# OAuth 2.0 for Native Apps

William Denniss
Google Identity Platform

IETF94 – Yokohama

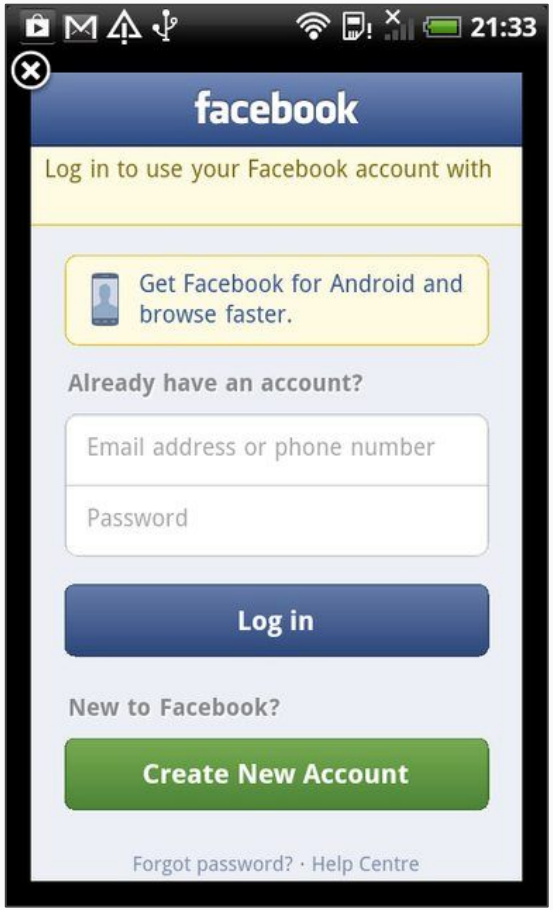
# RFC6749 isn’t opinionated enough

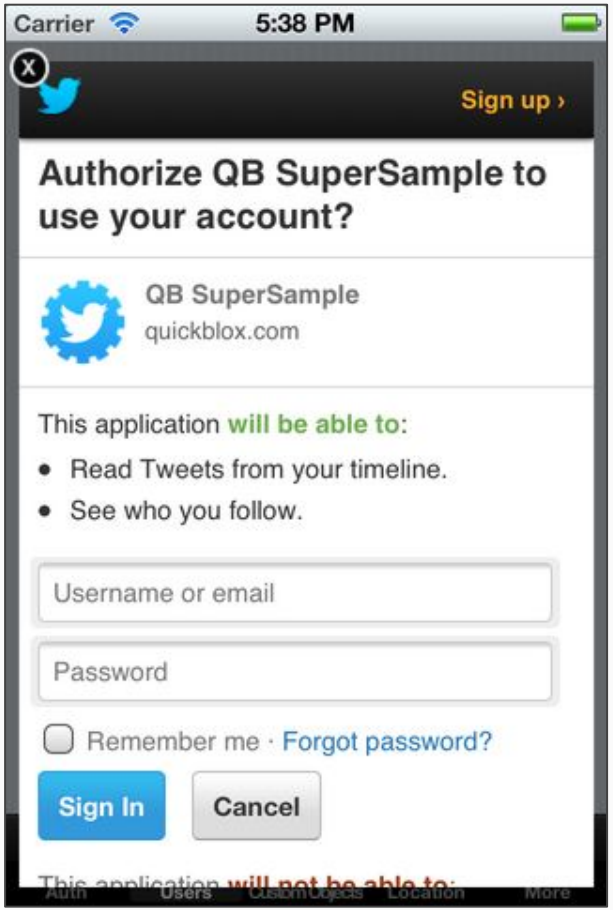
## 9. Native Applications

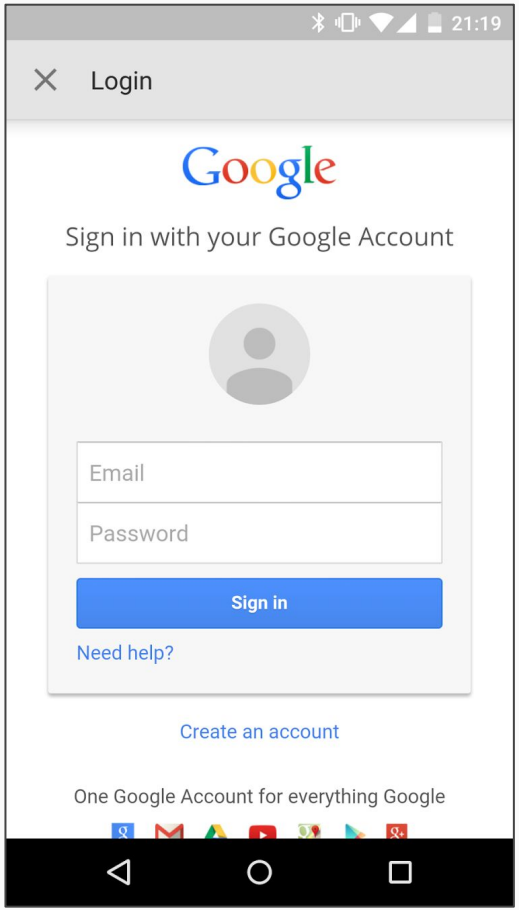
Native applications are clients installed and executed on the device used by the resource owner (i.e., desktop application, native mobile application). Native applications require special consideration related to security, platform capabilities, and overall end-user experience.

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.



