Thales Gemalto Mobile Protector
Secure online transactions with your smartphone
Next generation security for new generation services

Using a mobile phone to perform financial transactions has become so natural. For banks the challenge is not only to deliver the full spectrum of possible mobile banking services like creating new beneficiaries, transferring money to external accounts or managing your banking card. Banks also need to deliver additional services by an always connected device such as mobile wallet, proximity payment, Peer to Peer payment or mobile commerce. Banks who fail to expand services to mobile, may risk customers leaving for more innovative competitors. At the same time the threat posed to mobile phone is greater than ever. Reports from security specialists confirm years after years that mobile malware keep growing in numbers, but also in complexity. After the wave of famous SMS malware (like Eurograbber) which forward to hackers the One Time Code received to validate transactions, fraudsters now try to disguise themselves as genuine bank applications to collect user credentials and card details. Latest versions even prevent users from alerting their bank to fraudulent transactions. Also as mobile phones are more susceptible to theft than PCs, users need to take precautions and protect credentials against abuse if a device is stolen or misplaced.

These risks are well highlighted by regulations like FFIEC in the US or the PSD2 in Europe. While a growing majority of banks now view mobile services as the next frontier, they have yet to keep up with the necessary security posture needed to protect these services.

Thales Gemalto Mobile Protector is a Software Development Kit providing APIs to easily implement multi-factor authentication and mitigate against malware attacks. Thales Gemalto Mobile Protector can help banks protect online services and consumers as well as comply with regulations.

Multi-factor authentication

Effective security relies on multiple and independent authentication factors to ensure that no single point of compromise can lead to unauthorized account access. But implementation of such a solution can sometimes be difficult and does not always provide an optimal user experience.

Thales Gemalto Mobile Protector overcomes these challenges by allowing banks to easily implement multiple authentication factors while offering an easy and simple user experience.

Advanced security

Thales Gemalto Mobile Protector leverages Thales’ unrivalled experience in digital security. The multi-layer encryption model makes the solution safe against after-theft-attacks. The personalization phase, which consist of enrolling the mobile device and provisioning secret keys, is secured by a proprietary protocol which protect the solution against Man-In-The-Middle as well as SSL weaknesses (BEAST, CRIME, etc.).

Malware protection

Excellent cryptographic implementation is required to provide efficient protection, but it can’t be the only layer of defense against malware.

Thales Gemalto Mobile Protector also includes several security features which contain the risks of malware attacks. The most critical parts are developed in native language and concealed with Thales unique obfuscation techniques to prevent reverse engineering from hackers. It also provides detection techniques to prevent the application from being linked to a debugger or hooked and thus forces hackers to spend time identifying these protections and trying to bypass them.
**Optimized user experience**

After installing the application developed with Thales Gemalto Mobile Protector, customers simply enroll by entering a registration code when first launched. This enrolment can be further facilitated by using QR code. Once the application is personalized, customers benefit from the best experience, either using simple PIN code or their biometric characteristic to authenticate themselves to mobile services.

Thales Gemalto SDK’s various layers of authentication can be combined to achieve an optimal balance between user experience and risk mitigation. For example, a simple login request may rely either on fingerprint authentication or device binding. However, for more risky transactions it is possible to combine the PIN and a biometric factor (or several biometric factors), thus allowing financial operations that would not have been possible with the use of a static password.

**Flexible integration**

As part of Thales’ versatile Thales Suite, Thales Gemalto Mobile Protector fits perfectly into a bank’s security lifecycle. It can be accompanied by your choice of complementary products such as Thales Gemalto Confirm Authentication Server (CAS) to validate authentication and signature, Thales Gemalto Mobile Secure Messenger to perform Out-of-Band authentication or Thales Gemalto Assurance Hub (GAH) to take smart authentication decision based on risk analyses.

And since it uses open standards, it can also integrate easily with third party authentication schemes.

**Future proof**

Security in general, and especially in the mobile world, is in constant evolution and requires permanent investments to keep up with the latest threats and attacks. Thales Gemalto mobile security solution benefits from a clear and continuously innovative technology roadmap which relies on Thales’ experience in digital and mobile security and unrivalled experience in secure element.

---

**KEY FEATURES**

**Enhanced Features**

- One Time Password, Challenge/Response and Transaction Data Signing
- Easy to implement native API
- PIN Authentication with randomized Secure Pin Pad
- Biometric Authentication with Fingerprint and Facial Recognition
- Device Binding
- Jailbreak/Root detection, Anti-Debug, Anti-Hooking
- Advanced Obfuscation
- Secure Storage
- Secure Channel (on top of SSL)
- HSM based key protection
- Security audited by independent third party

**Multi-Channel and use cases protection**

- eBanking
- ePayment
- eCommerce

**Supported platforms**

- iOS (8.X and above)
- Android (4.X and above)
- Windows Phone (8.X and above)

**Supported Algorithms**

- OATH (HOTP/TOTP) and OCRA
- EMV CAP (mode 1, 2, 3, 2TDS)
- FIDO UAF

Thales Gemalto Mobile Suite help banks comply with:

- EU PSD2 regulation
- FFIEC Retail Payment Service Appendix 5 on Mobile Financial Security
- NIST 800-63-3 Digital Authentication Guideline