V-KEY
STRONGER WITH V-OS

# V-OS VIRTUAL SECURE ELEMENT

## HARDWARE SECURITY IN SOFTWARE FORM

## BENEFITS

- ERADICATES COSTLY HARDWARE DEPENDENCY
- OPTIMAL PERFORMANCE AND TESTED FOR SCALABILITY
- SEAMLESS DEVELOPER INTEGRATION
- CONFIGURABLE SECURITY POLICIES
- OVER-THE-AIR UPDATES
- GLOBALLY CERTIFIED

## SOFTWARE SECURITY SOLUTION YOU CAN TRUST

V-OS is the world's first and only true patented Virtual Secure Element (VSE) based on Global Platform specifications. It is designed to meet the security requirements for FIPS 140-2 Level 3 and FIDO security targets, and  is Common Criteria (CC) EAL 3+ certified.

Today, security sensitive mobile applications such as Mobile Authenticators, Mobile Wallets, and Mobile Banking applications depend on hardware secure elements (SEs) such as dongles, SIM, microSD cards, and ARM TrustZone (or TEE) to execute critical transactions. However, these hardware solutions are costly, cumbersome to distribute and manage, and limit their proliferation.

At an abstract level, V-OS is an operating environment similar to how Microsoft Windows is an operating system (hence the name V-OS). Applications written to run on V-OS are designed to leverage its standard cryptographic libraries for data encryption and decryption, secure data storage, secure file IO (input/output operations a.k.a. reading and writing files), encrypted runtime memory, and attestation capabilities.

### ABOUT V-KEY

V-Key is an internationally-acclaimed software-based digital security company, headquartered in Singapore. V-Key's pioneering technology powers ultra-high security solutions on premise and Cloud-based, for digital identity management, user authentication and authorization, IoT, as well as electronic payments for major banks, payment gateways, and government agencies. Today, V-Key secures millions of users around the world, enabling digital leaders to create powerful customer experiences that combine high security and delightful convenience.

To better serve different business needs and models, V-OS VSE is made to be extensible. It can be deployed in 2 different ways:

## 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 better security but are still considered native-level protections. Function calls into V-OS ensure that the native APIs and other mobile application code is not being tampered with by an attacker.

## V-OS Trusted Applications

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

V-Key offers a range of solutions built on V-OS VSE to provide organizations and end-users the maximum security needed:

- **V-OS App Protection**
- **V-OS Smart Token**
- **V-OS Messaging**
- **V-OS Face Biometrics and eKYC**
- **V-OS Trusted Identity Services**

## PRODUCT FEATURES

- 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

### WHAT IS V-OS

V-OS is V-Key's patented solution and the world's first virtual secure element to be FIPS 140-2 validated (US NIST), Common Criteria EAL3+ certified and accredited by the Infocomm Media Development Authority of Singapore (IMDA). V-OS uses advanced cryptographic and cybersecurity protections to comply with standards previously reserved only for expensive hardware solutions. Integrated seamlessly with biometrics, PKI-based technology and out-of-band authentication, V-OS makes delightful user experiences possible while being uncompromisingly secure. V-OS has been the subject of multiple rigorous penetration tests. It has also been stress-tested by e-commerce players, government agencies, regulatory bodies and financial services companies.

## HOW IS V-KEY 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 protections to protect against debugging/tampering/code injection. Architecturally, primary weakness of such solutions is cryptography and runtime protection mechanisms being run natively in the ARM processor codes. Therefore, attackers can easily bypass these protection mechanisms in order to gain access to the cryptography; this is commonly known as a "code-lifting" or "decryption oracle" attack.

In contrast, V-Key's protection mechanisms run within the V-OS virtual machine. Attackers cannot tamper with or bypass these protection mechanisms without first breaking into the V-OS virtual machine itself. Moreover, protection mechanisms themselves prevent an attacker from easily breaking into V-OS. V-Key's architecture therefore allows the runtime protections and static protections of V-OS to interlock in order to provide much stronger security that cannot be easily overcome by an attacker.

V-OS can be used to enable a plethora of use cases that require banking and government- grade cybersecurity, including but not limited to:

- Mobile 2nd-Factor Authentication (2FA) tokens
- Mobile electronic Know Your Customer (eKYC) processes
- Virtual payment cards, similar to Android Pay/Samsung Pay/Apple Pay
- Mobile app biometric verification
- Mobile identity
- Virtual SIM cards

### TECHNICAL SPECIFICATIONS

**Out-of-the-Box Support:**
**Block Ciphers:** AES (CBC, ECB, CCM, CTR, XTR, KW), 3DES-CBC, DES
**Stream Ciphers:** RC4, HC128, RABBIT
**Public Key:** RSA (PKCS#1, OAEP, SHA-1/256), ECC (P-256, P-384, P-521, SHA-1/256)
**Hash:** SHA-1/256, HMAC (SHA-1/256), MD5
**Key Derivation:** KDF-HMAC, PBKDF2 PRNG: ANSI X9.31 AES/DES, Hash DRBG SHA256
**Other Features:** OATH/OCRA, SSL/TLS, Mutual TLS
**Platforms:** Apple iOS, Google Android, Huawei EMUI/Harmony OS, IoT Devices

VKEY2021_MAR

SPEAK TO A V-KEY SALES REPRESENTATIVE TODAY. CONTACT INFO@V-KEY.COM

GLOBALPLATFORM®
THE STANDARD FOR MANAGING APPLICATIONS ON SECURE CHIP TECHNOLOGY

FIPS VALIDATED 140-2

Common Criteria

fido™ ALLIANCE MEMBER

SG:D ACCREDITED

V-KEY
STRONGER WITH V-OS

V-OS VIRTUAL SECURE ELEMENT | V-OS APP PROTECTION | V-OS SMART TOKEN
V-OS FACE BIOMETRICS AND EKYC | V-OS MESSAGING | V-OS TRUSTED IDENTITY SERVICES

◆ info@v-key.com ◆ www.v-key.com