Entrust ajuda Xumi a criar e proteger uma nova tecnologia de pagamentos móveis

DESAFIO EMPRESARIAL

A tecnologia near-field communication (NFC) permite que dois dispositivos colocados próximos um do outro troquem dados. Nos últimos anos, a tecnologia NFC permitiu pagamentos sem contato através de carteiras móveis, assim como cartões sem contato.

Enquanto os pagamentos NFC introduzem um novo nível de conveniência para consumidores e comerciantes, eles também abrem novos caminhos para fraudes. De acordo com Juliana Cafik, diretora da Xumi, à medida que as carteiras móveis e o "tap-to-pay" se tornarem comuns, as fraudes em pagamentos NFC aumentarão. Qualquer compra fraudulenta significa perda de mercadorias e taxas onerosas de estorno para os comerciantes.

A Xumi é uma provedora de pagamento seguro cujo objetivo é impedir transações de pagamento fraudulentas antes que elas aconteçam; ou seja, evitá-las, em vez de detectá-las após o fato. Suas soluções empregam camadas de proteção contra fraudes exclusivas para aumentar a segurança tanto para titulares de cartões quanto para comerciantes.

> **«Nosso desafio técnico foi criar um ambiente seguro no telefone celular do consumidor para abrigar um cartão de crédito sem ter que acessar um ambiente de execução confiável (TEE) ou ter que construir e inventar novos algoritmos e métodos de criptografia. Para isso, os HSM nShield da Entrust foram essenciais.»**
>
> – Juliana Cafik, Principal, Xumi

SAIBA MAIS EM ENTRUST.COM/HSM

Xumi

Nos pagamentos móveis, os consumidores precisam de uma carteira para guardar seus cartões de crédito e os comerciantes precisam de um ponto de venda para dispositivos móveis, assim como transações na web e transações tradicionais. A tecnologia necessária precisa ser consistente para ambos. E também precisa ser segura para ambos.

DESAFIO TÉCNICO

"A indústria de pagamentos está fraturada", disse Cafik. "Há uma divisão sistêmica entre o produto de consumo, que é um cartão ou conta de algum tipo, e as aplicações comerciais, que recebem as transações provisionadas por um conjunto completamente diferente de partes com tecnologias completamente diferentes.

Devido a esta falta de conexão, não se pode confiar nessas duas partes desconhecidas, o consumidor e o comerciante, 100% do tempo. E é por isso que há tanta fraude. A única maneira de corrigir este problema é criar uma tecnologia que trate com segurança ambas as extremidades da transação.

"Nosso desafio técnico foi criar um ambiente seguro no telefone celular do consumidor para abrigar um cartão de crédito sem ter que acessar um ambiente de execução confiável (TEE) ou ter que construir e inventar novos algoritmos e métodos de criptografia. Para isso, os módulos de segurança de hardware (HSM) nShield® da Entrust foram essenciais", disse Cafik.

SOLUÇÃO

Os HSMs Connect nShield são dispositivos de hardware reforçados e resistentes a adulterações que fortalecem os processos criptográficos gerando e protegendo as chaves usadas para criptografar e descriptografar dados e criar assinaturas digitais e certificados.

Os HSM nShield da Entrust permitem aos seus usuários:

- Atender e superar os padrões regulatórios estabelecidos e emergentes para segurança cibernética
- Obter níveis mais altos níveis de segurança de dados e confiança
- Manter serviços de alto nível e agilidade de negócios

"Temos múltiplos métodos de proteção, incluindo criptografia, autenticação, ofuscação de código, criptografia e outras tecnologias", disse Cafik. "Mas os HSM nShield da Entrust nos permite criar uma arquitetura tanto para o lado consumidor quanto para o lado comerciante da transação, e assim criar um novo padrão de segurança para carteiras móveis e pontos de venda móveis, sem ter que acessar o TEE de um telefone celular".

