# Ověřování identity v prostředí internetu

## Způsoby ověření uživatele

* Neověřujeme
* Jméno a heslo
* Unikátní a tajný údaj
* Jméno nestačí
* Míra bezpečnosti závisí na délce hesla
* PassPhrase – dlouhá věta
* Heslo lze prolomit sociálním inženýrstvím nebo bruteforcem
* Celá komunikace musí být šifrována + protokol HTTPS s ověřením certifikátu na obou stranách

### Dvoufázové ověření

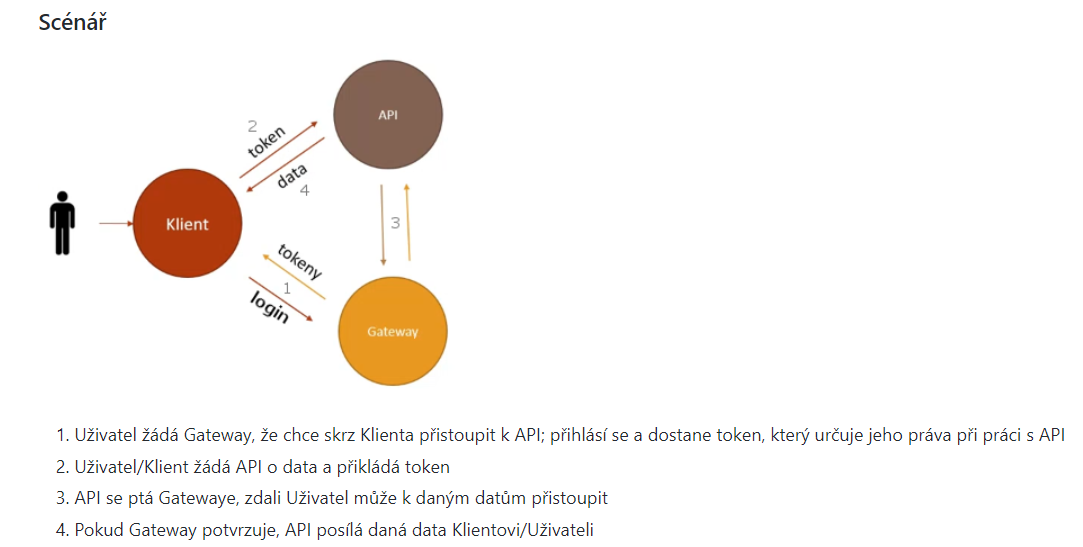
* dodatečný kód zaslaný na email, sms

### Biometrické ověření

* otisk prstu, sken rohovky
* nesmí být jako jediný údaj, nemusí být unikátní hash

## OAuth2

* Standart pro přihlašování
* Přihlašování přes aplikaci 3. strany, které obě strany důvěřují
* **Token** – náhodný kód identifikující oprávnění klienta
* **Scope** – část dat, ke kterým lze přistoupit
* Role:
  + User – uživatel se snaží dostat ke zdroji dat (resource)
  + Resource – chráněná data na serveru
  + Resource owner – uživatel vlastnící data, dá přístup jinému
  + Client – aplikace skrze kterou user k datům přistupuje
  + Resource server – server na kterém jsou data uložena, spojeno s AS, API
  + Authorization server – po úspěšné autentifikaci předává klientovi acces token, API



