilité commerciale pour son application de paiement mobile. L'application de Xumi a déjà obtenu le certificat de niveau 2 de l'Open Web Application Security Project (OWASP). Le projet d'Application Security Verification Standard (ASVS) de l'OWASP fournit une base de test des contrôles de sécurité techniques des applications web et donne aux développeurs une liste d'exigences à respecter pour sécuriser le développement.[1]

Une fois la démonstration de faisabilité de Xumi terminée, la société compte mettre en place d'autres HSM nShield d'Entrust sur un site de secours afin d'assurer une récupération complète en cas de défaillance, le basculement instantané et l'équilibrage de charge. L'organisation continuera à travailler avec les experts d'Entrust pour assurer une réactivité maximale pour les transactions rapides.

Cafik déclare « L'équipe de ventes d'Entrust a été très présente et nous a beaucoup aidés lors de la mise en place de ce projet. Ils connaissaient bien leur sujet et nous ont accompagnés à chaque étape En fait, heureusement qu'ils étaient là, car ils nous ont conseillé d'utiliser un algorithme sur courbe elliptique, et nous constatons aujourd'hui à quel point ils avaient raison.

Dès le départ, l'équipe d'Entrust nous a fourni exactement ce dont nous avions besoin. Pour une entreprise comme la nôtre, c'est un avantage énorme. Nous sommes une petite structure. Nos développeurs sont excellents, mais ils sont peu nombreux, et si ce HSM avait dû changer de configuration plusieurs fois, ça aurait été très difficile pour nous.

Ils ont été très pédagogues et ont fait leur possible pour comprendre ce que nous allions faire avec le HSM afin d'anticiper les défis que nous allions rencontrer. Ils ne nous ont pas fait perdre de temps, et je les en remercie. »

Xumi

Besoin opérationnel

- Une technologie de paiement mobile qui prenne en compte les besoins de sécurité des consommateurs et des vendeurs

Besoin technologique

- Créer une technologie sécurisée permettant d'instaurer la confiance directement entre le dispositif mobile d'un client et l'application de paiement d'un vendeur

Solution

- Les HSM nShield Connect XC
- Le support des experts d'Entrust

Besoin technologique

- Création d'une architecture transaction adaptée au consommateur et au vendeur sans devoir accéder au TEE de l'appareil mobile
- Communications client-serveur et informations de configuration sécurisées
- Conformité aux exigences PCI DSS pour le serveur vendeur
- Délais de création d'une démonstration de faisabilité commerciale réduits

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 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

Entrust est une marque commerciale, une marque déposée et/ou une marque de service de la société Entrust aux États-Unis et dans d'autres pays. ©2020 Entrust Corporation.

Nous contacter :
HSMinfo@entrust.com