SMART on FHIR i HSØ

SYKEHUSPARTNER

Anders Halling, Domenearkitekt IAM

FHIR Fagforum 11.02.26

SMART on FHIR i Helse Sør-Øst
Status

- Fragmentert landskap
- Stort behov for samhandling mellom applikasjoner
- Alt egner seg ikke for APIer, i alle fall ikke i utprøvende faser
- «Store» applikasjoner bruker CCOW seg imellom for kontekstsynk
  - Slutter å fungere når applikasjoner gradvis benytter mer web-teknologi.
- Delvis SSO mellom applikasjoner som støtter identitetsføderering
- Mange applikasjoner fortsatt med tett kobling til AD eller med lokale brukerdatabaser

SMART on FHIR i Helse Sør-Øst
Status

- Vi har etablert en løsning som delvis oppnår det samme som SMART on FHIR
  - Oppnår at en applikasjon kan få utstedt et accesstoken, med sluttbrukeridentitet, som fungerer f.eks. mot DIPS slik at vi har føderert identitet og tilgangskontroll ende til ende.
- Oppnås ved at føderingsløsningen har oversikt over tilganger i ulike fagsystemer, og kan populere personlige tokens med aktuell brukerrolle etter autentisering eller ved token exchange.


```
"sub": "UXHAFN",
"scope": "dips-fhir",
"client_id": "I_MetaVDips",
"aud": "https://dips.hso.no",
"hso:subject:application-role:system": "http://dips.com/UserRoleGUID",
"hso:subject:application-role:id": "35FC8749-585E-58E0-E063-0D40B40A5345",
"hso:subject:application-role:assigner": "https://www.siv.no"
```


- Krever mye spesialtilpasning
- Utfordring med de 5% av ansatte som har mer enn én rolle i f.eks. DIPS.
  - Hvordan vite hvilken DIPS-rolle som er aktuell i den kontekst de er i i det andre fagsystemet?

SMART on FHIR i Helse Sør-Øst
Identifiserte behov

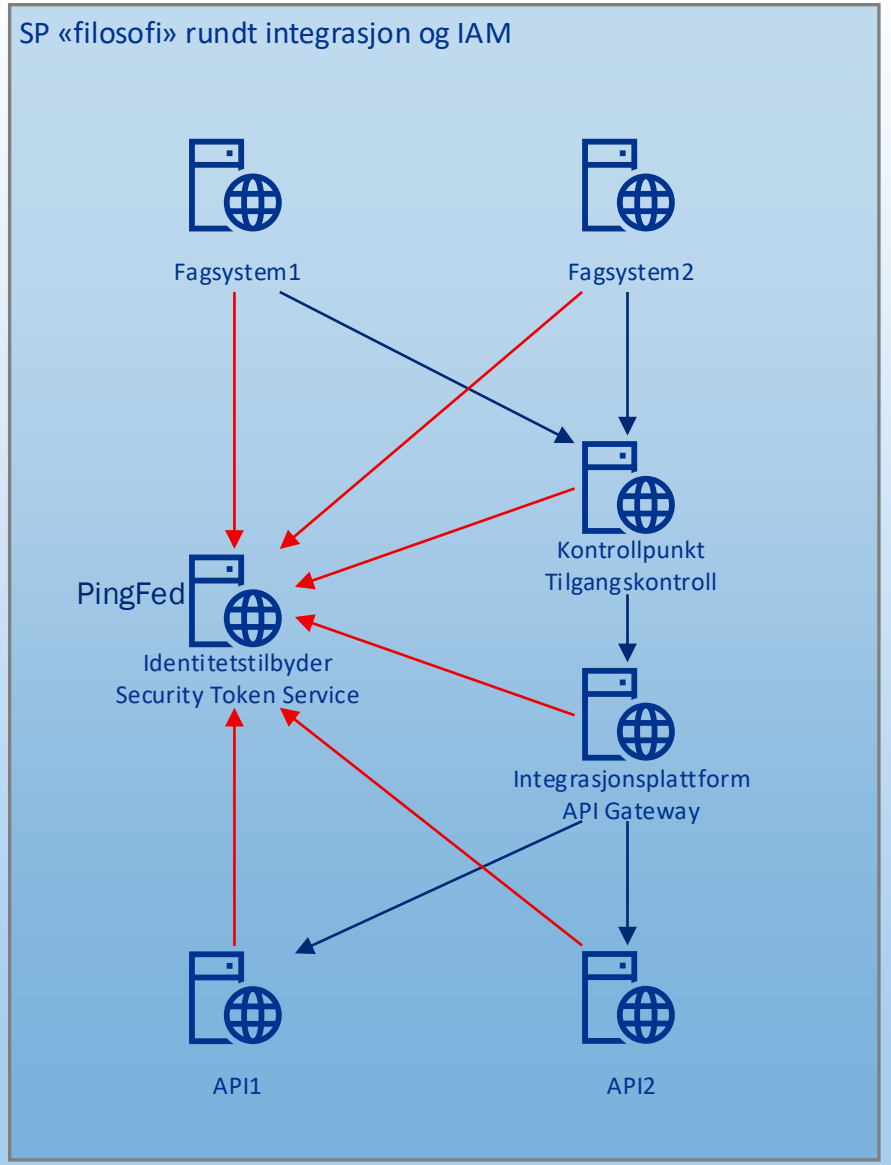
- Sanntidsvisning av ambulansejournal Bliksund EWA – visning i DIPS
  - Pasienter på vei inn til sykehus
  - Live-data inkl. streaming av EKG (MDR) og chat
- Trygg ernæringsdokumentasjon – visning i DIPS
  - Felles løsning for sengepost, klinisk ernæringsfysiolog og kjøkken
  - Konseptutredning av en Webapplikasjon på PEGA-plattformen
- Bestilling og svar – visning i DIPS
  - Rekvirering og svar på lab-prøver på tvers av virksomheter – SaaS-tjeneste fra DIPS ASA
- Radiologi 2.0 – visning av multimedieobjekter og SETW i DIPS
  - Sectra slutter å støtte uthopp+CCOW i 2027, SMART on FHIR foreslått som erstatning

