CRYPTOMATHIC MASC PRODUCT SHEET

Comprehensive and dynamic protection for banking apps

CRYPTOMATHIC MASC

Protect the Integrity and Valuable Data of Mobile Apps

Banking customers expect their mobile apps to offer full-service facilities with minimum friction. Mobile apps are required to be freely available on public servers, providing a playground for attackers to download and exploit weaker applications in their own time. A poorly-designed mobile banking app can offer a huge attack surface for hackers. Cryptomathic Mobile App Security Core (MASC) is a banking app security solution that provides comprehensive data protection and proactive defense mechanisms with multiple, mutually reinforcing security layers. MASC's security framework consists of self-defending mechanisms, application hardening, secure connectivity, secure storage and device & API protection.

MASC Benefits

- Protect your application without sacrificing development speed - allowing a small team to handle and enforce the security of the app

- Passive and active protections, e.g. secure enrollment, anti-tamper, app integrity, certificate pinning and access-control to keys

- Extensive configuration options to enable you to adapt the applied protection to your security and performance requirements

- Defense mechanisms are regularly refined and updated so your application protections are always ahead of the attackers

- MASC SDK is supplied with an easy-to-integrate API

MASC is used to protect millions of banking app users by providing a range of multi-layered protections and dynamic defense mechanisms that are constantly evolving. MASC accelerates app development by taking responsibility for the security-critical requirements. The comprehensive security framework provided by MASC is proven to:

- Protect sensitive data and cryptographic keys

- Implement device, API and authentication assurance

- Apply anti-debug and anti-tamper mechanisms • Enforce a gateway for secure communications

- Manage HTTPS access tokens and session cookies on behalf of the app

- Support device fingerprinting and malware detection tools

CRYPTOMATHIC MASC

App protected with MASC   Backend
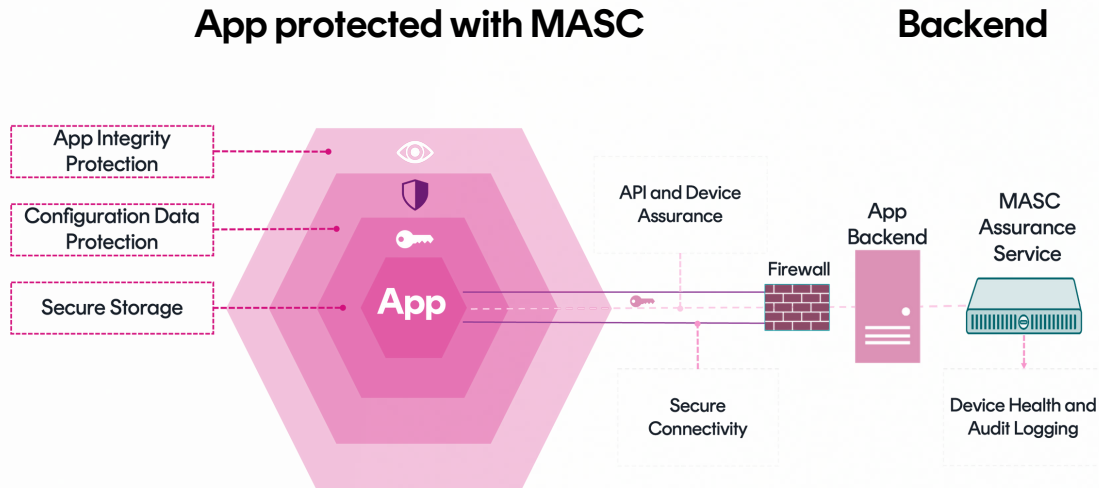
Technical Architecture

Cryptomathic MASC is a platform independent security SDK for Android and iOS, delivering a framework that allows for continuous updates and rearrangement of the active protections to always stay ahead of attacks, including counterfeiting and tampering. Dynamic and static defense mechanisms are embedded throughout the multiple security layers. The defense mechanisms mutually reinforce each security layer to radically improve both the quality and depth of protection provided.

MASC protects and tunnels the communications between the app and the server and also provides a library that enables the back-end to monitor and respond in real-time to subversive activity occurring on the app and device. In coordination with the back-end component, MASC provides assurance that the back-end is talking to a genuine, trusted app instance. Device health is relayed to the backend to inform about rooting, jailbreaking, presence of common hacker tools, etc.

Technical Summary

Security Features:

- Multiple layers of code and data obfuscation to protect secrets
- Runtime application self-defense: anti-debug, anti-tamper, application integrity and emulator detection
- HTTPS handling with host and certificate whitelisting controlled by the security team
- Root and jailbreak information is relayed to the backend as part of device health reports
- Secure store with optional PIN and biometric protection

- Secret protection: keeps protocol secrets away from the upper app layers.
- API protection: the backend can quickly discard requests not coming from genuine app instances

Languages:

- Java, Kotlin, Objective-C, React-Native, Swift

Operating System:

- Android
- iOS

CRYPTOMATHIC MASC

Cryptomathic MASC: Evolving App Security

MASC delivers a proven framework to enhance app security while giving app developers the freedom to deliver the best user experience. It has been in production with leading banks for several years, successfully protecting millions of banking-app instances. MASC protection measures are constantly being refined and updated (along with the standard mobile app updates) to remain resistant and resilient to both known and unknown attacks. Cryptomathic's battle-hardened evolutionary security design ensures that mobile apps and their security framework remain resistant against known and future attacks.

Customer References

Multinational Bank

As part of its digitalization strategy, a large multinational financial institution started its European roll-out of a retail banking app across multiple countries. Protecting the app integrity and sensitive data against known and unknown attacks was the highest priority. MASC was identified as the most comprehensive solution to meet the strict security requirements. By providing a complete security framework, MASC helped to streamline development, enabling the development team to successfully launch the first national roll-out on schedule.

Tier 1 European Bank

To meet customer demand, a large European bank launched a feature-rich mobile banking app for their retail customers. MASC was chosen as the best solution to protect the app against attacks and to provide platform independent secure storage and access-control for the keys. With more than 5 years in production and millions of active app users, the protections provided by MASC continues to keep the banking app secure and protect customer sensitive data

Don't just take our word for it!

We have observed several white and black hat hackers posting on various internet forums to share their experience and ideas on penetrating and compromising banking applications - with varying degrees of success. A select few mobile banking applications were identified as impenetrable so far. In fact, after careful review we were able to confirm that the mobile apps they were speaking of as impenetrable, were the ones secured with MASC - for which some hackers concluded that these banks must have a stellar security team working for them.

WHO WE ARE

Cryptomathic is a global provider of secure server solutions to businesses across a wide range of industry sectors, including banking, government, technology manufacturing, cloud and mobile. With over 30 years' experience, we provide systems for Authentication & Signing, EMV, Key Management and PKI & ID, through best-of-breed security solutions and services. We pride ourselves on strong technical expertise and unique market knowledge, with two-thirds of employees working in R&D, including an international team of security experts and a number of world-renowned cryptographers. At the leading edge of security provision within its key markets, Cryptomathic closely supports its global customer base with many multinationals as longstanding clients.

www.cryptomathic.com   **enquiry@cryptomathic.com**

+45 8676 2288