OAuth 2.0

By Lars Debbrecht

Table of Contents

What is OAuth 2.0?

- OAuth 2.0 is the industry-standard protocol for authorization
- Gain limited access to services on behalf of the User
- Supersedes OAuth 1: simplification and more user friendly

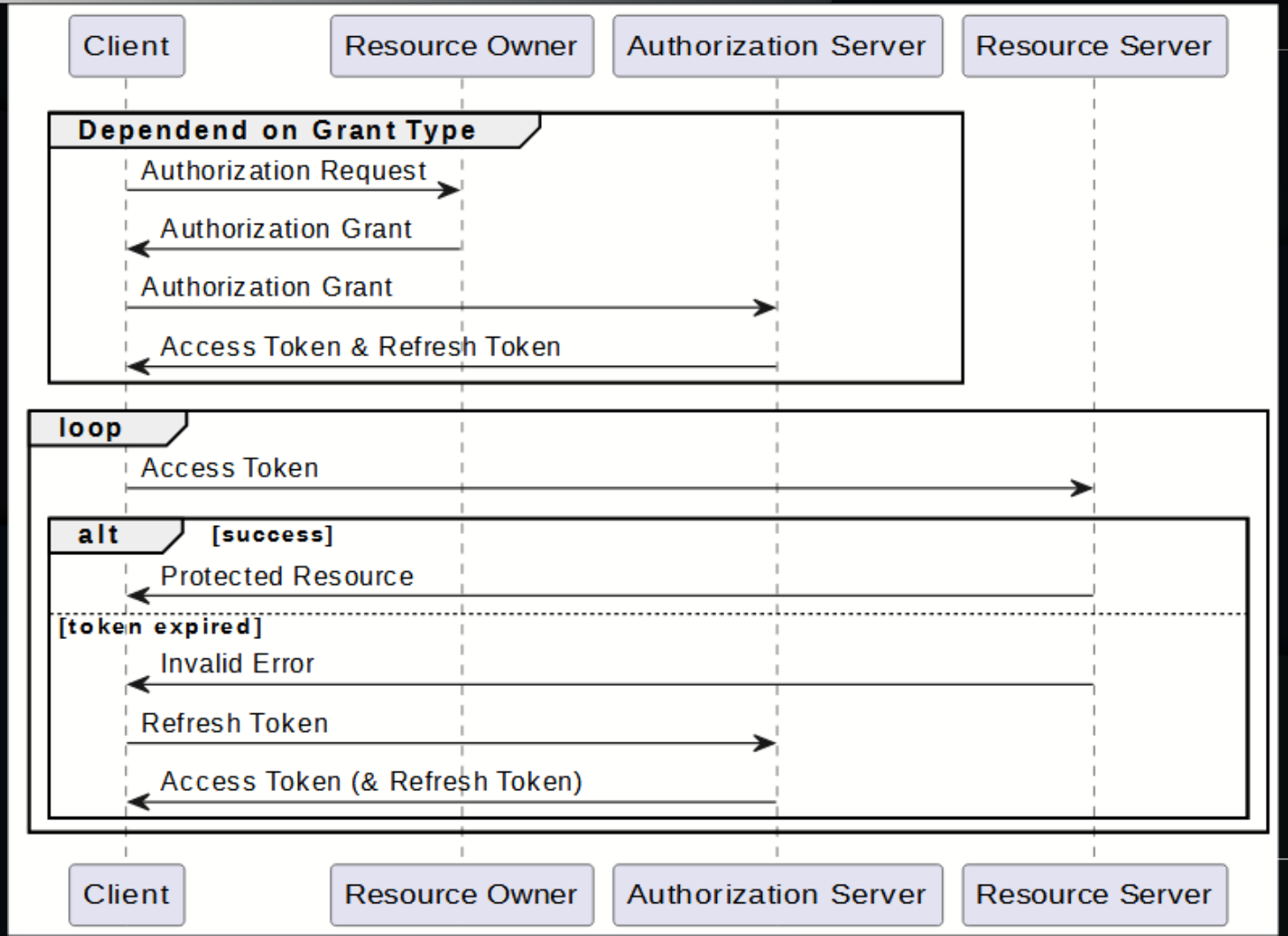
Where can you encounter OAuth 2

- Paypal payments
- Google registration
- Banking

Actors in OAuth 2

- Client
  - Public or Private
- Resource Owner / User
- Authorization Server / OAuth Provider
- Resource Provider / Server

