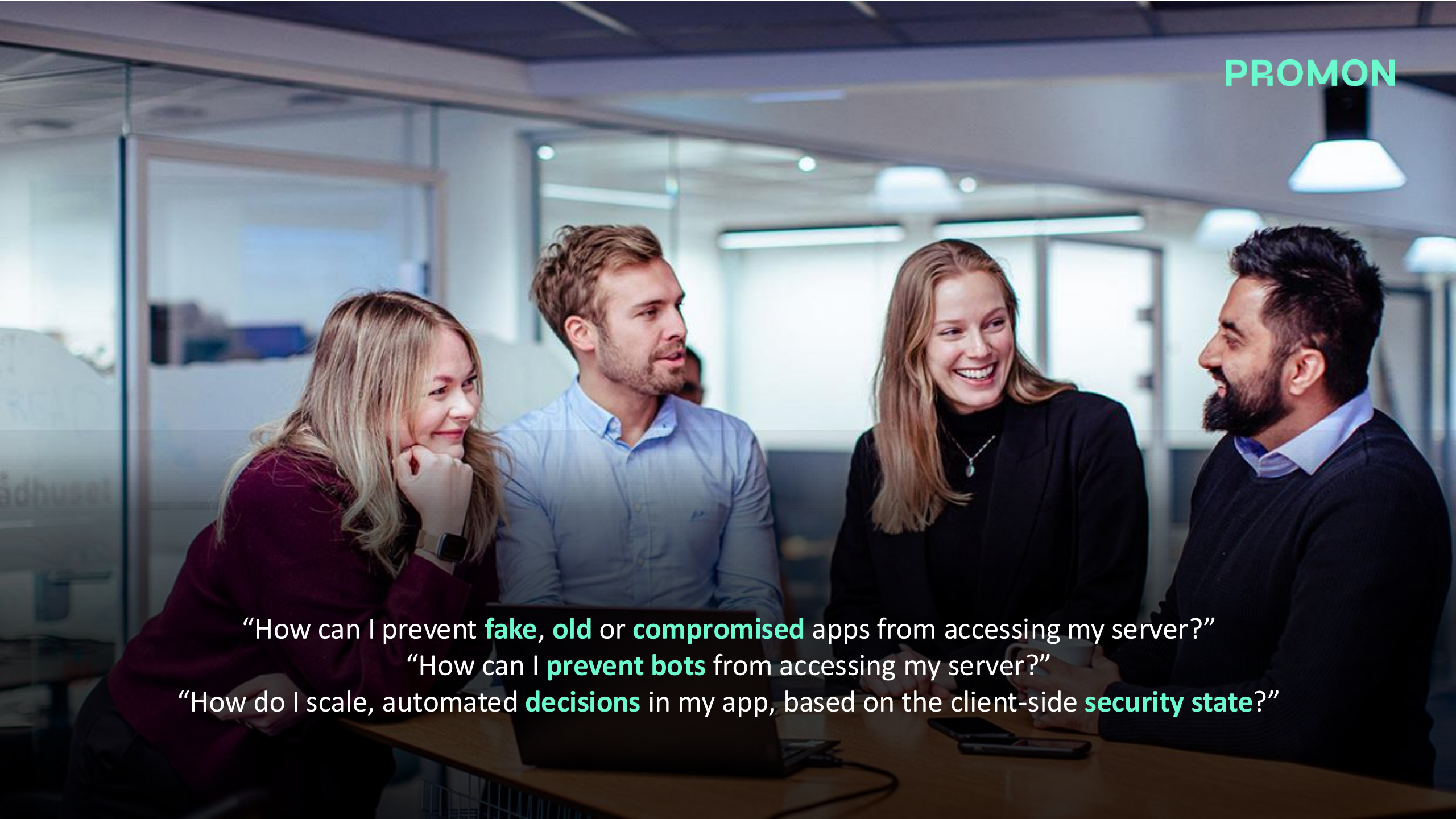
PROMON

Promon App Attestation™

Positioning, Packaging, Resources, FAQ


PROMON
“How can I prevent fake, old or compromised apps from accessing my server?”
“How can I prevent bots from accessing my server?”
“How do I scale, automated decisions in my app, based on the client-side security state?”

