What is it for?
As the use of smartphones increases and people replace their personal computers with handsets and tablets, the demand for banking on-the-go, anywhere, is increasing daily.

Users expect to launch a mobile app on their smartphones and quickly and easily gain access to their personal banking information at any time, through frictionless authentication that has minimal impact on their behavior.

They expect remote, trusted banking on any device and the ability to shift seamlessly from one device to. They also expect their financial assets to be safe, always.

Banking and paying are a lot easier... but these new services are attracting fraudsters. And, unsurprisingly, this step change is accompanied by new and increasingly numerous mobile security threats. Mobile financial apps containing valuable data like User credentials, Personal Information, account number, transfers data, balance are prey to more and more attacks.

New types of malware are spreading through very different methods: from non-official app stores, from emails containing viruses in their attachments, through trojanized legitimate applications, and from computers to mobile phones.

In this context, mobile-banking service providers need to solve a complex puzzle when it comes to protecting their applications:

- Maximize user reach despite mobile-device fragmentation
- Address the lack of control of mobile devices in the field and how they are used
- Maintain end-user convenience with authentication solutions that work for everyone

Gemalto Digital Banking Mobile Security toolkit delivers best-in-class security to protect all mobile financial applications against threats and malware attacks, while fulfilling banking requirements. It ensures appropriate security features for all types of digital touchpoints in online channels. Gemalto Digital Banking Mobile Security toolkit is developed and maintained by Gemalto with banking-grade security vetted by internal and external audits.
How does it work?
Gemalto Mobile Security Toolkit is a comprehensive Mobile Application Shielding offering, made of an SDK and development tools, that integrates all the best practices Gemalto has built and implemented over the years in the digital banking world to secure mobile applications and guarantee their data integrity.

The list of possible vulnerabilities of unprotected mobile applications is long. Gemalto Mobile Security Toolkit allows you to focus just on developing your mobile application, not on its security. It enables you to implement the latest protection techniques while saving you time, energy and money. Gemalto Mobile Security Toolkit will enable your mobile apps to:

**Defend**
- Integrity of mobile app
- Sensitive assets

**Detect**
- Unsafe environments
- Attack attempts

**React**
- Stop execution
- Perform custom actions such as warning users or sending an alert to a risk-management server

Advanced and tailor-made security features
Gemalto Mobile Security Toolkit relies on 4 main pillars:

**RASP (Runtime Application Self Protection)**
This security technology is built into an application and is capable of controlling application execution, detecting and preventing real-time attacks. It can detect unsecure environments and also hackers or malware trying to scrutinize applications at runtime and/or tamper their behaviour. It includes, but is not limited to, the following technologies:

- JB/Root detection
- Anti-Hooking
- Anti-Debugger
- Anti-Tampering
- Anti-Emulator

**Secure Storage**
This offers a platform-independent secure area to store applications’ sensitive data, thanks to techniques such as multi-layers encryption, device binding and White Box Crypto (WBC). The objective of WBC is to perform secure cryptography in unsecure environments, on any type of smartphone, allowing a uniform security-assurance level on all platforms and providing isolation from the operating system. Gemalto WBC benefits from Gemalto’s renowned expertise in smart card security, such as protection against side-channel attacks.

**Obfuscation**
Gemalto has developed its own technology to obfuscate native code with some patent techniques. The main benefits are:

- Diversification of our SDK per bank, not allowing the replication of an attack from on bank to another.
- Impact limited to performance only, to apply the strongest obfuscation only on critical parts.
- Banks can use their standard compilation tools.

**Secure Interface**
Gemalto Secure Keypad (GSK) does not rely on the platform keyboard services as everything is drawn. It does not keep the password in memory but only indexes it in a table and offers a random display of digits as well as customizable User Interface.

Gemalto Mobile Security Toolkit protects your banking application from the most sophisticated and targeted malware, securing the most valuable asset for a bank: consumer trust.

Technical specifications
**Supported platforms**
- iOS 9 and above
- Android 4.4 and above

**RASP protection**
- Jailbreak/Root detection.
- Jailbreak/Root hiding tools detection
- Anti-Hooking
- Anti-Debug
- Static Anti-Tampering
- Anti-Emulator
- Dynamic Anti-tampering

**Secure Storage**
- AES
- SHA 256
- Device Binding
- White Box Crypto

**Native code Advanced Obfuscation with Gemalto proprietary techniques**

**Custom Reactions (crash or application call back)**

**Secure Keyboard**
- Customizable UI
- End-to-End encryption