V-KEY
STRONGER WITH V-OS

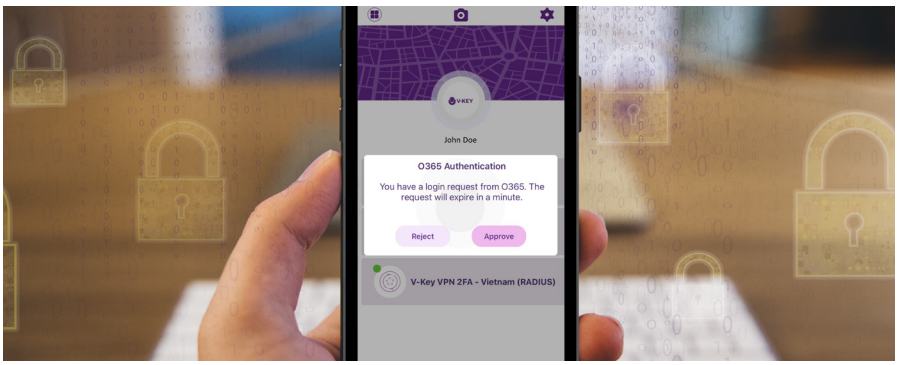
V-OS CLOUD

Trusted Identity as a Service (IDaaS) Securing the Enterprise

BENEFITS

- TRUSTED ENTERPRISE AUTHENTICATION
- GUIDED SETUP FOR FAST DEPLOYMENT
- CUSTOMISE YOUR AUTHENTICATOR APP
- MONTHLY USER SUBSCRIPTION FEES
- NO ADDITIONAL HARDWARE INVESTMENT
- OVER-THE-AIR UPDATES TO STAY CURRENT
- SCALABLE FOR COMPANIES OF ANY SIZE
- GLOBALLY CERTIFIED

While there is a demand for uncompromising security in banking apps to ensure the protection of digital identity and financial assets, corporate data rarely receives the same attention. Employees may not know what their Microsoft Office 365 security policies are, or whether if the policies are adequate to protect them from fraudulent access. Secure access to corporate systems, applications, and files has typically been based on a username and sometimes multiple passwords with no other means of authentication, and this is not sufficient.



SENSITIVE ENTERPRISE DATA DESERVES AN ENTERPRISE-GRADE MOBILE SOLUTION.

Most enterprise employees today access corporate data on their mobile devices as much as they do on their company-issued laptops. Most often than not, employees use their own devices that are exposed to the dark world of malicious apps and code. The majority of mobile cyber threats are designed with the intent to steal identities and facilitate access to sensitive data, leading to numerous reports on massive data leaks. Digital Identity threats not only come from the dark web, but many are also insider threats.

Trusted Identity access combines technologies to provide multiple factors of verification and authentication when employees log in to their systems. In the past, hardware tokens solved this problem, however they are expensive to deploy, need to be replaced, and often got lost. Today, mobile apps and soft tokens are used to fulfil the same purpose. This means the technology must ensure the integrity of the mobile app and the digital identity of your employee.

Often, IT Administrators rely on the default Authentication methods provided by online services and are constantly on guard against lost or forgotten passwords being reused from other online services. Using just Username and Password is insufficient to guarantee authentication and grant access, especially through web browsers. There is an increasing need to enhance cyber security awareness and secure sensitive corporate data against theft from lost or stolen tokens, password fatigue, leaked shared secrets, phishing, and even keyloggers. To provide employees secure access from any device at any time, a second (or third) factor must be considered. This can be achieved with V-Key's Trusted Identity Services running in V-OS Cloud.

PRODUCT FEATURES

PKI-BASED AUTHENTICATION

SUPPORTS RADIUS/ SAML INTEGRATION

DEVICE BINDING

IN-BUILT APP PROTECTION

ECC (P-256) / AES-256 ENCRYPTION

CC EAL3+ / FIPS 140-2

WHAT IS V-OS?

V-OS is the world's first virtual secure element that uses advanced cryptographic and cyber security protections to comply with standards previously reserved only for expensive hardware solutions. V-OS enables digital leaders to create powerful customer experiences that combine high security and delightful convenience. Globally certified, V-OS individualizes Trusted Apps on your device and protects user keys from cyber threats.

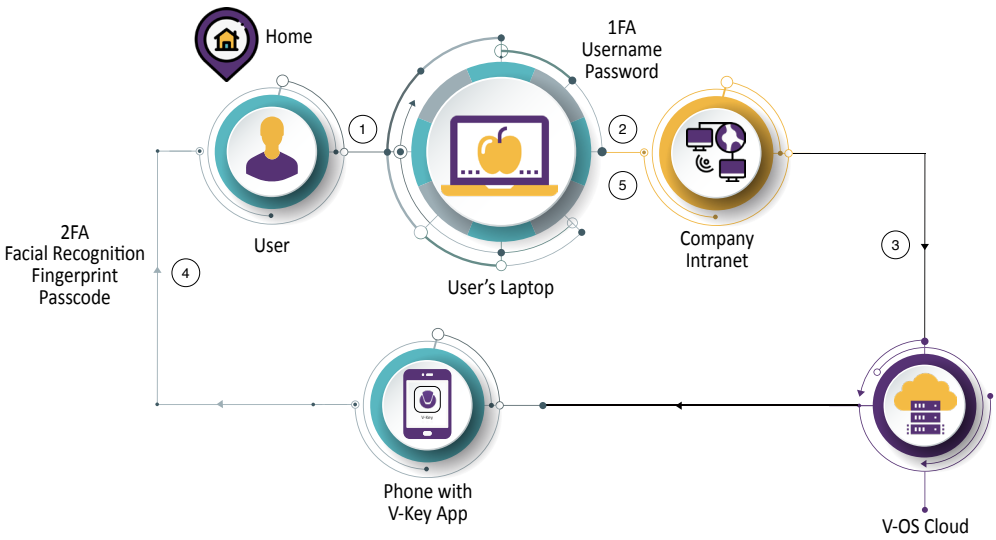
V-OS TRUSTED IDENTITY SERVICES.

Deployed from V-OS Cloud, a customisable app is configured to your organisational needs and is individualized for each employee. The cloud platform provides operational efficiency in the deployment of Trusted Identity services. It also optimises the cost of implementation and maintenance, and focuses on ensuring usability on any IOS or Android device.

All you need is to download the Virtual-Key (V-Key) app from either Apple App Store or Google Play Store to the mobile phone in order to receive the 2-Factor-Authentication (2FA)

V-OS Cloud Services include

- 2FA for VPN/RADIUS
- 2FA for Office 365 (O365)/SAML



V-Key
V-Key App
V-Key
Free

Virtual Key (V-Key) App Available in :

ANDROID APP ON Google play

Download on the App Store

Experience V-OS Trusted Identity Services in 5 simple steps.

1. User launches VPN/Office 365/Enterprise software on laptop
2. Authentication process is triggered and user inputs Username & Password (1FA) on laptop
3. Upon successful verification of 1FA, V-Key App on user's mobile device will receive 2FA push notification from V-OS Cloud
4. User need to verify (either fingerprint, facial recognition or passcode) their identity through the V-Key App
5. When the 2FA is successfully verified, user will be able to access the services

SPEAK TO OUR CLOUD ADMINISTRATOR 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 EKYC - V-OS MESSAGING - V-OS CLOUD SOLUTIONS

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

V-JUNE2020