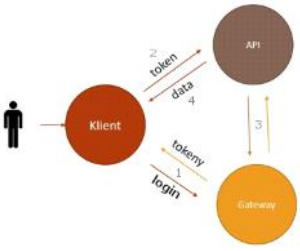
20 Ověřování identity v prostředí internetu

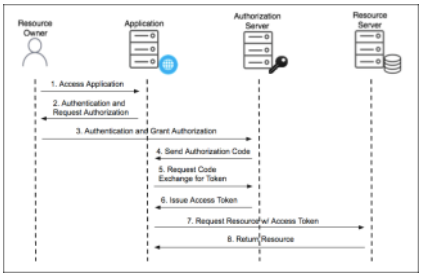
Wednesday, 19 January 2022 09:05

jméno, heslo, dvoufázové ověřování, biometrické ověřování, OAuth2, resource, owner, authorization server, OpenID, poskytovatelé ověření, access_token

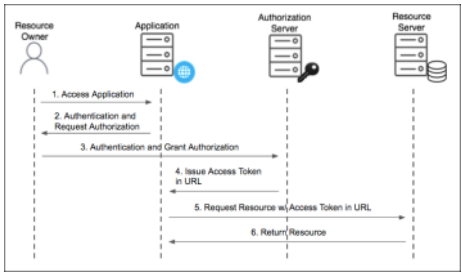
- ověření
  - zabezpečení údajů pro určitou skupinu uživatelů nebo samotného uživatele
  - mělo by být sjednoceno napříč platformami v rámci aplikace (web, mobil, desktop, …)
  - komunikace musí být šifrovaná
  - způsoby:
    i. žádné
    ii. username + heslo
      - 1 unikátní + 1 tajný údaj
      - heslo by mělo být šifrováno (nejčastěji SHA)
      - míra bezpečnosti závislá na síle hesla
    iii. dvoufázové ověření
      - ověření z druhého zařízení
      - při přihlášení přijde e-mail, SMS nebo se využije authenticator
    iv. biometrické ověření
      - otisk prstu, 3D sken obličeje
      - těžko se falšuje
      - měl by mít náhradu v případě chyby skenování
- OAuth2
  - přihlašování přes aplikaci třetí strany
    - např. Google, Facebook, Apple
  - založeno na důvěře
  - role:
    i. User
      - uživatel snažící se přistoupit k informacím
    ii. Resource
      - chráněná data na serveru
    iii. Resource Owner
      - vlastník Resource dat
        - může k nim dát přístup jinému uživateli
    iv. Client
      - aplikace skrze kterou User přistupuje k Resource
    v. Resource Server
      - server, na kterém jsou Resource uložená
    vi. Authorization Server
      - předává access token uživateli (po autentifikaci)
  - token
    - náhodný kód identifikující oprávnění
  - scope
    - část Resource, ke kterým lze přistoupit
    - může být rozdílná pro různé skupiny uživatelů
  - Authorization Grant
    - použit klientem pro získání tokenu
    - druhy:
      1) Authorization Code
        - krátkodobý autorizační kód, za který uživatel dostane token
      2) Implicit
        - zjednodušený (authorization server neposílá clientovi autorizační kód)
      3) Resource Owner Password Credentials
        - client posílá uživatelské jméno a heslo
      4) Client Credentials
        - API bez kontextu uživatele
        - server-to-server
      5) Refresh Token
        - obnovení platnosti tokenu
  - proces:
    i. uživatel žádá gateway, aby mohl přistoupit k datům na API; gateway pošle token
    ii. uživatel žádá API o data a přikládá token (zpravidla v Authorization headeru)
    iii. API se ptá gatewaye, jestli může uživatel s daným tokenem přistoupit k datům
    iv. jestli gateway potvrdí autorizaci uživatele, tak mu API posílá data
  - OpenID
    - nadstavba nad OAuth2
    - token vydaný Oauth2 je náhodný
      - OpenID tam přidává identity layer - zakódovaná data (obvykle JWT - Javascript Object Notation):
        - header
          - algoritmus
        - data
          - ID uživatele, issuer (vydavatel tokenu), audience (kterému klientovi byl token poskytnut)
        - kontrolní součet



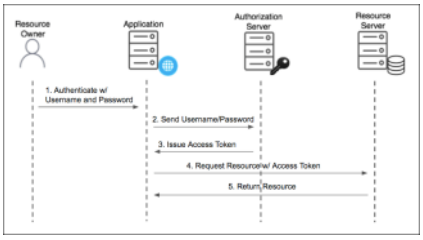
Authorization Code



Implicit



Resource Owner Password Credentials



Client Credentials