"A segurança do sistema serve tanto para o aplicativo móvel quanto para o servidor", acrescentou Cafik. "O HSM nos ajuda a criar estruturas que podem ser usadas para verificar a confiança de ambos os lados e não depender de dispositivos móveis. Isto é particularmente útil para o servidor. Nosso principal objetivo é proteção contra fraudes em pagamentos, portanto, o servidor tem que ser capaz de satisfazer todos os requisitos de segurança do PCI DSS (Payment Card Industry Data Security Standard) para criptografar informações pessoais e de pagamento armazenadas e ser capaz de configurar as operações em um ambiente altamente seguro. O HSM é essencial para isso. Também utilizamos HSM para proteger a comunicação entre o servidor e o cliente e proteger informações de configuração".

Xumi

> **A equipe de vendas da Entrust foi realmente útil na implementação deste projeto. Eles sabem muito e nos guiaram a cada passo do caminho.**
>
> – Juliana Cafik, Principal, Xumi

O HSM Connect nShield da Entrust tem sido parte do projeto desde o início e é fundamental para a segurança do ambiente operacional geral, fornecendo um ponto de segurança, de acordo com Cafik.

RESULTADOS

A Xumi está se preparando para levar sua aplicação de pagamentos móveis à prova comercial de conceito com os parceiros CyberSource e Global Payments. A aplicação Xumi já tem certificação de nível 2 do Open Web Application Security Project (OWASP). O projeto OWASP Application Security Verification Standard (ASVS) fornece uma base para testar os controles técnicos de segurança das aplicações para web e também fornece aos desenvolvedores uma lista de requisitos para o desenvolvimento seguro.[1]

Após Xumi completar sua prova de conceito, a empresa planeja colocar em funcionamento mais um site de backup para garantir a recuperação total e completa de desastres, hot failover e balanceamento de carga. A empresa continuará a trabalhar com especialistas da Entrust para garantir a máxima capacidade de resposta para transações rápidas.

Cafik observou: "A equipe de vendas da Entrust foi realmente útil na implementação deste projeto. Eles sabem muito e nos guiaram a cada passo do caminho. Não há palavras para explicar a capacidade deles, além disso, eles recomendaram que utilizássemos o algoritmo de curva elíptica, e agora estamos vendo os verdadeiros benefícios dessa recomendação.

"Desde o início, a equipe da Entrust forneceu exatamente o que precisávamos. Trata-se de uma enorme vantagem para uma empresa como a nossa. Somos uma empresa pequena. Temos alguns desenvolvedores que são excelentes. Se o HSM precisasse ser configurado várias vezes, isso teria sido um grande desafio para nós.

Eles foram muito atenciosos na tentativa de entender o que iríamos fazer com o HSM e de pensar antes nos problemas que poderíamos enfrentar. Eles não nos fizeram perder tempo, e estou muito grato por isso".

Xumi

Necessidades empresariais

- Uma tecnologia de pagamento móvel que integra as exigências de segurança tanto dos consumidores quanto dos comerciantes

Necessidades tecnológicas

- Criar uma tecnologia segura que permita a confiança diretamente entre um dispositivo móvel do consumidor e uma aplicação de pagamento de um comerciante.

Solução

- HSM Connect XC nShield
- Suporte de especialistas da Entrust

Necessidades tecnológicas

- Criar de uma arquitetura para o consumidor e o comerciante da transação sem acesso ao TEE do dispositivo móvel
- Comunicações seguras entre cliente e servidor e informações de configuração
- Conformidade com requisitos do PCI DSS no lado do servidor do comerciante da transação
- Menos tempo para a prova comercial do conceito

SOBRE A ENTRUST

A Entrust mantém o mundo movendo-se com segurança, permitindo identidades, pagamentos e proteção de dados confiáveis. Hoje, mais do que nunca, as pessoas exigem experiências seguras e contínuas, quer estejam cruzando fronteiras, fazendo uma compra, acessando serviços de governo eletrônico ou entrando em redes corporativas. A Entrust oferece uma gama incomparável de soluções de segurança digital e emissão de credenciais no centro de todas essas interações. Com mais de 2.500 colegas, uma rede de parceiros globais e clientes em mais de 150 países, não é de admirar que as organizações mais confiáveis do mundo confiem em nós.

[1] https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project

Saiba mais em
entrust.com/HSM

ENTRUST

Entre em contato conosco:
HSMinfo@entrust.com