SOLUTION BRIEF

Secure Fintech: A Complete Guide to Mobile App Security in the Financial Sector

Key Benefits of the Approov Solution

- Positive app authentication
- Blocks all forms of API Abuse
- Runtime secrets protection for 3rd party APIs
- Protection from Man-in-the-Middle attacks
- Tamper Detection and Jailbreak/Root Detection
- Confidence that the client environment is always secure
- Elimination of API keys and secrets from mobile code
- Dynamic management of security policies, certificates and secrets
- Cross platform support for iOS, Android and Harmony OS
- Support for Non-GMS Android devices
- Compliance with Regulatory Standards
- Real-time analytics for control and compliance
- Easy integration and operation

Financial Services Apps and Their APIs are Exposed

Finance apps are a target for hackers because they present the opportunity to directly divert funds and steal money. They are also attractive due to the wealth of sensitive customer data which they store and access. In addition, APIs used by apps for payment and other services are under attack from fake apps.

Mobile Banking is a Target for Hackers

Mobile banking is outpacing online banking across all age groups due to its convenience and availability. However, this surge is accompanied by a dramatic growth in financial fraud and theft of personal banking credentials and credit card information.

Crypto Apps Are Under Attack

Crypto apps are even more exposed than banking apps because of the emerging nature of the business of crypto.

Compliance is Key

Companies operating in the financial sector are obligated to adhere to regulations to be compliant and interoperable, particularly relating to the use of APIs. These include:

- Payment Card Industry (PCI) Mobile Payments on COTS (Commercial-off-the-Shelf) devices (MPoC) standard
- The Directive on Payment Services (PSD2)
- The Open Banking Implementation Entity (OBIE) in the UK

Another essential and related legal requirement is protecting user data, which comes in various forms across the world and has more geographical coverage. Most countries now have privacy laws, for example:

- 17 New Privacy Laws Around the Globe
- Europe’s General Data Protection Regulation (GDPR)
- The California Consumer Privacy Act (CCPA)
- German Telecommunications and Telemedia Data Protection Act (TTDSG)
- Brazilian General Data Protection Law (LGPD)
- Singapore’s Personal Data Protection Act (PDPA)
- South Korea’s Personal Information Protection Act (PIPA)

Of course, good security hygiene is a lot more than just meeting the requirements of the relevant standards and regulations; it should imply the application of best practice security solutions in a coherent configuration to protect against the threats of today and of tomorrow.

How Do Hackers Target Finance Apps?

Fake finance apps containing malicious software (malware) like trojans and keyloggers can steal login credentials and financial data from users. Phishing tactics try to trick users into revealing sensitive information through fake apps, emails, or websites impersonating legitimate financial institutions.

Unencrypted data transmission and weak encryption practices for storing sensitive data on devices or during transfer make them vulnerable to Man-in-the-Middle attacks.

Insecure login methods lacking multi-factor authentication or weak password policies make it easier for unauthorized access. Poor authorization controls could allow users to access or manipulate financial data they shouldn't.

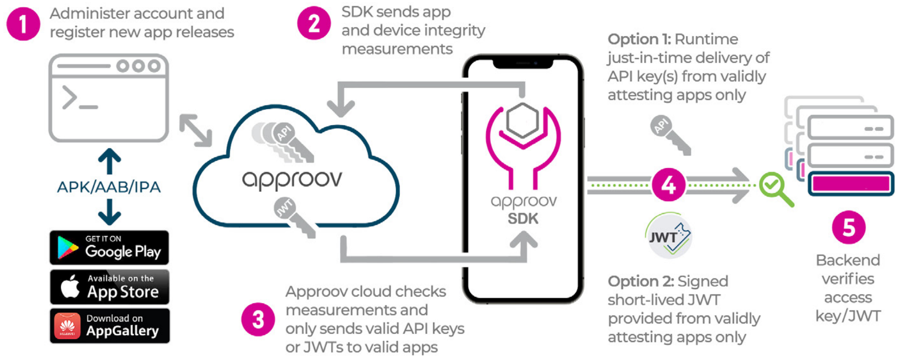
Frameworks and tools installed on devices can gain access at runtime to financial apps and steal data or change the way they operate. Additionally, vulnerabilities in the mobile operating system itself can be exploited to target financial apps.

Approov Protection for Mobile Apps and APIs

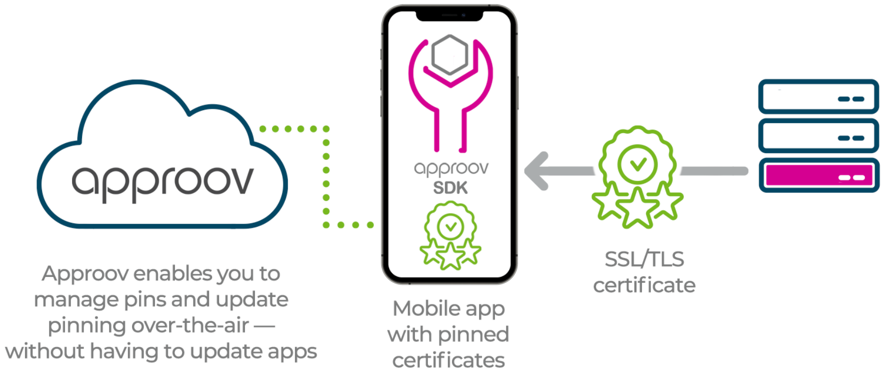
Approov Mobile Security provides a comprehensive multi-factor, end-to-end mobile app and API security solution that prevents any manipulation of the app, device or communications channel to the backend, and removes secrets from your app code. Only safe and approved apps can successfully use your APIs. Bots and fake or tampered apps are all turned away and data is protected. Approov helps you achieve financial industry compliance.