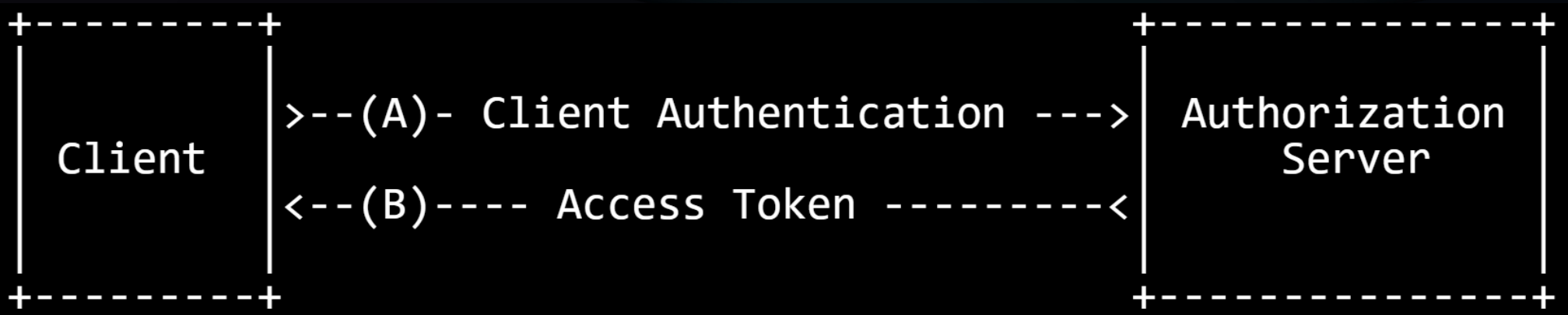
Overall Flow



Grant Types

- Client Credentials Grant
- Resource Owner Password Credentials Grant
- Implicit Grant
- Authorization Code Grant

