V-KEY
STRONGER WITH V-OS

V-OS Virtual Secure Element

Mobile Digital Identity, Authentication and Authorization

Stronger with V-OS

STRONGER WITH V-OS

- Mobile Identity
- V-OS App Protection
- V-OS Smart Token
- V-OS Messaging
- V-OS Face Biometrics
  V-OS eKYC

Virtual Secure Element

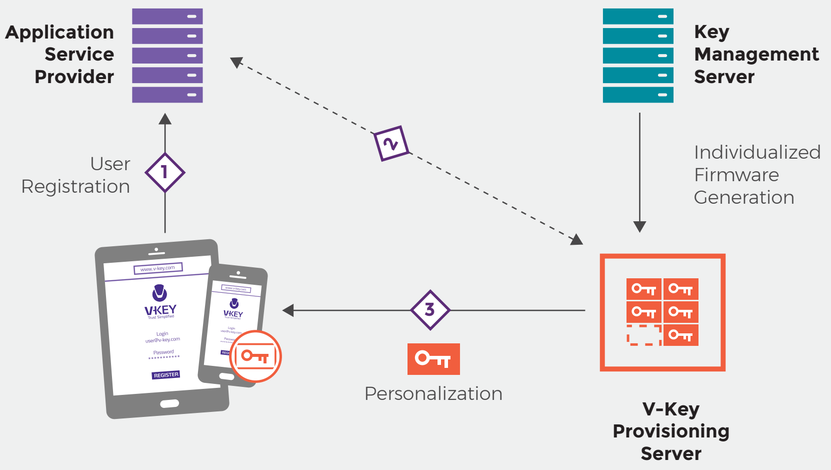
V-OS is the world's first and only true patented Virtual Secure Element (VSE) based on Global Platform specifications and designed to meet the security requirements for FIPS 140-2 Level 3.

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.

V-OS' patented and advanced cryptographic capabilities were created so that Trusted Applications can execute securely and reliably, and process and store sensitive data on mobile devices without the need for a hardware SE. It isolates trusted business logics from untrusted mobile application and software environment, and prevents an attacker with control of the underlying operating environment from accessing or exposing sensitive logic or data.

V-OS
Secure
Element

V-OS Personalization and Provisioning Process


Application Service Provider
Key Management Server
User Registration
1
2
Individualized Firmware Generation
3
Personalization
V-Key Provisioning Server

VIRTUAL SECURE ELEMENT FEATURES AND SPECIFICATIONS

Tamper-Resistant Design

a. V-OS achieves isolation through layered tamper detection and response mechanisms such as anti-debugging, device binding, and anti-reverse engineering, to protect against hackers and malware.

b. Sensitive cryptographic keys, data, and application codes are protected using advanced techniques in and around V-OS such as binary code morphing, memory encryption, and whitebox cryptography techniques.

Eradicate Costly Hardware Dependency

a. For a fraction of the costs and effortless over-the-air deployment, V-OS is able to minimize total costs of ownership and drive faster market penetration.

b. Personalized keys and cryptographic protections can be dynamically provisioned for the highest levels of security, and to support key rotations and tokenization requirements.

Certified Cryptography

a. V-OS is a patented cryptographic virtual machine that ensures the integrity of crypto processing as well as protects encryption keys and sensitive information.

b. It is designed to meet security requirements for FIPS 140-2 Level 3 and Common Criteria EAL3+.

Seamless Developer Integration

a. V-OS comes with a flexible and extensible SDK framework incorporating individualization and personalization capabilities for easy integration into your secure mobile applications.

b. 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)

Hash: SHA-1/256, HMAC (SHA-1/256), MD5

Key Derivation: KDF-HMAC, PBKDF2

PRNG: ANSI X9.31 AES/DES, Hash DRBG SHA1/256

Other Features: OATH/OCRA, SSL/TLS

Platforms: Apple iOS and Google Android

GLOBALPLATFORM The Standard for Managing Applications on Secure Chip Technology FIPS VALIDATED 140-2 fido alliance member SG:D ACCREDITED

V-KEY STRONGER WITH V-OS

V-Key is a global leader in software-based digital security, and is the inventor of V-OS, the world's first virtual secure element. Contact us today to schedule an appointment and demonstration.

E info@v-key.com **W** v-key.com **T** +65 6850 5155