DIGIPASS® for Mobile

Security meets convenience: Enhanced mobile application security paired with a frictionless user experience

Banks, financial institutions and enterprises offering online and mobile applications face multiple challenges. Online and mobile applications are highly susceptible to cyber attacks and fraud, which, over recent years, have become increasingly sophisticated. At the same time, adoption of mobile applications depends on an intuitive and seamless experience for users. How do you ensure security of your mobile application while keeping it convenient and transparent for your mobile users?

DIGIPASS for Mobile balances the need for stronger application security with demands for user convenience by delivering comprehensive, built-in security for your mobile applications, combined with a frictionless, "hands-free" authentication and e-signing experience for your mobile users. And when combined with DIGIPASS for Apps, DIGIPASS for Mobile offers a comprehensive and integrated security framework for your mobile applications.

ENHANCED APPLICATION SECURITY

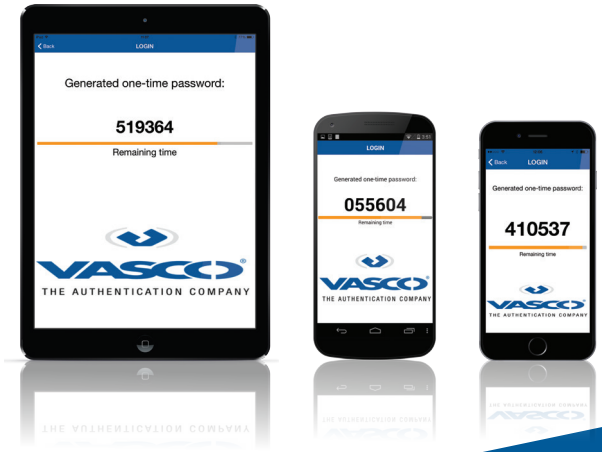
For any mobile application, creating a secure environment for the user authentication process is critical. That's why DIGIPASS for Mobile goes beyond authentication to ensure that any application running on a mobile platform is self-protected in all the aspects of application runtime:

- **Jailbreak & Root Detection:** Ensures the security of mobile platforms by detecting if rooting or jailbreak evidence is present, so you can take proper action depending on your security policies.
- **Application Hardening:** Supports best in class hardening techniques including memory zeroing, reverse engineering protection, secure storage, and white box cryptography to keep applications and users safe from potential attacks.
- **Device Binding:** Securely links an authorized user to his authorized device(s), which can prevent cloning or repurposing of cryptographic keys. The DIGIPASS for Mobile application itself is also bound to device-dependent components and linked to the user via a secure PIN code.
- **Secure Channel Communications:** Ensures the integrity of digital transactions by providing an encrypted, independent and cross-platform secure channel between the server and the client device, so that only devices authorized to receive transaction information will be able to decrypt and sign it.
- **Enhanced Risk Analysis:** Offers unique risk scoring capabilities that are embedded into the authentication and signing processes based on user, platform and context elements of the application, delivering stronger protection as well as server-side risk analysis.

TRANSPARENT USER EXPERIENCE

When it comes to user adoption of your mobile application, user experience can often be a determining factor in its success or failure. DIGIPASS for Mobile offers convenient, user-friendly two-factor authentication and e-signing options that take security "friction" out of the equation:

- **QR Code Scanning:** Users simply capture the QR code with a mobile device, enter a PIN code and can instantly log on to an application or validate a transaction. Integrates with VASCO's patented CrontoSign technology as well as Open QR codes.
- **Transparent OTP:** Offers "hands free" authentication and signing when a user is conducting an online session, and is flexible enough to provide transparent OTP or generate an e-signature that is automatically directed to the relevant server. To the user, this means no need to type any information, and a secure and completely friction-free authentication experience.
- **Multi-Device Support:** Ensures that a user can securely leverage any pre-registered device for application authentication and transaction signing, regardless of platform. Secure channel capabilities ensure that encrypted information sent from the server can only be decrypted and accessed by the pre-authorized set of devices for that user.
- **Inter-Application Security:** Between applications, DIGIPASS for Mobile will perform needed security checks, generate the OTP, and pass it directly to the applicable server, so that the user can instantly establish secure access for virtually any application on the client-side.



STREAMLINED INTEGRATION, PROVISIONING AND DEPLOYMENT

Application development and deployment can be an arduous process, which is why we designed DIGIPASS for Mobile to be flexible and friendly for developers throughout the process. VASCO Professional Services also offers a complete suite of implementation options, providing full-service support for everything you may need, from parameter selection and testing to complete design customization, multi-device provisioning, App store publishing and training.

- **Customization:** Offers a fully customizable GUI, a complete set of branding and publishing tools, localization capabilities, flexible menu and form design options, and granular security and policy tools.
- **Integration:** Provides a web sample to simplify the integration into your current server architecture. A typical test pilot can be up and running within one day and can demonstrate how the software will integrate prior to production.
- **Provisioning:** Enables flexible provisioning by offering a set of provisioning protocols using asymmetric keys as well as alternative options. Can also be done via an HSM server-side implementation to allow for the most secure key provisioning. Complete VASCO-operated provisioning services are available via DIGIPASS as a Service.
- **Deployment:** Offers off-line or online deployment options as well as deployment through QR codes. DIGIPASS for Mobile has been successfully deployed on a large scale throughout the banking community, and can be deployed simultaneously with other VASCO devices,
- **Support:** Supports almost any mobile device platform, including iPhone, Android, Blackberry and Windows, as well as eight different crypto-applications, allowing an extended use in different settings such as IVR, online connections, signatures, offline transactions, etc.

DIGIPASS FOR MOBILE TECHNICAL SPECIFICATIONS

Response Only	Time only, event only or Time + event-based AES/Triple DES Encryption Algorithm Response : 6 to 16 decimal/hexadecimal Check digit 256 seconds Time Step
Host Confirmation Code	AES/Triple DES Length from 4 to 10 Decimal/Hexadecimal (1 to 10 in challenge/response mode)
Challenge/Response	Time only, event only or Time + event-based AES/Triple DES Encryption Algorithm Challenge length from 4 to 16 decimal Response length from 6 to 16 decimal/ hexadecimal Check digit 256 seconds Time Step
MAC/signature	Time only, event only or Time + event-based AES/Triple DES Encryption Algorithm Length from 4 to 16 decimal/hexadecimal Up to 8 customizable data fields Data field length from 4 to 16 digits 256 seconds Time Step
PIN management	PPIN length options: no PIN or 4 to 250 digits Max number of wrong entries from 1 to 9 On wrong PIN: invalid password generation or reset PIN check options : Checksum/Hashcode/None PIN change option PIN derivation iteration from 0 to 15 000
Standard algorithms	HOTP TOTP OCRA

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 patented DIGIPASS®, DIGIPASS PLUS®, VACMAN®, IDENTIKEY® and aXsGUARD® authentication products. VASCO's prime markets are the financial sector, enterprise security, e-commerce and e-government.

www.vasco.com

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

BOSTON (North America)
phone: +1.508.366.3400
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