9. Native Applications

Native applications are clients installed and executed on the device used by the resource owner (i.e., desktop application, native mobile application). Native applications require special consideration related to security, platform capabilities, and overall end-user experience.

The authorization endpoint requires interaction between the client and the resource owner's user-agent. Native applications can invoke an external user-agent or embed a user-agent within the application. For example:

- **External user-agent** - the native application can capture the response from the authorization server using a redirection URI with a scheme registered with the operating system to invoke the client as the handler, manual copy-and-paste of the credentials, running a local web server, installing a user-agent extension, or by providing a redirection URI identifying a server-hosted resource under the client's control, which in turn makes the response available to the native application.
A lot of people went the embedded route...
The user user-friendly definition of Single Sign-on is you sign-on *once,* not that you sign-on multiple times with the same credentials.
Web View is insecure

I'm a sign, not a cop.

Keep out

Or enter.

I'm a sign, not a cop.
Even trusted developers create risk

In the News: [Apple Removes Over 250 iOS Apps With Ad SDK That Collects Personal User Data](https://www.apple.com/newsroom/2021/06/apple-removes-over-250-ios-apps-with-ad-sdk-that-collects-personal-user-data/)
Browser views allow for a secure browser context inside the native app.
Choose certificate

The app Chrome has requested a certificate. Choosing a certificate will let the app use this identity with servers now and in the future. The app has identified the requesting server as auth.startssl.com:443, but you should only give the app access to the certificate if you trust the app.

www.startssl
E=bilid1600@gmail.com,CN=bilid1600@gmail.com

You can install certificates from a PKCS#12 file with a .pfx or a .p12 extension located in external storage.

INSTALL

DENY  ALLOW

“auth.startssl.com” requires a client certificate

Select the certificate to use when you connect to this website.

bilid1600@gmail.com

Cancel

... with all the browser features like Mutual TLS
Other external user-agent techniques remain valid.
Progress since IETF93
Chrome for Android 45 released

iOS 9 released
iOS 9 & Android’s Chrome 45 Deployed Widely

92.6% of devices eligible for Chrome 45 (Android 4.1+)

61% of devices already on iOS 9

Source: Google

Source: Apple
ios 9 adoption

Source: mixpanel.com
100% of users supported through browser fallback.
PKCE is now RFC7636
Proof of concept samples available. You can implement this best practice today!

https://github.com/WilliamDenniss/native-apps-ios-concept

https://github.com/WilliamDenniss/native-apps-android-concept
The Google Sign-in library on iOS implements this best practice today.

https://developers.google.com/identity/sign-in/ios/
Production-ready OSS OAuth SDKs coming soon!

Release announcement will be sent to oauth@ietf.org.
OAuth 2.0 for Native Apps

A draft best practice on how to correctly perform web-based OAuth flows for native apps.