# Nok Nok

# App SDK

As private information is dispersed across an increasing number of cloud accounts, users find themselves frustrated with having to remember more usernames and passwords to log in to various accounts. Authentication methods often cause higher friction in the log in process when users are required to undergo multiple actions to authenticate to applications or perform steps that demand more effort. Often, this process results in failure, with the consequence of user frustration leading to lower engagement rates and abandoned transactions. A complete authentication solution must deliver ease of use and at the same time, strong security.

## Introducing Nok Nok App SDK

Nok Nok App SDK improves the user authentication experience by taking advantage of the existing authenticators and security capabilities present in billions of mobile devices. As part of Nok Nok's S3 Authentication Suite, the App SDK enables any application to leverage these capabilities by plugging them into an end-to-end framework based on the FIDO Protocols. Using the App SDK, users can authenticate faster, more securely, and easily with methods such as fingerprint and face biometrics or PIN codes. App SDK can take advantage of secure hardware such as Trusted Execution Environments (TEE) and Secure Elements (SE) to protect critical components of authentication on the device. The App SDK eliminates the need for users to carry separate devices for authentication and simplifies the authentication process. Users can even use their current mobile devices as an authenticator to web applications running on their laptops by using the Out-of-Band authentication feature of App SDK. The App SDK supports the user lifecycle journey by providing robust account recovery methods such as Email One-Time-Password (OTP), SMS OTP, and Photo ID combined with a live picture.

The Nok Nok App SDK improves the usability of authentication, increasing engagement and transaction completion rates. The Nok Nok App SDK encourages the adoption of strong authentication and minimizes many security risks created by the use of passwords. Improved security encourages greater trust in the application, increasing application adoption and usage.

## Key Benefits

### Better User Experience

Users can authenticate with user-friendly biometric authentication methods, improving engagement and transaction completion rates.

### Improved Security

Public key cryptography-based authentication protocol protects from phishing and man-in-the-middle attacks.

### Policy-Driven

Choose the best authentication method for the user, and enforce policy based on risk signals delivered by the device.

### Reduced Costs

Using the existing security capabilities of devices that users already possess removes the need for the distribution and tracking of separate tokens.

### Privacy Preserving

User biometrics templates are stored securely on the device. Only public keys are stored on the server which also removes the risk of a scalable attack.

### Future Proof

New devices and new forms of authentication can easily be enabled to work with existing applications.

## TECHNICAL SPECIFICATIONS

| | |
|---|---|
| Account Recovery Methods | - Email OTP<br>- SMS OTP<br>- Photo ID + Live Picture (Selfie) |
| Authenticators | - PIN-protected authenticator<br>- Fingerprint (Touch ID, Android Fingerprint API)<br>- Iris, face, voice, and other biometrics<br>- Out-of-Band authenticator<br>- Apple Watch authenticator<br>- Keyguard authenticator (Android 5.0 and above) |
| Risk Signals | - Geolocation and travel speed violation<br>- Device ID<br>- Friendly Fraud<br>- Device Health (Android only)<br>- Shared Device<br>- Jailbreak Detection |
| Secure Hardware | - Secure Element<br>- Trusted Execution Environment (Android)<br>- Secure Enclave (iOS)<br>- Key Attestation (Android 7.0 and above on supported devices) |
| FIDO Protocols | - FIDO UAF Certified™<br>- FIDO U2F Certified™<br>- FIDO2 Certified™ |
| Applications, Programming Languages and Operating Systems | - Objective-C, C++, Swift, Cordova for Native Apps on iOS™ 8 or higher<br>- Java, Cordova for Native Apps on Android™ 4.4 or higher<br>- JavaScript for Web Apps |

**ABOUT NOK NOK LABS**
Nok Nok empowers global organizations to improve the user experience to access digital services, while meeting the most advanced privacy and regulatory requirements. Nok Nok Labs and its industry leading customers and partners include Fujitsu Limited, Ericsson, Hitachi, Lenovo, NTT DATA, NTT DOCOMO, One-Span and Samsung. For more information, visit www.noknok.com.

Nok Nok Labs, 2890 Zanker Road, Suite 203  San Jose, CA 95134 USA