OAuth 2.0

- Standardiseeritud volitamise (*authorization*) veebirakendustele
- OAuth 2.0 on protokoll, millega saab delegeerida klientidele piiratud juurdepääsu veebiteenusele või API-le
- Selleks on kasutusele volitamisserver, mis annab klientidele juurdepääsutõendeid (*access token*)
- Erinevad token'ite liigid:
  - access token (tavaliselt bearer token)
  - refresh token
  - ID token
- Erinevad tokeni tüübid:
  - Bearer token (esitaja token)
  - MAC token

OAuth otspunktid (*endpoints*)

- Server discovery
- Server JWK set
- Authorization
- Token
- Token introspection
- Token revocation
- UserInfo
- Logout

OAuth protokoll

- Teenus suunab kasutaja brauseri ümber volitusserverisse
- Volitusserver autendib kasutaja nii nagu ise sobivaks peab
- Volitusserver autendib suunab kasutaja brauseri tagasi esialgsesse teenusserverisse
  - Eelhäälestatud ninmekirti lubatud serveritest, kuhu tohib tagasi suunata
- Lisapäringud tokenite uurimiseks (*introspection*)

OpenID Connect (OIDC)

- Kasutab OAuth voogusid (*flow*) kasutaja identifitseerimiseks lisaks volitamisele
- ID Token — signeeritud JSON Web Token (JWT)