SMART on FHIR i Helse Sør-Øst
Egenskaper ved behovene

- Fellestrekk med behovene:
  - Behovene går ut på å utvide andre kliniske applikasjoner inn i DIPS arbeidsflate, ikke på å utvide funksjonaliteten i DIPS som sådan.
  - Appene er i utgangspunktet ikke tenkt å hente data fra host-EPJ utover launch-kontekst.
  - De skal hente data fra sitt eget «modersystem» som vil kreve at sluttbrukeren blir autentisert i, og får et accesstoken som virker mot, modersystemet i tillegg til DIPS.
- Mellomvarekomponenter som API-gatewayer og IAM kontrollpunkter kan ikke forholde seg til et SMART-token fra DIPS.
  - HSØ benytter PingFederate som IdP og Security Token Service, Azure APIM som API GW (under innføring) og PingAccess som IAM Kontrollpunkt.

SMART on FHIR i HSØ

- SMART on FHIR er basert på direkte aksess (på lag 5) fra SMART-app til FHIR-APIer i host EPJ.
- HSØ/SP har et mer sentralisert integrasjonslandskap der vi peker API-klienter på IAM-kontrollpunkter og API-gatewayer.



SMART on FHIR i Helse Sør-Øst
Mulige løsninger

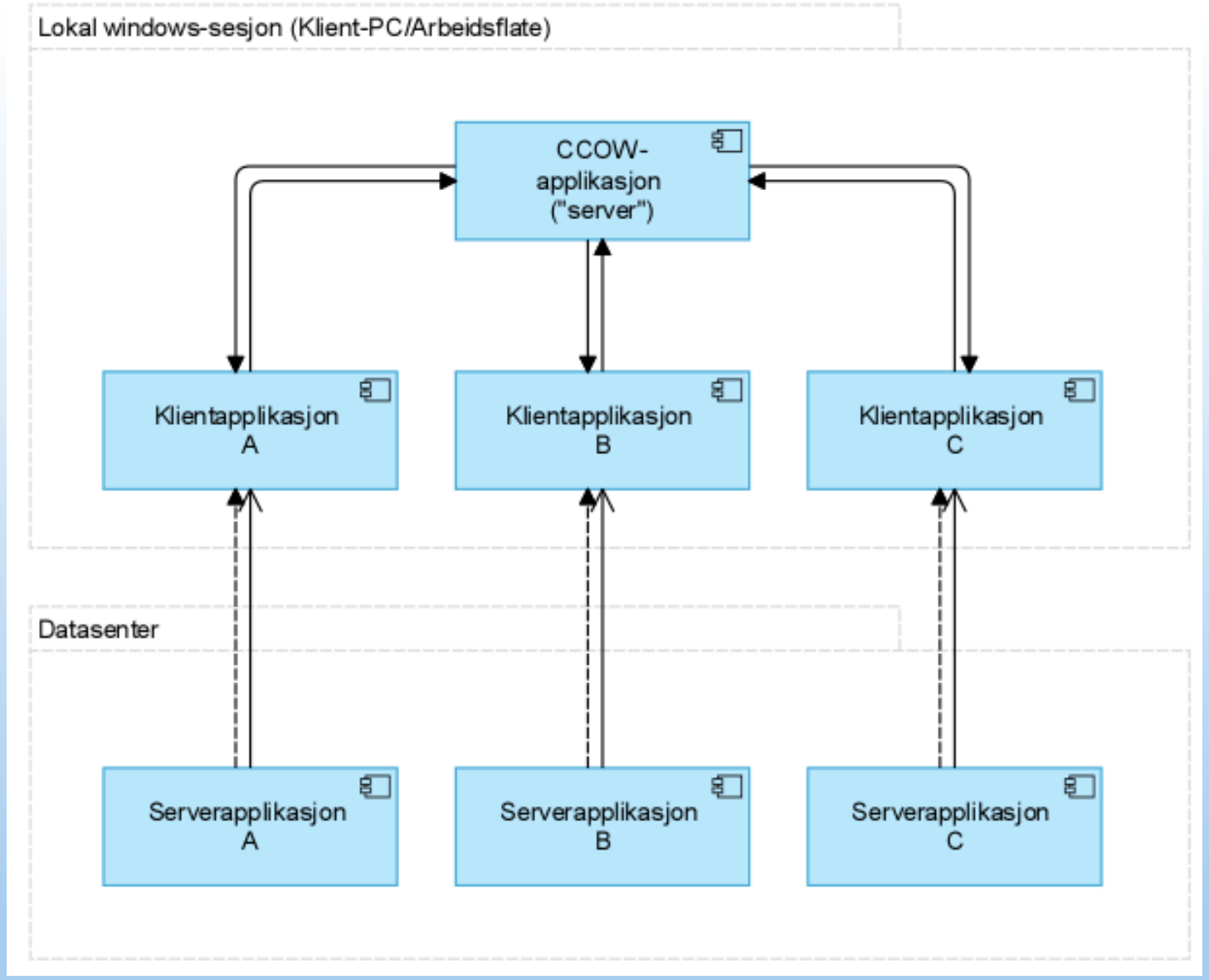
- Et løsningsmønster som ser ut til å gå igjen for slike behov er å bygge inn to uavhengige OAuth/OIDC-klienter i SMART-appen
