Entrust le permite a Xumi crear y proteger una nueva tecnología de pagos móviles

RETO EMPRESARIAL

La tecnología de comunicación de campo cercano (NFC) permite que dos dispositivos colocados juntos intercambien datos. En los últimos años, la tecnología NFC ha permitido pagos sin contacto a través de billeteras móviles, así como tarjetas sin contacto.

Si bien los pagos NFC introducen un nuevo nivel de conveniencia para los consumidores y comerciantes, también abren nuevas vías para el fraude. Según Juliana Cafik, directora de Xumi, a medida que las billeteras móviles y el toque para pagar se generalicen, las tasas de fraude para los pagos NFC aumentarán. Y cada compra fraudulenta significa pérdida de bienes y costosas tarifas de devolución de cargo para los comerciantes.

Xumi es un proveedor de pago seguro cuyo objetivo es detener las transacciones de pago fraudulentas antes de que sucedan, para prevenirlas en lugar de detectarlas a posteriori. Sus soluciones emplean capas de protección contra el fraude únicas para aumentar la seguridad, tanto para los titulares de tarjetas como para los comerciantes.

> **«Nuestro desafío técnico fue crear un entorno seguro en el teléfono móvil de un consumidor para alojar una tarjeta de crédito sin tener que acceder a un entorno de ejecución confiable (TEE) o tener que crear e inventar nuevos algoritmos y metodologías de cifrado. Aquí es donde hacen su aparición los HSMs nShield de Entrust.»**
>
> – Juliana Cafik, Principal, Xumi

Xumi

En los pagos móviles, los consumidores necesitan una billetera para guardar sus tarjetas de crédito y los comerciantes necesitan un punto de venta para dispositivos móviles, así como transacciones basadas en la web y físicas. La tecnología subyacente debe ser coherente para ambos. Y necesita ser segura para ambos.

RETO TÉCNICO

"La industria de pagos está fracturada", dice Cafik. "Existe una división sistémica entre el producto de consumo, que es una tarjeta o cuenta de algún tipo y las aplicaciones comerciales, que reciben las transacciones provistas por un conjunto de entidades completamente diferente con conjuntos de tecnologías completamente diferentes.

Debido a esta desconexión, no se puede establecer confianza entre esas dos entidades desconocidas, el consumidor y el comerciante, el 100 por ciento del tiempo. Razón por la que se da tanto fraude. La única forma de solucionar este problema es crear una tecnología que maneje de forma segura ambos extremos de la transacción".

"Nuestro desafío técnico fue crear un entorno seguro en el teléfono móvil de un consumidor para alojar una tarjeta de crédito sin tener que acceder a un entorno de ejecución confiable (TEE) o tener que crear e inventar nuevos algoritmos y metodologías de cifrado. Aquí es donde entran en juego los módulos de seguridad de hardware (HSMs) nShield® de Entrust", dice Cafik.

SOLUCIÓN

Los HSMs nShield Connect son dispositivos de hardware reforzados y a prueba de manipulaciones indebidas que fortalecen los procesos criptográficos al generar y proteger las claves utilizadas para cifrar y descifrar datos y para crear firmas y certificados digitales. Los HSMs nShield de Entrust les permiten a los usuarios:

- Cumplir y superar los estándares regulatorios establecidos y emergentes en materia de ciberseguridad
- Logran altos niveles de seguridad de datos y confianza
- Mantener altos niveles de servicio y agilidad empresarial

"Contamos con múltiples metodologías de protección, que incluyen cifrado, autenticación, ofuscación de código, criptografía y otras tecnologías", señala Cafik. "Pero los HSMs nShield de Entrust nos permiten construir una arquitectura tanto para el consumidor como para el comerciante de la transacción y así crear un nuevo estándar de seguridad para billeteras y puntos de venta móviles, sin tener que acceder al TEE de un teléfono móvil".

