

EHMI Endpoint Register

– den nye sikre motor for sundhedsvæsnets
adresseringsservice

E-sundhedsobservatoriets årskonference 2026

Understøtter dette af Digital Sundhed Danmarks seks mål:

Udvikle og udbrede brugervenlige digitale løsninger og infrastruktur

Ole Vilstrup, Digital Sundhed Danmark/Christian Gasser, Lakeside



Oplægsbeskrivelse

Enhanced Healthcare Messaging Infrastructure, EHMI, er sundhedsvæsenets nye meddelelsesinfrastruktur baseret på ”[Målbillede for meddelelseskommunikation i sundhedsvæsenet](#)”. En af opgaverne for EHMI er at etablere et nyt endepunkts- og meddelelsesregister, som på sigt kan erstatte SOR-EDI.

Men hvordan sikrer vi, at data fra SOR og SOR-EDI er brugbare – ikke kun til meddelelseskommunikation, men til sundhedsadressering i bredere forstand? Og hvordan flytter vi det danske sundhedsvæsens centrale adresseringsmotor fra en national dansk implementering til en sikker løsning forankret i åbne internationale standarder som HL7 FHIR, OAuth og EU's eDelivery?



Oplægsbeskrivelse

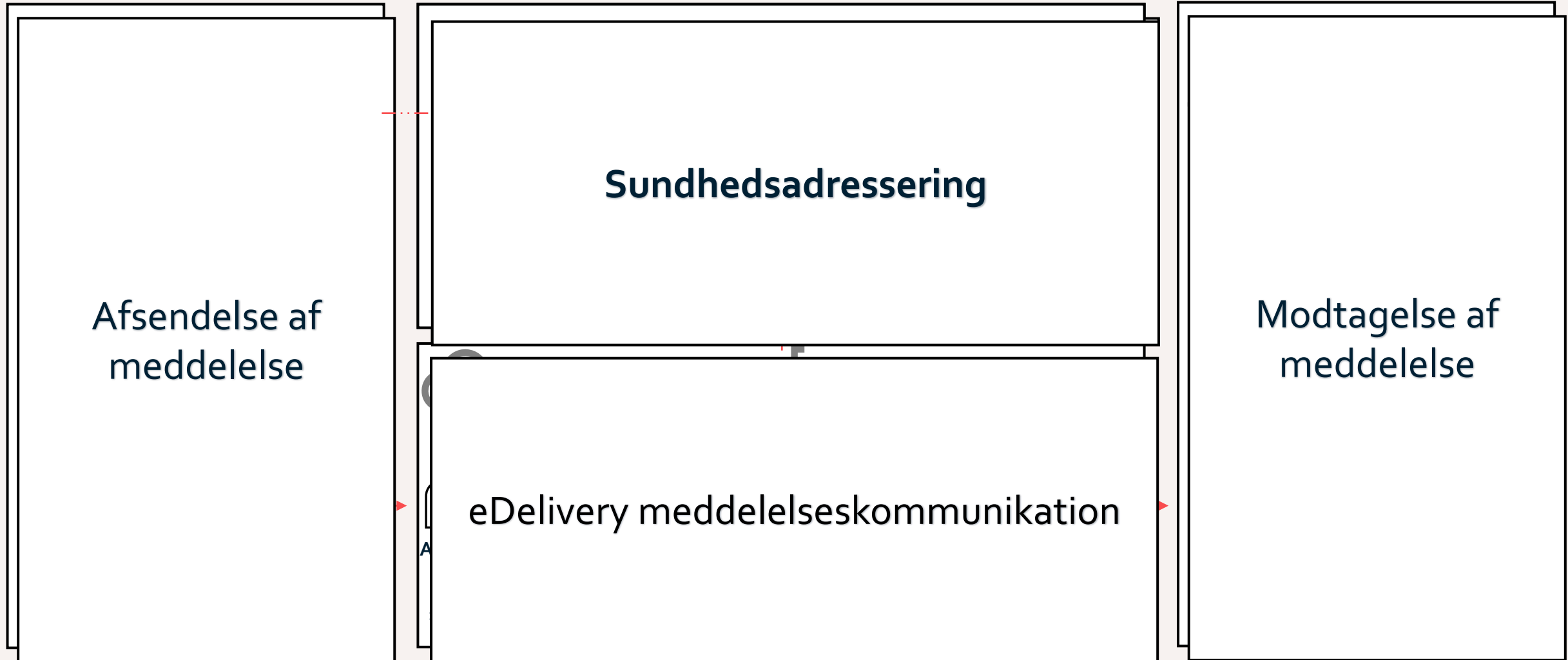
I oplægget præsenterer vi EHMI's Endpoint Register, EER, som fundamentet for fremtidens adressering på sundhedsområdet. Vi viser, hvordan EER understøtter orkestrering af adresseinformation og indgår i både EHMI Addressing Service, EAS, og i den nye eDelivery meddelellesmotor, som Erhvervsstyrelsen har som kernen i deres NemHandels-løsning.