Key Benefits of the Approov Solution

- App and Device Attestation: As mentioned, one of the critical attack surfaces employed by hackers is to clone or copy apps in order to imitate genuine apps, either to directly steal user authentication data or to extract information from backend systems by mimicking genuine apps. The core functionality of Approov makes sure that only a genuine app is accessing APIs and backend systems and any attempted access by modified apps, scripts and bots are blocked. This disables one of the key attack methods used by hackers.


1
Administer account and register new app releases
2
SDK sends app and device integrity measurements
Option 1: Runtime just-in-time delivery of API key(s) from validly attesting apps only
APK/AAB/IPA
API
approov
JWT
approov SDK
4
GET IT ON Google Play
Available on the App Store
Download on AppGallery
JWT
5
Backend verifies access key/JWT
3
Approov cloud checks measurements and only sends valid API keys or JWTs to valid apps
Option 2: Signed short-lived JWT provided from validly attesting apps only

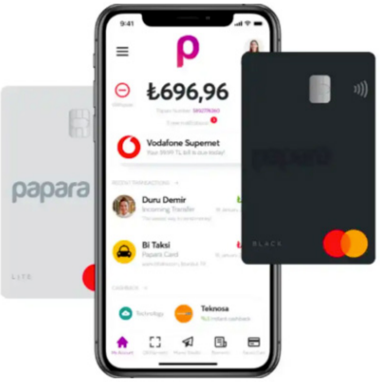
- Man-in-the-Middle Attacks: A major threat for mobile apps is MitM attacks since these can be carried out by hacking the mobile device the app is running on. A hacker intercepts the traffic in the communication channel and can inject new commands. Approov implements dynamic certificate pinning, which secures the communications channel completely, but does it in a way that service continuity can always be ensured, even when certificates are updated.


approov
Approov enables you to manage pins and update pinning over-the-air — without having to update apps
approov SDK
Mobile app with pinned certificates
SSL/TLS certificate

- Hacking the client environment: Another hacker technique is to interfere with the mobile client environment to interfere with the operation of the app to steal data or change the logic. Jailbroken iOS devices or rooted Android devices pose considerable risk, as enhanced privileges allow more advanced hacking tools to run that compromise your app. There are a wide range of reverse engineering and function hooking tools available for both iOS and Android. You must get visibility and control of the client. environment to protect against such attacks. Approov, for example, detects if your app is running on jailbroken or rooted devices, detecting Frida, Xposed, Cydia, as well as being able to see if debuggers, emulators or cloners are running on the device.
- Runtime Secrets Management: Mobile crypto apps need to access public and private APIs to do their job and will need to use API keys to access these APIs. If you carelessly expose these API keys, hackers will ruthlessly exploit them to imitate your app and access the APIs for nefarious purposes. You must therefore endeavor to keep API keys and other secrets out of your mobile code. Fortunately there are ways to have these delivered securely and just-in-time to the app when needed, and only if the app passes attestation tests. For example, Approov securely manages API keys for you and delivers them to your app only when needed and only when safe.
- Dynamic Security Policy Management: Security may need tuning but that shouldn't be hard to manage: You will need tools that provide the devops team with run time visibility and dynamic control over security policies. As an example, Approov supports the devops team with the implementation of highly granular security policies which can be updated instantly over-the-air.
- API Data Breach Mitigation: Finally if hackers do get their hands on your keys and secrets (e.g. from a cloud repository), your APIs can be exposed to attack. You need a mitigation plan for if (or when) this happens so that your service is not interrupted as you rotate keys. Approov allows you to rotate keys and certificates without having to update deployed apps. You can be confident that no matter what happens you can keep your apps running and secure.

Case studies

Papara is a very fast growing electronic money and payment services company based in Turkey. To understand how they reduced operating costs by 90% in 30 days across a range of security threats please check out their case study: https://approov.io/customer/papara/



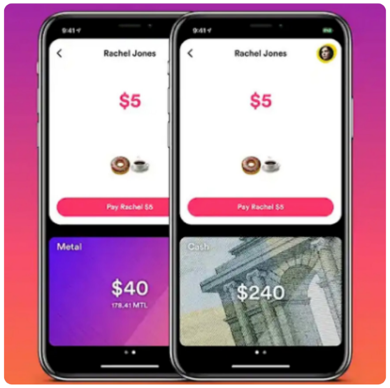
> **We are very happy with Approov. It works well and matches exactly to the use cases we were initially concerned about. Blocking so much fraudulent traffic from scripts and automators significantly lifts the pressure on Papara's systems as well as on our finances. We have also found the Approov team to be very flexible and proactive with respect to managing our service.**
>
> \- Emre Kenci, CTO, Papara

papara

Crypto platforms, much in the news recently, face a different set of challenges from a security perspective. Metallicus set out to become the 'PayPal of crypto' but automated traffic threatened to get in the way of their vision. Check out their case study to understand what steps they took: https://approov.io/customer/metalpay/

MetalPay

> **Our integration with Approov was one of the quickest ones we've been able to roll out and the results were visible instantly. Looking at the traffic we've been able to counter with Approov and the financial fraud that usually comes with it I'd be willing to guesstimate at least a 10x return on our investment with Approov.**
>
> \- Glenn Marien, CTO and Co-founder Metallicus



Contact us for a free technical consultation - our security experts will show you how to protect your revenue and business data by deploying Approov Mobile Security https://approov.io/info/contact