

NETS Singapore gains enterprise-grade payment app protection using Zimperium



Industry

Payments Industry

Location

Singapore and environs

Solution

zKeyBox
zShield

Customer Profile

NETS is Singapore's leading electronic payment service provider. Founded in 1985 by a consortium of banks, NETS operates Singapore's national debit scheme and enables digital payments for merchants, consumers, and banks across the entire payments value chain.

NETSPay is the company's mobile application which allows users to make digital payments via NETS bank cards. Once consumers have digitized their cards, they can simply tap or scan with their mobile phone to make payments.

In 2019, the company introduced NETS Click, an in-app payment mode. NETS Click allows consumers to securely add their NETS bank card and use it to pay for purchases with just one click. Third party mobile apps that use the solution display NETS Click as a payment method option.

The Challenge

Mobile contactless payments offer immense convenience for consumers and businesses alike but they open up potential security risks.

Unlike EMVchip cards and POS systems, smartphones support multiple purposes and include broad functionality that makes them more vulnerable to attack than a dedicated device. Often they lack a Secure Element (SE) or Trusted Execution Environment (TEE)¹ for processing and storing secret information like cryptographic keys and tokens.

Moreover, mobile payment applications run in unknown environments outside the developer or payment service provider's control. They must be able to operate securely even if a hostile party has compromised the device.

To address fintech risks, regulatory bodies issue security requirements that financial application software must meet.

¹ A TEE is a second, hardware-separated secure operating system and keystore that runs alongside the normal operating system (e.g., Android).

Application code protection essential for compliance


These regulatory guidelines specify multiple anti-tampering and anti-reverse engineering measures to protect application code. Recommended security mechanisms include the use of code obfuscation, anti-tampering mechanisms to prevent injection of malicious code, integrity checkers, and detecting and disabling operation on a rooted or jailbroken device.

Token protection

NETSPay utilizes host card emulation(HCE) technology to securely process transactions. HCE cannot rely on a Secure Element or TEE being available, yet sensitive token information and keys need to be protected at all times, even if the device has been rooted or otherwise compromised.

Challenge highlights

- Protect the confidentiality and integrity of payment account data
- Meet security mandates and regulatory requirements
- Secure token information
- Protect application code against tampering and reverse-engineering Deploy a solution with minimal impact to the software development process



Zimperium's enterprise-grade application shielding and key protection helped NETSPay gain broad acceptance by partners and customers alike.

The Solution

After looking at several security solutions, NETS chose Zimperium's zShield and zKeyBox solutions to build strong code and key protections into their NETSPay solution. Its flexibility and ease-of-use would also help them ramp up quickly.

zShield

The team embedded automated self-defense capabilities into NETSPay and NETS Click using Zimperium's [zShield](#). It employs multiple anti-tamper mechanisms, advanced obfuscation, and runtime application self-protection (RASP) to stop anyone from reverse engineering the code, stealing sensitive data, or hijacking the software for malicious purposes. zShield slotted neatly into the existing software development environment and required minimal maintenance once integrated—a secure application is automatically created at build time. NETS credits their quick deployment of zShield to Zimperium's expert and responsive support.

zKeyBox

NETS leveraged Zimperium's [zKeyBox](#) to protect the cryptographic operations that secure the HCE process. zKeyBox delivers market-leading white-box cryptography to ensure the tokens and encryption keys used by NETSPay and NETS Click remain safe at all times—whether they are stored, in transit, or in use. A powerful, drop-in replacement for standard cryptographic libraries, it regularly undergoes pentesting through third-party labs and even protects keys against sophisticated side-channel attacks.

The Result

By deploying both Zimperium solutions, the NETSPay development team was able to build a self-defending application that automatically thwarts hacking attempts. App performance impact was minimal thanks to Zimperium's robust profiling optimization tool. NETS was able to meet compliance requirements and bring their contactless payment solutions to market more quickly.

Zimperium's enterprise-grade application shielding and key protection, together with NETS own rigorous penetration testing process, helped NETSPay gain broad acceptance by partners and customers alike. The same advantages propelled NETS Click into the spotlight. Its innovative technology, allowing customers to securely pay with digitized bank cards on third-party merchant mobile apps, earned NETS the Singapore Business Review's 2020 Technology Excellence Award in the Fintech-Payments category. NETS Click has already been successfully deployed on a group of merchant third-party apps in various industries.

Result Highlights

- Passed all penetration testing requirements
- Ensured compliance with regulatory requirements
- Met tight development and testing schedules
- Protected applications against reverse-engineering, tampering, and attacks from current as well as potential new threats
- Secured token information and keys at all times, even on compromised devices



Learn more at: zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com
Zimperium, Inc
4055 Valley View, Dallas, TX 75244