Datasheet

PROMON

Promon SHIELD™ App Attestation

Mobile app and API security made simple

Mobile apps are not always trustworthy and should be treated as such. Today, mobile apps handle sensitive user information such as financial, personal health, and social media data. Authentication is insufficient to ensure full security, and if a rogue app connects, the APIs are prone to abuse, leading to breaches, non-compliance, and loss of user trust. Additionally, without a protected app, attackers could modify the app's behavior, steal sensitive data, or use the app as a vector for malware or other attacks.

The time for app and API attestation is now

With Promon SHIELD™ App Attestation, you can verify the authenticity and integrity of your mobile apps accessing your APIs in real time, ensuring that they have not been compromised or tampered. What's more, the module also checks the integrity of the mobile devices running your apps.

Promon SHIELD™ 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 provides protection at rest and at runtime. The SHIELD App Attestation module is Promon's first solution for at-reach protection — connecting to external APIs and services.

Furthermore, the integration is seamless, requiring minimal code integration, and the attestation data is carried in-band in the apps' existing network communication. The back-end element is designed to be stateless, delivering simple backend maintenance. Your apps can be quickly secured and distributed in minutes through our integration tool.

PROMON

With Promon SHIELD App Attestation:

Transition from static to dynamic app attestation

While Google and Apple's attestation approach is limited to session-based verification when the app is launched, SHIELD™ App Attestation provides transaction-based, continuous validation. This ensures the mobile app is executed in a secure and unmodified environment while connecting to your APIs. With real-time validation, the module enhances security and safeguards against potential tampering, providing higher protection for your app and data.

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 Promon SHIELD™ with the App Attestation module also validates the app and device integrity.

Get full control

Promon SHIELD™ App Attestation is self-contained and agnostic from iOS and Android. It provides a sovereign approach that doesn't rely on third-party services. Thus businesses can control the entire chain of trust in their country/operating zone. Promon's App Attestation module greatly reduces the risk of having a vector of attack if the "attestation server" is down by having a direct, in-band approach. There is no rate limit as it is self-hosted by the customer and is impossible to intercept due to being an in-band payload.

PROMON

Strengthen your app and API security

Enhance security

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

Improve compliance

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

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.

SHIELD App Attestation vs. traditional attestation

	SHIELD App Attestation	Apple	Google
Customizable	Yes	No	No
Runtime protection	Best	No	No
Cross platform	Yes	No	No
Depend on third-party services	No	Yes	Yes

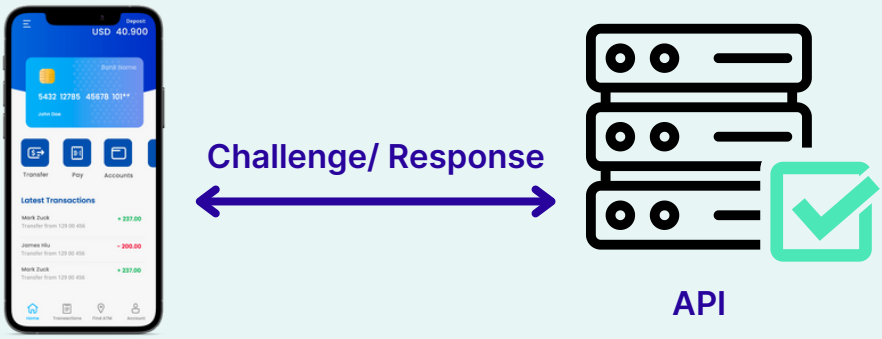
PROMON

How it works

Promon SHIELD™ App Attestation can be easily adapted for apps that are already talking to a backend server by piggybacking challenge and response tokens on existing communications.

The challenge-response mechanism:

1. Uses a shared secret between the backend server and the app — handshake foundation
2. Is protected with Promon SHIELD™'s white-box cryptography — important to ensure message integrity ensure and prevent repackaging.
3. Uses a Message Authentication Code to calculate responses — important to avoid dictionary attacks.



App and API protection tailored to your needs

- Gaming
- Banking and Open Banking
- Streaming
- eCommerce

Get in touch

To learn more about how to protect your apps and APIs, visit our website or schedule a demo with one of our experts.

PROMON

www.promon.co