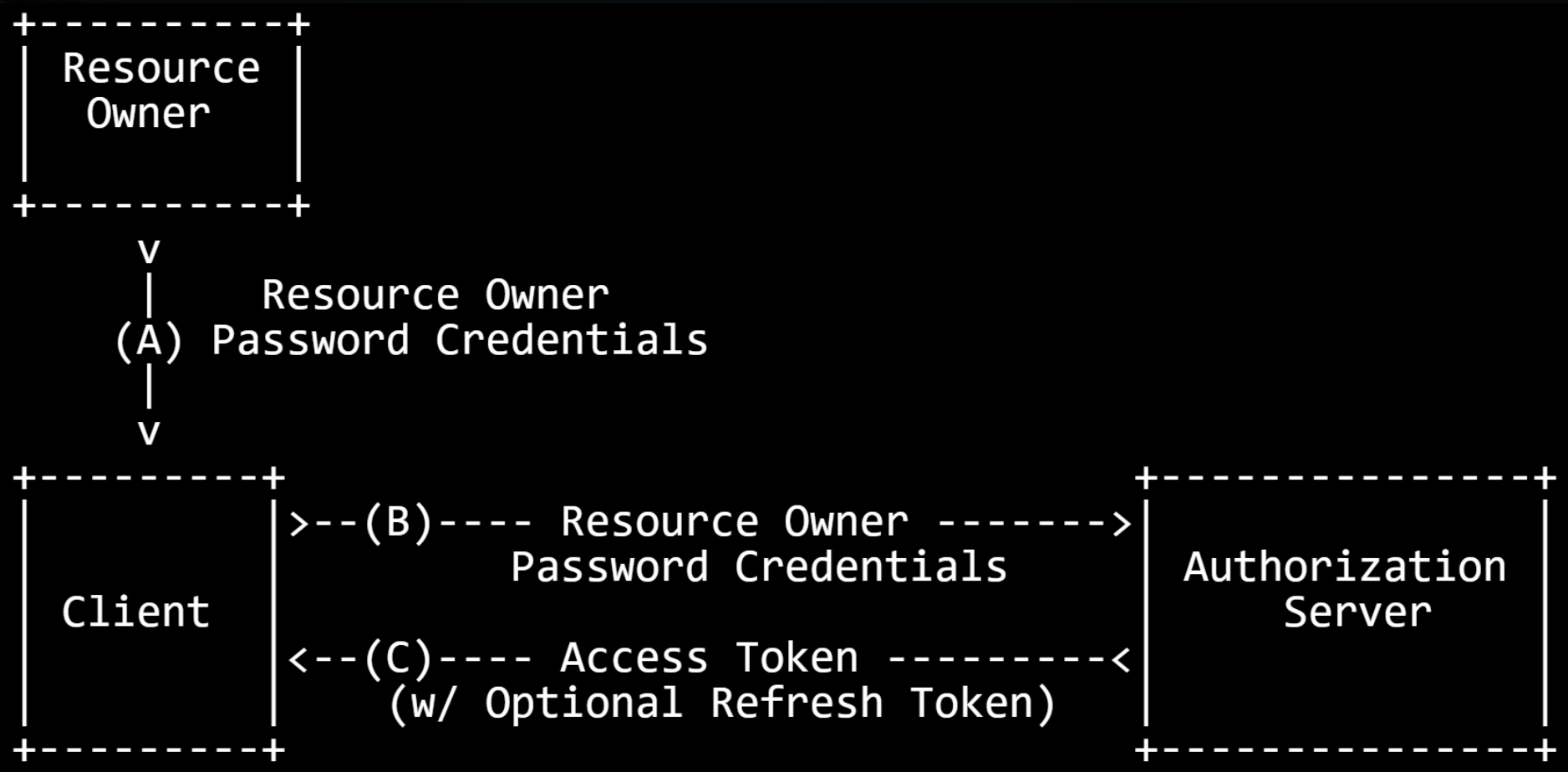
Client Credentials Grant



Client Credentials Grant

- Get access to resources under the Clients control
- Only with private Clients
- No Refresh Tokens