API attacks on the rise

78%

The amount of API attacks that come from seemingly legitimate users but are, in fact attackers with maliciously achieved authentication[1]

35%

The amount of account takeover attacks targeting APIs specifically[2]

$41-75 billion

The annual cost of API insecurity[3]

1. Salt Security, 2. Imperva, 3. VentureBeat

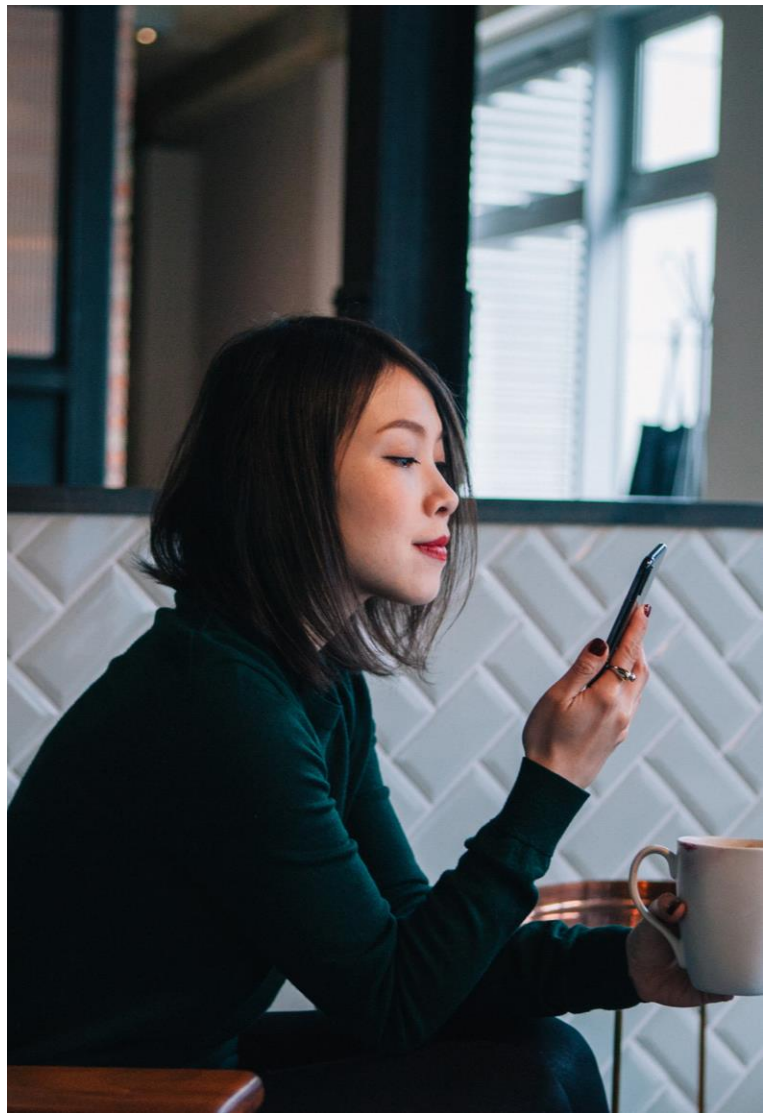
PROMON

Market pain points

- **Security threats:** Not all mobile apps can be trusted. 61% of apps in the wild could be repackaged or suffer from malware already present in the device running the app
  - Generic attestation has limitations: if the attestation server is not reachable (or if the app 'thinks' it is not reachable), then a fallback, way less secure mechanism is used
  - Protection at runtime is not possible because verification is done only at launch time
- **Compliance:** API-related hacks and data breaches have impacted organizations across the world
  - The average annual API-related global insured cyber loss is estimated at USD 205-376 million. Cyber insurers could reduce up to 375 million/year of their claims if they required their clients to have better API security.

A new way to achieve API security with best-in-class mobile app protection

Promon App Attestation is the first pillar for security *at reach* allowing customers to bind the authenticity and integrity of their mobile apps to their APIs in real-time.



PROMON

Why Promon App Attestation

Why? Mobile devices and apps are not always trustworthy and shouldn't be treated as such. Without a SHIELD-protected app, attackers could modify the app's behavior, steal sensitive data, or use the app as a vector for malware or other attacks.

