Version 1.1

Confidential

# V-Key Technology Overview

## Whitepaper



V-KEY

STRONGER WITH V-OS

## Document Metadata

| Property | Content |
|---|---|
| Document Title | V-Key Technology Overview Whitepaper |
| Document Version | 1.1 |
| Release Date | 2018-11-01 |

## Revision History

| Version | Author | Date | Description/Changes |
|---|---|---|---|
| 0.3 | V-Key | 2017-02-13 | Past releases |
| 0.4 | V-Key | 2018-10-09 | Converted to new document template |
| 1.0 | V-Key | 2018-11-01 | Latest updates |
| 1.1 | V-Key | 2022-10-06 | Updates and corrections |

## CONFIDENTIAL

# Table of Contents

# 1 Introduction

**Mobile Security, Simplified**

V-Key believes that security should be provided to users and enterprises in a simple and easy-to-use manner. Mobile security must operate transparently in the background, providing assurance for everyday usage while enabling rather than impinging on the user experience. At the same time, enterprises need security solutions that can be easily integrated, wrapping their existing mobile applications with military-grade security while allowing their developers to continue using the same mobile frameworks that they are accustomed to.

**Convergence Changes Everything**

Until relatively recently, devices had fixed roles—a mobile phone to make a call, a computer to manipulate data. Those distinctions have blurred. Now, we expect the digital world to revolve around us as individuals, regardless of the device we are using. We want to be able to make payments and access our email with our mobile phones or use our mobile devices as our wallets.

**Security Delivers Trust**

We can only operate freely in this digital environment if we can prove who we are. We will only trust systems to run these important aspects of our lives if we know they're secure. The businesses providing these services must be able to identify their valid users and ensure their digital properties are protected. So security—for our identity, our information, and our interaction—is paramount. V-Key enables these digital interactions by providing the bedrock of trust in mobile applications.

# 2 V-Key's Security Foundation

As mobile phones today lack a proper Hardware Security Module that allows for the secure storage of cryptographic keys and for secured cryptographic computation, V-Key implements a security sandbox that implements these protections in user-space software.

## 2.1 V-OS Secure Virtual Machine

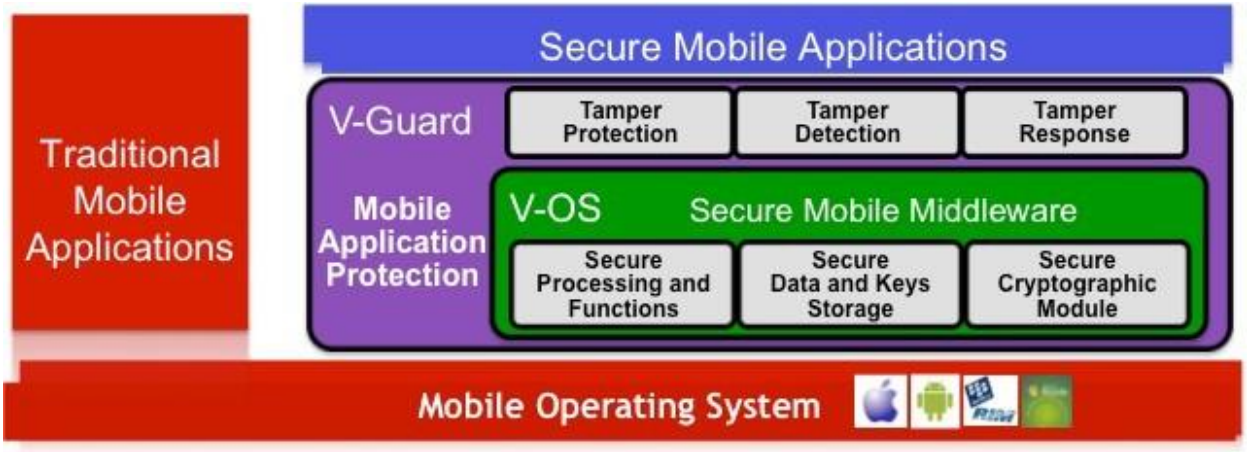



***Figure 1. V-OS Secure Virtual Machine***

At the base of V-Key, a virtual machine named V-OS implements a secured sandbox for trusted storage and execution. As a secure sandbox, V-OS is able to perform cryptography and other security-critical functions within the virtual machine in a manner that protects them from tampering by attackers.

