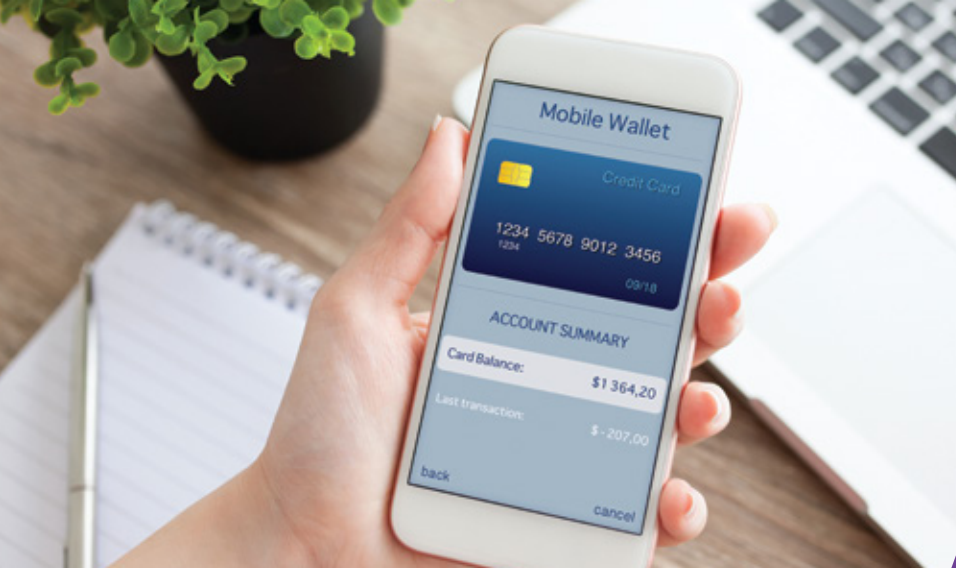

V-KEY
STRONGER WITH V-OS

SINGAPORE BANK
CASE STUDY

DIGITAL MOBILE WALLET

THE OVERVIEW

SECURE, SEAMLESS CLOUD-BASED PAYMENTS

A multi-award winning bank in South East Asia with a global presence was looking to enhance their mobile banking app to appeal to both their local and international retail customers. Headquartered in Singapore, the bank identified an opportunity to take a leap in digitized payments and set themselves apart from the other mobile banking apps in the region.

Leveraging new developments in cloud-based payments (CBP) by VISA and MasterCard, coupled with data analytic capabilities for deeper customer insight, our customer was ready to offer a unique and powerful platform to deliver end-to-end financial services to its customers.

THE BUSINESS PROBLEM

TURNING THE SMARTPHONE INTO A DIGITAL MOBILE WALLET

With the newly-launched CBP standards enabling mobile contactless payments, the bank sought to create a mobile wallet app that completely replaces the customer's physical wallet. They wanted customers to be able to use it anytime and anywhere, regardless of internet connectivity.

This was possible by tokenizing the card and creating single-use proxies for the real card number. Using single-use tokens significantly reduce the risks of fraud and exposure to cloning should the cards fall into the wrong hands.

However, storing multiple single use tokens on the smartphone presented itself as a significant risk as the mobile wallet app would then need to rely on an inherently insecure smartphone operating system and hardware to store the tokens. While plenty of smartphones possess security chip hardware, these were often not open for use by third-party apps.

The bank needed an independent solution to securely store multiple single-use tokens, while ensuring protection from malware, cloning, duplication, tampering, modification, and other malicious intents.

SOLUTION-AT-A-GLANCE

- Cloud-based Payments
- Virtual Cards
- Trusted Identity
- App Security

- V-OS App Protection
- V-OS OTP Token

THE CUSTOMIZED SOLUTION

PURPOSE-BUILT TRUSTED APPLICATIONS, STRONGER WITH V-OS

The process began with the bank electing to adopt MasterCard's CBP standard for their mobile wallet. To secure MasterCard's CBP function calls, logic, and multiple single-use tokens, the bank chose V-Key's Virtual Secure Element (VSE), a software-based framework that comprises its own Software Execution Environment (SEE) and secure data storage. V-OS App Protection was also key to this deployment as they needed to ensure tamper protection and detection functionality within the app.

To integrate the MasterCard CBP Software Development Kit (SDK), the teams combined to develop a novel and customized Trusted Application (TA) that could run securely within V-OS. This TA would be embedded into the mobile wallet to handle the unique implementation of MasterCard's CBP standards.

Functioning independently from the mobile device's OS and hardware, V-OS VSE transformed the mobile phone into a mobile wallet, by protecting CBP function calls and logic, as well as the multiple single-use tokens for offline payments.

THE TECHNOLOGY

IMPLEMENTING HIGH-PERFORMANCE SECURITY ON INHERENTLY UNSECURE DEVICES

In the design of the Trusted Application, our Professional Services team worked with our banking customer to develop and deploy the V-OS Product Suite into a full-fledged mobile security solution.

With V-OS lies two key functions; firstly, with a method known as device fingerprinting, V-OS captured hardware information that uniquely individualizes the device. This prevents malicious agents from cloning the mobile phone onto another device to extract sensitive and personal information. V-OS has also been crafted to be anti-reverse engineered by malicious actors. This effectively and seamlessly turned the customer's mobile device into a trusted 2FA device, at a fraction of the total lifetime cost of the hardware token alternative.

The custom TA also handled the storage and cryptographic processing of the single-use tokens, which meant the payment authorization keys were protected both at-rest as well as during an NFC payment transaction. During NFC payment, the authorization computation was performed entirely within V-OS VSE. At no time were the secret keys ever exposed to the native operating system. This meant that the bank could trust the transaction logs from offline payments stored on the customer's device, which could then be reconciled and monitored for fraud at the bank's servers.

With V-OS App Protection, an "always-on" tamper protection solution that monitors the runtime environment of the mobile wallet app, the bank was protected against malicious viruses, trojans, ransomware, unauthorized remote access, debugging, function hooking or code injections. Even in rooted or "jailbroken" devices, a practice common in Southeast Asia, the mobile app would be able to detect and virtually "harden" itself in an unsecure environment.

V-OS App Protection also comes with policy management capabilities, as well as a threat intelligence and reporting system to provide our enterprise customers direct analysis of their customers' mobile behavior. This allows the Bank's administrators to also monitor threat levels and situations in real-time.

THE RESULT

A Truly, Fully Digital Mobile Wallet

Within months, our banking customer was able to offer its customers an Advanced Mobile Wallet integrated with CBP, ahead of other competing banking apps and Apple Pay. With the security layer fully managed by the V-OS Product Suite, the app could focus on delivering an exceptional user experience with no compromise to highly-regulated Digital Banking Security standards.