Why us? App Attestation is a solution that delivers integrity validation and authenticity of the application. It's baked into the Promon SHIELD™ multi-layered mobile app protection, which delivers protection at rest and at runtime. App Attestation is Promon's first solution for *at-reach protection* — connecting to external APIs and services. The integration is seamless, requiring minimal code integration, and the attestation data is carried in-band in the apps existing network communication. The backend element is designed to be stateless, delivering simple backend maintenance. Your apps can be quickly secured and distributed in minutes through our integration tool.

Why now? Mobile apps are already essential for businesses and their customers, and the risks associated with mobile app security are growing. And with the rise of hyper-connected apps, enforcing security in real-time is crucial. App Attestation allows for security to be integrated between the client and the server or API, protecting your apps, APIS, and users from malware, and allowing you to comply with industry standards and regulations.

PROMON

Go from static to dynamic app attestation

Unlike the “static” attestation approach from Apple and Google, which is limited to session-based verification typically only when the app is launched, Promon App Attestation™ is transaction-based. It validates continuously, as needed.

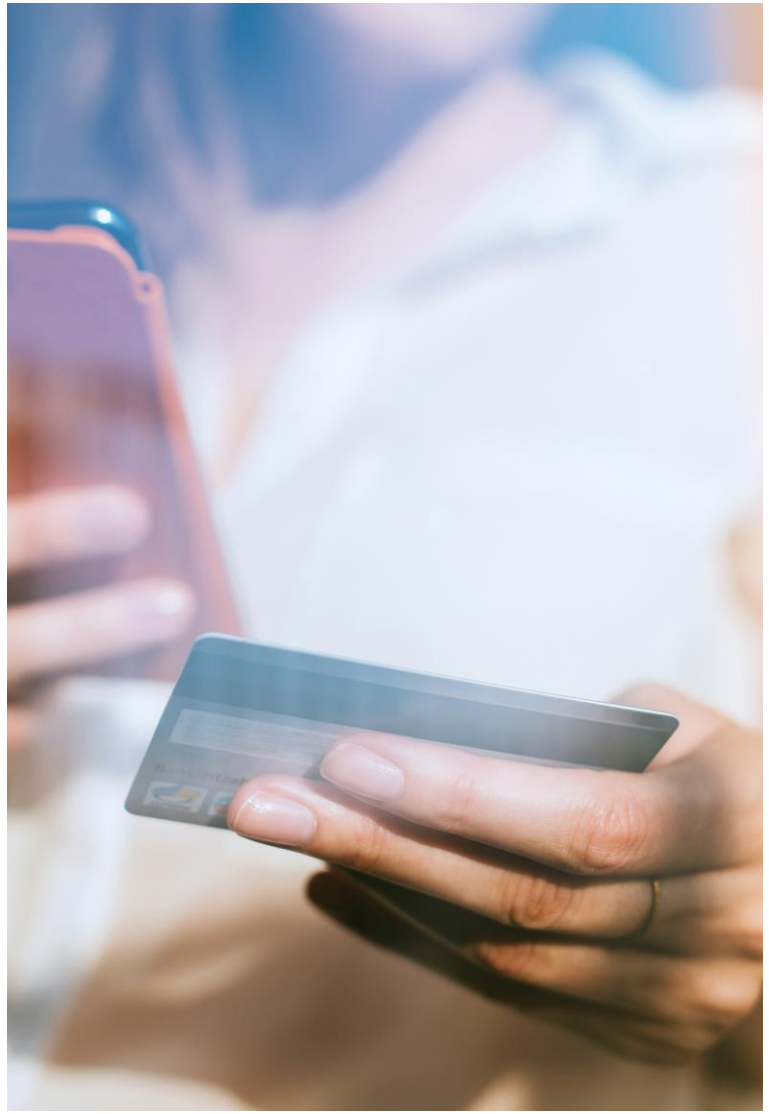
- The integrity and authenticity of the app are verified in real time, providing a higher level of security and protection against potential tampering
- The app's integrity is upheld throughout all transactions and interactions with APIs

PROMON

Go beyond authentication and secure your app at runtime

The Promon SHIELD™-protected app authenticates to the server with the embedded assurance that the app is uncompromised. Google and Apple don’t check if the application was tampered with and don’t validate the device integrity, while the App Attestation module also checks the app’s security state through:

- root or jailbreak checks
- runtime hooks found
- repackaging checks
- hooking frameworks present