Derudover gennemgår vi FAPI sikkerhedsprofilen, som er den OAuth profil, der er valgt til EER og andre EHMI services.

Vi perspektiverer også til den videre udvikling af EER, hvor flere operationelle metadata kan indgå og understøtte endnu bedre adressering, f.eks. ift. Henvisningstabellen.

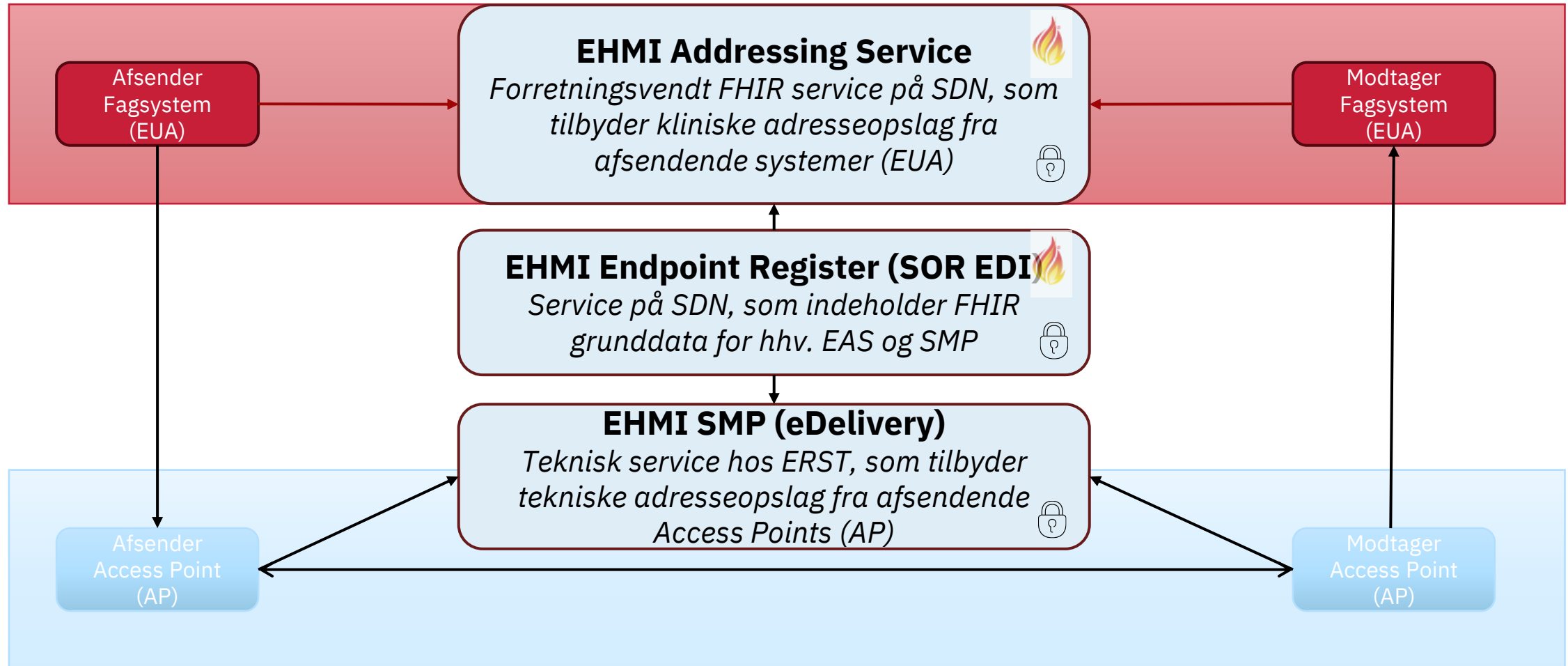


EHMI - et økosystem for sundhedskommunikation



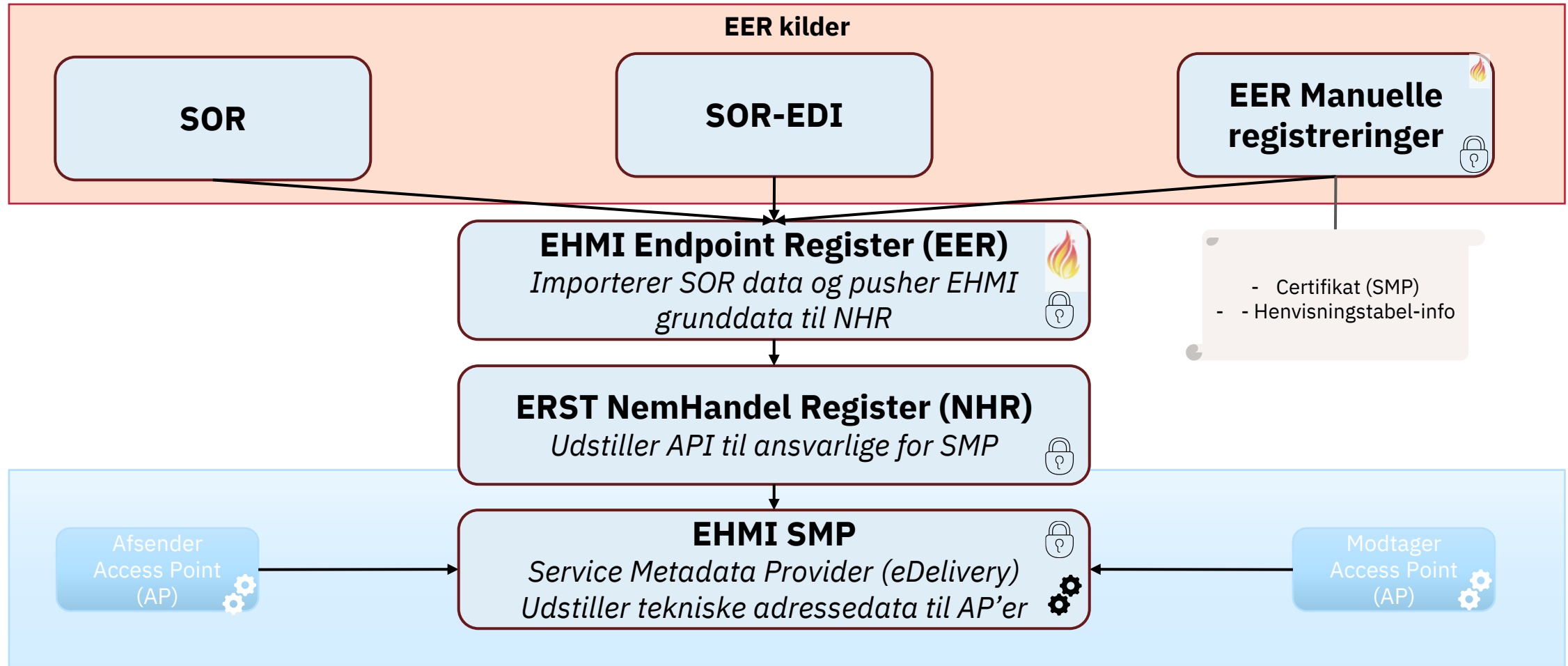


EHMI's adresserings løsning (EAS+EER+SMP)