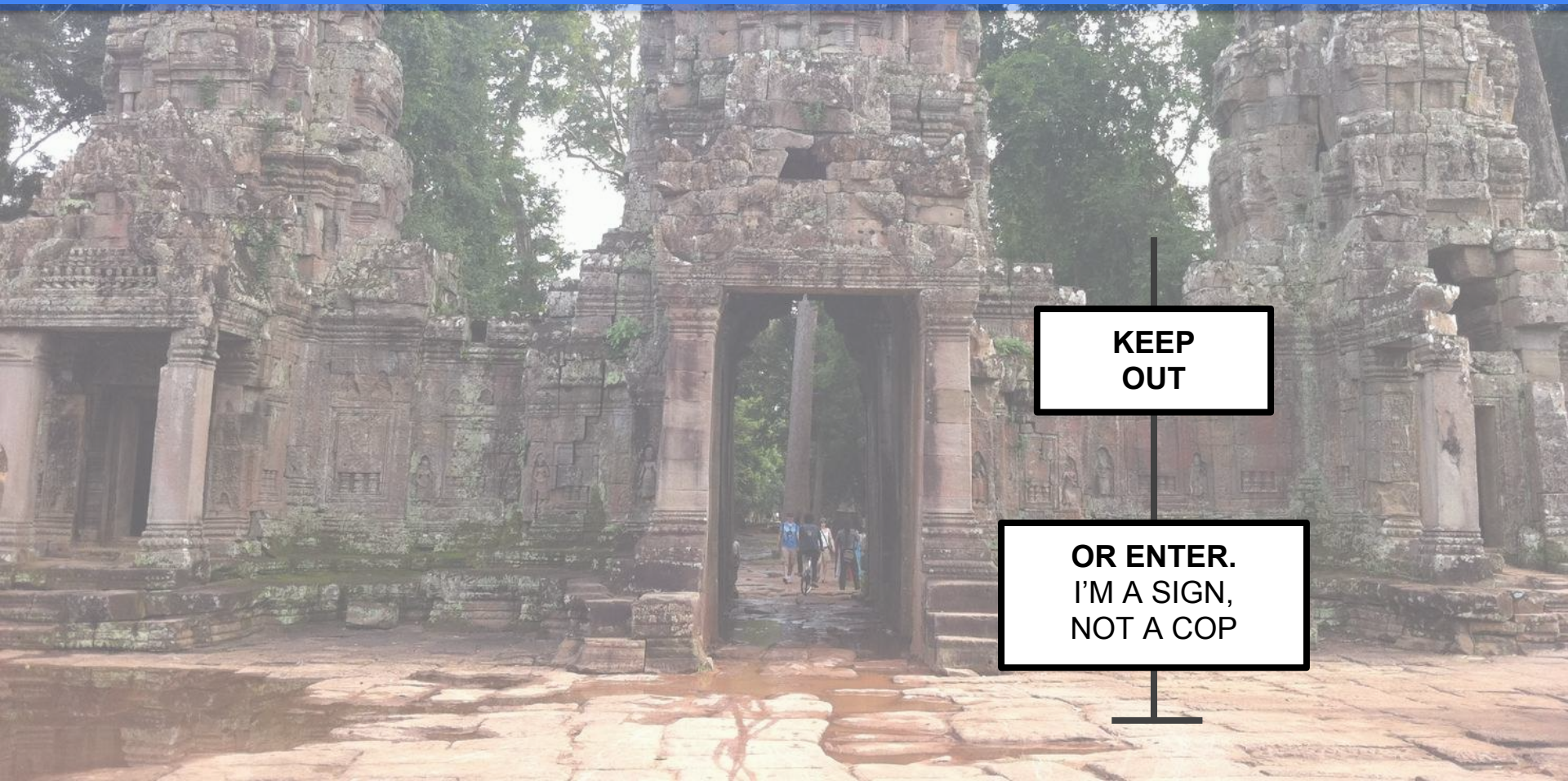

A lot of people went the embedded route…

# WebView does not achieve SSO