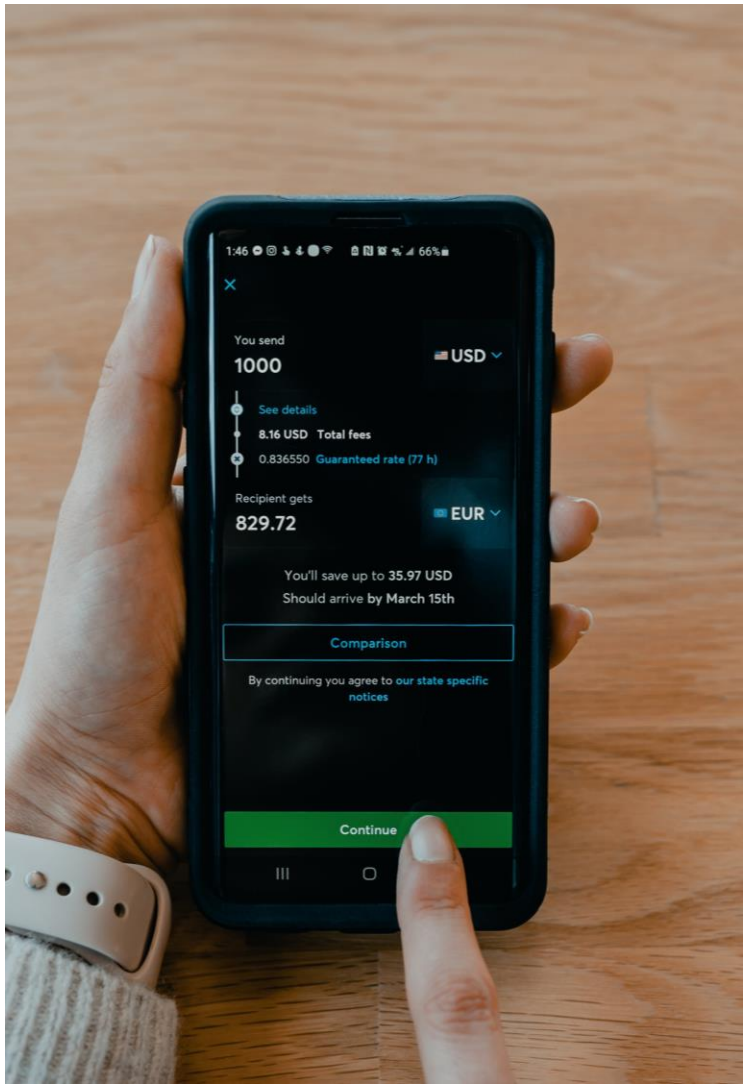


PROMON

Full control

The Promon App Attestation™ module is self-contained and agnostic from iOS and Android.

- Provides a sovereign approach that doesn’t rely on third-party services; businesses control the entire chain of trust in their country/operating zone
- Greatly reduces the risk of having a vector of attack if the “attestation server” is down by having a direct, in-band approach
- No rate-limit as it is self-hosted by the customer
- Impossible to intercept due to being an in-band payload



PROMON

Promon App Attestation™ vs. the competition

	Apple/Google*	Approov.io	App Attestation
Deployment complexity	No	Relying on Apple & Google + specific technology in addition	Minimal
Customizable	No	The additional security is configurable	Yes
Runtime protection	No	No	Best
Cross platform	No**	Yes	Yes
Dependent on third-party services	Yes	Yes	No

