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 the theft of sensitive data. It's clear that today's unprecedented global mobile migration has raised security stakes to new levels - your users are conducting highly complex, sensitive transactions from multiple devices, over both known and unknown networks, and each step introduces new security risks. When it comes to your mobile applications, how can you ensure the right levels of security without creating additional challenges for your mobile users?

DIGIPASS for Apps is a comprehensive developer's toolkit (SDK) that natively integrates application security, two-factor authentication and electronic signing into your mobile applications. Through a complete library of APIs, you can 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.

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 easily integrated.

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.

> DIGIPASS for Apps is a unique single framework and a comprehensive library of APIs that give developers all the necessary building blocks required to secure their mobile applications.

Runtime Application Self-Protection	Natively integrated application security technology that dynamically monitors application execution to detect and prevent attacks on mobile applications
Jailbreak & Root Detection	Key application security elements used to determine if a mobile device has been compromised by removing important application download restrictions
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
Push Notification	Device independent push notification that securely sends any message/content between server and mobile device including alerts, transactions, and authentication data
Cronto Authentication	Patented color QR code scan provides a highly secure and user-friendly authentication and transaction signing experience
Secure Storage	Strong encryption for all application data stored on a mobile device, independent of any operating system or device
Device Binding	Securely links an authorized user to their authorized device(s), which can prevent cloning or repurposing of cryptographic keys

Face Authentication	A frictionless biometric option that utilizes facial data points and next generation liveness detection to quickly and accurately authenticate users
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
Geolocation	Utilizes the location of a mobile device, as a key risk analysis element, to determine the level of device trust
One-time Password Authentication	A time sensitive password, dynamically validated by a central server that also enforces PIN strength, to ensure fast, simple and secure user authentication
Transaction Signing	Fully integrated transaction signing balances user convenience and strong security for even the most sensitive mobile transactions
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

A global leader in authentication, electronic signatures, and identity management

Complete Mobile Application Security

SECURE USER

DIGIPASS for Apps offers extensive authentication options including user-friendly fingerprint and facial biometrics and other proven two-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 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 the world leader in providing two-factor authentication and digital signature solutions to financial institutions. More than half of the Top 100 global banks rely on VASCO solutions to enhance security, protect mobile applications, and meet regulatory requirements. VASCO also secures access to data and applications in the cloud, and provides tools for application developers to easily integrate security functions into their web-based and mobile applications. VASCO enables more than 10,000 customers in 100 countries to secure access, manage identities, verify transactions, and protect assets across financial, enterprise, E-commerce, government and healthcare markets. Learn more about VASCO at vasco.com and on Twitter, LinkedIn and Facebook.

www.vasco.com