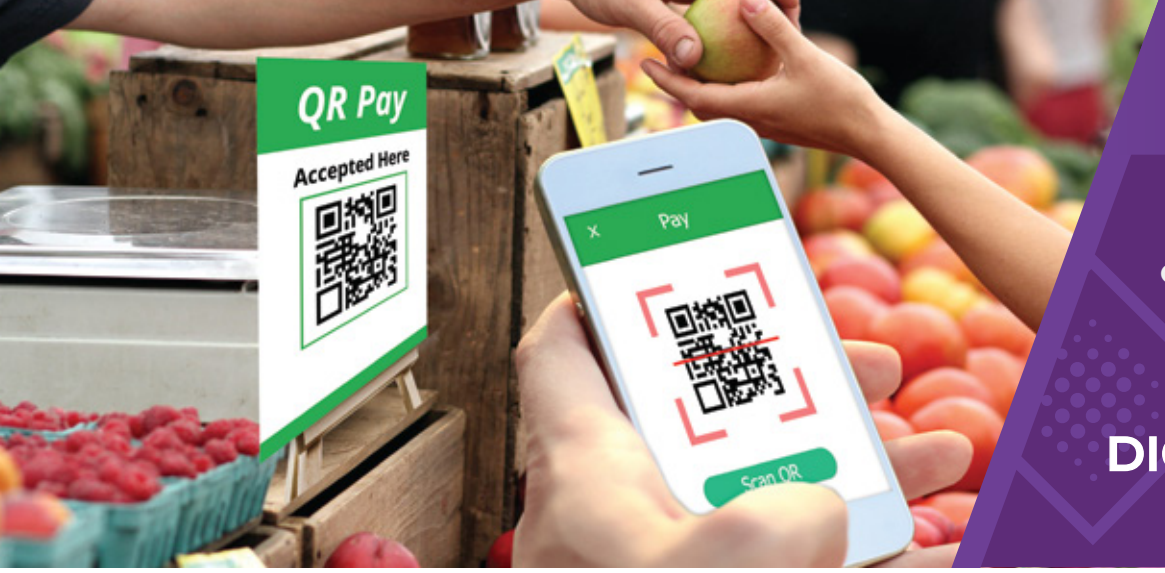

V-KEY
STRONGER WITH V-OS

CASHLESS PAYMENT
CASE STUDY

SECURE DIGITAL WALLET

THE OVERVIEW

ENABLING CASHLESS PAYMENTS

A leading payment services group in Singapore, known for enabling cashless transactions across major banks, merchants, and consumers, developed a mobile application to bring its payment offering to the smartphone. The intended mobile app represented a crucial step forward for the payment services group, as it sought to transform its financial services platform, and to activate fully digital and cashless transactions.

With over S$1 Trillion worth of transactions every year, the mobile app would bring the convenience of cashless transactions to personal mobile phones, and establish the Group as a relevant, innovative, and forward-looking player in the financial services industry.

SOLUTION-AT-A-GLANCE

- Trusted Identity
- Cross-Platform Solution
- Virtual Card
- Secure Keypad
- Convenience, UX

- V-OS App Protection

THE BUSINESS INITIATIVE

DELIVERING SECURE PAYMENTS TO A SMARTPHONE

With 30 years of innovating and delivering cashless transactions, our customer was intent on driving a mobile experience to its users. With smartphones becoming more powerful and more accessible, services like online shopping, video-streaming, mobile payments – both debit and credit, are among the growing list of lifestyle services migrating onto these devices via purpose-built apps.

However, while the smartphone remains the fastest growing platform globally, it is also the most insecure. While some manufacturers have built-in hardware-based security, these are often proprietary and have limited functionality for third-party developers. Mobile apps are left exposed to external threats, making smartphones the primary target for man-in-the-middle attacks, malware, ransomware, trojans, and viruses all disguised within other malicious apps that threaten to expose and steal personal data and critical transaction information.

The inherent lack of security of smartphones poses a series of challenges. Core to the user experience is the user's ability to use a Personal Identification Number (PIN) to authenticate and authorise transactions, which is a well-established practice and familiar to users. In-store Point-of-Sale (POS) merchant devices allow customers to input their PINs securely. However, with the use of native keyboards and third-party

keyboards, it is difficult to assure the same levels of security. Many keyboard applications have been known to be vulnerable to hackers, who would record and monitor keystrokes in their attempt to steal passwords and PINs.

Another consideration is to look at how to improve the User Experience (UX). Out-of-band SMS OTPs, the most commonly-used solution, meant that users have to leave the app, and input a string of numbers from SMS into the app, which they have to remember. This is inconvenient, and has been proven to be unreliable. In some instances, SMS OTPs arrive minutes after being requested due to poor network coverage, and this means that users are left helpless while trying to authorise transactions instantaneously. Finding a secure and convenient 2FA solution is critical to any payment platform.

THE INNOVATIVE SOLUTION

CROSS-PLATFORM MOBILE APP SECURITY, BUILT INTO THE APP

Our customer wanted to develop an independent and truly secure solution, which should minimally allow customers to seamlessly authenticate and authorize transactions in the same manner as using a PIN, while maintaining the same, if not better, security for PIN input. It was also crucial for the security solution to be cross-platform capable, and able to deliver a consistent authentication process on any device.

A full-fledged mobile application security solution would allow the Group to turn any smartphone into a virtual cashless payment card, by digitizing personal information like card and bank details and storing it within the mobile app on the customer's phone. This would give customers the option to completely replace the cards for both online and in-store purchases, across the Group's merchant network of over 100,000 contactless payment terminals across Singapore.

It also allowed customers to use the app as a means to perform other transactions, like paying bills, transferring money to other users of the mobile app, and even a money management tool, opening more opportunities for the Group to offer innovative and relevant services to its customers.

THE TECHNOLOGY

TRANSFORMING THE SMARTPHONE INTO SMART WALLET

With V-OS, the mobile app was able to securely store and process data within a secure framework, allowing the smartphone to preserve the same user experience as using a physical card with enhanced security on the mobile device. As part of the V-OS offering, V-OS also created a device "fingerprint" that allowed for a passive second-factor authentication that protected against malicious agents from cloning the mobile phone onto another device to extract sensitive and personal information. A passive 2FA also gave the Group confidence to allow up to $100 transactions without the use of a PIN. The Anti-Fraud Keyboard was a proprietary application developed to run entirely within the secure framework, shielding it from backdoors and rootkits.

With V-OS App Protection, an "always-on" tamper protection solution that monitors the runtime environment of the mobile application, the app is effectively protected against malicious viruses, trojans, ransomware, unauthorized remote access, debugging, function hooking or code injections. V-OS App Protection ensured the protection of data-in-transit, data-at-rest, and data-in-use, and actively defends against advanced persistent threats.

THE RESULT

With the mobile app fully secured against a variety of threats, our customer launched a mobile wallet which allowed its users to virtualize their existing cards. This gave them an expanded payment infrastructure where more users and more merchants would transact through a mobile app.