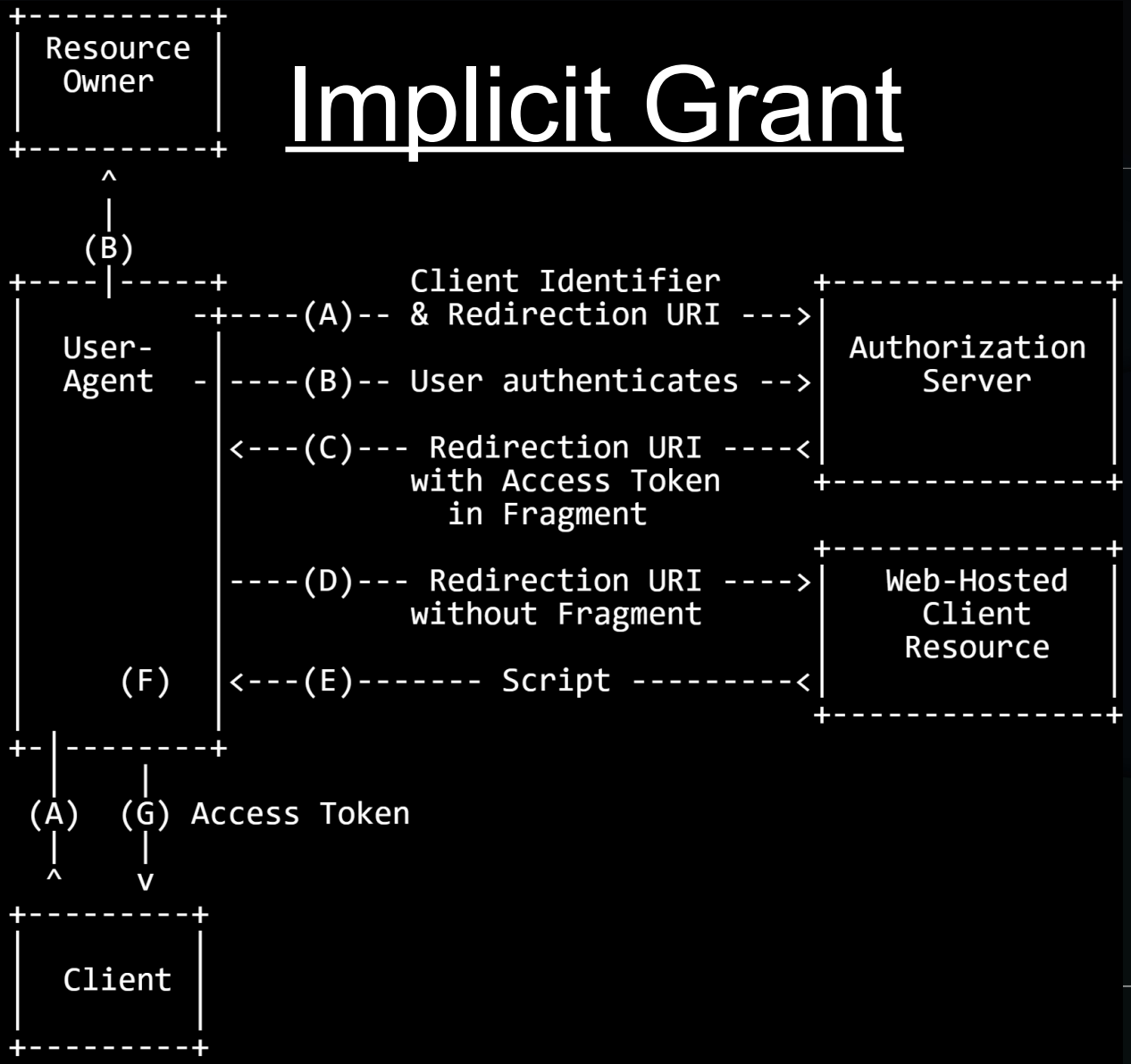
Resource Owner Password Credentials Grant



Resource Owner Password Credentials Grant

- Resource Owner has to trust the Client
- Only use this if other grant types are not viable
- Can be used when migrating to OAuth2 from different authorization methods

