![V-KEY — STRONGER WITH V-OS]

V-OS Cloud Solutions

Mobile Digital Identity, Authentication and Authorization

Stronger with V-OS

V-OS Cloud

With V-OS Cloud, customers can deploy the same powerful V-OS App Protection and V-OS Smart Token solutions without additional V-Key server software on premise. This reduces total cost of ownership, shortens time to value, and simplifies customer support.

V-OS Virtual Secure Element

Building on the industry-leading V-OS Virtual Secure Element, V-Key has developed a highly secure framework that integrates with mobile apps to secure them against advanced persistent threats, trojans, and rootkits. V-OS provides banking and government-grade Two-Factor Authentication (2FA) and transaction signing on mobile devices being FIPS 140-2 validated by NIST's Cryptographic Module Validation Program (CMVP).

V-OS App Protection

V-OS secures sensitive processing and data, ensuring app integrity when deployed, and safeguarding user privacy even if the device is lost or compromised.

- Device integrity checks for malware
- Filesystem integrity checks to detect backdoors and rootkits
- App integrity checks against tampering
- Network integrity checks against MITM attacks on Data-in-Transit
- Secure Cryptographic functions for both Data-at-Rest and Data-in-Use
- Secure Anti-Keylogger Keyboard

V-OS Smart Token

V-OS Smart Token is a versatile and highly secure hardware token replacement that easily integrates with existing OTP-based Authentication Servers or PKI-based technology components.

- OATH-compliant TOTP technology
- Standards-based PKI technology
- Authenticate with a single tap
- Out-of-band authentication for all channels

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

App Protection

Available as an SDK for easy integration into existing mobile apps to immediately start protecting them. V-OS Cloud provides the V-OS App Protection Server for threat intelligence security management:

- Designed as the Mobile Threat Command and Control system, enterprises can configure security policies to manage attack response and control
- Collect real-time app threats
- Over-the-Air policy updates

Two-Factor Authentication (2FA)

SMS-based OTP 2FA is vulnerable to phishing and malware attacks. This is why leading institutions like NIST have officially deprecated SMS. With Smart Token powered by V-OS Cloud, secure 2FA can be achieved using either PKI or OTP technology without compromise and without deploying additional servers on premise.

- PKI signature can be verified by V-OS Cloud seamlessly
- TOTP can be authenticated against any existing authentication server using standard OATH/OCRA protocols

Integration with Standard Authentication Protocols and APIs

Authentication request can be triggered through RADIUS for ease of integration with existing systems such as VPN servers. Alternatively, REST or SAML protocols can also be used for integration. Additional integrations with enterprise platforms such as Office 365 will also be possible through Active Directory connectors.

Customer app integration with V-OS Smart Token SDK

Available as an SDK for easy integration into existing mobile apps. APIs available for:

- On-device PKI key-pair generation
- Creating Certificate Signing Request for certificate signing by CA
- Authentication with on-device private key
- OATH support for Time-based One-Time Password (TOTP)

- Transaction Signing support with OATH Challenge-Response Algorithm (OCRA)
- Flexible integration options with enterprise authentication servers using SAML protocol
- Supports multiple keys for different purposes, and multiple tokens per device, or across devices

SPECIFICATIONS

Platforms
- Apple iOS
- Google Android

PKI crypto
- ECC (P-256)
- Strong Cryptography

OTP
- OATH-compliant TOTP
- OCRA-complaint Transaction Signing
- Requires customer-supplied OATH/OCRA-compliant Authentication Server

V-OS Cloud provides the ability to rapidly deploy V-Key's App Protection and Smart Token solutions easily without the need to set up servers on premise.

GLOBALPLATFORM
The Standard for Managing Applications on Secure Chip Technology

FIPS VALIDATED 140-2

fido alliance member

SG:D ACCREDITED