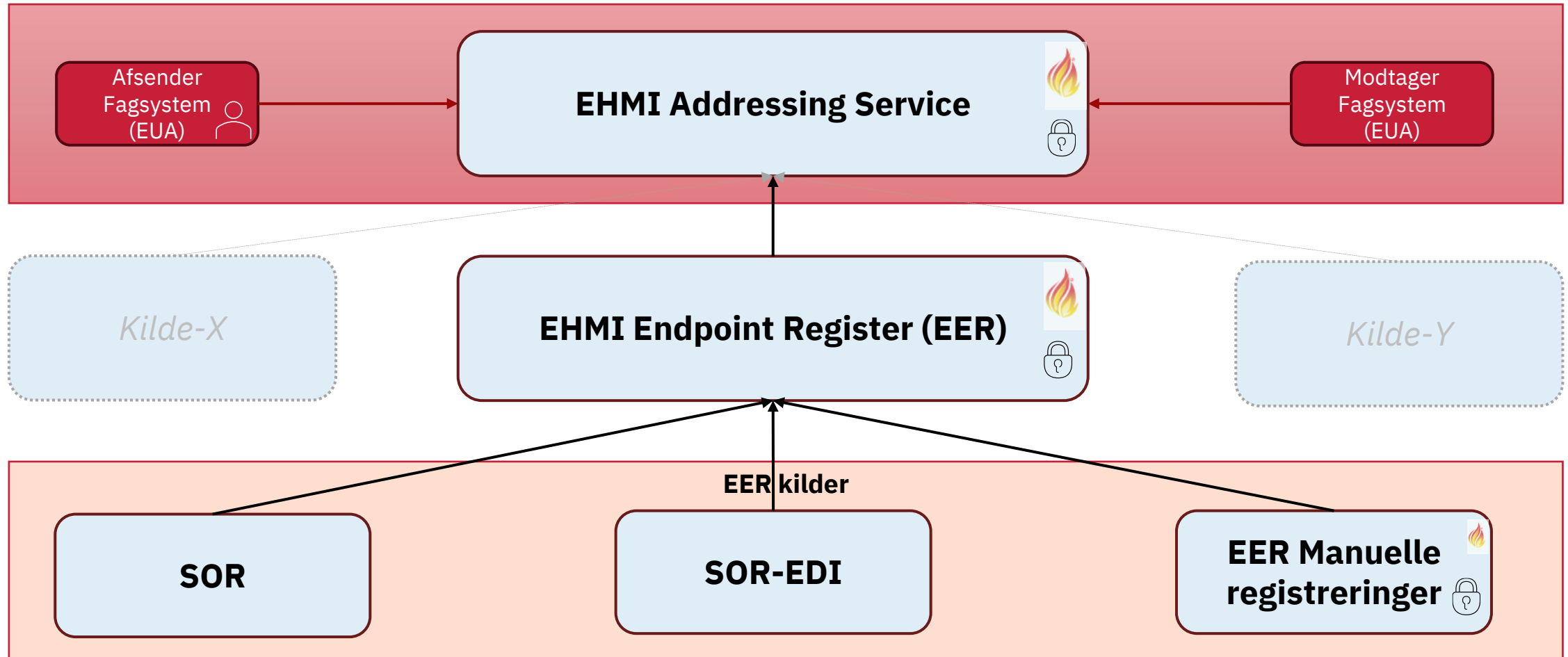


Fra SOR til teknisk adressering





Fra SOR til Forretningsadressering

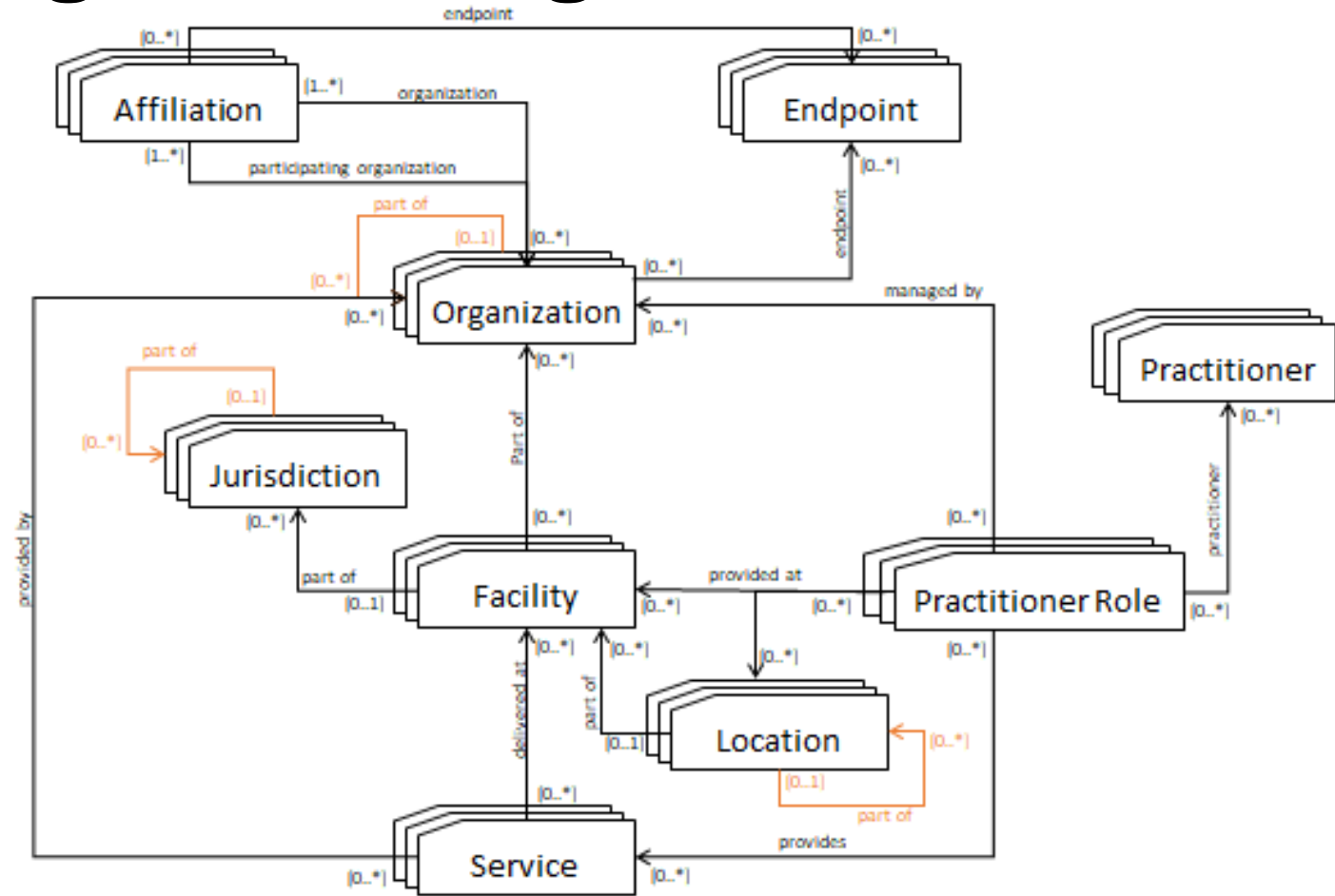




Målbilledet - Forretningsadressering

Ifm. arbejdet med Målbillede for meddelelseskommunikation blev IHE's mCSD model valgt som bedste adresseregister kandidat, da denne er FHIR-baseret og derfor er let at integrere med de fremtidige standarder på sundhedsområdet. Den er desuden modulært opbygget og rummer derfor muligheden for inkrementel udvikling af servicen.

IHE = Integrating the Healthcare Enterprise (international standardiseringsorganisation)
mCSD = Mobile Care Service Directory