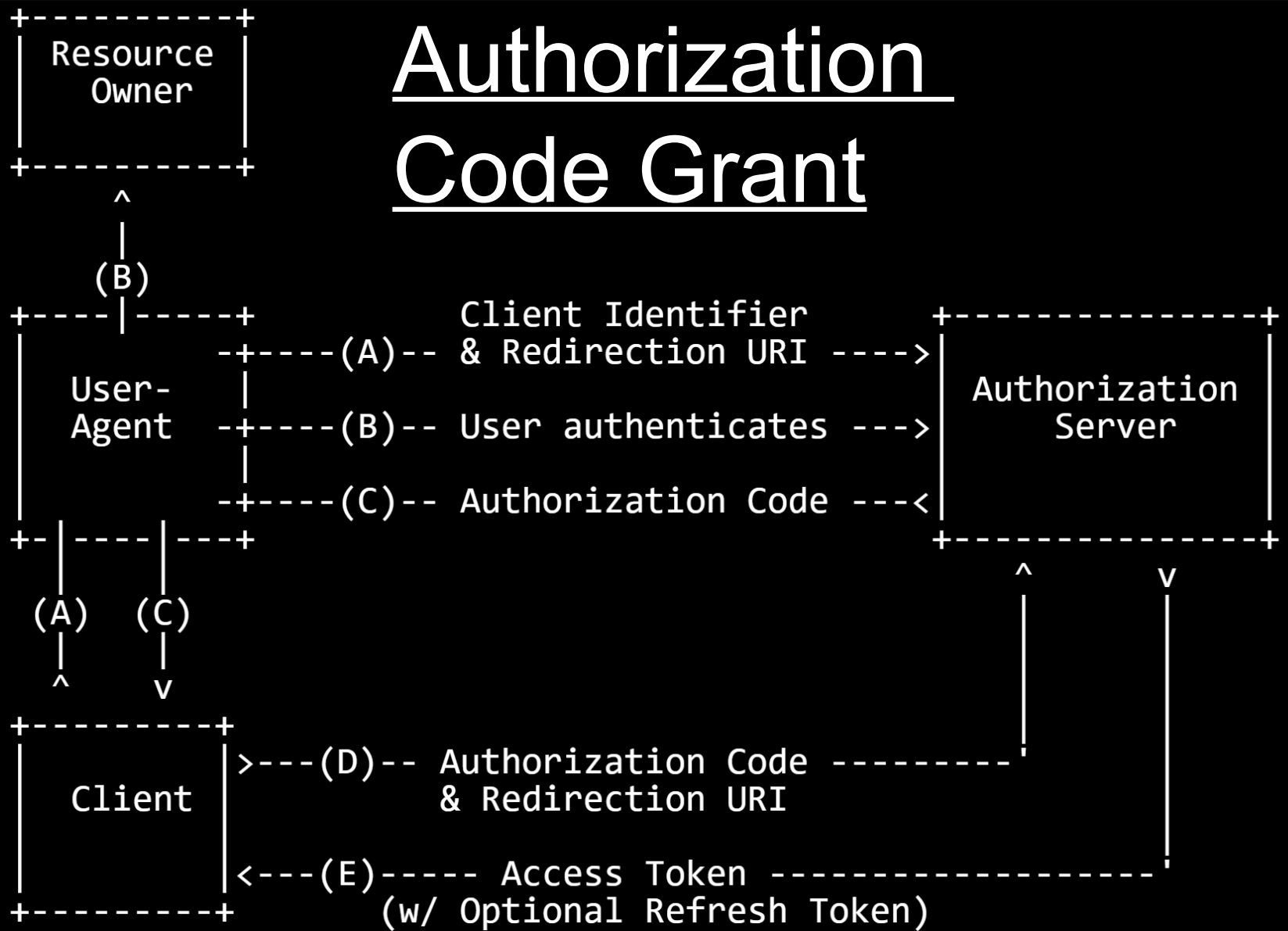
Implicit Grant



Implicit Grant

- Optimised for public Clients
- Clients needs to be able to execute scripts (e.g. Browser)
- Access token exposed to Resource Owner and maybe other application on device
- No guarantee that correct client recieves Access token

