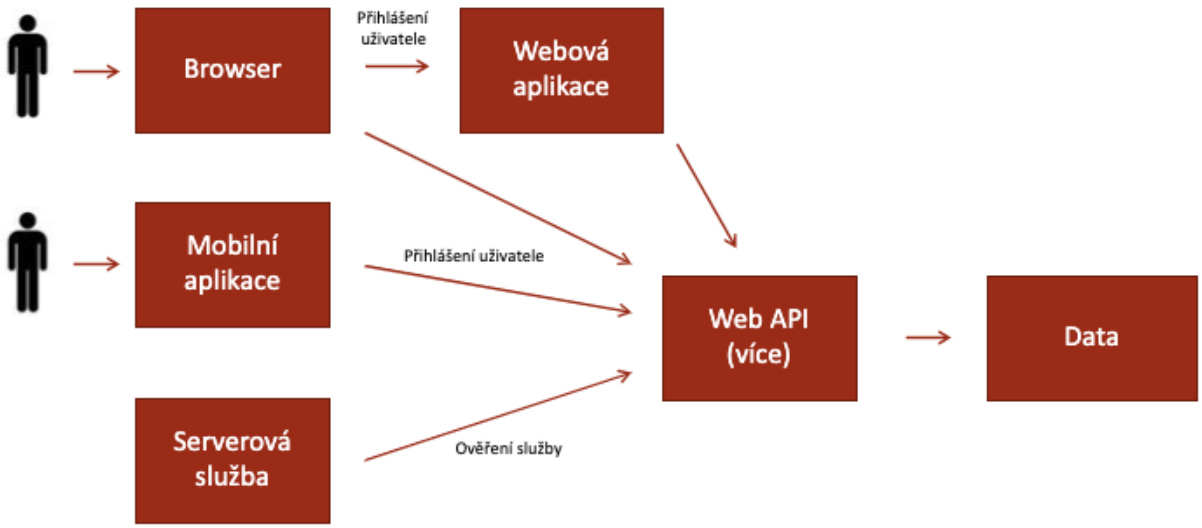
Ověřování identity v prostředí internetu

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

Joseph Soukup – P4



Ověření

- První možnost je, že neověřujeme uživatele
- Uživatelské jméno/Email + heslo
    - Proč nestačí uživatelské jméno
        - Hodně lidí stejný
        - Není bezpečný
    - Proč nestačí jen heslo
        - Hodně lidí stejné heslo
    - Požadavky na heslo:
        - Písmena + čísla + speciální znaky
        - Min délka 8
        - Žádná slova ze slovníku
        - Nic osobního
        - Žádná věty
        - Žádné posloupnosti (123456789)
    - Password nebo Passphrase:
        - Password – krátké se znaky
        - Passphrase – dělší seskupení slov
        - Passphrase protože:
            - Jednodušší na zapamatování
            - Password jsou jednodušší na hacknutí
            - Splňuje i podmínky pro hesla
            - Passphrase: skoro nemožný na hacknutí

Dvoufázové ověřování

- Při přihlašování uživatel při autentizaci poskytne dva důkazů (faktorů) potvrzujících identitu:
    - Znalost – něco co ví pouze uživatel

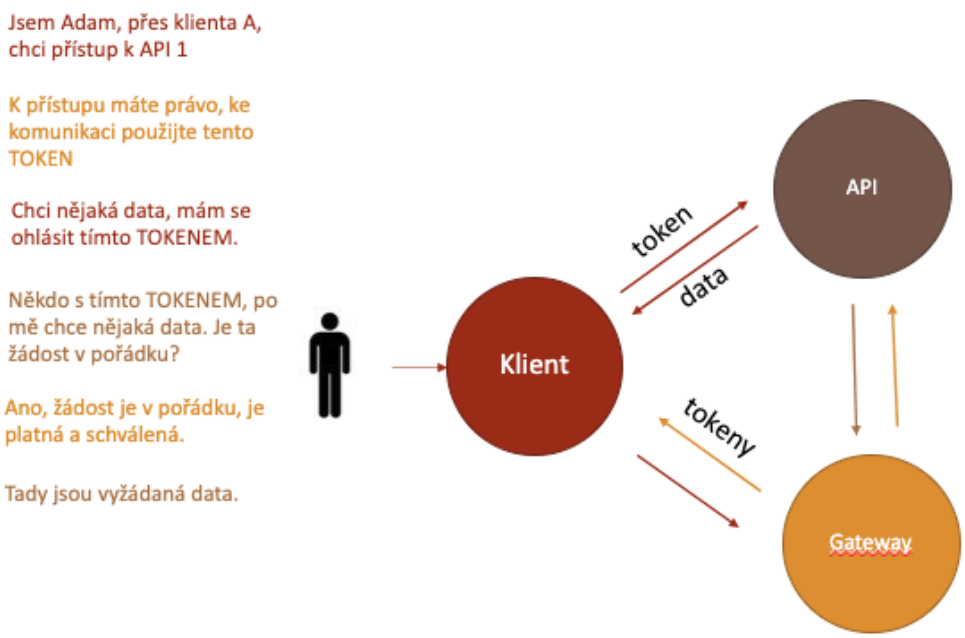
    - Vlastnictví – něco co má pouze uživatel
    - Charakteristika – něco, čím je pouze daný uživatel
- Chránění před krádeží digitální identity
- První většinou Jméno a heslo, druhým pak například PIN, otisk prstu, snímek sítnice oka, elektronický token, …
- Google, Facebook, Steam, Internetové bankovnictví, …