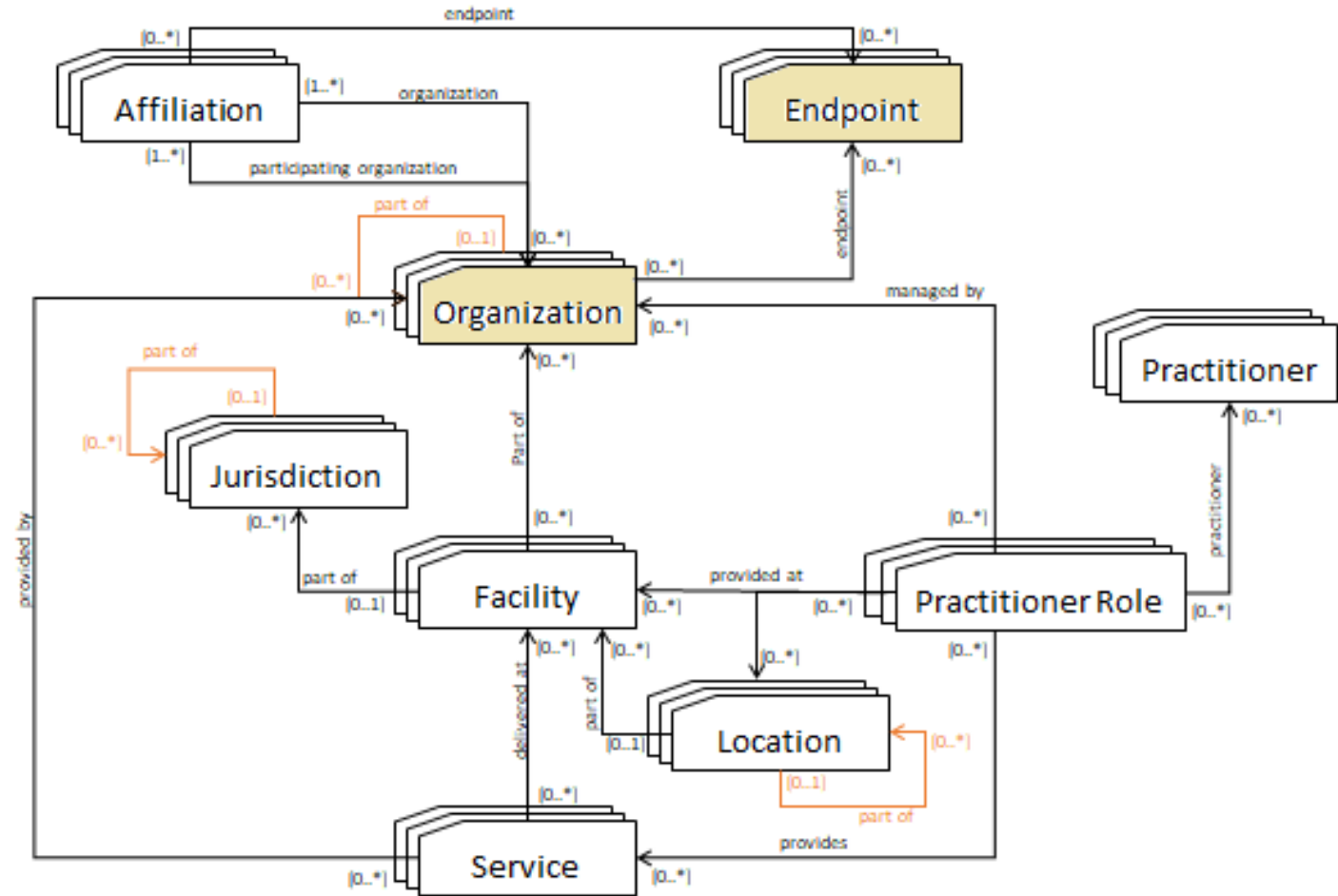




EHMI Endpoint Register (EER) – version 1

I version 1 fokuseres udviklingen af EER på mCSDs Organization og Endpoint ressourcer.

