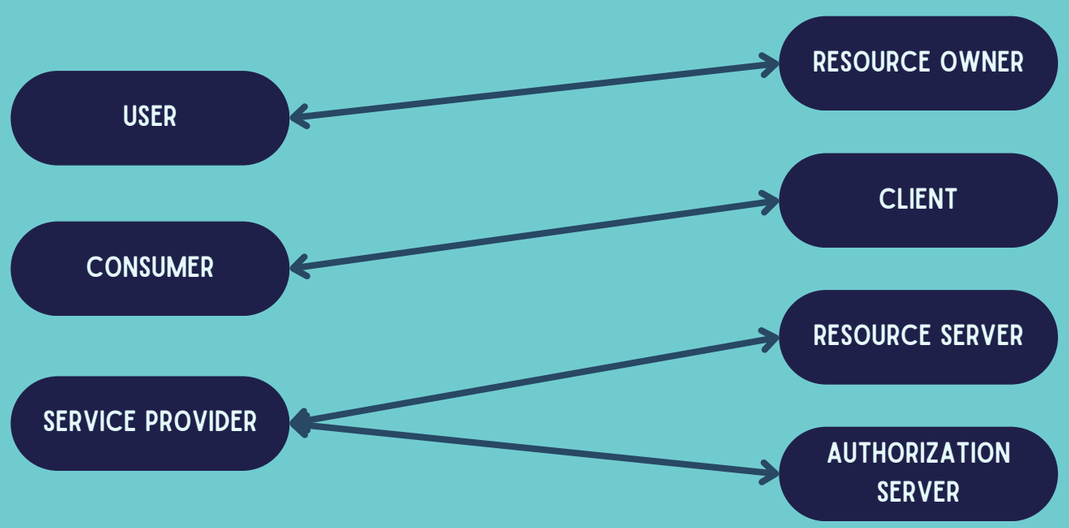
Where did it come from?
Where did it go?
What the heck is an OAuth Flow?

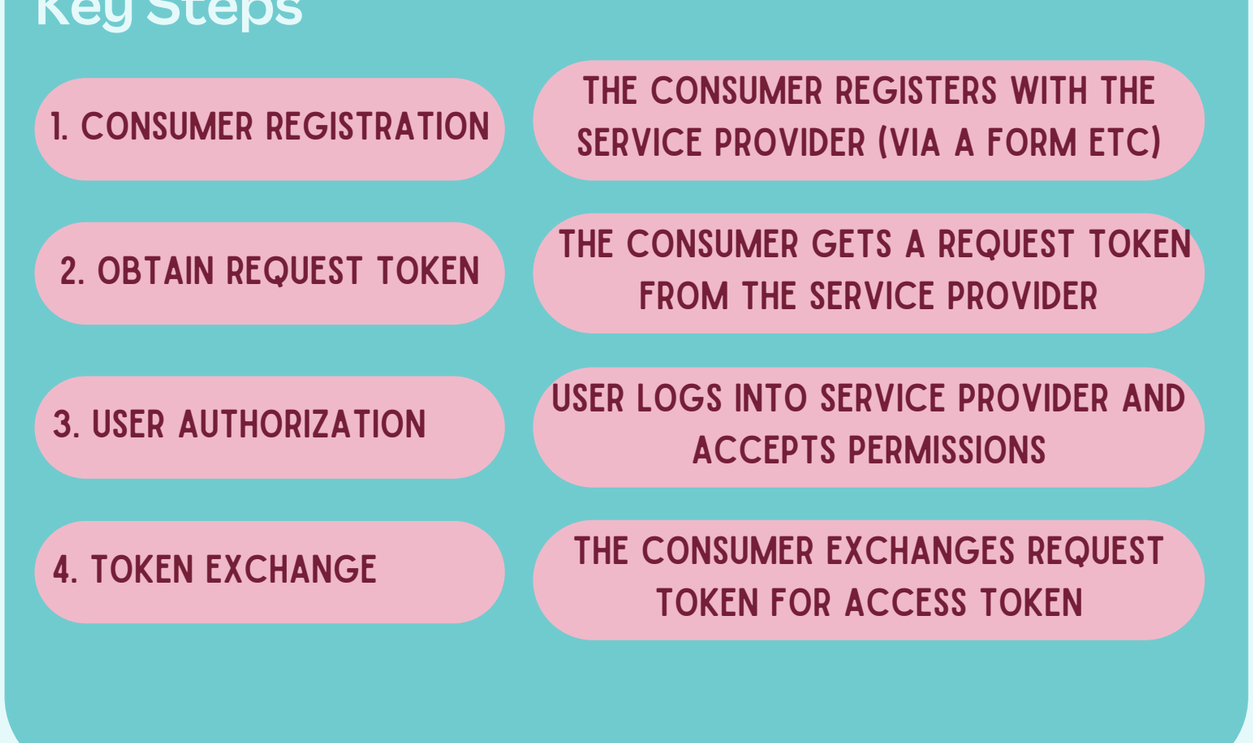
Terminology

OAUTH 1.0	OAUTH 2.0	MEANING
USER	RESOURCE OWNER	WANTS TO GIVE PERMISSION FOR AN APP TO ACCESS RESOURCES IN ANOTHER APP
CONSUMER	CLIENT	AN APP REQUESTING ACCESS TO STUFF ON A USERS BEHALF
SERVICE PROVIDER	AUTHORIZATION SERVER	HANDLES GETTING PERMISSION FROM THE USER TO GIVE AN APP PERMISSION
ALSO THE SERVICE PROVIDER	RESOURCE SERVER	IN OAUTH 2.0 CAN HOLD USER RESOURCES WITHOUT GRANTING ACCESS TO IT

