20 - Ověřování identity v prostřední internetu

- při ověřování uživatele je nutná šifrovaná HTTPS komunikace

Jméno a heslo

- nejjednodušší a nejpoužívanější způsob ověřování
- heslo by mělo splňovat určité bezpečnostní požadavky
  - velká písmena, číslice, speciální znaky
- zadává se přímo do aplikace
- hesla by měla být uložená v hashi, nikoliv v šifře
  - hash nelze rozluštit zpětně
  - MD5, SHA-1, SHA-2

Dvoufázové ověření

- kromě zadání jména a hesla musí ještě uživatel ověřit aplikaci z jiného zařízení
  - typicky z mobilního telefonu
- SMS zpráva / autentifikátor v mobilní aplikaci
- útočník se případně musí zmocnit navíc uživatelova telefonu
- bezpečnější než pouze jméno a heslo

Biometrické ověření

- měří jedinečné biologické charakteristiky
- nejčastěji otisk prstu nebo obraz obličeje
- velmi těžko se falšuje
- bývá kombinován s klasickou metodou zadání hesla v případě nefunkčnosti (špinavé prsty, rouška)

Access token

- náhodně generovaný kód
- slouží pro identifikaci clientova oprávnění

OAuth2

- standard pro přihlašování do aplikací
- autorizační framework

User

- člověk, který se snaží získat přístup k Resource

Resource

- žádaná data, která jsou chráněna

Client

- aplikace, která pod jménem uživatele žádá o data

Resource Owner

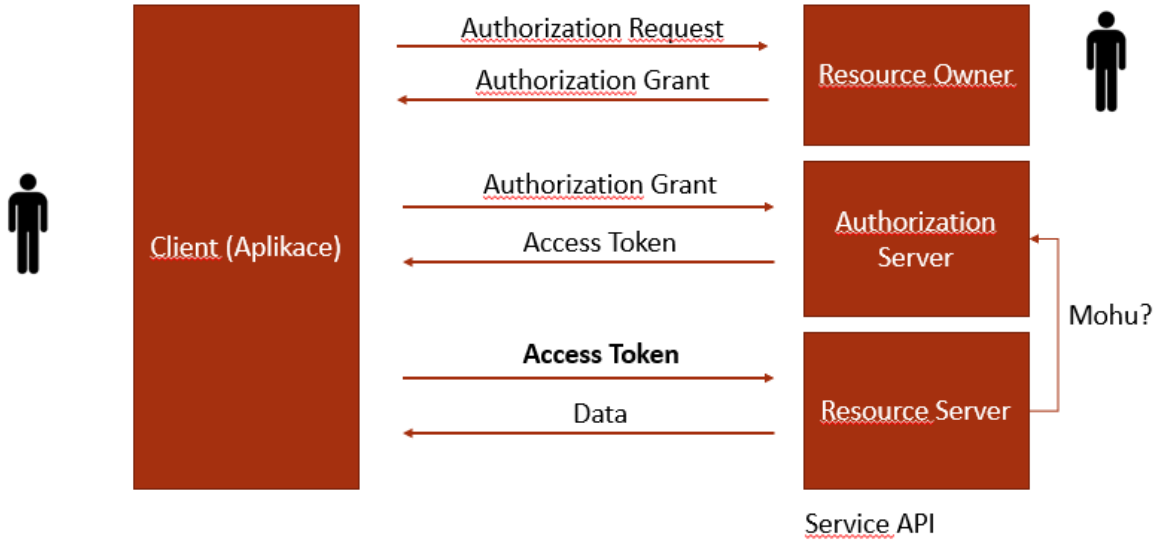
- uživatel, který umožní Clientovi přístup k datům

Resource Server

- místo, kde jsou uloženy data (API)

Authorization Server

- místo, které poskytuje ověření identity (API)
- bývá spojeno s Resource Server



OpenID

- rozšíření pro OAuth2
- přidává identity layer
  - token nese navíc informaci o uživateli