Gemalto Mobile Security Core

Establishing the trusted foundations necessary to enable both the Gemalto Mobile ID Smart App and broader Digital ID Document Wallet portfolio to detect, react to and defend against the threat of mobile malware.

What is it for?

Accessibility is key to the success and adoption of digital services. The sheer volume of smartphones worldwide (an estimated six billion by 2020, according to IHS market research), therefore offers governments a compelling opportunity to provide citizens with a trusted mobile identity to access online public services securely and conveniently.

Citizens expect their government-backed mobile identity app to support quick and easy access to online public and private services, at any time, through frictionless authentication that requires minimal change in their normal behavior. Of course, they also expect the mobile identity provided by public authorities to be safe, always.

Mobile identity solutions can deliver outstanding convenience, with access to online public services and the process of completing online transactions made far easier. However, this step change is accompanied by new and increasingly numerous mobile security threats. Novel types of malware are spreading via a diverse range of methods: from non-official app stores, from emails containing viruses in their attachments, from legitimate applications that have been Trojanized, and from computers to mobile phones.

When it comes to protecting their applications, governments and official national digital identity providers embarking on national mobile identity schemes need to solve a complex puzzle:

> 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

Mobile identity apps containing user identity credentials and private keys must be protected at all times. This is why Gemalto Mobile Security Core has been designed to deliver best-in-class security to protect Gemalto Mobile ID Smart App and, more broadly, Gemalto Digital ID Document Wallets against threats and malware attacks, while fulfilling government requirements. It ensures appropriate security features for all types of digital touchpoints in online channels. Gemalto Mobile Security Core is developed and maintained by Gemalto, with government-grade security vetted by internal and external audits.

How does it work?

Gemalto Mobile ID Smart App and Gemalto Mobile ID Document Wallet are built on Gemalto Mobile Security Core. This comprehensive mobile application shielding suite integrates all the best practices Gemalto has built and implemented over many years in the digital identity and mobile authentication world to secure Gemalto applications and guarantee their data integrity.

The list of potential vulnerabilities within unprotected mobile applications is long. With Gemalto Mobile Security Core inside, Gemalto Mobile ID Smart App ensures you benefit from the latest protection techniques, and offers your citizens and residents a safe mobile based digital identity.

Gemalto Mobile Security Core

Gemalto Mobile Security Core enables Gemalto Mobile ID Smart App and Gemalto Digital ID Document Wallet to:

Defend
> Integrity of the 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 & tailor-made security features

Gemalto Mobile Security Core relies on four 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 with their behavior. It includes, but is not limited to, the following technologies:
> JB/Root detection > Anti-Tampering
> Anti-Hooking > Anti-Emulator
> Anti-Debugger

Secure Storage
This offers a platform-independent secure area to store applications' sensitive data, thanks to techniques such as multi-layer 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 a number of patented techniques. The main benefits are:
> Diversification of the security mechanisms per customer, preventing the replication of an attack from one identity scheme to another.
> Impact limited to performance only, to apply the strongest obfuscation only on critical parts.
> Governments can use their standard compilation tools.

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

Gemalto Mobile Security Core protects Gemalto Mobile ID Smart App and Digital ID Document Wallet from the most sophisticated and targeted malware, thereby securing one of the most valuable assets: **citizens' TRUST.**

TECHNICAL SPECIFICATIONS

Supported platforms
> iOS 10.0 and above
> Android 5.0 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

GEMALTO.COM

gemalto
security to be free