OAuth 1.0 ⇄ OAuth 2.0



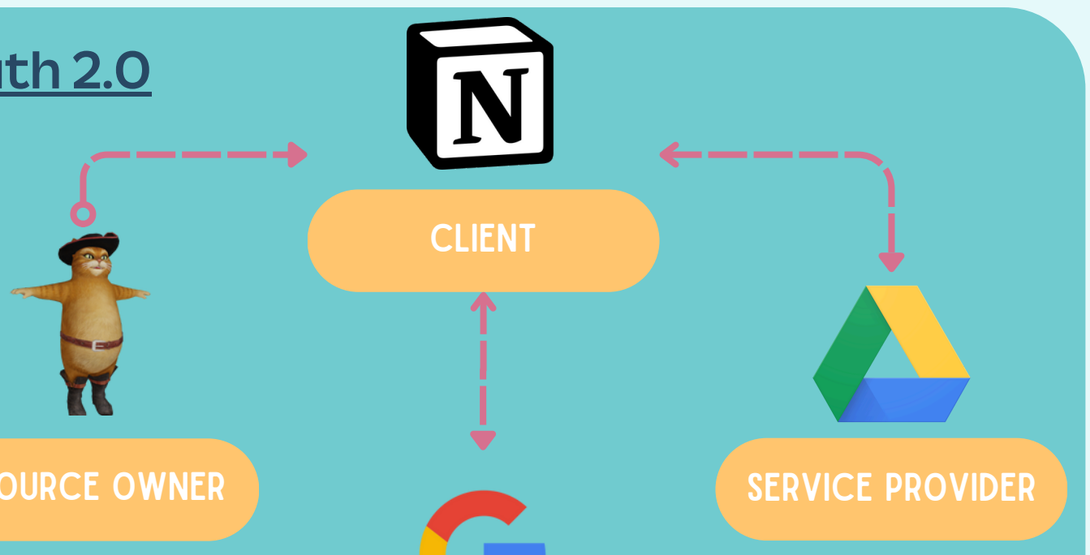
OAuth 1.0



Key Steps

1. CONSUMER REGISTRATION	THE CONSUMER REGISTERS WITH THE SERVICE PROVIDER (VIA A FORM ETC)
2. OBTAIN REQUEST TOKEN	THE CONSUMER GETS A REQUEST TOKEN FROM THE SERVICE PROVIDER
3. USER AUTHORIZATION	USER LOGS INTO SERVICE PROVIDER AND ACCEPTS PERMISSIONS
4. TOKEN EXCHANGE	THE CONSUMER EXCHANGES REQUEST TOKEN FOR ACCESS TOKEN

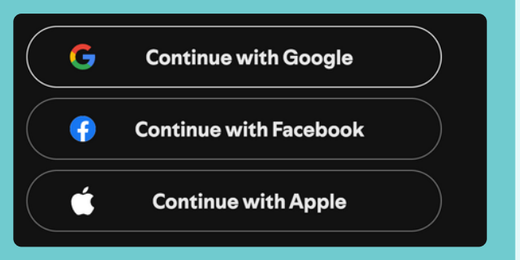
OAuth 2.0



Key Steps

1. CLIENT REGISTRATION	CLIENT REGISTERS WITH SERVICE PROVIDER
2. USER AUTHORIZATION	THE CONSUMER GETS A REQUEST TOKEN FROM THE SERVICE PROVIDER
3. VALIDATE YA STATE	RESOURCE OWNER IS REDIRECTED BACK TO CLIENT AND STATE IS VALIDATED
4. TOKEN EXCHANGE	THE CLIENT EXCHANGES REQUEST TOKEN FOR ACCESS TOKEN

Open ID Connect (OIDC)



Resources (We Used and You can too)

What	What it's about
The OAuth 2.0 Playground	Lets you try the various OAuth flows step by step interactively!!!
OAuth 2.0 Core (RFC 6749)	The og OAuth2 RFC doc
Threat Model and Security Considerations (RFC 6819)	A great place to start for thinking about oauth2 security
OAuth 2.0 for Native Apps (RFC 8252)	Doc for native apps oauth2 (mobile and co)
OpenID Connect	Website/docs for OIDC and how it works
OAuth 1.0	The very first oauth spec!! (OAuth 1.0)
OAuth 1.0 Security Advisory	The OAuth1.0 session fixation attack
OAuth 1.0a	The final revision of OAuth1 (evolving from the session fixation attack above)
Differences in OAuth1 and 2	Quick summary of OAuth1 and 2 key differences
OAuth2.0 and the Road to Hell	A scathing review of OAuth2.0 from its prior chief editor and key contributor to OAuth1 (read if you want to know about oauth drama).