Unlike other virtual machines, whose security models seek to prevent any potential attackers or malware from leaving the virtual machine, the V-OS virtual machine security model is designed to keep attackers and malware within the underlying operating system from gaining access to the information and processing contained within the virtual machine. In this way, it provides a black box for security-critical processing to be performed exclusively within the virtual machine.

The virtual machine executes a 32-bit RISC Assembly instruction set architecture loosely based on MIPS. No heap is implemented, and a randomly-generated stack cookie protects against stack-based attacks. The virtual machine itself protects against stack underflows / overflows and is able to mark memory segments for read / write / execute protection.

The sandbox also limits system calls to those necessary for the cryptographic computation and security-critical calls. This makes it extremely difficult for an attacker to reverse-engineer V-Key in order to obtain either the details of the cryptographic algorithms used or the cryptographic keys stored within the sandbox, or to hack V-OS to bypass the protection mechanisms.

The embedded microcode in the sandbox is also able to lock the usage of the virtual machine to the user's phone by verifying the UUID, in instances where the mobile application is intended for use only on a single device. This can also help to prevent the application data from being copied and used on another device by an attacker.

## 2.2 V-OS App Protection Tamper-Proof Layer

On top of the V-OS layer, V-Key implements a tamper-prevention, detection, and response layer, named V-OS App Protection. This layer is implemented as Assembly codes within the virtual machine and includes anti-reverse engineering and anti-static analysis techniques such as binary code morphing, anti-debugging techniques, jailbreak and trojan detection techniques, and anti-API hooking checks. These provide a trusted environment for the sandbox to operate and ensure that the sandbox and the phone have not been tampered with.

V-OS App Protection implements several best-of-breed techniques to ensure a trusted mobile environment. These include several jailbreak / root-detection techniques, combinations of heuristic and signature-based detections for possible malware, and functional checks to validate the integrity of the underlying mobile operating system.

Several of these techniques are also believed to be unique to V-OS App Protection. For example, V-OS App Protection is able to identify the libraries loaded by jailbreak tweaks and trojans into the current application; this is particularly important in a sandboxed environment typical in a modern mobile operating system where an application may not have full access to system applications, folders, and files.

In instances when tampering or an untrusted mobile environment has been detection, the sandbox can respond by disabling usage of the sandbox, zeroing the cryptographic information or other security parameters, or generating responses that inform a third-party of the attempted tampering, depending on the requirements of the mobile application.

## 2.3 Dynamic Protections

The V-OS and V-OS App Protection layers make it extremely difficult for an attacker to gain access to security tokens, even with full access to the mobile phone. They are ableto do this because the interaction of the secured virtual machine model and the dynamic protection mechanisms maintains control over the mobile environment and denies an attacker the ability to control the virtual machine execution flow for analysis.


Each instance of V-OS is protected with a unique set of microcodes, encrypted to that individual instance. These are only decrypted into the virtual machine memory at runtime and are wiped after execution to prevent reverse engineering. This, combined with a proprietary set of virtual machine codes and other dynamic protections such as anti-debugging protection mechanisms, prevent an attacker from analyzing the virtual machine processing and its content.


In order to continually harden the security of the sandbox over time, V-OS provides a mechanism for trusted updates of the virtual machine microcode. This enables V-Key to keep ahead of evolving attacks by hackers and malware writers, providing additional protection for V-OS and V-OS App Protection by allowing the introduction of new protection mechanisms and security features.

# 3 Securing Digital Identity

V-Key provides a complete solution, the V-OS Smart Token family, for advanced authentication on the mobile phone. With the rock-solid V-OS and V-OS App Protection as a security foundation, the V-OS Smart Token provides a secure second- factor authentication solution on mobile in a convenient and user-friendly package for both users and enterprises. This is available either as a stand-alone mobile token application, or as a library for enterprises to integrate into their own mobile applications for seamless authentication.

## 3.1 Seamless Integration with V-OS Smart Token

### 3.1.1 One-Tap Authentication

To the user, the authentication experience is seamless; when integrated with an existing mobile application, the authentication is performed automatically when the user logs in or is prompted to confirm a transaction. Even with a separate mobile token application, the user will receive a push notification that launches the application and requires a single tap from the user to confirm the login or transaction. Both the push notification and authentication response are protected using a HTTPS connection to the authentication server.

