V-KEY
STRONGER WITH V-OS

HEALTH HUB
CASE STUDY

MOBILE APP SECURITY

THE OVERVIEW

SECURE STORAGE OF PERSONAL HEALTH INFORMATION

A government agency tasked with the management and design of national healthcare IT infrastructure, sought to relaunch its existing mobile app with a new set of on-demand personalized features for all citizens. The agency, whose users comprised of over 5 million citizens, was also tasked with custodianship and safeguarding of citizen healthcare data. This is a responsibility defined by the Electronic Transactions Act, which compelled the agency to ensure that any one of its citizen-facing services were protected by strong authentication standards and protocols.

Aligned to Singapore's Smart Nation initiatives, the vision needed to be innovative, easy-to-use, and secure. The features of the agency's mobile app needed to deliver new levels of access to health and medical information on personal mobile devices, such as medical history and health screening reports, for all citizens.

THE BUSINESS PROBLEM

BALANCING UX AND SECURITY REQUIREMENTS

As the custodian of the nation's health data, it was important for the agency to ensure a robust and resilient data security solution for its services. As the agency managed highly connected and deeply integrated healthcare databases for its country's citizens, the risks of data compromise were extremely high.

This represented a conundrum: the smartphone, while a convenient and powerful platform to deliver personalized services, was inherently insecure and vulnerable to unauthorized access.

While some smartphones proport to have built-in security, these are often hardware secure elements not accessible by third-party developers. Mobile Operating Systems, their apps, and the data within these apps are hence susceptible to man-in-the-middle attacks when information is transmitted between hardware and software . Other known malicious forms of malware, ransomware, trojans, and viruses, have also been known to successfully extract personal data.

To better protect citizen data, the agency assessed that the mobile app required stronger encryption and better protection from threats. More importantly, the security solution needed to ensure that the app's usability and user journey were not impacted as many users were already very comfortable with the functionality.

SOLUTION-AT-A-GLANCE

- Convenience, UX
- Data Security
- Optimising Performance

- V-OS App Protection

THE INNOVATIVE SOLUTION

STRONG MOBILE APP SECURITY, SEAMLESS USER EXPERIENCES

The app was designed to provide two distinct categories of information; Firstly, it served general information and news on health care matters; and Secondly, the new features looked to provide access to personal healthcare records like immunization, health screening reports, prescription data, to name a few.

This is a lot of data, and the volume of data on the mobile app, if encrypted in entirety, would slow down the app and impact useablity. Full encryption of the data would also impact the mobile device's battery life – an increasingly important user experience factor and consideration when designing an app meant for regular use.

This was where the secure storage features of V-OS provided a perfect solution for the agency. V-OS was able to store different levels and forms of data (strings, files, or even entire databases) giving the agency the flexibility to select the data it needed to encrypt, thereby optimizing the resources on the mobile device. The agency was then able to decide that it only required to encrypt a single module on the phone, instead of the complex task of encrypting the whole database.

In addition to encrypting the module, it was crucial to ensure the security and protection of data on the app against threats. With millions of potential users, the app needed to ensure that it would keep data secure even in a variety of situations, especially in cases where a citizen's phone was already compromised, or if the user had not updated their operating system to address known vulnerabilities.

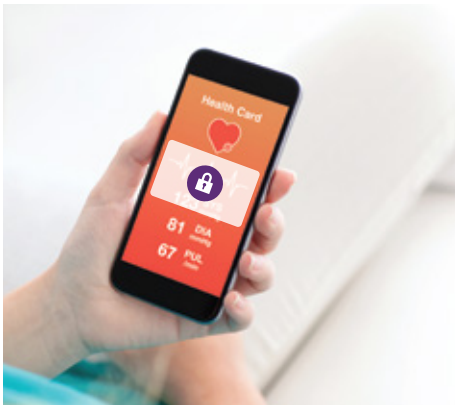
THE TECHNOLOGY

FLEXIBLE, AGILE DEPLOYMENT FOR NEW FUNCTIONALITY

V-OS was deployed to secure a specific module within the agency's mobile app, which powered the new functionalities using private patient data. Without the need to encrypt the entire app, the agency's development team was able to deploy the module secured by V-OS without re-developing the app, reducing the time taken for implementing the new features.

Furthermore, being cross-platform ready, V-OS was ready to be deployed on both iOS and Android versions of the agency's app. Once implemented, every instance of V-OS on a citizen's device would create a "fingerprint" of the device it was installed on, that allowed for a passive second-factor authentication process to protect against malicious actors seeking to clone the mobile phone onto another device to extract sensitive and personal information.

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



THE RESULT

With V-OS providing a strong security platform, the healthcare agency was able to confidently launch its offering to citizens looking to access their medical data conveniently and securely on their phones.