V-KEY
STRONGER WITH V-OS

V-OS Smart Token

The Future of Authentication and Authorization is **Stronger with V-OS**.

Virtual Secure Element

Building on the industry-leading patented V-OS Virtual Secure Element, V-Key developed a highly secure framework that is FIPS 140-2 validated by NIST's Cryptographic Module Validation Program (CMVP) providing banking and government-grade mobile Two-Factor Authentication (2FA) and transaction signing.

STRONGER WITH V-OS

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

V-OS Authorization

Move Beyond SMS

There is a reason SMS has been officially deprecated by leading institutions like NIST. Using SMS for OTP Authentication has been subject to social phishing attacks.

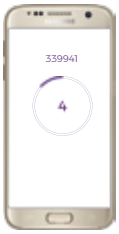
- Replaces insecure SMS
- Handles delivery failure with repeat attempts
- Seamless user experience
- Built-in non-repudiation

Send Rich Media and Content

V-OS Authorization isn't just for replacing SMS. It's about empowering customers on mobile.

- Paperless processing
- Pave the way for automation
- Reduce operational costs
- Save time

V-OS Authentication



Smart Token

Versatile and highly secure hardware token replacement that is easily integrated with existing OTP systems.

- Easily-read OTP display
- Out-of-band authentication for all channels
- OATH-compliant OTP technology

Push Auth

Authentication requests delivered straight to the app via secure push notifications for authenticating on all channels.

- Authenticate with a single tap
- Out-of-band authentication for all channels
- PKI technology

Seamless Auth

In-app mobile authentication that combines maximum convenience with top-notch security.

- Fully automated interaction
- In-app mobile authentication only
- OTP or PKI technology

V-OS SMART TOKEN FEATURES AND SPECIFICATIONS

Security, Simplicity

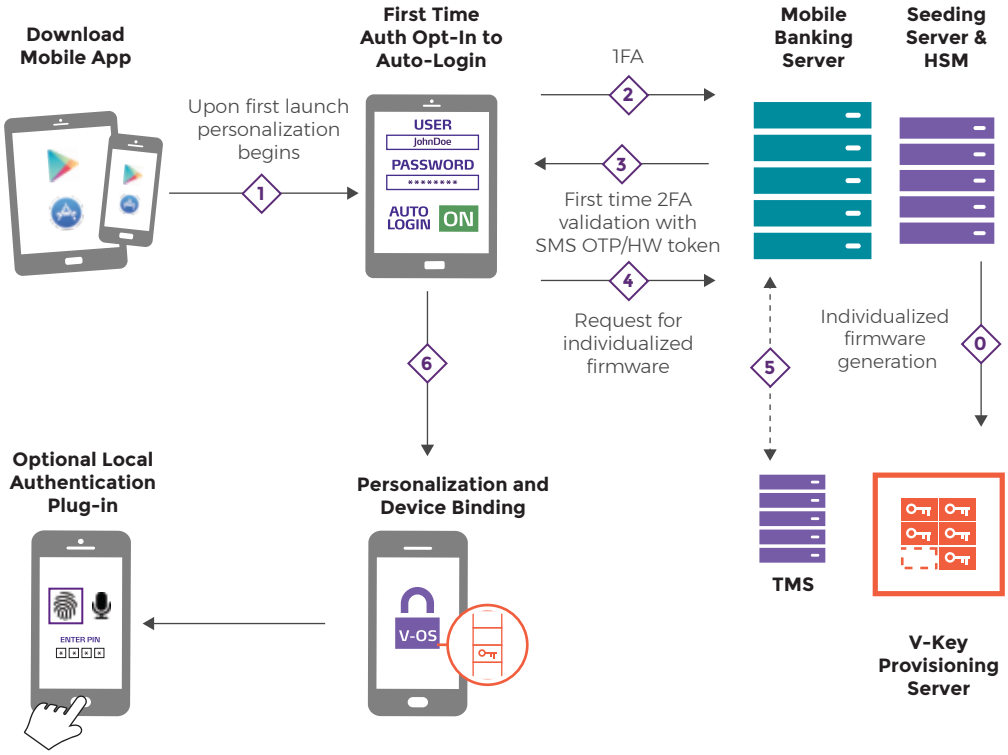
- Device-binding with sophisticated Anti-spoofing mechanism
- OTA provisioning for continuous security policy update and enforcement
- Threat-aware and equipped with multi-layered in-depth defense
- Built on V-OS for trusted cryptography processing and secure key personalization, distribution, storage, and rotations
- Hardened with V-OS App Protection
- Clock integrity for time-based authentication and dynamic signature generation
- Re-calibration capability – time synchronized with trusted source

Seamless Developer Integration

- Available as a stand-alone mobile token app, or an SDK library for easy integration into existing mobile apps
- Open Authentication (OATH) support for Time-based One-Time Password (TOTP)
- Transaction Signing with OATH Challenge-Response Algorithms (OCRA)
- Flexible integration options with enterprise authentication servers
- Supports multiple keys for different purposes, and multiple tokens per device, or across devices
- Policy can be linked with a centralized Risk Assessment Engine

Multi-factor Authentication Support

- Designed for easy integration with other biometrics or 3rd party multi-factor authentication libraries
- Extensible to support, Android biometrics, and V-OS Face Biometrics on any device.
- Could be easily extended to support other controls such as Geo-fencing and Time-fencing



GLOBALPLATFORM
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