OAuth 2.0 for Native Apps

William Denniss, John Bradley

History

First draft of OAuth 2.0 from early 2010 did not even *mention* Native Apps.

Not a huge surprise, the Apple app store had launched 1.5 years prior, and the “mobile first” phenomenon was in its infancy.

Final spec includes a mention of Native Apps, documents two possible options for auth flows: embedded (webview) & native (system browser) user-agents.

SSO

Single sign-on means You Only Login Once.

... not that you only login with the same password everywhere.

Kindly discard that login scope token on your way out

Today, embedded user-agents give the full account access token and scoped OAuth token to the third-party app.

Asking them to please discard the former does not equate to security.

In Summary

Embedded user-agents are BAD

External user-agents are GOOD

The OAuth WG should be opinionated on this.

For your consideration

This proposed best practice explains why external agents are the correct method for authorization flows, and how to use them.

https://tools.ietf.org/html/draft-wdenniss-oauth-native-apps-00