

0AUTH

OAuth2 — Use case

- * I just released YAWN (Yet Another aWful social Network)
- * It's great but, for some reason, people do not create contents
- * So I want them to import them from that crappy Facebook
- * How can I get YAWN to access data from FB?

Pre-requisites

- * YAWN should register with the Facebook (name, website, callback URL)
- * YAWN is provided with Client ID and Client Secret.
 - * The ID is public and is the name of YAWN for the FB
 - * The secret is only known to YAWN and FB and is used by the FB to identify YAWN

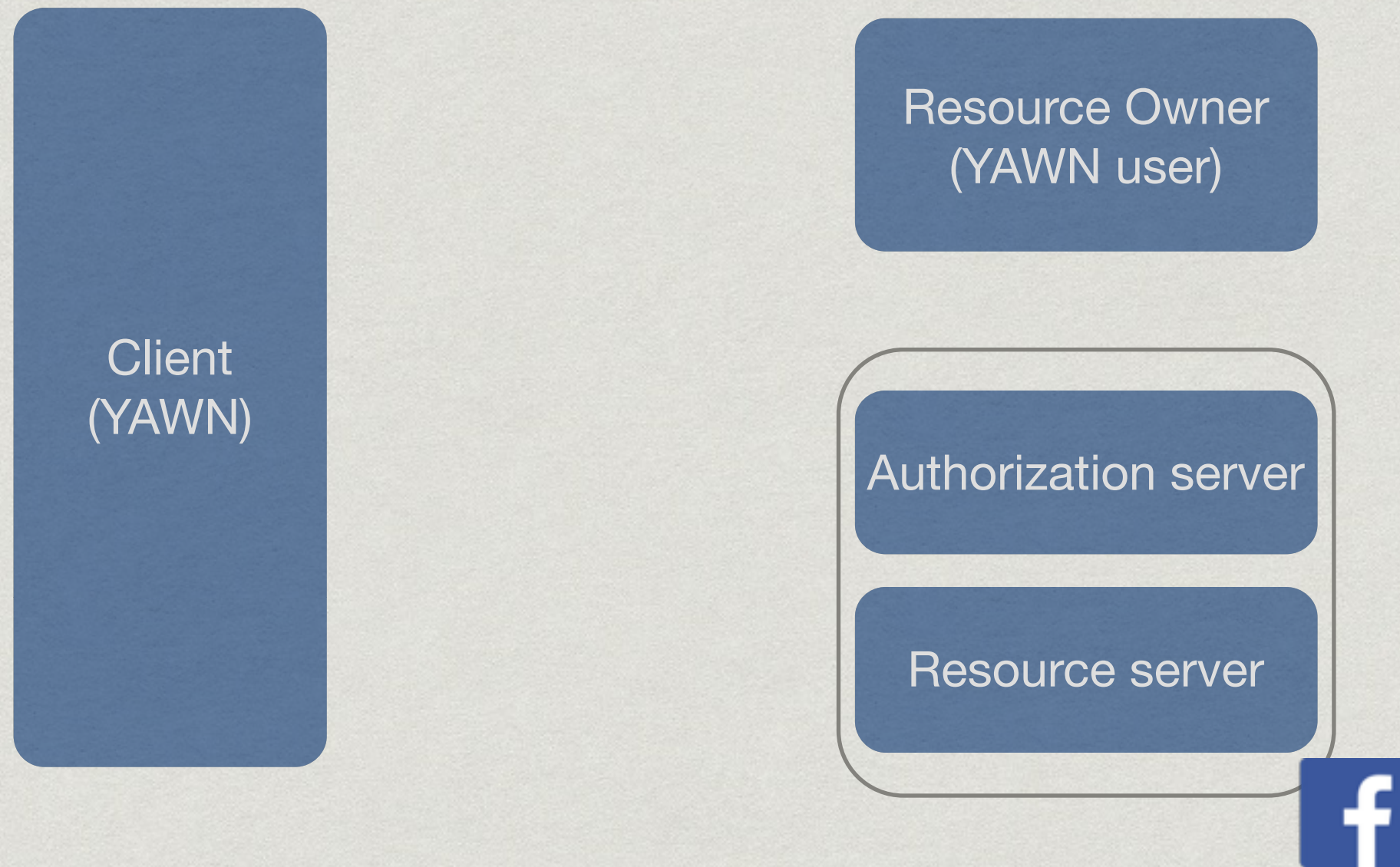
OAuth2 — Players

Client
(YAWN)