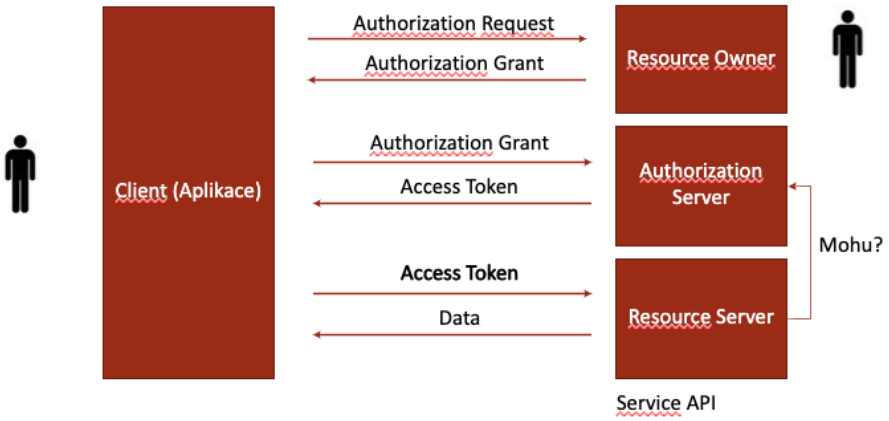
Biometrické ověřování

- Biometrické zařízení zajišťuje bezpečnostní identifikaci a autentizaci
- Tyto zařízení měří jedinečné biologické charakteristiky subjektu (bimetrie)
- Otisky prstů, obraz obličeje, snímek sítnice nebo lidský hlas => jednoznačné určení identity
- Poskytování řízení přístupu k bezpečnostně citlivým oblastem = počítačové systémy nebo jiné oblasti s omezeným přístupem
- Mobil – otisk, obličej
- Počítače – otisk prstu, či ruky nebo obraz obličeje
- Vstup do budovy – sítnice

OAuth2

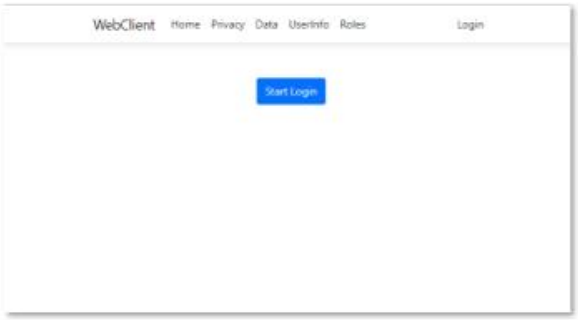
- Standart pro přihlašování
- Role:
    - **User** – člověk snažící se o přístup k **Resource**
    - **Resource** – chráněná data
    - **Resource Owner** – uživatel umožňující clientovi přístup ke svým datům
    - **Client** – aplikace (uživatel), žádající o přístup k datům
    - **Resource Server –** API obsahující sdílená data
    - **Authorization Server –** API poskytující ověření identity a vydávající přístupové tokeny
- Resource a Authorization Server bývají spojeny
- **Token –** náhodný Kód identifikující clientova oprávnění
- **Scope –** určení, o kterou konkrétní část dat usilujeme

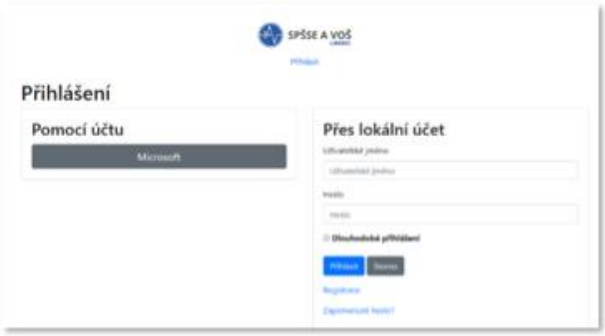




- Registrace klienta na autorizačním serveru:
  - Jméno aplikace
  - Website
  - Callback URL (kam bude uživatel přesměrován)
  - ClientID (identifikuje clienta)
  - Client Secret (má být použit při přístupu k účtu uživatele)
- Authorization Grant:
  - **Authorization Code** – komunikace mezi servery, výměna kódu za token, kód je krátkodobý
  - **Implicit –** komunikace s webovou nebo mobilní aplikací, zjednodušený, vyměňuje token za ID
  - **Resource Owner Password Credential –** důvěryhodné (vlastní aplikace), ID a heslo jsou vyměněny rovnou za token
  - **Client Credentials –** API, komunikace bez kontextu uživatele

- **Device Code –** jednoúčelová zařízení
- **Refresh token –** obnovení platnosti tokenu





-
- Omezení:
  - Pro aplikace, které jsou schopné udržet v tajnosti své ID a secret
  - Pokud aplikace není schopná udržet svůj secret v tajnosti, pokusí se o autorizaci bez secretu
- Browser based application:
  - Nemohou udržet tajný secret, proto jej neposílají
  - Stejná jako server-side application
- Nativní aplikace:
  - Nejsou schopné udržet v bezpečí secret
  - Musí zobrazit potvrzení žádosti o schválení v okně prohlížeče
- Scénář Refresh tokenu:
  - Pokud Access token vyprší, je možné poskytnout jednorázový Refresh_token, který vrací nový access i Refresh token
  - Access token většinou 30 minut

OpenID

- Rozšíření OAuth2.0 o identity layer
- Token nese informaci o uživateli
- Dnes obvykle JWT Token
- Zakódovaná JSON data, uvnitř kterých jsou informace o uživateli a skutečně náhodný řetězec
- Sub = subject = ID uživatele
- Iss = issuer = kdo token vydal
- Aud = audience = client, kterému byl token poskytnut

Poskytovatelé ověření

- Google – Gmail
- Microsoft
- Apple
- Github