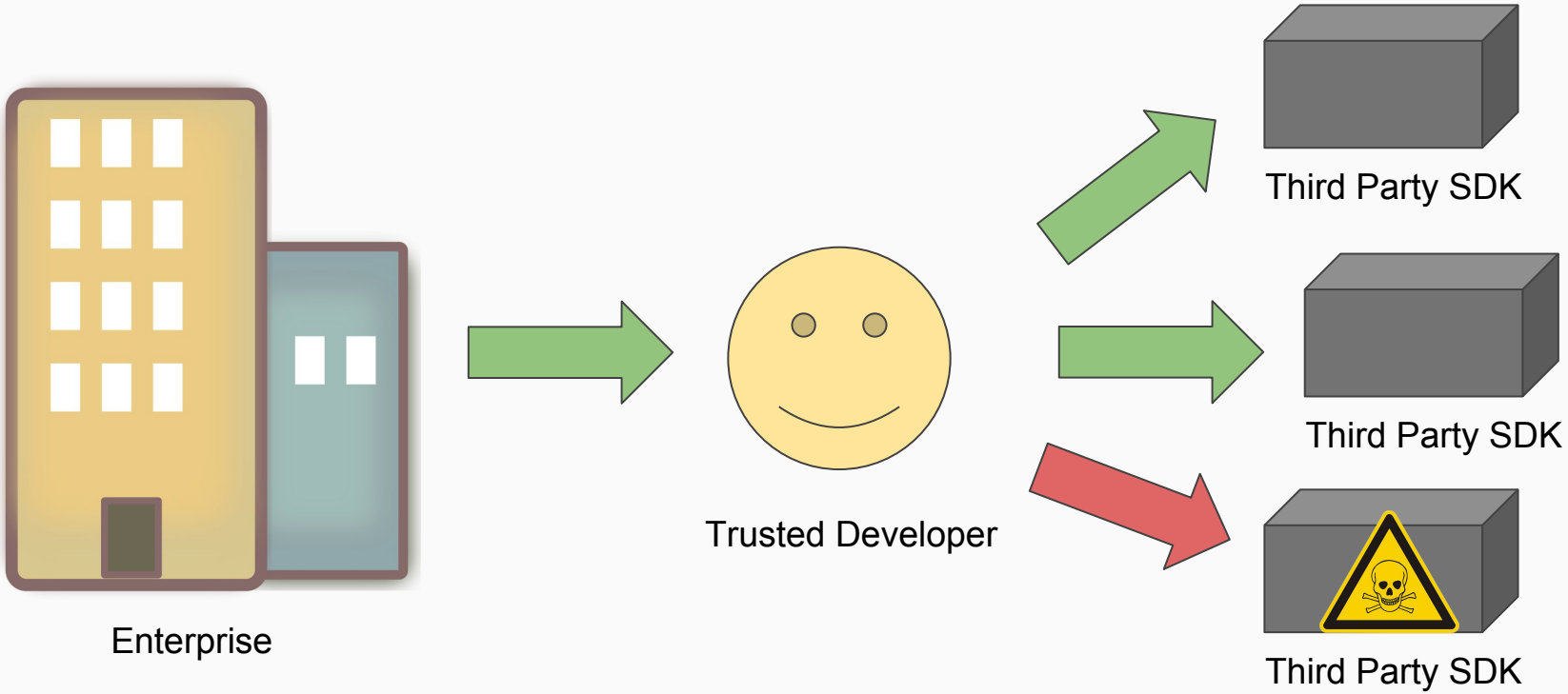
The user user-friendly definition of Single Sign-on is you sign-on ***once*.**

