



Aalto University
School of Science

Tietoturva-arkkitehtuurin vaihdossa - Monoliitista Mikropalveluihin

Tommi Jäske

Department of Computer Science
Aalto University, School of Science

Version 1.0, April 8, 2020

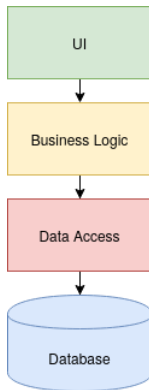
Sisältö

- ▶ Tarkoitus
- ▶ Monoliitti- ja mikropalvelut
- ▶ Jakaminen
- ▶ Kommunikointi
- ▶ Tunnistaminen ja valtuuttaminen
- ▶ Muut kysymykset
- ▶ Loppupäätelmät

- ▶ Keskeiset tietoturvakysymykset

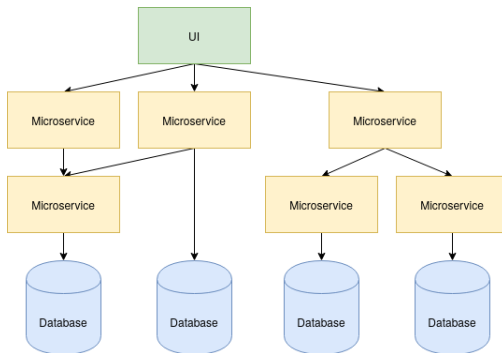
Monoliitti

- ▶ Skaalaus
- ▶ Monimutkaisuus
- ▶ Isot julkaisut



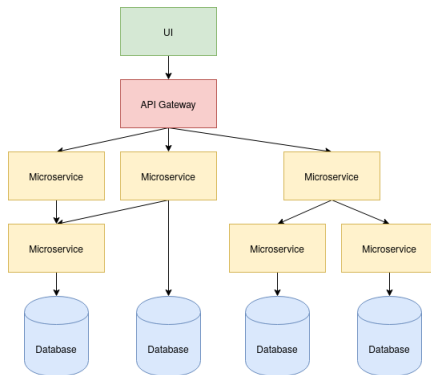
Mikropalveluarkkitehtuuri

- ▶ UNIX -periaate
- ▶ yksinkertaiset palvelut
- ▶ itsenäisyys



API Gateway

- ▶ Hyökkäyspinta rajattu
- ▶ Pilkkominen toiminto kerrallaan

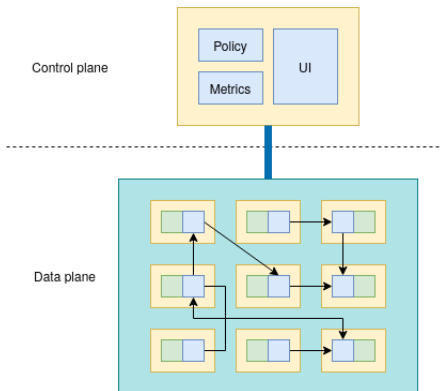


Kommunikointi

- ▶ prosessi vs verkko
- ▶ REST API
- ▶ SSL/TLS
- ▶ Service Mesh

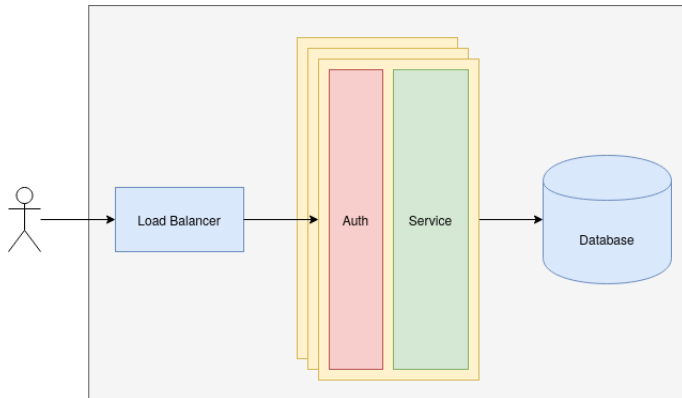
Kommunikointi - Service Mesh

- ▶ Hallinnointi
- ▶ Proxy - sidecar
- ▶ Sertifikaatti
- ▶ Istio, Consul, Linkerd...