### 3.1.2 Plug-and-Play for Enterprises

For enterprises seeking to integrate V-OS Smart Token's authentication library into their own applications, V-Key provides a plug-and-play library that adds second-factor authentication seamlessly into existing mobile applications, as well as a V-Key Enterprise Dashboard that provisions and manages the authentication tokens. V-OS Smart Token's authentication library supports one- time password generation for authentication, challenge-response, and transaction signing.

## 3.2 Best-of-Breed Cryptography

### 3.2.1 Authentication

The sandboxed token microcode will generate a single-use PIN for use in second-factor authentication using the following parameters derived within the sandbox: the 256-bit encryption-key, the 160-bit UUID, and the 32-bit current time since 1970 (in 30-second steps).

### 3.2.2 Advanced Token Features

For transactions that are deemed risky, such as funds transfers, there will be an additional input to the cryptographic algorithm, as per OATH standards: this can be either a challenge number, or the hashed concatenation of the account number and transaction amount.


### 3.2.3 Cryptographic Algorithms

The sandbox currently uses OATH-compliant algorithms for OTP generation, challenge-response, and transaction signing. The token can generate either a 6-digit or 8-digit PIN depending on the bank's requirements. This PIN is calculated from the cryptographic response by taking modulo $10^7$ for a 6-digit PIN, and modulo $10^9$ for an 8-digit PIN.

### 3.2.4 Trusted Time Source

The token will use the device time if the time is set to be synced automatically with the network; otherwise, it will require an internet connection to connect to a trusted time server.

## 3.3 Simplified Activation

### 3.3.1 Integrated Activation


When integrated with a bank or enterprise mobile application, the V-OS Smart Token will be activated the first time the user logs in using his or her username and password within the mobile application. The activation process will download a unique V-OS Smart Token microcode along with its corresponding set of 256-bit random seeds into the application storage. The seeds, encrypted by microcode embedded secrets upon provisioning, are re-encrypted to device-bound secure storage after first launch. They are then used to generate the one-time passwords used for second-factor authentication during login, and transaction signatures for bank transactions.

### 3.3.2 Stand-alone Activation

In cases when the V-OS Smart Token standalone mobile token application is used, the bank or enterprise will generate a token serial number and registration code, which will be provided to the user via an out-of-band means, such as displaying to the user after the user logs in to the enterprise website with his or her username and password, or sent via a hardcopy letter. At the enterprise, this will be tied to the user's account for future one-time password or transaction signing purposes. On the standalone mobile token application (referred to as mobile app), the user will enter the issued token serial number so that mobile app can download its corresponding unique V-OS Smart Token along with its encrypted seed data from V-Key registration server. Similar to the Integrated Activation process, the provisioned token microcode embeds a set of 256-bit random seeds used to generate one-time passwords and transaction signatures. The embedded token seeds must be decrypted by user input of the registration code on the first use, after which they are re-encrypted to device bound secure storage.

More information about the cryptographic implementation of V-OS Smart Token and usage under various deployment scenarios is available in a V-OS Smart Token Cryptographic Whitepaper {available upon request).

# 4 Securing Digital Information

Mobile phones today can readily be hacked by attackers, through mobile phone vulnerabilities, malicious mobile applications, or through compromised desktop computers. V-Key provides the V-OS App Protection wrapper to securely and silently protect mobile applications against a multitude of threats on the mobile phone, acting as an invisible mobile application firewall against a compromised mobile phone operating system.

## 4.1 Secure Wrapping with V-OS App Protection

### 4.1.1 Solid Security Foundation

The V-OS App Protection wrapper contains the same security foundation as all of V-Key's products: the V-OS sandbox provides a secure sandbox for security-critical processing and data, while the V-OS App Protection mechanisms secure the mobile environment for the mobile application.

### 4.1.2 Simple Wrapping

V-Key's innovative security is provided as a convenient V-OS App Protection wrapper for existing enterprise mobile applications. In this way, enterprises can quickly and easily include all of V-OS App Protection's innovative security features in their existing mobile applications, without the need to rewrite their codes or change their development methodology.

## 4.2 Invisible Mobile Application Firewall

### 4.2.1 Securing Mobile Applications


V-OS App Protection acts as a mobile application firewall by providing a trusted environment for secure processing and data storage for the mobile application to use. Cryptography and security-critical functions are moved into the V-OS secure sandbox, while V-OS App Protection's advanced protection mechanisms secure the application from mobile threats.