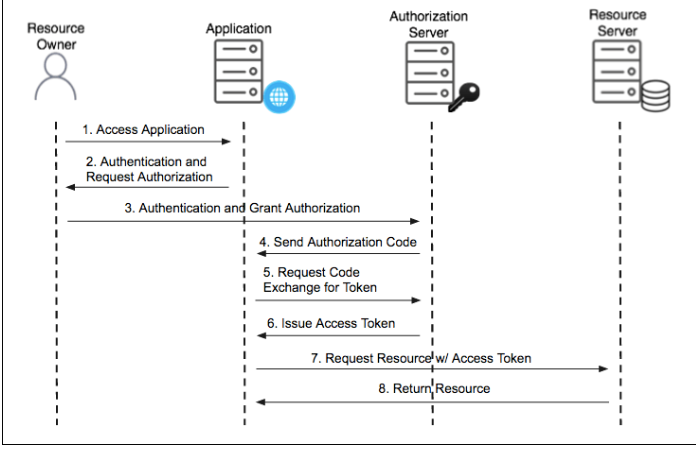
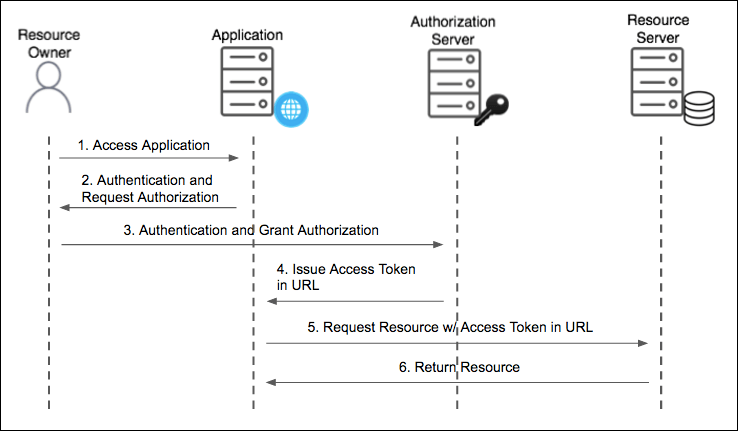
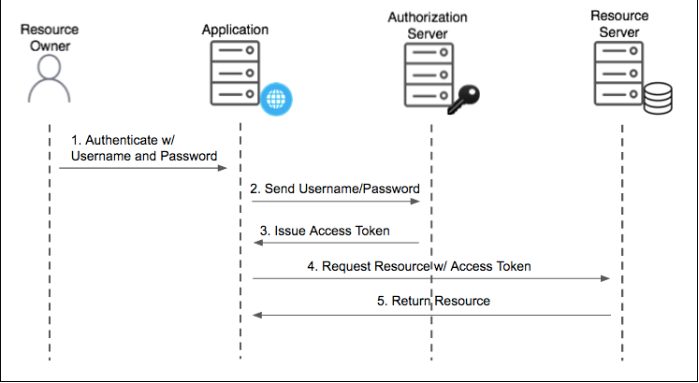
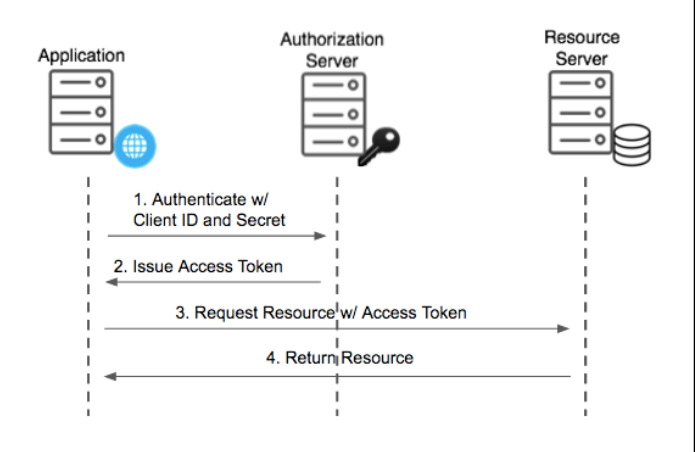
## OpenID

* Nadstavba nad OAuth2
* Token od Oauth2 je náhodný řetězec bez informací, autorizován klient
* Umožňuje používat jeden účet pro více webů
* OpedID token obsahuje informace o uživateli
* Obvykle JSON
  + Sub – id uživatele
  + Iss – kdo vydal token
  + Aud – klient, kterému byl token poskytnut

Obsah obrázku text

Popis byl vytvořen automaticky

## Authorization Grant

* Použit klientem pro získání klientu
* Více druhů
* **Authorization code** – komunikace mezi servery, krátkodobý kód za token
* 
  + Běžné pro server-side aplikace
* **Implicit** – zjednodušený mechanismus pro prohlížečové klienty, vyměňuje token za ID a secret
* 
* **Resource Owner Password Credentials** – důvěryhodné aplikace, ID a heslo jsou vyměněny rovnou za token, mobilní a desktop aplikace
* 
* **Client Credentials** – pro api bez kontextu uživatele
* ****
* **Device Code** – jednoúčelová zařízení
* **Refresh token** – obnovení platnosti tokenu

## Použití access tokenu

Obsah obrázku text

Popis byl vytvořen automaticky