***not*** that you sign-on multiple times with the same credentials

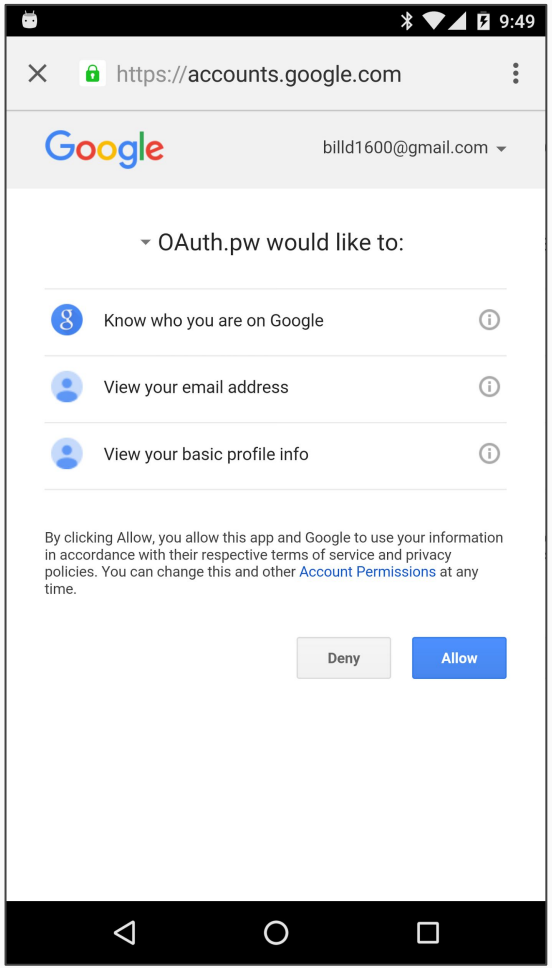
# Web View is insecure

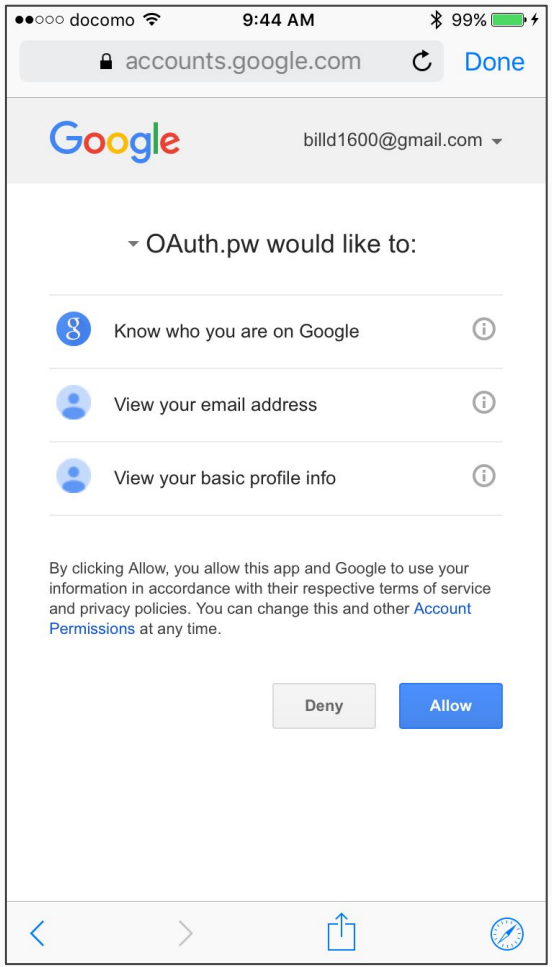


# Even trusted developers create risk

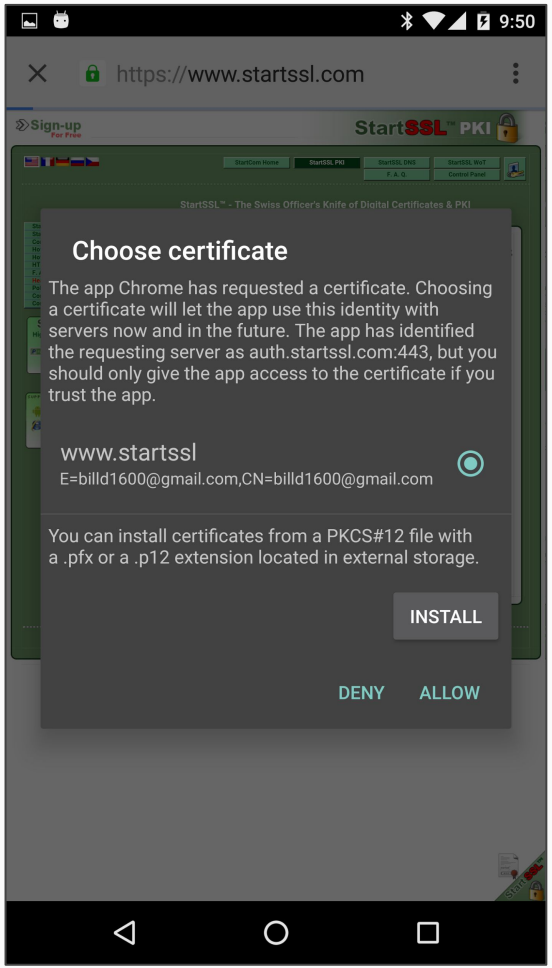


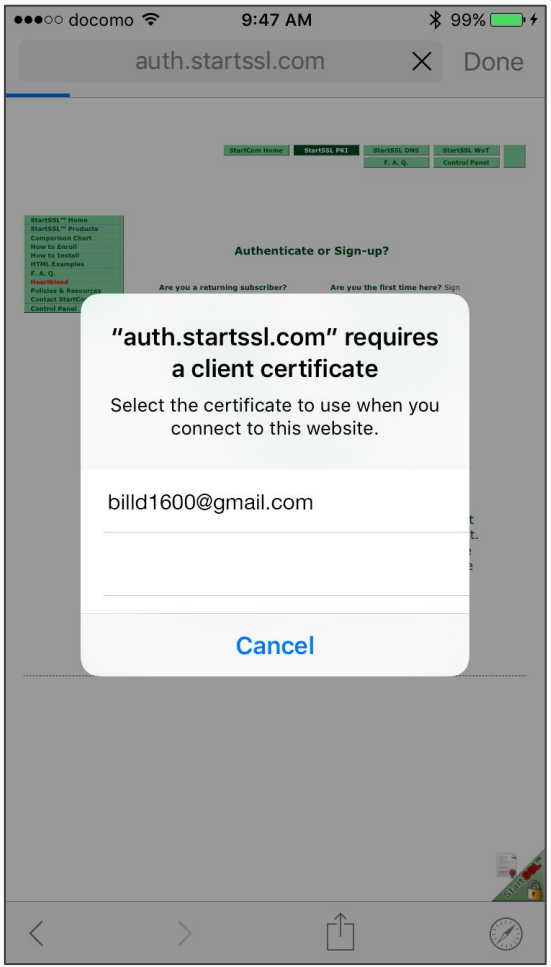

In the News: [Apple Removes Over 250 iOS Apps With Ad SDK That Collects Personal User Data]




*Browser views allow for a secure browser context inside the native app*




*… with all the browser features like Mutual TLS*

# What we are not doing

Other external user-agent techniques remain valid.