### 4.2.2 Invisible Protection

For users and developers, the V-OS App Protection is an invisible wrapper that protects a mobile application. The user experience remains exactly the same, while developers continue to call the same native APIs they are used to when developing the mobile application. V-OS App Protection starts automatically when the mobile application is launched, continually checks the integrity of the mobile environment in the background, and transparently intercepts security-critical functions to provide additional protection for the application.

### 4.2.3 Mobile Actionable Intelligence

Using the same V-Key Enterprise Dashboard, enterprises can monitor the threats detected on their user phones through the applications wrapped with V-OS App Protection. Enterprises can start by collecting intelligence on the threats detected before deciding how they want to take action against them. This enables enterprises to understand their mobile landscape and plan how to support their users in recovering their devices from such attacks.

## 4.3 Threats Protected Against

### 4.3.1 Malware

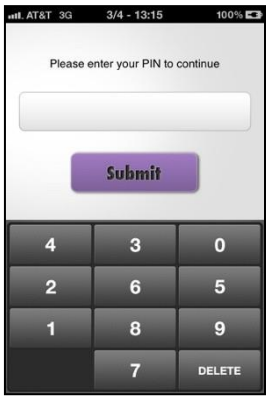
V-OS App Protection checks the mobile environment for possible threats, ranging from low-risk threats such as jailbreaking to high-risk vectors such as mobile trojans and other forms of malware. Enterprises can choose to disable the execution of their application when a pre-defined threat level is breached; for example, a banking application may choose to allow itself to run on a jailbroken phone, but not when the phone contains keylogging trojans.

### 4.3.2 Keylogging

V-OS App Protection implements several protections against keylogging in order to provide defense-in-depth against this common attack against mobile applications. Firstly, V-OS App Protection scans the mobile environment for keyloggers using a combination of heuristic checks and for the signatures of known keyloggers (just as it does for other forms of malware). Secondly, V-OS App Protection provides secure keyboards for both numerical PIN entry and text entry, which effectively provides a keylog-proof replacement keyboard for a mobile application. This secure keypad can optionally provide randomized key locations to provide even more security, if required.

### 4.3.3 Data Stealing

Mobile applications typically store security-critical information within the phone's native secure storage. This is encrypted using the user's access PIN, but is accessible when the phone is being used and thus can be easily stolen by an attacker. V-OS App Protection can transparently add additional encryption of the application data stored in the native secure storage so that it cannot be stolen by an attacker. This data can remain accessible to other applications from the same enterprise or can optionally be locked to the current device.


### 4.3.4 Theft of Cryptographic Information

V-OS App Protection can provide cryptographic computation and storage within V-OS for mobile applications, in order to help enterprises, protect cryptographic information. To use this feature, enterprises pre-load private cryptographic keys and data within the V-OS microcode used by the V-OS App Protection wrapper. When deployed to the mobile applications, this cryptographic information is encrypted and protected from theft by hackers and other attackers.

# 5 Securing Digital Interaction

V-OS App Protection provides a a **banking and government-grade secure messaging and communications** solution for iOS and Android mobile apps. It can be used to enable various use cases that require secure communications, including:

- A secure chat client for customer engagement and servicing
- A secure chat client backed by an artificially intelligent chat bot
- A secure peer-to-peer chat client
- A secure message inbox for real-time dissemination of sensitive or critical information

## 5.1 Built on the World's First Virtual Secure Element

V-OS Smart Token is built on V-OS, the world's first virtual secure element. V-OS is FIPS 140-2 Validated by NIST, accredited by IMDA (Singapore), and remains unbroken after multiple rigorous penetration tests.

Because of this, V-OS Smart Token automatically comes with banking and government-grade cybersecurity resiliency.

## 5.2 Problems Solved

**Insecure SMS Replacement**

Message is designed to act as a secure alternative to SMS, for organizations that push information directly to their end-users' mobile devices.

SMS or Short Message Service has become a ubiquitous channel for organizations, including banks and government agencies, to communicate with users. However, SMS suffers from some fundamental security flaws, including but not limited to:

- Messages are unencrypted and can be intercepted in-transit
- Vulnerable to being intercepted by malware on the phone itself, especially on Android
- The SMS network, known as SS7, has been proven to be vulnerable to intrusion attempts, and can potentially provide an attacker complete access to a user's SMS (and voice calling) history[1]

**Secure End-to-End Communications**

A standard alternative to SMS is to rely upon in-app notifications or push notifications, which can be encrypted using industry-standard techniques such as public key infrastructure (PKI).

