VASCO
TRUST FOR THE DIGITAL WORLD

DIGIPASS
for APPS

DIGIPASS® for Apps

An all-in-one developer's toolkit designed to improve security and user convenience across your mobile application ecosystem

Mobile applications are changing the way business is done, offering instant access to services for your users. Unfortunately, motivated hackers are taking advantage of the many complexities created by the mobile ecosystem to exploit vulnerabilities, resulting in sophisticated fraud schemes and theft of sensitive data.

INCREASE SECURITY AND REDUCE FRICTION

DIGIPASS for Apps is a comprehensive developer's toolkit (SDK) and unique single framework that natively integrates application security, two-factor authentication and electronic signing into your mobile applications. Through a complete library of APIs, you have all the necessary building blocks to extend and strengthen security for your applications and deliver unprecedented convenience to your users, while streamlining the application deployment and lifecycle management process. Benefits of DIGIPASS for Apps include:

- **Fraud Prevention:** A unified framework that enhances security across all core components of your application – communication, storage, platform, provisioning, interface and user.
- **User and Transaction Protection:** Broad, flexible, and fully integrated two-factor authentication and electronic signing supports the demand for user convenience for even the most sensitive mobile transactions.
- **Risk Scoring:** Risk scoring that is driven by user, platform and context elements is embedded into the authentication process, meeting requirements for enhanced server-side analytics and streamlined compliance management.

SIMPLIFY WITH ORCHESTRATION

The DIGIPASS for Apps Orchestration SDK makes it easy for developers to add authentication and security features into new mobile app projects. Paired with IDENTIKEY Risk Manager, it also allows for more flexible authentication processes (e.g., PIN to fingerprint to face) with minimal development effort. Additionally, the Orchestration SDK builds-in plug-and-play support for new biometric options as they become available, and without developers having to recode the app, resubmit it to app stores or persuade users to update – effectively future-proofing their app.

DIGIPASS for Apps helps you enhance security and manage applications at every level, from provisioning through user activation, across multiple user devices. DIGIPASS for Apps is suitable for any server side environment — it doesn't require in-house cryptographic expertise, is fully customizable, runs without GUI issues, meets all graphical requirements and is integrated with a minimum of development effort via the DIGIPASS for Apps Orchestration SDK.

For users, DIGIPASS for Apps provides a convenient, frictionless experience, supports a broad range of options for accessing mobile applications and conducting transactions, and supports most commonly available mobile platforms including Android, iOS, Windows Phone, and BlackBerry.

Runtime Application Self-Protection
Natively integrated application security technology that dynamically monitors application execution to detect and prevent attacks on mobile applications

Jailbreak and Root Detection
Key application security elements used to determine if a mobile device has been compromised by removing important application download restrictions

Device Identification
Leverages unique attributes of the mobile device to provide a persistent identification, unaffected by mobile OS updates. Defeating hacker attempts to spoof the mobile device

Geolocation
Utilizes the location of a mobile device, as a key risk analysis element, to determine the level of device trust

Device Binding
Securely links an authorized user to their authorized device(s), which can prevent cloning or repurposing of cryptographic keys

Secure Storage
Strong encryption for all application data stored on a mobile device, independent of any operating system or device

Secure Channel
End-to-end encryption supporting the highest level security between server and mobile device exchanges including text, photos, QR codes and authentication data

E-Signatures
A seamless and fully compliant solution enabling users to e-sign documents anywhere, anytime and on any device

Behavioral Authentication
A frictionless biometric option that continuously operates in the background, invisible to end users, that scores behaviors like keystroke, touch and mouse motion for accurate authentication

Face Authentication
A frictionless biometric option that utilizes facial data points and next generation liveness detection to quickly and accurately authenticate users (supports Apple Face ID).