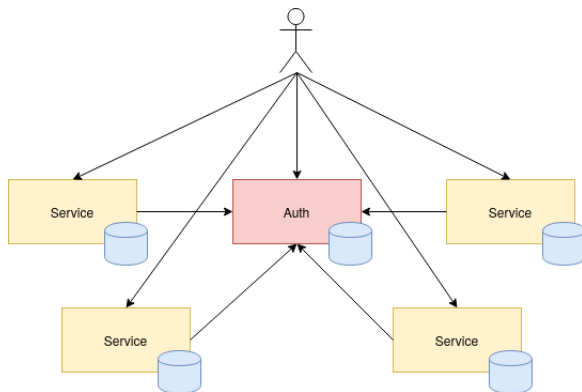
Tunnistaminen ja valtuuttaminen - Monoliitti

- ▶ Ulkoraja
- ▶ Prosessi



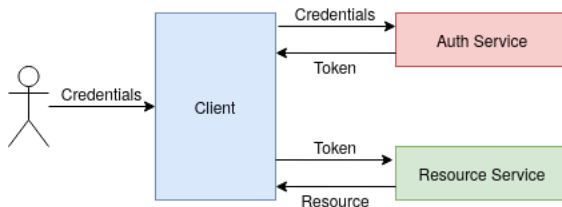
Tunnistaminen ja valtuuttaminen - Mikropalvelu

- Kyselyt
- Käyttövaltuuksien tarkistaminen
- Valmiit toteutukset



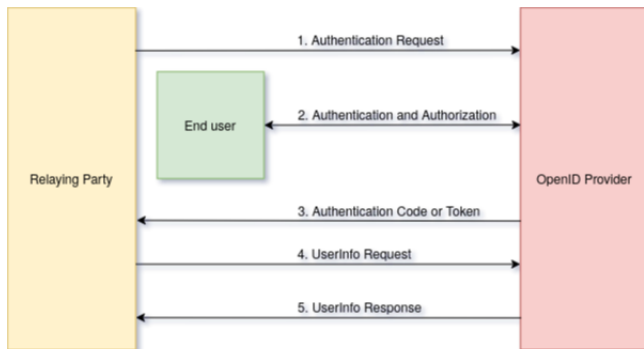
Tunnistaminen ja valtuuttaminen - Käyttöoikeustietue (Token)

- ▶ Käyttäjä ID
- ▶ Käyttövaltuudet
- ▶ Voimassaolo



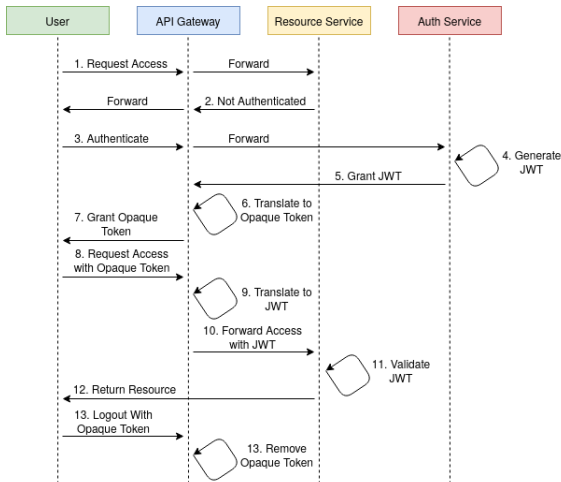
Tunnistaminen ja valtuuttaminen - OpenID Connect

- Sovellus - käyttäjä - Identity provider
- Suostumus
- Käyttäjätiedot (UserInfo Endpoint)



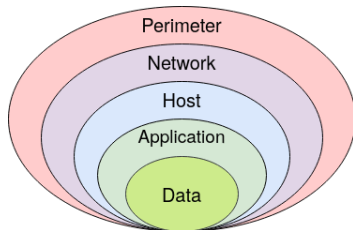
Tunnistaminen ja valtuuttaminen - sisäinen JWT

- Kulku
- Uloskirjautuminen



Muut kysymykset

- ▶ Asetukset
- ▶ Julkaisujen tiheys ja sisältö
- ▶ Osaaminen
- ▶ Kehittäjät ja tiimit
- ▶ Syväpuolustus



Loppupäätelmät

- ▶ Kommunikointi - Service Mesh
- ▶ Tunnistaminen ja valtuuttaminen
- ▶ Syväpuolustus - ei voi luottaa
- ▶ Valmiit toteutukset