However, in general, the mobile app's encryption key and digital certificate, used to securely communicate with a server, has few or no cybersecurity protections, and can be easily stolen or hijacked by a malicious actor. This makes securing end-to-end communications for high security mobile app use cases in banking, finance, and government unfeasible with the majority of current solutions.

[1] http://securityaffairs.co/wordpress/39409/cyber-crime/ss7-flaw-surveillance.html

## 5.3 Benefits

**Securing Data in Transit**

V-OS Messaging provides encrypted end-to-end communications between the mobile app client and the server. This communication cannot be interpreted or decrypted by a malicious third- party that manages to intercept the message in transit.

**Securing Data at Rest**

Even if communications are encrypted in transit, the mobile client is a very likely attack surface for a malicious actor, as the mobile app is where the encryption key, digital certificate, and message history are kept. The encryption key and digital certificate used for this end-to-end encryption are protected inside the mobile app itself and is extremely resistant to intrusion or tampering.

The use of a PKI technology foundation not only guarantees end-to-end encryption, but provides two additional benefits:

**Verifying the Identity of Communicating Parties**

The parties involved in any kind of communication can identify themselves to each other using their digital certificates, thus reducing the likelihood of a third-party masquerading as one of the original parties.

**Non-Repudiation**

Any party that sends a message, such as the client or server, cannot deny that they sent a message. This is because every message sent by the client or server can be digitally signed by the originating party.

# 6 Built to Industry Best Standards

## 6.1 Standards Overview

The eventual goal of this architecture is to allow V-Key's security module to be certified to FIPS 140-2 Level 3. To date, no other software architecture has been designed to achieve this. FIPS 140-2 in fact implicitly allows for software cryptographic modules to be certified to higher levels by specifically excluding the physical security requirements listed for modules implemented entirely in software.

## 6.2 Common Criteria EAL3+ Validated

V-OS Virtual Secure Element Version 4 is validated for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1 at EAL3+.

The security target is derived from the following protection profile: Protection Profile for General Purpose Operating Systems, Version 4.1, March 9, 2016.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI).

## 6.3 FIPS 140-2 Validated

FIPS 140-2 is a NIST standard on Security Requirements for Cryptographic Modules. The V-OS Cryptographic Module has attained FIPS 140-2 Level 1 Certification (Cert #2706).

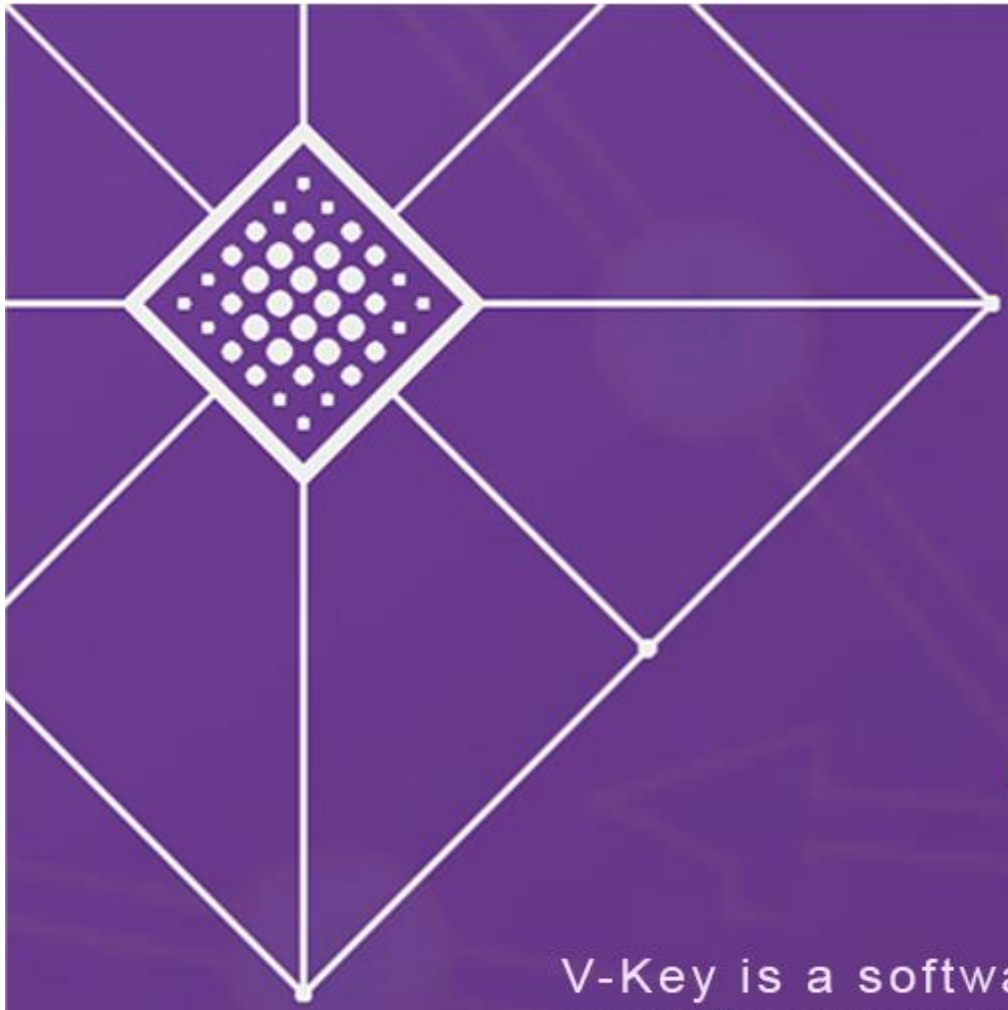
This architecture allows the V-Key security module to be certified at FIPS 140-2 Security Level 3, providing security assurance above and beyond that of normal software and hardware security modules and applications.