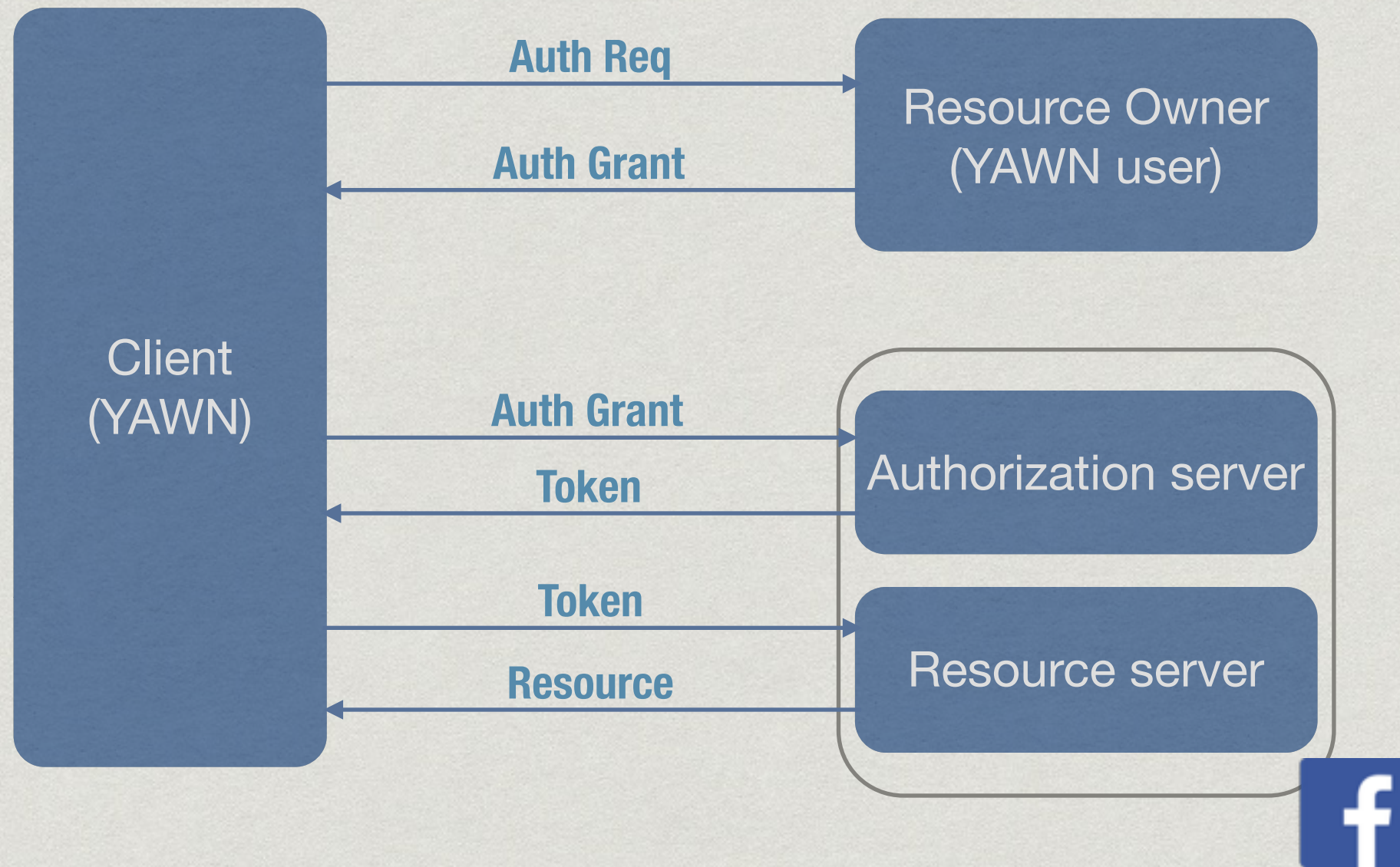
Resource Owner
(YAWN user)