"La seguridad del sistema cubre tanto la aplicación móvil como el lado del servidor", agrega Cafik. "El HSM nos ayuda a crear estructuras que se pueden utilizar para verificar la confianza en ambos lados y para ser independientes de los dispositivos móviles de los consumidores. Esto es particularmente útil desde el punto de vista del servidor. Nuestro principal objetivo es la protección contra el fraude en los pagos, por lo que la responsabilidad del servidor debe poder satisfacer todos los requisitos de seguridad del Estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS) para cifrar la información personal y de pago almacenada y poder configurar las operaciones en un entorno de alta seguridad. El HSM es fundamental para esto. También utilizamos HSMs para asegurar la comunicación entre el servidor y el cliente y proteger la información de configuración".

Xumi

> **El equipo de ventas de Entrust fue de gran ayuda en la implementación de este proyecto. Ellos estaban muy bien informados y nos guiaron en cada paso del camino.**
>
> – Juliana Cafik, Principal, Xumi

El HSM nShield Connect de Entrust ha sido parte del diseño desde el principio y es clave para la seguridad del entorno operativo general al proporcionar una raíz de confianza, según Cafik.

RESULTADOS

Xumi se está preparando para llevar su aplicación de pagos móviles a una prueba de concepto comercial con sus socios CyberSource y Global Payments. La aplicación de Xumi ya ha sido certificada en el Nivel 2 por Open Web Application Security Project (OWASP). El proyecto del estándar de verificación de seguridad de aplicaciones (ASVS) de OWASP proporciona una base para poner a prueba los controles técnicos de seguridad de las aplicaciones web y también, les proporciona a los desarrolladores una lista de requisitos para un desarrollo seguro.[1]

Una vez que Xumi complete su prueba de concepto, planea instalar más HSMs nShield Entrust en un sitio de respaldo para garantizar una recuperación total y completa ante desastres, así como una conmutación por error en caliente y equilibrio de carga. La organización seguirá trabajando con los expertos de Entrust para garantizar la máxima capacidad de respuesta para transacciones rápidas.

Cafik observa “El equipo de ventas de Entrust fue de gran ayuda en la implementación de este proyecto. Ellos estaban muy bien informados y nos guiaron en cada paso del camino. En retrospectiva, no hay palabras suficientes al respecto, porque recomendaron que usemos el algoritmo de curva elíptica y ya estamos viendo los verdaderos beneficios de esa recomendación”.

“Desde el principio, el equipo de Entrust proporcionó exactamente lo que necesitábamos. Eso es un gran beneficio para una empresa como la nuestra. Somos una empresa pequeña. Tenemos algunos desarrolladores que son realmente excelentes. Si ese HSM tuviera que ir y venir con diferentes configuraciones, habría sido un gran desafío para nosotros.

Fueron muy atentos al tratar de comprender lo que íbamos a hacer con el HSM y se anticiparon a los desafíos que podíamos enfrentar. No nos hicieron perder el tiempo y estoy muy agradecido por eso”.

Xumi

Necesidades del negocio

- Una tecnología de pagos móviles que incorpora los requisitos de seguridad de consumidores y comerciantes.

Necesidades tecnológicas

- Crear una tecnología segura que permita la confianza directamente entre el dispositivo móvil de un consumidor y la aplicación de pago de un comerciante.

Solución

- HSMs nShield Connect XC
- El apoyo de expertos de Entrust

Necesidades tecnológicas

- La creación de una arquitectura tanto para el consumidor como para el comerciante de la transacción, sin acceder al TEE del dispositivo móvil.
- Comunicaciones seguras cliente-servidor e información de configuración
- Cumplimiento de los requisitos del PCI DSS por parte del servidor comercial de la transacción
- Reducción del tiempo de prueba de concepto comercial

ACERCA DE ENTRUST

Entrust ayuda a que el mundo se mueva de forma segura al permitir la protección fiable de identidades, pagos y datos. Hoy más que nunca, las personas exigen experiencias seguras y sin problemas, ya sea que crucen fronteras, realicen una compra, accedan a servicios de gobierno electrónico o inicien sesión en redes corporativas. Entrust ofrece una variedad incomparable de soluciones de seguridad digital y emisión de credenciales en el núcleo de todas estas interacciones. Con más de 2500 colegas, una red de socios globales y clientes en más de 150 países, no es de extrañar que las organizaciones más confiables del mundo confíen en nosotros.

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

Aprenda más en
entrust.com/HSM

ENTRUST

Contacte con nosotros:
HSMinfo@entrust.com