Let's talk mobile.

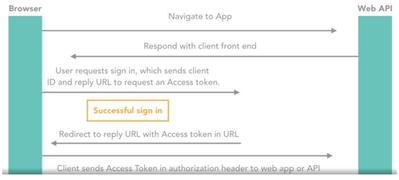
Implicit or Hybrid Grant Type

Designed specifically for untrusted or "public" clients, where a malicious user could get access to the source code

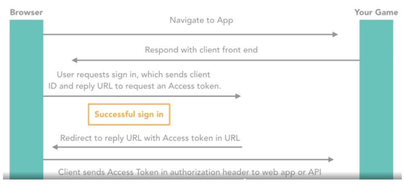
In other words, we can't count on it to keep our client_secret safe.

This is only for users who explicitly grant authorization via an authentication and user-consent flow.

Authorize Endpoint



Facebook Authorize Endpoint



Implementing It

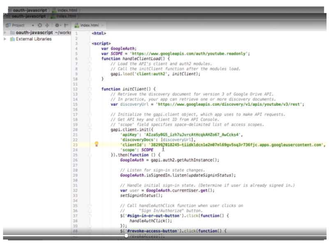
- For Android or iOS/Swift

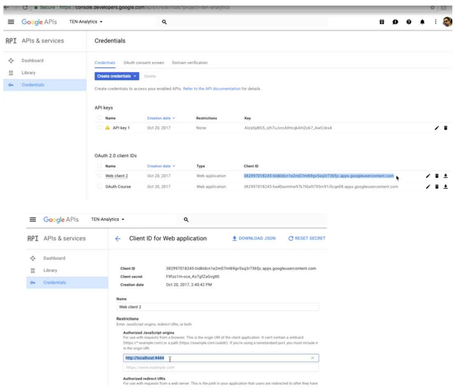
  Use AppAuth, formally backed by OpenID Foundation, etc.

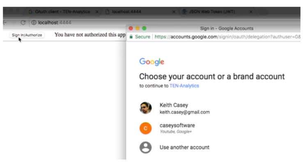
  Respects the OAuth flows, cookie/session storage, etc.

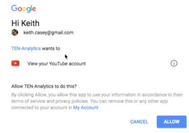
- For single-page apps

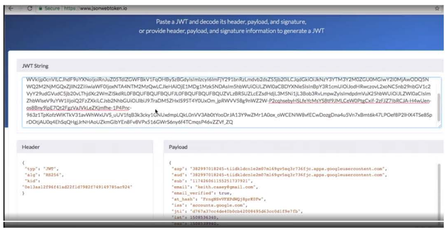
  Use Passport for a modular/pluggable approach to authentication and authorization, regardless of your provider.

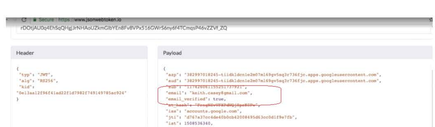












Hybrid or Implicit Flow Security Considerations

AppAuth and Passport

Evaluate these first. Don't create your own.

Security Considerations

- Remember what an Access Token is

  It's permission to act as the user.

  We have to store and use it securely at all times.

- Must use secure communications

Security Considerations

- Test your redirect_uri whitelist

  This is where the server sends the resulting access token.

  Confirm that your server doesn't accept any arbitrary redirect_uri.

  Probably fine with a mainstream server, but check anyway.

- All resource servers must validate the access tokens

  You don't have to love it, but you have to do it.