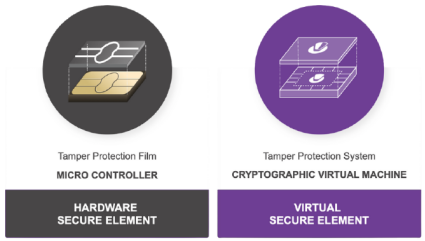
V-OS VIRTUAL SECURE ELEMENT

A Virtual Operating System Trusted by More Than 200 Million Devices Globally

Enable Secure Transactions From Insecure Devices

V-Key's internationally-patented V-OS Virtual Secure Element (VSE) decouples trust from infrastructure. Based on cryptographic breakthroughs and advanced cybersecurity protections, V-OS lets you virtually embed a secure, isolated enclave to protect keys, confidential logic, and other business-critical data on any phone, IoT or compatible device.



V-OS is the world's first VSE to be FIPS 140-2 Level 3 validated (US NIST), achieve FIDO security targets, and be Common Criteria EAL3+ certified. It has also been accredited by the Infocomm Media Development Authority of Singapore (IMDA).

By providing a lightweight software key protection solution that complies with standards once reserved only for expensive hardware solutions, V-OS enables every app at the endpoint to have a VSE that creates a consistent level of security among all the Bring Your Own Device (BYOD) devices that connect to your backend, independent of the device OS or hardware.

Bridging the Trust Gap: A Design Flaw of Hardware Security Protected Apps

V-Key's research team has released a white paper detailing a general architectural design flaw that hackers can exploit to get an app's authenticator keys or other important cryptographic elements -- even if the phone's trusted execution environment is used. When mobile authenticators are targeted, hackers can make unauthorised transactions or sign bogus documents, regardless of any hardware-based protection provided by a phone. This is especially true for jailbroken phones, rooted devices, or models susceptible to what is known as a "privilege escalation vulnerability". The targeted app doesn't even need to be running or be tampered with to be compromised. V-Key calls this very serious design flaw the, **Trust Gap.**

The best solution to bridge this Trust Gap is to provide a means to identify each end point in the system -- whether they be apps, servers, or even individual IoT devices. V-OS can provide a secure element bound to every app which can serve as proof of an app's identity and integrity without the need for any external authenticators, and without compromising the user experience.

WHAT WE DO

V-Key is a software-based digital security company whose technology powers security solutions that deliver the highest level of defence and control for digital identity, user authentication, access and authorisation -- without compromising the user experience. It is trusted by government, banking, and mega-app clients across the region to connect people, organisations, and devices everywhere by securing the global digital economy.

OUR MISSION

To provide a secure Universal Digital Identity to power trusted digital services globally.

V-Key provides trusted, reliable, and secure Digital ID services that enable people to truly and safely participate in the modern economy.

TO DOWNLOAD THE TRUST GAP WHITE PAPER:

Need more info? Contact insidesales@v-key.com

V-OS VIRTUAL SECURE ELEMENT • V-OS APP IDENTITY
V-OS MOBILE APP PROTECTION • V-OS MOBILE SMART TOKEN • V-KEY SMART AUTHENTICATOR

info@v-key.com **www.v-key.com**

A Technical Brief: What Makes V-OS Different?

A number of software protection solutions rely on a combination of code obfuscation and some form of Whitebox Cryptography (WBC) for static protection and runtime protection against debugging, tampering or code injection attacks. Architecturally, the primary weakness of such solutions are the cryptography and runtime protection mechanisms that run natively in the ARM processor codes. Unfortunately, attackers can easily bypass these mechanisms in order to gain access with an exploit commonly known as a "code-lifting" or a "decryption oracle" attack.

By contrast, V-Key's protection mechanisms only run within the ultra-secure V-OS virtual machine. Attackers cannot tamper with, or bypass these protection mechanisms without first breaking into the virtual secure element itself. Moreover, several built-in protection mechanisms prevent an attacker from easily breaching V-OS (including but not limited to root/jailbreak detection, as well as protection against static app tampering, dynamic app tampering through hooking or code injection, debugging, key logging, stealing of critical data, man-in-the-middle attacks, among others). Most importantly, with V-OS Virtual Secure Element technology, any cryptographic keys protected by V-OS will not be retrievable as plaintext by any attacker.

- TAMPER-RESISTANT DESIGN
- ANTI-REVERSE ENGINEERING
- CERTIFIED CRYPTOGRAPHY
- ENCRYPTED DATA AT-REST AND IN-USE
- TIME LOCKING
- ANTI-CLONING AND CODE LIFTING PROTECTIONS
- PROPRIETARY REDUCED INSTRUCTION SET COMPUTER(RISC) BASED INSTRUCTION SET ARCHITECTURE (ISA)
- ANTI-DEBUGGING, ANTI-HOOKING AND ANTI-CODE INJECTION
- APP INTEGRITY AND LIBRARY SIGNATURE CHECKS
- EMULATOR AND ROOT/JAILBREAK DETECTIONS

V-OS Deployment Modes

V-OS Native APIs

Any native application can access out-of-the-box V-OS features for developing secure applications. These features leverage aspects of V-OS's security isolation in a black-box manner to achieve enterprise-grade security despite still being considered native-level protections. Function calls into V-OS ensure that the native APIs and other mobile application code cannot be tampered with by an attacker.

V-OS Trusted Applications

Easily create Trusted Applications (TA) for situations that demand maximum security. A TA is simply a program written for the V-OS runtime environment. It can be used to encapsulate part of or all the logical code representing a critical process and can define its own trusted storage and communication protocols. The critical difference between a TA and native mobile app is that the entirety of the TA's code is secure within V-OS's isolated execution environment.

V-OS USE CASE: CRUNCHFISH

Crunchfish AB is a pioneering Fintech company based in Malmö, Sweden that offers unique offline payment solutions.

Crunchfish's Digital Cash is an e-Wallet solution that provides an instant offline payment and online settlement, regardless of connection issues, infrastructure failures or overloaded servers. The Digital Cash solution is a Trusted Application (TA) firmly protected by the **V-OS Virtual Secure Element**, a trusted execution environment where Digital Cash's cryptographic keys are securely stored, and where all credentials, transactions and logs can be safely kept away from the unsecure environment of mobile operating systems.

V-OS Use Case: RedTea Mobile

Redtea Mobile is an eSIM (embedded SIM) service and solution provider enabling out-of-box cellular connectivity compliant with GSMA eSIM standards, eSIM terminal technology, and eSIM based applications. The V-OS VSE provides a security foundation on which Redtea can build a range of Digital Identity services for its eSim which can be used in both Mobile and IoT devices.

info@v-key.com www.v-key.com

For more info, please contact insidesales@v-key.com