Entrust ermöglicht Xumi den Aufbau und die Sicherung einer neuen mobilen Zahlungstechnologie

GESCHÄFTLICHE PROBLEMSTELLUNG

Die NFC-Technologie (Near Field Communication) ermöglicht den Datenaustausch zwischen zwei Geräten, die sich in physischer Nähe zueinander befinden. In den letzten Jahren hat sie vor allem dafür gesorgt, dass kontaktlose Zahlungen über mobile Geldbörsen sowie kontaktlose Karten immer populärer wurden.

Solche NFC-Zahlungen machen die Transaktion für Käufer und Verkäufer zwar einfacher, eröffnen aber auch neue Betrugsrisiken. Laut Xumi-Chefin Juliana Cafik werden die Betrugsraten bei NFC-Zahlungen steigen, je mehr mobile Geldbörsen und kontaktloses Zahlen zur Normalität werden. Jeder betrügerische Kauf bedeutet Warenverlust und kostspielige Rückbuchungsgebühren für die Händler.

Als sicherer Zahlungsanbieter möchte Xumi betrügerische Zahlungstransaktionen stoppen, bevor sie passieren, und sie verhindern, anstatt im Nachhinein darauf aufmerksam zu werden. Die Lösungen des Unternehmens bieten einen einzigartigen Schutz vor Betrug, um die Sicherheit sowohl für Karteninhaber als auch für Händler zu erhöhen.

> **«Unsere technische Herausforderung bestand darin, eine sichere Umgebung für Kreditkarten auf dem Mobiltelefon eines Verbrauchers zu schaffen, ohne auf einen Trusted Execution Environment (TEE) Bereich zugreifen oder neue Algorithmen und Verschlüsselungsmethoden entwickeln und erfinden zu müssen. Hier kommen die Entrust nShield HSMs ins Spiel.»**
>
> – Juliana Cafik, Xumi-Chefin

WEITERE INFORMATIONEN AUF ENTRUST.COM/HSM

Xumi

Bei mobilen Zahlungen benötigen die Verbraucher eine Geldbörse (Wallet), um ihre Kreditkarten aufzubewahren, und die Händler brauchen eine Verkaufsstelle (Point of Sale) für mobile Geräte sowie webbasierte und stationäre Transaktionen. Die zugrunde liegende Technologie muss für beide konsistent und sicher sein.

TECHNISCHE PROBLEMSTELLUNG

„Die Zahlungsverkehrsbranche ist sehr inhomogen“, so Cafik. „Es gibt eine systembedingte Kluft zwischen dem Verbraucherprodukt, bei dem es sich um eine Karte oder ein irgendwie geartetes Konto handelt, und den Händleranwendungen, die Transaktionen entgegennehmen, die von einer völlig anderen Gruppe von Marktteilnehmern mit ganz anderen Technologien bereitgestellt werden.“

Aufgrund dieser Trennung kann zwischen Verbraucher und Händler nicht in 100 Prozent der Fälle eine vertrauenswürdige Beziehung aufgebaut werden, was wiederum zu den vielen Betrugsfällen führt. Dieses Problem kann nur behoben werden, wenn eine Technologie genutzt wird, die beide Seiten der Transaktion sicher handhabt.

„Unsere technische Herausforderung bestand darin, eine sichere Umgebung für Kreditkarten auf dem Mobiltelefon eines Verbrauchers zu schaffen, ohne auf einen Trusted Execution Environment (TEE) Bereich zugreifen oder neue Algorithmen und Verschlüsselungsmethoden entwickeln und erfinden zu müssen. Hier kommen die nShield® Hardware-Sicherheitsmodule (HSMs) von Entrust ins Spiel“, erläutert Cafik.

LÖSUNG

nShield Connect HSMs sind robuste, manipulationssichere Hardware-Geräte, die kryptographische Prozesse stärken. Dies erfolgt durch die Erstellung und den Schutz von Schlüsseln, die zur Ver- und Entschlüsselung von Daten sowie zur Erstellung digitaler Signaturen und Zertifikate dienen. Mit Entrust nShield HSMs können Nutzer:

- bestehende und neue gesetzliche Normen für Cyber-Sicherheit einhalten und übertreffen
- einen höheren Grad an Datensicherheit und Vertrauen erreichen
- ein hohes Serviceniveau und die Flexibilität des Unternehmens erhalten

„Wir arbeiten selbst mit mehreren Schutzmethoden, darunter Verschlüsselung, Authentifizierung, Code-Verschleierung, Kryptographie und andere Technologien“, sagt Cafik. „Mit den Entrust nShield HSMs können wir allerdings eine Architektur sowohl für die Verbraucher- als auch für die Händlerseite der Transaktion konstruieren und dadurch einen neuen Sicherheitsstandard für mobile Geldbörsen und Verkaufsstellen entwickeln, ohne auf die TEE eines Mobiltelefons zugreifen zu müssen.“

