# V-OS MESSAGING

## SECURE END-TO-END COMMUNICATIONS

## BENEFITS

- ENTIRE PKI KEY MANAGEMENT CONDUCTED OVER-THE-AIR
- STRONG AND FAST PUBLIC KEY CRYPTOGRAPHY USING ECC
- ELIMINATES SMS RELIANCE AND ASSOCIATED COSTS
- GLOBALLY CERTIFIED

## SMS NOTIFICATIONS ARE NOT SECURE

Short Message Service (SMS) is a popular delivery channel for pushing messages to end-user mobile devices.

However, SMS suffers from these fundamental flaws:

- Unencrypted messages that can be intercepted in-transit
- Vulnerable to being intercepted by malware on the phone itself, especially on Android
- Lack of message delivery and read receipt
- The SMS network, known as SS7, has been proven to be vulnerable to intrusion, and can provide an attacker complete access to SMS and voice history

Organizations can make use of in-app notifications or push notifications. However, more and more confidential information gets transmitted and sent online through mobile phones. The mobile app's encryption key and digital certificate have few or no protections, and can be easily stolen or hijacked.

Organizations need to find other ways to secure notifications that are being pushed to end-users. How else can messages be pushed to end-users in a convenient and secured way?

### 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.

## V-OS MESSAGING

Confidentiality and integrity of data being sent to users is ensured as V-OS Messaging secures sensitive information such as:

Encryption Keys

Digital Certifications

Messages

V-OS Messaging provides a secured communication channel to the end user by encrypting in-app notifications. Besides protecting users, systems are shielded against attacks that bypass underlying communication layers. End-to-end encryption is guaranteed through the use of industry-standard techniques and technology such as Public Key Infrastructure (PKI). Communications cannot be interpreted or decrypted by malicious 3rd party interceptors and SMS stealers as parties are able to identify themselves through digital certificates.

# PRODUCT FEATURES

- KNOW IF USERS HAVE RECEIVED OR READ THE ENCRYPTED MESSAGE
- SECURE MESSAGING WITHOUT BORDERS - WORKS IN COUNTRIES LIKE CHINA
- WORKS ON CLOUD OR ON-PREMISE
- INDIVIDUALIZED KEY PAIRS FOR MULTIPLE USE CASES
- MESSAGE DELIVERY USING PUSH NOTIFICATION ADAPTERS SUCH AS APNS, FCM OR HMS
- SECURELY DELIVERS RICH MEDIA CONTENT TO USERS EVEN IN UNTRUSTED CLOUD NETWORK

## WHAT IS V-OS

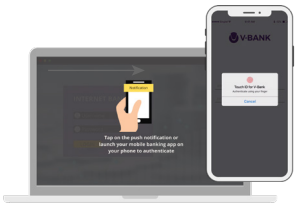
V-OS is V-Key's patented solution and the world's first virtual secure element to be FIPS 140-2 validated (US NIST), Common Criteria EAL3+ certified and accredited by the Infocomm Media Development Authority of Singapore (IMDA). V-OS uses advanced cryptographic and cybersecurity protections to comply 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.

# SECURE DATA PUSH

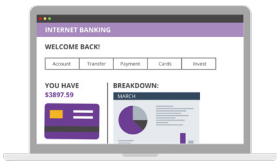
## 1-Step Notification

1. 


Customer logs into his banking account on the web browser and gets a push notification on mobile app

2. 


Customer verifies identity on mobile app using unique private key and is sent to server for validation

3. 


Authentication is successfully validated and customer can now do internet banking on web browser

Utilizing the same technology framework as V-OS Smart Token and because of their similarities, V-OS Messaging is usually deployed with V-OS Smart Token. V-OS Messaging can be used in conjunction with V-OS Smart Token to further strengthen the security of the use case to achieve a 1-Step Notification journey.

## 2-Step Notification

1. 

User receives a secure message on phone to view a confidential document

2. 


User clicks on the notification and is requested for identity verification

3. 


Once approved, encrypted rich media (document) is downloaded

4. 

Finally, the decrypted document shown to the user

**PLATFORMS SUPPORTED:**

**Client OS:**
Android 4.4 to 11 & iOS 7 to 14

**Server OS:**
Red Hat Enterprise Linux (RHEL), CentOS

**Server:**
JBoss EAP, WebLogic, Embedded Container (Tomcat)

**Database:**
MySQL, MariaDB, Oracle, Microsoft SQL Server

With V-OS Messaging, companies and end-users need not worry about storing the confidential document onto the cloud and risk it getting exposed to parties unintended to view it. It can be directly stored and downloaded from secured V-Key servers. This also allows for a bigger document size as V-Key servers have no limitations.

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

VKEY2021_MAR