



Aalto University
School of Science

Tietoturva-arkkitehtuurin vaihdossa - Monoliitista Mikropalveluihin

Tommi Jäske

Department of Computer Science
Aalto University, School of Science

Version 0.1, April 6, 2020

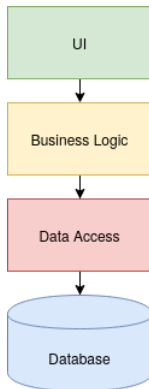
Sisältö

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

- ▶ Keskeiset tietoturvakysymykset

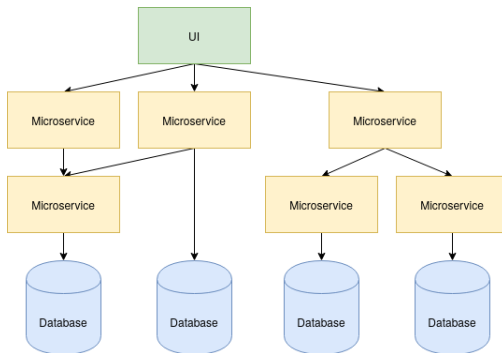
Monoliitti

- ▶ Skaalaus
- ▶ Monimutkaisuus
- ▶ Isot julkaisut



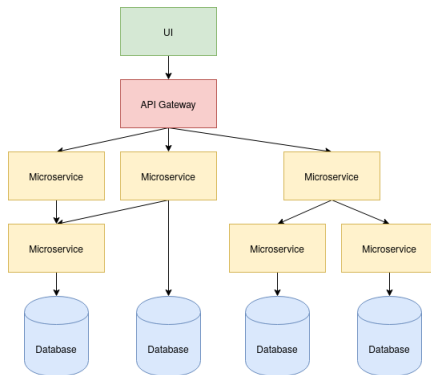
Mikropalveluarkkitehtuuri

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



API Gateway

- ▶ Hyökkäyspinta rajattu
- ▶ Useita tehtäviä

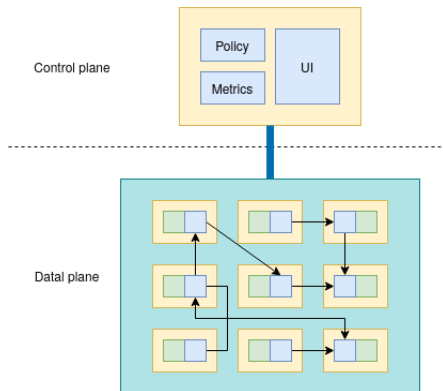


Kommunikointi

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

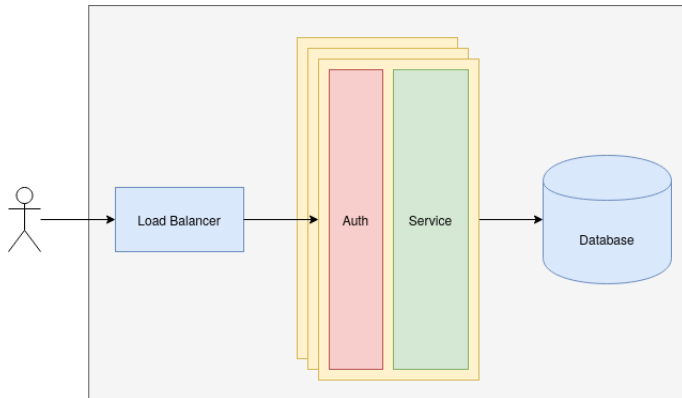
Kommunikointi - Service Mesh

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



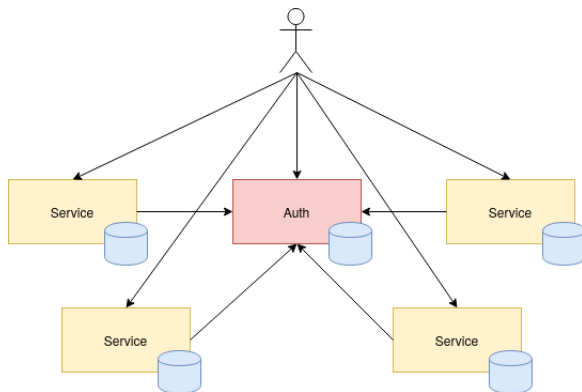
Tunnistaminen ja valtuuttaminen - Monoliitti

- ▶ Ulkoraja
- ▶ Prosessi



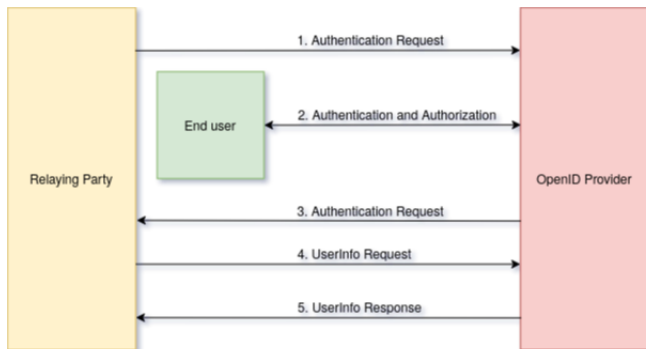
Tunnistaminen ja valtuuttaminen - Mikropalvelu

- Kyselyt
- Käyttövaltuuksien tarkistaminen
- Valmiit toteutukset



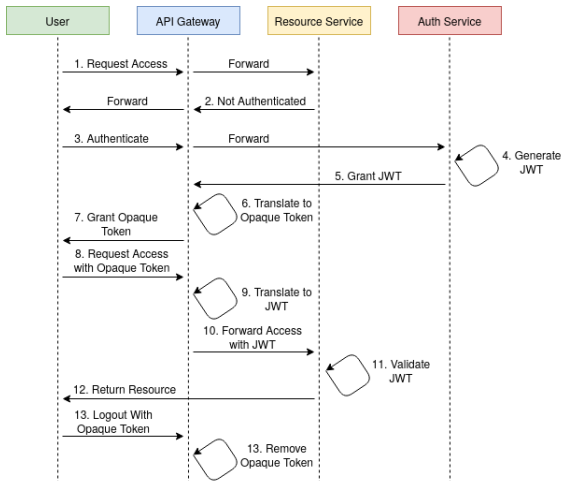
Tunnistaminen ja valtuuttaminen - OpenID Connect

- ▶ Sovellus
- ▶ Suostumus
- ▶ Käyttäjätiedot (UserInfo Endpoint)



Tunnistaminen ja valtuuttaminen - sisäinen JWT

- Kulku
- Uloskirjautuminen



Muut kysymykset

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

Loppupäätelmät

- ▶ Kommunikointi - Service Mesh
- ▶ Tunnistaminen ja valtuuttaminen
- ▶ Syväpuolustus
- ▶ Valmiit toteutukset