  - Én klient mot host-EPJ, og en annen mot modersystemets IdP/Autorisasjonsserver.
  - SMART-appen må da ha kontroll på to sesjoner og to sett av tokens.
  - SMART-appen må særlig passe på at det er samme sluttbruker i begge sesjonene
  - Økt kompleksitet rundt SSO. Det er risiko for dobbeltautentisering pga. ulike sesjonslevetider eller utilgjengelige session cookies (embedded browser).
- Utfordring med å transportere to tokens i tilfeller der mellomvare forholder seg til en annen STS enn målsystemet, og det ikke kan løses med token exchange på veien.

Kontekstsynk - FHIRcast som erstatning for CCOW?

- I dag bruker HSØ en CCOW-applikasjon fra DIPS.
- Denne er lokal på PC-klient og fungerer uavhengig av DIPS.
  - Dvs. den kan fungere selvstendig mellom Kurve og PACS, uten at brukeren er logget på DIPS.
- Fungerer bare for native apps, ikke for web-applikasjoner.
- FHIRcast fungerer med webapplikasjoner siden den er serverbasert.
- FHIRcast er avhengig av en SMART authorization server, sluttbruker må logge på mot denne selv om de ikke har noe behov for å logge på host-EPJet som leverer den.
- CCOW: Hub and spoke der hub er en lokal applikasjon på klient-PC
- FHIRcast: Hub and spoke der hub er en serverapplikasjon på host-EPJ som eier authorization serveren.

