YESsafe
AppProtect+

AppProtect+ 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.

The time for App and API Attestation is Now

With YESsafe AppProtect's 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 with. What's more, the module also checks the integrity of the mobile devices running your apps.

AppProtect+'s App Attestation is a solution that delivers integrity validation and authenticity of the application. It's baked into our multi-layered mobile app protection, which provides protection at rest and at runtime. The App Attestation module is i-Sprint'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.

WITH APPPROTECT+ 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, AppProtect+ 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 i-Sprint-protected app authenticates with the server, ensuring that the app remains uncompromised. Unlike Google and Apple, which do not verify if the application has been tampered with or validate the device's integrity, AppProtect+ equipped with the App Attestation module, verifies both the app and device integrity.

GET FULL CONTROL

AppProtect+ App Attestation is agnostic from iOS and Android, offering a self-contained, sovereign approach that doesn't depend on third-party services. This grants businesses control over the entire chain of trust within their country or operating zone. With the AppProtect+ App Attestation module, the risk of a potential attack vector is significantly reduced, even if the "attestation server" experiences downtime, thanks to its direct, in-band approach. Moreover, since it is self-hosted by the customer, there are no rate limits, and interception is impossible due to its in-band payload nature.

STRENGTHEN YOUR APP AND API SECURITY

YESsafe
AppProtect+

ENHANCE SECURITY

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 and privacy by reducing the risk of systemic attacks. Increase user trust and avoid costly breaches and hacking incidents.

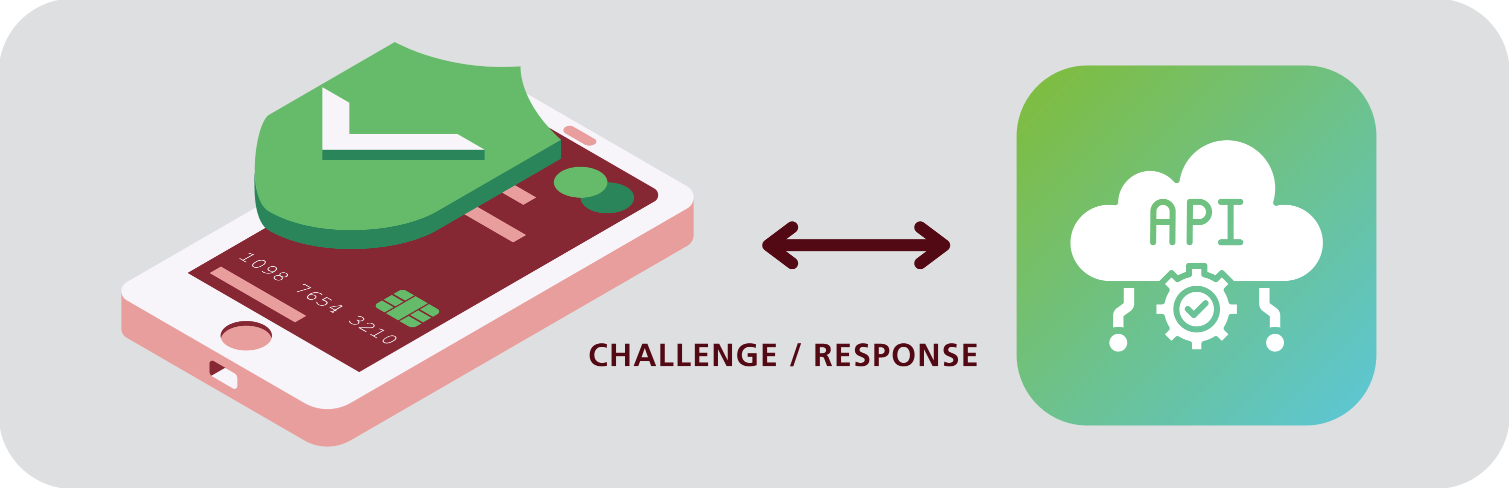
APPPROTECT+ ATTESTATION VS. TRADITIONAL ATTESTATION

Customisable	✓	✗	✗
Runtime Protection	✓	✗	✗
Cross Platform	✓	✗	✗
Independent from Third-party Services	✓	✗	✗

HOW IT WORKS

YESsafe
AppProtect+

AppProtect+ 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:

01 Uses a shared secret between the backend server and the app — handshake foundation

02 Protected with AppProtect+'s white-box cryptography — important to ensure message integrity and prevent repackaging.

03 Uses a Message Authentication Code to calculate responses — important to avoid dictionary attacks.

APP AND API PROTECTION TAILORED TO YOUR NEEDS

- Gaming
- Financial Institution
- Streaming
- eCommerce

Global Headquarters
Blk 750D Chai Chee Road #08-01
ESR BizPark @ Chai Chee (Lobby 1)
Singapore 469004
☎ +65 6244 3900
✉enquiry@i-sprint.com

For a complete list of our offices in China, Hong Kong, Japan, Malaysia, Thailand & United States, please visit www.i-sprint.com/contactus

i-Sprint
Trust without Boundaries

©2000-23 i-Sprint Innovations Pte Ltd. All rights reserved.
i-Sprint, i-Sprint logo, AccessMatrix, and AccessMatrix logo are registered trademarks of i-Sprint Innovations Pte Ltd. All other trademarks and registered trademarks are the property of their respective owners. i-Sprint reserves the right to make changes to the specifications or other product information at any time and without prior notice.