# Progress since IETF93

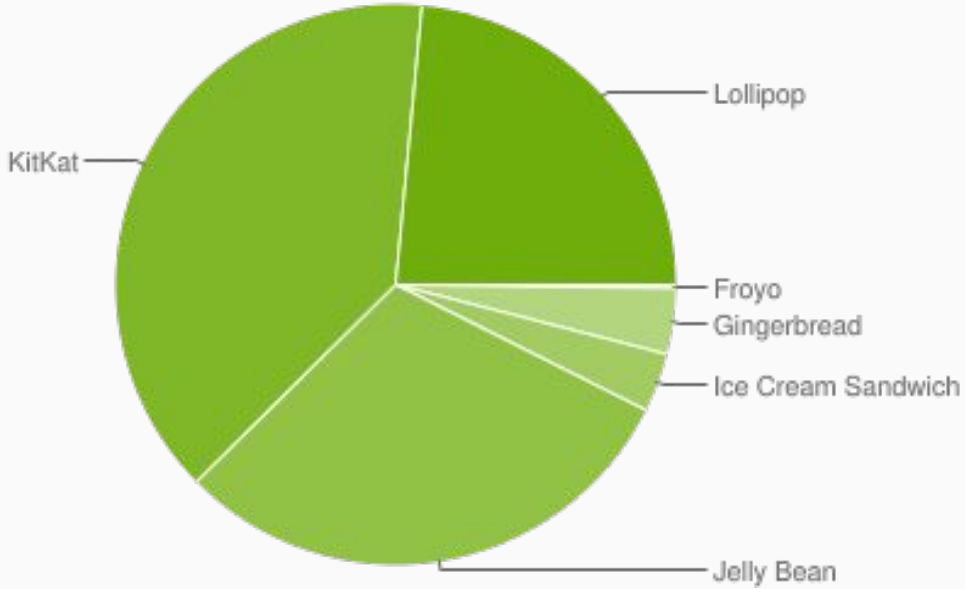
# Shipped dependencies

Chrome for Android 45 released

iOS 9 released

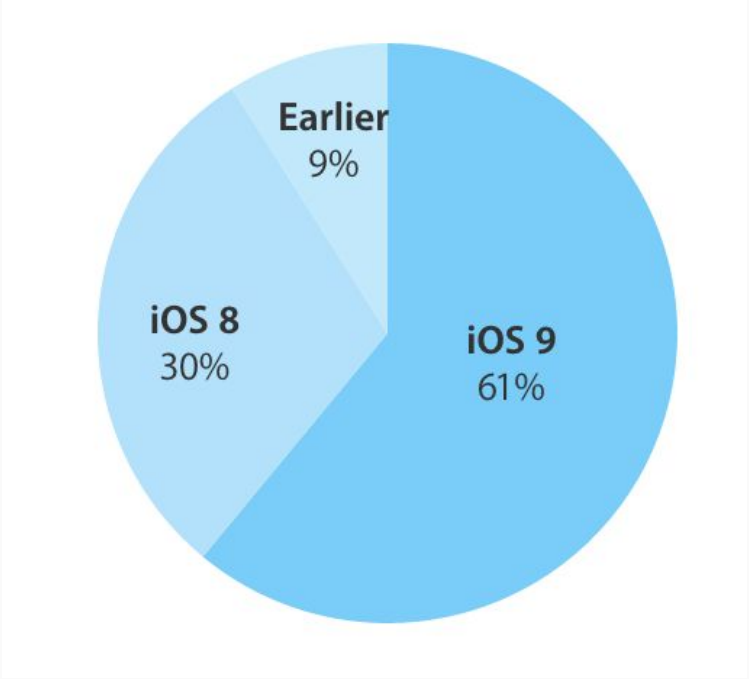
# iOS 9 & Android’s Chrome 45 Deployed Widely