* Apple App Attest and Google Play Integrity API
**

PROMON

Benefits

1. Enhance security

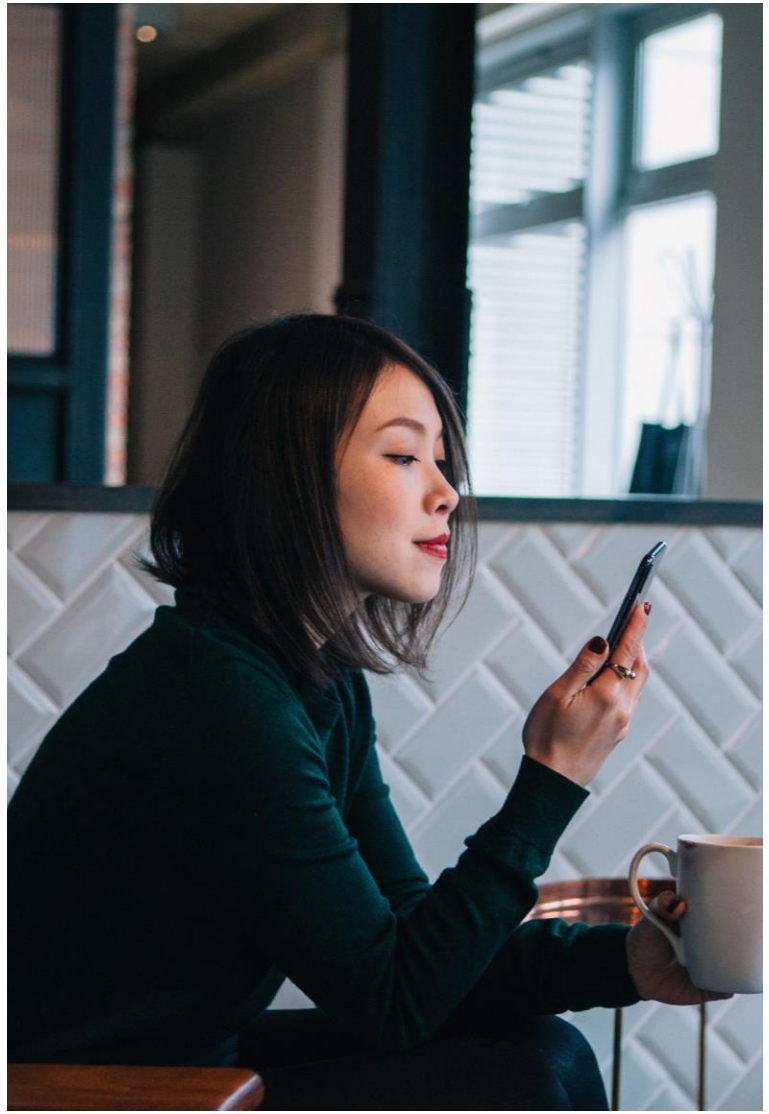
Stops rogue mobile apps or servers impersonating legitimate sources. The App Attestation module ensures the access to customers' APIs only comes from a validated mobile app, preventing attacks such as API injection and data tampering.

2. Improve compliance

Use App Attestation to secure the API connectivity without impacting regulatory constraints.

3. Build user trust

Demonstrate your commitment to security, privacy and reduce the risk of systemic attacks. You can increase user trust since your organization will avoid costly breaches and hacking incidents.

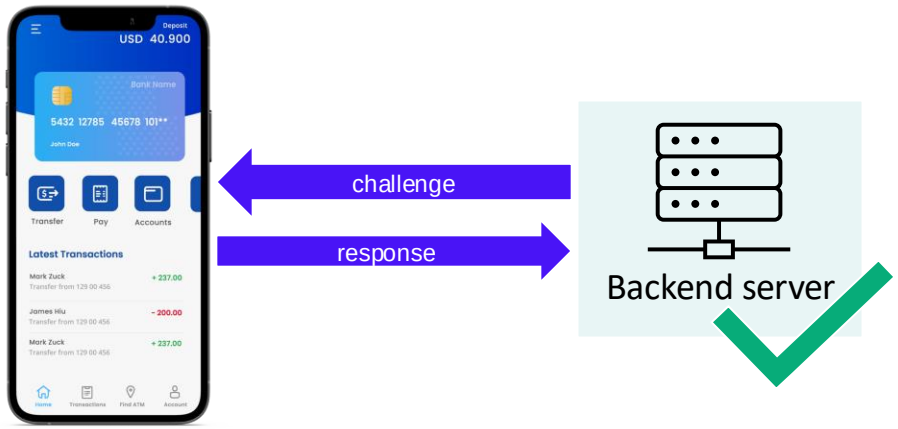


PROMON

How it works

The challenge-response mechanism:

1. Uses a shared secret between the backend server and the app - handshake foundation
2. Is protected with SHIELD's white-box cryptography which ensures self-protection and prevents repackaging
3. Uses a Message Authentication Code to calculate responses - important to avoid dictionary attacks



PROMON

Integration

Server-side integration

Promon provides a Java library for integration in a web application or gateway.