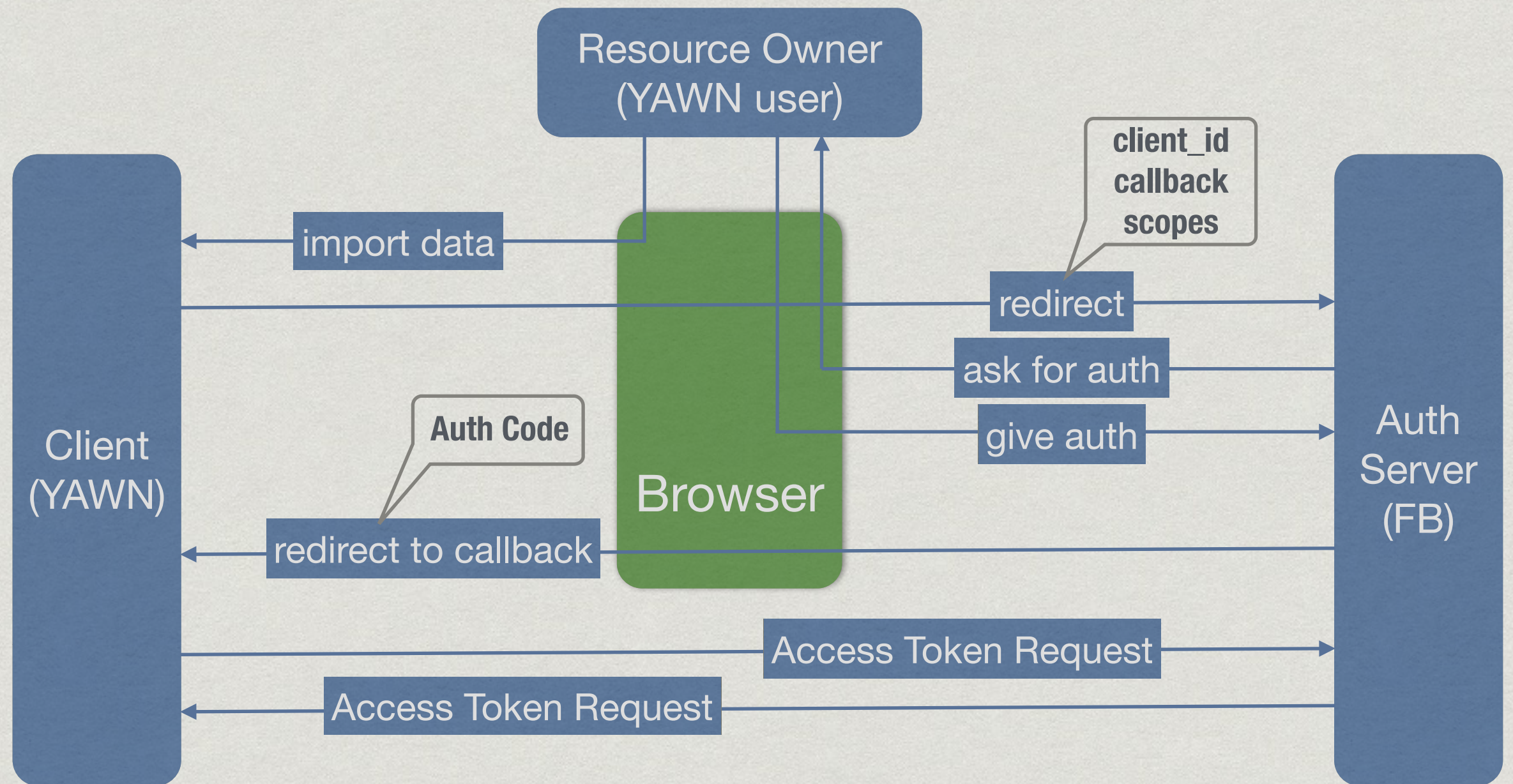
OAuth2 — Players



OAuth2 — Protocol



Grant Type: Authorization Code



Other grant types:

- * Implicit: the resource owner is provided by the Authorization server with the token and can share it with the client
- * Resource Owner Password Credentials: the resource owner provides its credentials to the client

Drawbacks

- * OAuth has been very successful
- * Thus all major players wanted to take part to the definition of OAuth2...
- * ... and spoiled it!

Bibliography

- * OAuth2 and the road to hell
- * OAuth2 spec