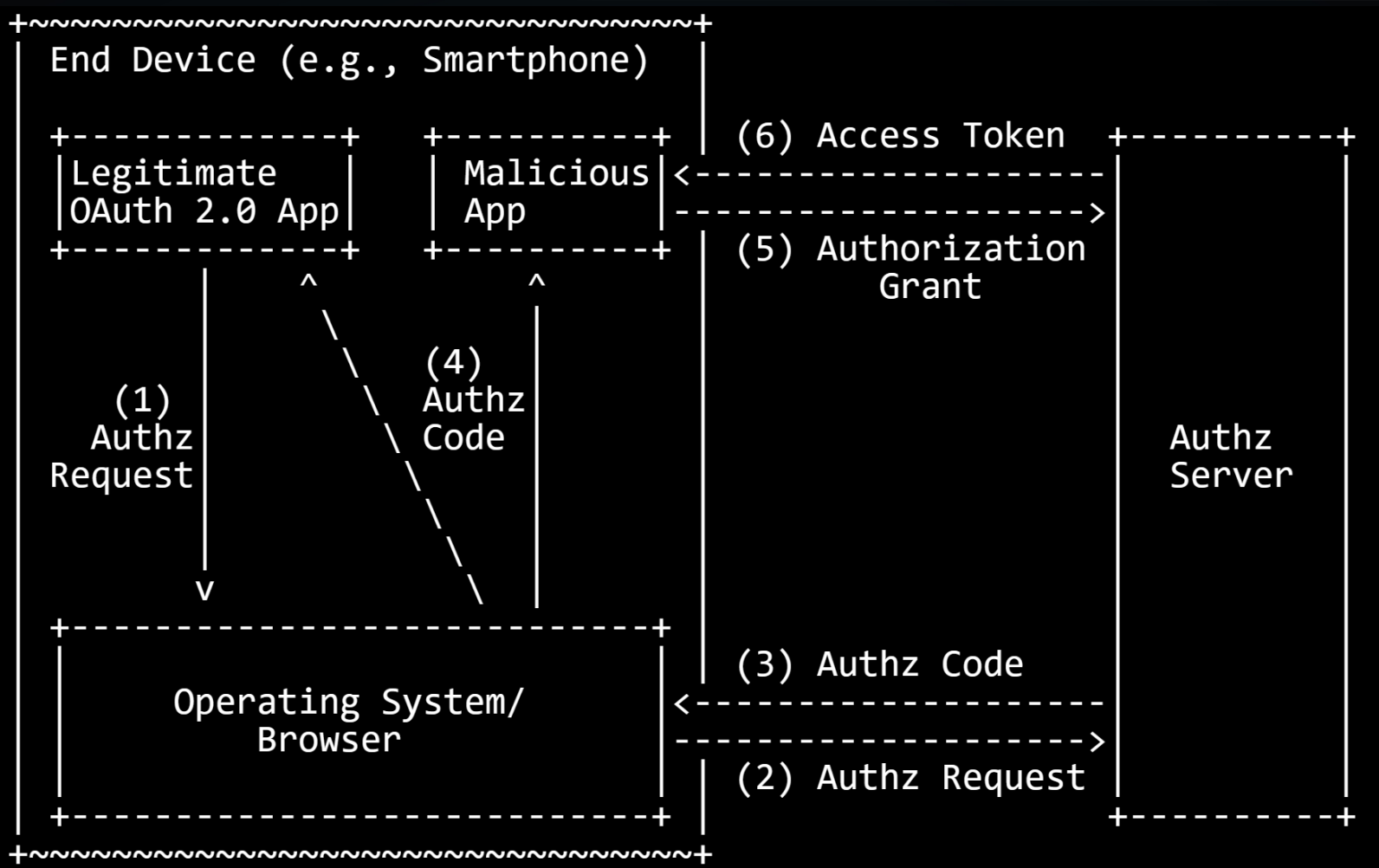
Authorization Code Grant



Authorization Code Grant

- Both Access as well as Refresh Tokens
- Optimised for confidential Clients
- Most common Code Grant
- Access Token never exposed to Resource Owner, only Client
- Vulnerable to authorization code interception attack

