nCIPHER
AN ENTRUST DATACARD COMPANY

www.ncipher.com

nCipher Security enables Xumi to build and secure new mobile payments technology

BUSINESS CHALLENGE

Near-field communication (NFC) technology allows two devices placed close together to exchange data. In recent years, NFC technology has enabled contactless payments via mobile wallets, as well as contactless cards.

While NFC payments introduce a new level of convenience for consumers and merchants, they also open new avenues for fraud. According to Juliana Cafik, principal at Xumi, as mobile wallets and tap-to-pay become mainstream, fraud rates for NFC payments will rise. And every fraudulent purchase means lost goods and costly chargeback fees for merchants.

Xumi is a secure payment provider whose goal is to stop fraudulent payment transactions before they happen – to prevent them, rather than detect them after the fact. Its solutions employ layers of unique fraud protection to increase security for both cardholders and merchants.

In mobile payments, consumers need a wallet to hold their credit cards and merchants need a point of sale for mobile devices, as well as web-based and brick-and-mortar transactions. The underlying technology needs to be consistent for both. And it needs to be secure for both.

TECHNICAL CHALLENGE

"The payments industry is fractured," says Cafik. "There's a systemic divide between the consumer product, which is a card or account of some sort, and merchant applications, which receive the transactions provisioned by a completely different set of parties with completely different sets of technologies.

Because of this disconnect, you cannot establish trust between those two unknown parties – the consumer and the merchant – 100 percent of the time. And this is why there is so much fraud. The only way to fix this is to create one technology that safely handles both ends of the transaction.

"Our technical challenge was to create a secure environment on a consumer's mobile phone to house a credit card without having to access a trusted execution environment (TEE) or having to build and invent new algorithms and encryption methodologies. This is where the nCipher Security and nShield hardware security module (HSM) comes in," Cafik says.

SOLUTION

nShield Connect HSMs are hardened, tamper-resistant hardware devices that strengthen cryptographic processes by generating and protecting the keys used to encrypt and decrypt data and to create digital signatures and certificates. nShield HSMs enable users to:

- Meet and exceed established and emerging regulatory standards for cybersecurity
- Achieve higher levels of data security and trust
- Maintain high service levels and business agility

"Our technical challenge was to create a secure environment on a consumer's mobile phone to house a credit card without having to access a trusted execution environment (TEE) or having to build and invent new algorithms and encryption methodologies. This is where the nCipher Security and nShield hardware security module (HSM) comes in."

"Our nCipher sales group was really helpful in implementing this project. They were very knowledgeable and guided us every step of the way."

– Juliana Cafik, Principal at Xumi

"We have multiple protection methodologies, including encryption, authentication, code obfuscation, cryptography, and other technologies," Cafik notes. "But the nShield HSM allows us to construct an architecture for both the consumer and merchant side of the transaction, and thereby create a new standard of security for mobile wallets and mobile point of sale, without having to access the TEE of a mobile phone."

"The security of the system covers both the mobile app and a server side," Cafik adds. "The HSM helps us create structures that can be used to verify trust on both sides and to be independent of consumer mobile devices. This is particularly helpful on the server side. Our main objective is to protect against payments fraud, so the server side has to be able to satisfy all the Payment Card Industry Data Security Standard (PCI DSS) security requirements for encrypting stored personal and payment information and be able to configure operations in a highly secure environment. The HSM is critical for this. We also use HSMs to secure communication between the server and the client and secure configuration information."

The nShield Connect HSM has been part of the design from the beginning and is key to the security of the overall operational environment by providing a root of trust, according to Cafik.

RESULTS

As of this writing, Xumi is preparing to take its mobile payments application into commercial proof of concept with partners CyberSource and Global Payments. Xumi's application has already been certified at Level 2 by the Open Web Application Security Project (OWASP). The OWASP Application Security Verification Standard (ASVS) Project provides a basis for testing web application technical security controls and also provides developers with a list of requirements for secure development.[1]

After Xumi completes its proof of concept, it plans to put in place a second nShield Connect HSM in a backup site to ensure full and complete disaster recovery, and hot failover and load balancing. The organization will continue to work with nCipher experts to ensure maximum responsiveness for fast transactions.

Cafik observes "Our nCipher sales group was really helpful in implementing this project. They were very knowledgeable and guided us every step of the way. And, in hindsight, I can't say enough about this, because they recommended we use the elliptic curve algorithm, and we are now seeing the true benefits of that recommendation.

"From the onset, the nCipher team provided exactly what we needed. That's a huge benefit to a company like ours. We're small. We have a few developers that are really excellent. And if that HSM had to go back and forth with different configurations, it would have been very challenging for us.

Business need

- A mobile payments technology that incorporates the security requirements of both consumers and merchants

Technology need

- Create a secure technology that enables trust directly between a consumer's mobile device and a merchant's payment application

Solution

- nShield Connect XC HSMs
- nCipher expert support

Result

- The creation of an architecture for both the consumer and merchant sides of the transaction without accessing the TEE of the mobile device
- Secure client-server communications and configuration information
- Compliance with PCI DSS requirements on the merchant server side of the transaction
- Reduced time to commercial proof of concept

They were very thoughtful in trying to understand what we were going to do with the HSM and thinking ahead of challenges we might face. They didn't waste our time, and I'm quite grateful for that."

ABOUT NCIPHER SECURITY

nCipher Security, an Entrust Datacard company, is a leader in the general-purpose hardware security module (HSM) market, empowering world-leading organizations by delivering trust, integrity and control to their business critical information and applications. Today's fast-moving digital environment enhances customer satisfaction, gives competitive advantage and improves operational efficiency – it also multiplies the security risks. Our cryptographic solutions secure emerging technologies such as cloud, IoT, blockchain, and digital payments and help meet new compliance mandates. We do this using our same proven technology that global organizations depend on today to protect against threats to their sensitive data, network communications and enterprise infrastructure. We deliver trust for your business critical applications, ensure the integrity of your data and put you in complete control – today, tomorrow, always. **www.ncipher.com**

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