Fingerprint Authentication
A simple and proven biometric authentication option that utilizes a fingerprint scan to quickly and accurately authenticate users

Risk Based Authentication
Real-time analysis that scores the risk profile of a transaction based on all of the available data points and can dynamically step up security when necessary

CRONTO® Authentication
Patented color QR code scan provides a highly secure and user-friendly authentication and transaction signing experience

QR Code Support
A flexible image scanning feature that reads standard QR Codes to secure communications

Transaction Signing
Fully integrated transaction signing balances user convenience and strong security for even the most sensitive mobile transactions

Push Notification
Device independent push notification that securely sends any message/content between server and mobile device including alerts, transactions, and authentication data

TRUST FOR THE DIGITAL WORLD

DIGIPASS
for APPS

Complete Mobile Application Security

SECURE USER

DIGIPASS for Apps offers extensive authentication options including truly frictionless behavioral biometrics that leverage keystroke dynamics, swiping patterns and more, user-friendly fingerprint and facial biometrics and other proven multi-factor solutions as well as a suite of innovative e-signature products - like Cronto® graphical cryptograms.

SECURE COMMUNICATIONS

DIGIPASS for Apps offers end-to-end encryption that introduces a new level of service between server and client applications, providing an encrypted secure channel for almost anything, including text, photos, and QR codes.

SECURE STORAGE

DIGIPASS for Apps delivers secure storage functionality through encryption for all application data, independent of any operating system or device. In addition, multi-device management allows users to utilize all devices through a single license.

For Android operating systems, VASCO supports secure storage protection through the Secure element feature of the device. Securing data on enabled Android phones is achieved via a second layer of encryption, providing an excellent defense against application cloning attacks as the encryption key stored in the Secure element cannot be extracted.

SECURE PLATFORM

DIGIPASS for Apps offers features such as geolocation, device binding, jailbreak and root detection to help you protect against platform vulnerabilities that could compromise the security of your mobile application.

SECURE PROVISIONING

DIGIPASS for Apps provides a full range of features for deployment, provisioning and activation, offering manual, online, and QR code-based processes, as well as protocol independent features that, leveraging the Orchestration SDK, streamline provisioning across multiple platforms.

SECURE INTERFACE

DIGIPASS for Apps provides PIN Management to protect against brute force attacks and dictionary attacks, as well as integration with fingerprint biometric readers. It also supports additional application hardening techniques like zeroing memory.

SECURE EXECUTION

DIGIPASS for APPS offers runtime application self-protection against execution environment corruption and reverse engineering threats through repackaging, debugger, emulator, hooking framework detection, keylogger or screenreader prevention as well as advanced obfuscation and anti-library injection.

About VASCO

VASCO is a leading supplier of strong authentication and e-signature solutions and services specializing in Internet Security applications and transactions. VASCO has positioned itself as global software company for Internet Security and designs, develops, markets and supports DIGIPASS®, CertiID™, VACMAN®, IDENTIKEY® and aXsGUARD® authentication products. VASCO's prime markets are the financial sector, enterprise security, e-commerce and e-government.

www.vasco.com

CORPORATE HQ
CHICAGO (North America)
phone: +1 630 932 88 44
info-usa@vasco.com

INTERNATIONAL HQ
ZURICH (Europe)
phone: +41 43 555 3500
email: info_europe@vasco.com

BRUSSELS (EUROPE)
phone: +32.2.609.97.00
email: info-europe@vasco.com

BOSTON (NORTH AMERICA)
phone: +1.508.281.66.70
email: info-usa@vasco.com

SYDNEY (PACIFIC)
phone: +61.2.8061.3700
email: info-australia@vasco.com

SINGAPORE (ASIA)
phone: +65.6323.0906
email: info-asia@vasco.com

Copyright © 2018 VASCO Data Security, Inc, VASCO Data Security International GmbH. All rights reserved. VASCO®, Vacman®, IDENTIKEY®, DIGIPASS® and ® logo are registered or unregistered trademarks of VASCO Data Security, Inc. and/or VASCO Data Security International GmbH in the U.S. and other countries. VASCO Data Security, Inc. and/or VASCO Data Security International GmbH own or are licensed under all title, rights and interest in VASCO Products, updates and upgrades thereof, including copyrights, patent rights, trade secret rights, mask work rights, database rights and all other intellectual and industrial property rights in the U.S. and other countries. Microsoft and Windows are trademarks or registered trademarks of Microsoft Corporation. Other names may be trademarks of their respective owners.