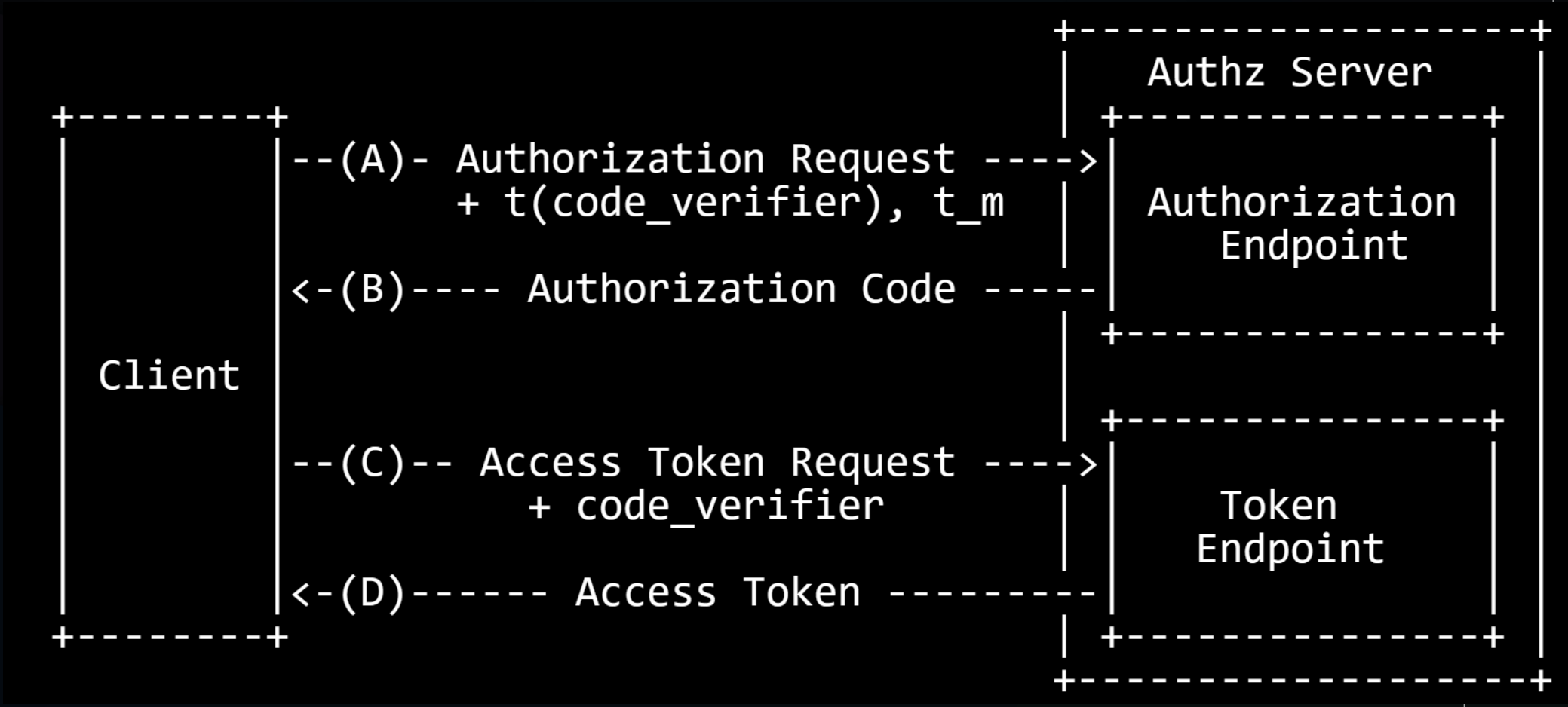
Authorization Code Interception Attack



PKCE – Proof Key for Code Exchange

- Prevents authorization code interception attack
- Only useable with Authorization Code Grant
- Additional verification of Client when exchanging Authorization code with Access Token

PKCE Proof Key for Code Exchange



Demo: Access to Users Google Drive Files using Google API and NodeJS

Questions?

Source

- oauth.net/2
- RFC 6749 (datatracker.ietf.org/doc/html/rfc6749)
- RFC 7636 (datatracker.ietf.org/doc/html/rfc7636)

Thank you for listening