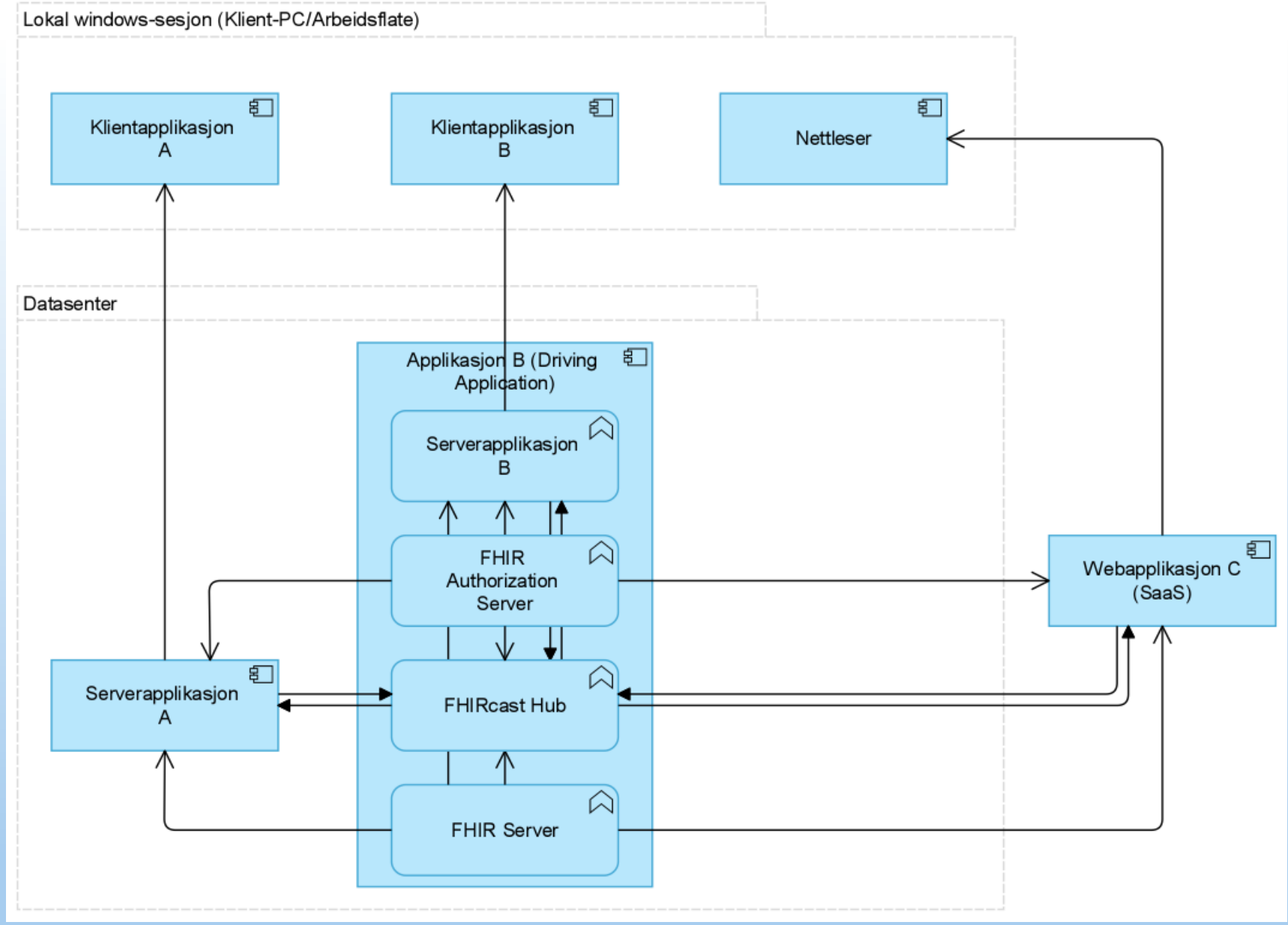
CCOW

- «lokal» serverapplikasjon på arbeidsflaten.
- Levert av DIPS, ingen utvikling
- Komplisert for leverandører
- Fungerer ikke med webapplikasjoner som kjører i nettleser



FHIRcast

- Kjører serverside
- Støtter webapplikasjoner
- Krever eksisterende SMART on FHIR-infrastruktur
- Applikasjoner må kunne «oversette» FHIR-ressurser til egne ressurs-Ider
- Brukere må eksistere i og kunne logge på «Driving application»

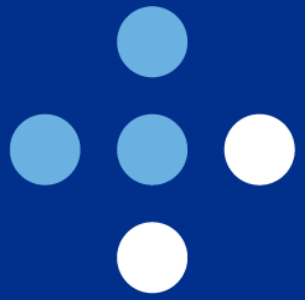


SMART on FHIR i Helse Sør-Øst
En IAM-arkitekts drøm:

- Peke auth-server i smart-configuration til PingFederate?
- Sette opp DIPS som IDP for PingFederate
- GET PingFederate/Authorize?clientID=SMART-app&acr_value=DIPS&launch=<launch>
- Ideell response fra PingFederate til SMART-app:

```
{
    "id_token": "...",
    "access_token": "...",
    "fhir-context": {
    "patient": "123"
    }
}
```

```
AccessToken:
{
    "iss": "pingfederate",
    "sub": "sluttbruker",
    "aud": "API-GW",
    "scope": "dips-fhir",
    "hso:smart-token": "<token fra DIPS>"
}
```



SYKEHUSPARTNER