| Security Area | Level 3 Requirements | Compliance |
|---|---|---|
| Cryptographic Module Specification | Specification of cryptographic module, cryptographic boundary, Approved algorithms, and Approved modes of operation. Description of cryptographic module, including all hardware, software, and firmware components. Statement of module security policy. | Yes |
| Cryptographic Module Ports and Interfaces | Data ports for unprotected critical security parameters logically or physically separated from other data ports. | Yes |
| Roles, Services, and Authentication | Identity-based operator authentication. | Yes |
| Finite State Model | Specification of finite state model. Required states and optional states. State transition diagram and specification of state transitions. | Yes |
| Physical Security | Production grade equipment. Locks or tamper evidence. Tamper detection and response for covers and doors. | Not subject to this requirement |

| | | |
|---|---|---|
| Operational Environment | Referenced PPs plus trusted path evaluated at EAL3 plus security policy modeling. | Yes, with Common Criteria certification |
| Cryptographic Key Management | Key management mechanisms: random number and key generation, key establishment distribution, key entry/output, key storage, and key zeroization. | Yes |
| | Secret and private keys established using manual methods shall be entered or output encrypted or with split knowledge procedures. | Yes |
| EMI/EMC | 47 CFR FCC Part 15. Subpart B, Class B (Home use). | Yes (underlying hardware) |
| Self-Tests | Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical functions tests. Conditional tests. | Yes |
| Design Assurance | Configuration management (CM). Secure installation and generation. Design and policy correspondence. Guidance documents. Secure distribution. Functional specification. High-level language implementation. | Yes |
| Mitigation of Other Attacks | Specification of mitigation of attacks for which no testable requirements are currently available. | Yes |

# 7 References


1. V-Key Patent: Cryptographic System and Methodology for Securing Software Cryptography, Nov 16, 2011 available from V-Key upon request
2. V-Key, Data Sheets (for V-OS, V-OS App Protection, V-OS Smart Token) available from V-Key upon request
3. V-Key, V-OS Smart Token Cryptographic Whitepaper available from V-Key upon request
4. US National Institute of Standards and Technology, FIPS PUB 140-2: Security Requirements For Cryptographic Module, May 25 2001 with Change Notice 4, 03 December 2002 available at URL: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
5. US National Information Assurance Partnership, U.S. Government Approved Protection Profile – U.S. Government Protection Profile for General-Purpose Operating Systems in a Networked Environment, CC Version 3.1, 30 August 2010 available at URL: http://www.niap-ccevs.org/pp/pp_os_br_v1.0.pdf



# About V-Key

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 authorization without compromising user experience. It is trusted by government, banking and mega-app clients across the region to connect people, organizations, and devices everywhere to secure the global digital economy.

V-KEY
STRONGER WITH V-OS

To learn more about V-Key or V-OS, please email us at info@v-key.com.
Or find us on the web at www.v-key.com.