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



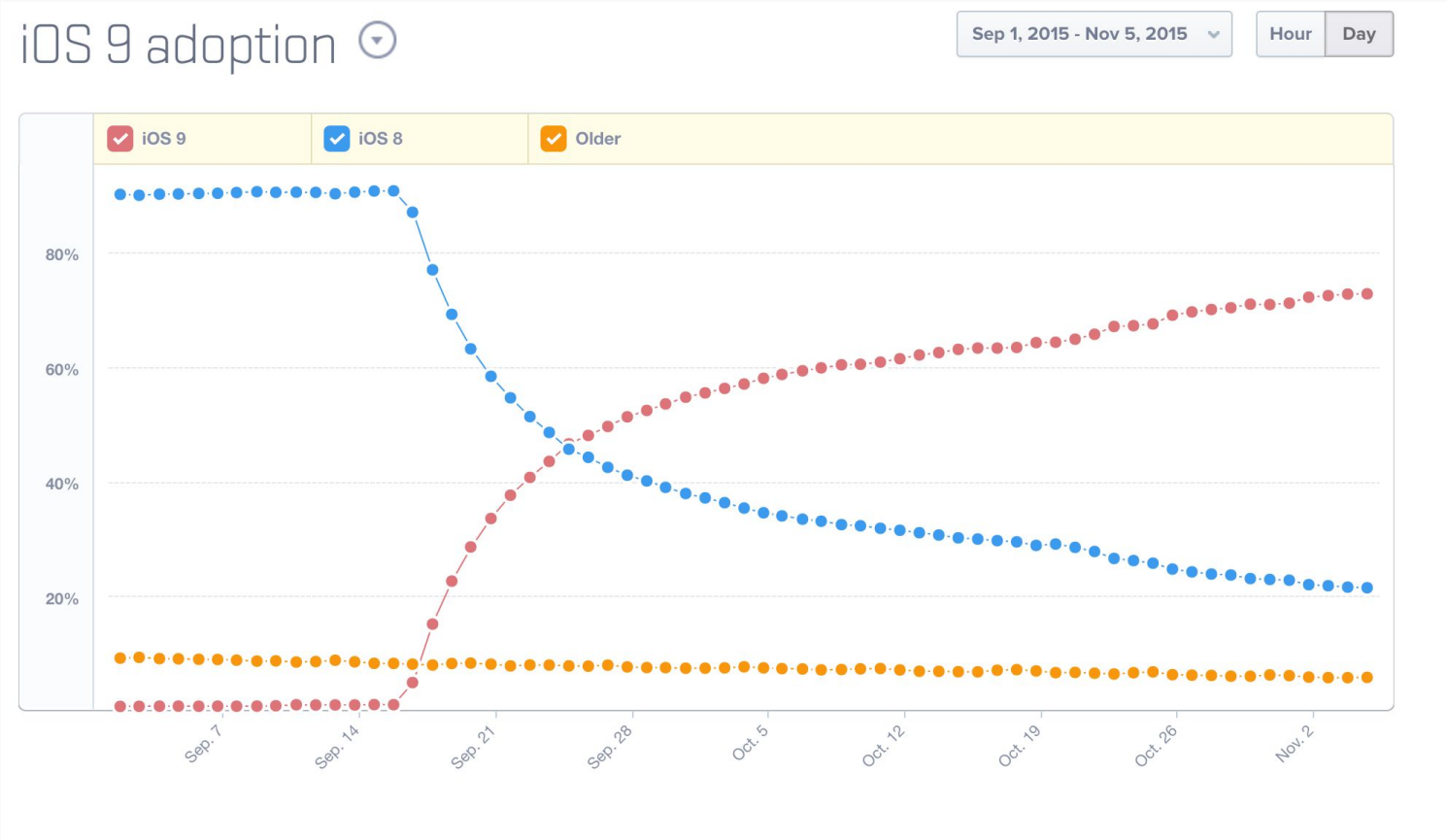

Source: Google

61% of devices already on iOS 9




Source: Apple

# iOS 9 Adoption




Source: mixpanel.com

# No user left behind

100% of users supported through browser fallback.

# PKCE is now RFC7636

# Proof of Concept code

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

# Production Examples

The Google Sign-in library on iOS implements this best practice today.

https://developers.google.com/identity/sign-in/ios/

# Coming Soon

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.

https://tools.ietf.org/html/draft-wdenniss-oauth-native-apps