Client-side integration

Integration is necessary, provided you have the latest Promon SHIELD™ version. It will include attestation APIs for Android and iOS.

Configure secrets

Simply configure App Attestation through SHIELD's config.xml file and re-shield as usual.

PROMON

Verticals and use cases (1)

Vertical	Context	Use cases
Gaming	When a mobile game publisher has to deal with cheaters who destabilize their business model and shorten the life of a game, they need to mitigate these risks through updates and maintenance, which, in turn, lead to higher management costs.	App Attestation prevents **friendly fraud** where the user is willing to have an altered version of the game or share their credentials. App Attestation is also effective against using a modified app to get an unfair advantage against other gamers and therefore get in-game benefits or cash-out gains, like in the case of **account farming**. Furthermore, deploying App Attestation will deliver filtered access to the gaming apps' APIs and allow game studios and publishers to **react if non-genuine apps are trying to connect to their servers**.
Banking & Open Banking	Open banking is an initiative that allows consumers to securely share their financial data with third-party organizations, such as fintech companies and other financial organizations. This data-sharing allows companies to offer consumers a broader range of financial services, such as personal finance management tools and tailored lending options. This is done through APIs. The data sharing is monitored and supervised according to existing government regulations, like PSD2 in the European Union or the Open Banking Act in the UK.	App Attestation is the safest and most effective way to **ensure rogue apps don't abuse the APIs**. By verifying the integrity and authenticity of the apps in real time, the module guarantees that only trusted and untampered versions of the apps can interact with the financial institution's servers. It ensures the security and integrity of the communication between the mobile app and the servers of different financial institutions, **preventing unauthorized access and data theft**. Even non-banking aggregators, such as indie or accounting services, can inadvertently inject rogue API usage into the banking ecosystem through their apps. The module is a crucial defense mechanism, detecting and preventing **unauthorized API usage** that could potentially harm the serving bank.

Verticals and use cases (2)

Vertical	Context	Use cases
Media / Streaming	Streaming and media companies like Netflix, Max, and others rely on mobile apps and APIs to deliver seamless and immersive entertainment experiences to their customers.	An attacker can hack the app OR can create a streaming decoder application and link straight to the streaming API. App Attestation, by connecting the streamer's mobile app with the APIs provides effective protection against these attacks. For example, App Attestation will **diminish DRM breaches on the server side** because even if DRM keys are leaked, the API can only be accessed by protected, unmodified applications. Streaming content remains secure and accessible only through legitimate channels, preventing unauthorized distribution and piracy. The module is also **effective against app tempering attempts**, such as reverse engineering or modifying the app's code, providing robust protection against malicious activities that may compromise the security and integrity of the streaming service.
Retail / eCommerce	Retail and eCommerce mobile apps play a crucial role in connecting businesses with their customers. However, this ecosystem also presents security challenges, as attackers can use rogue applications to abuse APIs and commit fraud, leading to financial losses and reputation damage for retailers.	App Attestation provides a vital defense against the misuse of APIs by rogue applications. By thoroughly **verifying the integrity and authenticity of the mobile apps** in real time, the module establishes a secure and trusted connection between the apps and the eCommerce platform's APIs. This ensures that only legitimate and untampered applications can access and utilize the APIs, preventing unauthorized access, data breaches, and fraudulent activities. App Attestation helps protect businesses from **fraudulent activities**, such as unauthorized transactions, account takeovers, and identity theft. **Chargebacks** can be a significant challenge for eCommerce businesses, resulting in financial losses and increased operational costs. App Attestation prevents unauthorized and fraudulent transactions, minimizing the risk of disputes and chargebacks, thereby improving the overall financial health of the business.

Case study: Stopping fraud for a leading food delivery service

About	Problem	Solution	Result
This leading delivery company works with over 160,000 restaurants and grocers in more than 200 locations across several countries in Europe. - Revenue: £1.8B GBP	Hackers were targeting the company's Driver app, altering geolocation and laundering money through fake restaurants and fake orders (£MM).	The company added Promon App Attestation to prevent app tampering and ensure that they can properly authenticate users	It worked. The fraud stopped, and the company is creating an App Shielding Centre of Excellence to roll out App Shielding to the rest of the company's apps.

PROMON

Thank you