



Empowering your Apps with the **NoPass™** SDK

NoPass™ SDK is a software developer kit that allows you to build the NoPass™ 3-factor authentication into your existing mobile applications. With our SDK you keep the user from having to install an additional app on their smartphone that performs authentication.



NoPass™ SDK main objective is to provide other developers with a convenient method for registration, authentication, and restoration. The SDK helps developers utilize the binaries and plug them into their existing code. This will accelerate the development of a new app or your company's existing app with NoPass™ Passwordless Authentication built in.

NoPass™ SDK improves the user authentication experience by taking advantage of the existing authenticators and security capabilities in billions of mobile devices. The NoPass™ SDK enables any application to leverage these capabilities by plunging them into an end-to-end framework based on FIDO Protocols. Using the NoPass™ SDK, users can authenticate faster, more securely, and easily with methods such as fingerprints and face biometrics or PIN codes. The NoPass™ SDK can take advantage of secure hardware such as the Trusted Execution Environment (TEE) and Secure Elements (SE) to protect critical components of authentication on the device. The NoPass™ SDK eliminates the need for users to carry a separate device for authentication and simplifies the authentication process.

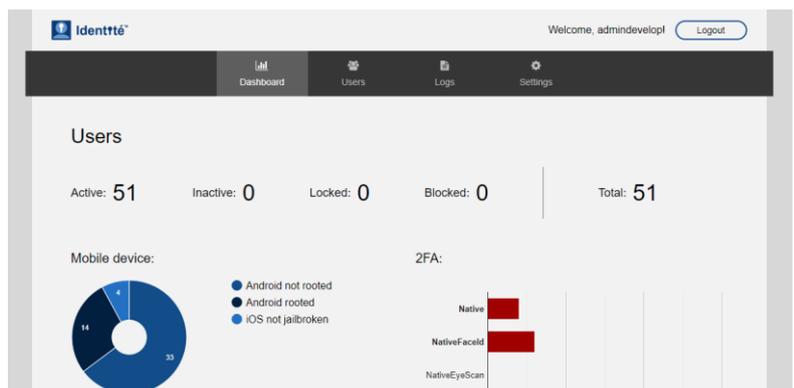
White labeling your App with **NoPass™** SDK

If your ecommerce businesses or company already has an app, using a second app on a users phone will be redundant. You have already made significant investments in its development and it would be better to compile the NoPass™ registration and authentication API's into your own app. The NoPass™ SDK was created for exactly this purpose.



NoPass™ SDK

The SDK gives developers access to a host of NoPass™ authentication, security and user management features. These features include secure Full Duplex Authentication™, decentralized access, user management, device hygiene management, all of which can be controlled from the NoPass™ Admin Panel. The NoPass™ SDK is available for use with iOS and Android devices.



Typical NoPass™ SDK Uses

- ✓ Embedded mobile soft token used for 2FA Biometrics login to Internet Banking, e-Government and Corporate portals
- ✓ High value Transaction signing with WYSIWYS (What You See Is What You Sign)
- ✓ Biometric MFA Login for remote network access: RADIUS, ADFS ...
- ✓ Hardware token replacement, leveraging the technologies embedded in the 3.5 billion smart phones worldwide

Key SDK features

Scalable authentication

Get scalable authentication built right into your application without the development overhead, security risks, and maintenance that come from building it yourself.

Password less authentication

Eliminate the risk of password-based attacks and deliver a seamless user experience using passwordless authentication.



Multi-Factor Authentication

NoPass™ enables you to quickly and easily add MFA to your security strategy without compromising user experience or creating extra work for your dev team.



Compliance

Detect whether the device is compromised or "jailbroken" (iOS devices) or "rooted" (Android devices).

Social Login

Take the headache out of social login with NoPass™ social login support. We handle the connections and provide an easy way for your users to log in with a social account.



Branding

Easily brand, rebrand or modify the look of apps already installed on devices without updating or reinstalling the app.



Analytics

Measure the usage metrics on different user authentications and make adjustments to the app's User Interface (UI) as needed.



Logging & Reporting

Log various events, actions, and other device activity to allow admins to generate log reports through the NoPass™ Admin Console.

Geofencing

Program certain behaviors into an app based on a device's proximity to configured areas, such as warning messages, restricting user access, and wiping apps.



Certificate Provisioning

Provision the certificates directly to your app giving you control over what data your device users can access through certificate authentication.

Technical Information

- ⚙ Supported on Android and iOS
- ⚙ Symmetric and Public Key signature capability
- ⚙ Simple and easy QR code registration and Installation
- ⚙ Biometrics and PIN support

- ⚙ Dynamic Linking, WYSIWYS (What You See Is What You Sign)
- ⚙ Strong User and Transaction Authentication: Knowledge, Possession, Inherence
- ⚙ Innovative and secure OTP (picture/code)

Benefits of NoPass™

Security

Login credentials are unique across every website, never leave the user's device and are never stored on a server.

Convenience

Users unlock login credentials with simple built-in methods such as fingerprint readers or face scans.

Scalability

The wide use of smartphones and our cloud deployment make it super easy to scale any existing authentication.

Cost efficiency

Save millions in helpdesk and password support costs.

Privacy

Protect your users from credential leaks and password phishing.

Development Speed

Accelerate your custom deployments with our iOS and Android SDKs.