„Die Sicherheit des Systems umfasst sowohl die mobile App als auch eine Server-Seite,“ fügt Cafik hinzu. „Das HSM hilft uns, Strukturen zu schaffen, mit denen das Vertrauen auf beiden Seiten überprüft werden kann und die unabhängig von den mobilen Endgeräten der Verbraucher sind. Das ist besonders hilfreich auf der Serverseite. Unser Hauptziel ist der Schutz vor Zahlungsbetrug, daher muss die Serverseite in der Lage sein, alle Sicherheitsanforderungen des Payment Card Industry Data Security Standard (PCI DSS) für die Verschlüsselung gespeicherter persönlicher Daten und Zahlungsinformationen erfüllen und den Betrieb in einer hochsicheren Umgebung konfigurieren können. All das hängt entscheidend vom HSM ab. Wir verwenden HSMs auch, um die Kommunikation zwischen Server und Client sowie Konfigurationsinformationen zu sichern.“

Xumi

> **Das Verkaufsteam von Entrust war bei der Umsetzung dieses Projekts sehr hilfreich. Die Beratung war sehr sachkundig und wir wurden auf jedem Schritt des Weges begleitet.**
>
> – Juliana Cafik, Xumi-Chefin

Das Entrust nShield Connect HSM war von Anfang an Teil des Designs und ist, laut Cafik, der Schlüssel für die Sicherheit der gesamten Betriebsumgebung, da es eine Root-of-Trust bietet.

ERGEBNISSE

Xumi ist dabei, seine Anwendung für mobile Zahlungen mit den Partnern CyberSource und Global Payments ins Stadium des kommerziellen Proof-of-Concept zu bringen. Die Anwendung von Xumi wurde bereits auf Stufe 2 durch das Open Web Application Security Project (OWASP) zertifiziert. Das Application Security Verification Standard (ASVS) Projekt von OWASP bietet eine Grundlage für das Testen der technischen Sicherheitskontrollen von Webanwendungen und stellt Entwicklern außerdem eine Liste von Anforderungen für eine sichere Entwicklung zur Verfügung.[1]

Nach dem Abschluss des Proof-of-Concept plant Xumi, weitere Entrust nShield HSMs an einem Backup-Standort einzurichten, um eine vollständige Notfallwiederherstellung sowie Hot Failover und Lastausgleich zu gewährleisten. Die Organisation wird weiterhin mit den Experten von Entrust zusammenarbeiten, um eine maximale Reaktionsfähigkeit für schnelle Transaktionen zu gewährleisten.

„Das Verkaufsteam von Entrust war bei der Umsetzung dieses Projekts sehr hilfreich“, betont Cafik. „Die Beratung war sehr sachkundig und wir wurden auf jedem Schritt des Weges begleitet. Im Nachhinein muss ich auch nochmal betonen, wie wertvoll der Hinweis war, Elliptische-Kurven-Kryptographie zu nutzen, denn wir sehen jetzt die wahren Vorteile dieser Empfehlung.“

Und weiter: „Das Team von Entrust hat von Anfang an genau das geliefert, was wir brauchten. Das ist ein großer Vorteil für ein Unternehmen wie unseres, denn wir sind klein und arbeiten nur mit ein paar Entwicklern, die übrigens hervorragende Arbeit leisten. Wenn es nun bezüglich des HSM ein dauerndes Hin und Her mit verschiedenen Konfigurationen gegeben hätte, wäre das für uns schwierig gewesen.

Das Entrust-Team hat wirklich mitgedacht und versucht zu verstehen, was wir mit dem HSM vorhaben. Sie haben sich auch Gedanken über mögliche zukünftige Herausforderungen gemacht, mit denen wir konfrontiert werden könnten. Es war eine sehr effiziente Zusammenarbeit, wofür wir sehr dankbar sind.“

Xumi

Geschäftliche Anforderungen

- Eine mobile Zahlungstechnologie, die Sicherheitsanforderungen von Verbrauchern und Händlern berücksichtigt

Technische Anforderungen

- Schaffung einer sicheren Technologie, die Vertrauen direkt zwischen dem mobilen Gerät eines Verbrauchers und der Zahlungsanwendung eines Händlers ermöglicht

Lösung

- nShield Connect XC HSMs
- Unterstützung durch die Experten von Entrust

Technische Anforderungen

- Schaffung einer Architektur sowohl für die Verbraucher- als auch für die Händlerseite der Transaktion ohne Zugriff auf die TEE des mobilen Geräts
- Sichere Client-Server-Kommunikation und Konfigurationsinformationen
- Einhaltung der PCI DSS-Anforderungen auf der Händler-Server-Seite der Transaktion
- Zeitverkürzung bis zum kommerziellen Proof-of-Concept

ÜBER ENTRUST

Entrust ermöglicht vertrauenswürdige Identitäten und Zahlungen sowie verlässlichen Datenschutz und hält damit die Welt sicher in Bewegung. Ein nahtloses und sicheres Umfeld ist heute mehr denn je unerlässlich, sei es bei Grenzübertritten, beim Einkaufen, beim Zugriff auf E-Government-Dienste oder beim Einloggen in Unternehmensnetzwerke. Entrust bietet für genau diese Interaktionen eine unübertroffene Bandbreite an Lösungen für digitale Sicherheit und die Ausstellung von Berechtigungsnachweisen.
Mit 2.500 Mitarbeitern und einem weltweiten Partnernetzwerk ist Entrust für Kunden in über 150 Ländern tätig, die sich bei ihren sensibelsten Operationen auf uns verlassen.

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

Weitere Informationen auf
entrust.com/HSM

ENTRUST

Kontakt:
HSMinfo@entrust.com