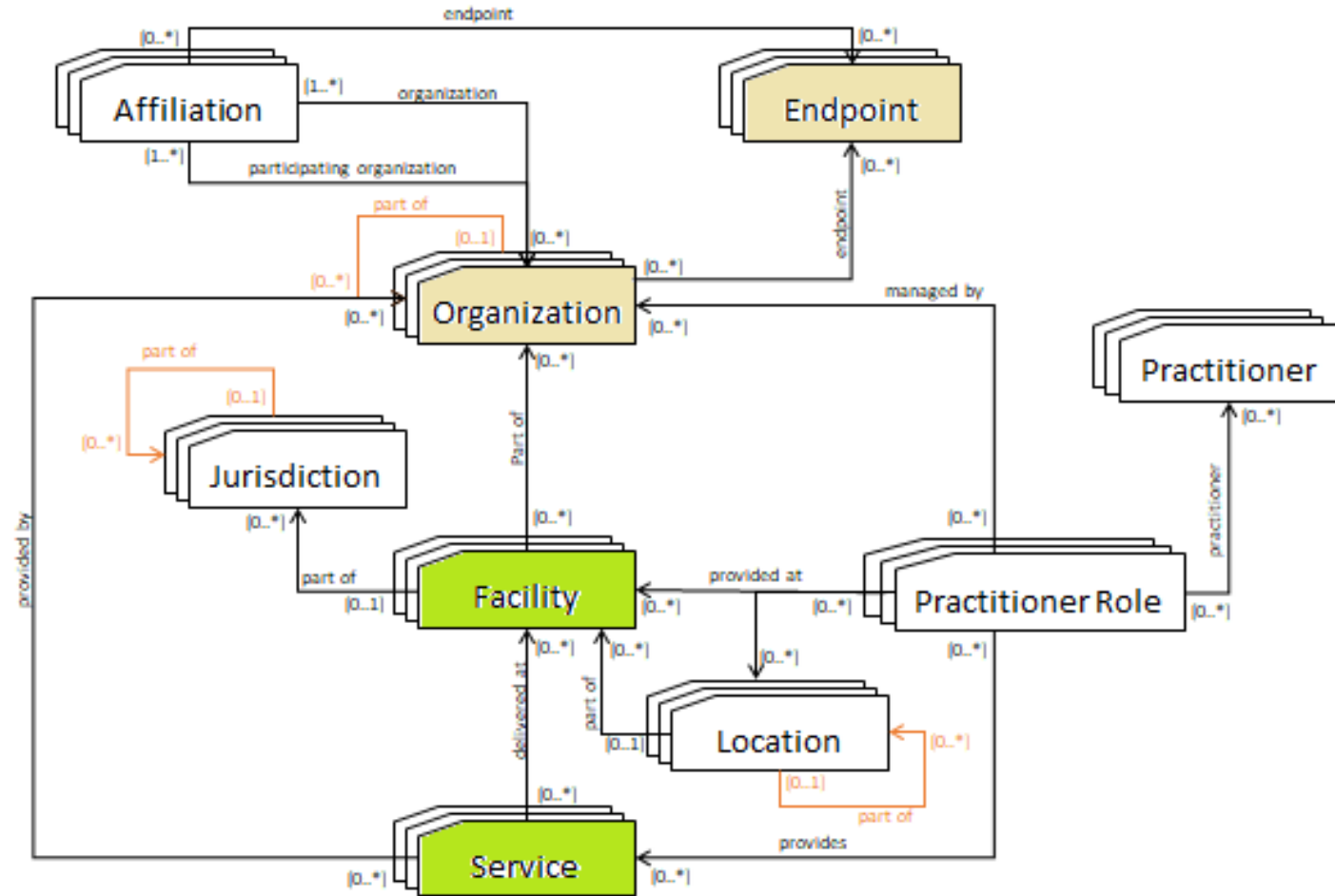
- De er de primære ressourcer ift. håndtering af den VANS-baserede udveksling i dag. Det svarer til en SOR-enhed og dens GLN-nummer





EHMI Endpoint Register (EER) – version 2

I version 2 bruger EER mere af mCSD ved at gøre brug af Facility og Service for at kunne håndtere metadata kravene fra pakketabellen.





Endpoint understøttelse i EER

Et endpoint i EER understøtter flere kommunikationsformer, blandt andre disse, som traditionelt bruges i sundheds-it kommunikation. Dette er en udvidelse ift. hvad SOR pt understøtter og gør det muligt i fremtiden at understøtte mere end bare meddelelseskommunikation via EHMI.



Meddelelses- kommunikation

Understøttelse af GLN nummer (lokationsnummer) endpoints og meddelelsestyper knyttet til en SOR-enhed.



Dokumentdeling

Understøttelse af dokumentdelings endpoints for en SOR-enhed i form af url'er. Kan knyttes til et GLN nummer også.



API

Understøttelse af API-endpoints, f.eks. REST eller SOAP baserede endpoints. REST er ofte forbundet med FHIR kommunikation.

Sikkerhed i EHMI

Alle services afvikles på sundhedsdatanettet (SDN)

Alle kommunikationsforbindelser mellem kommunikerende parter afvikles krypteret

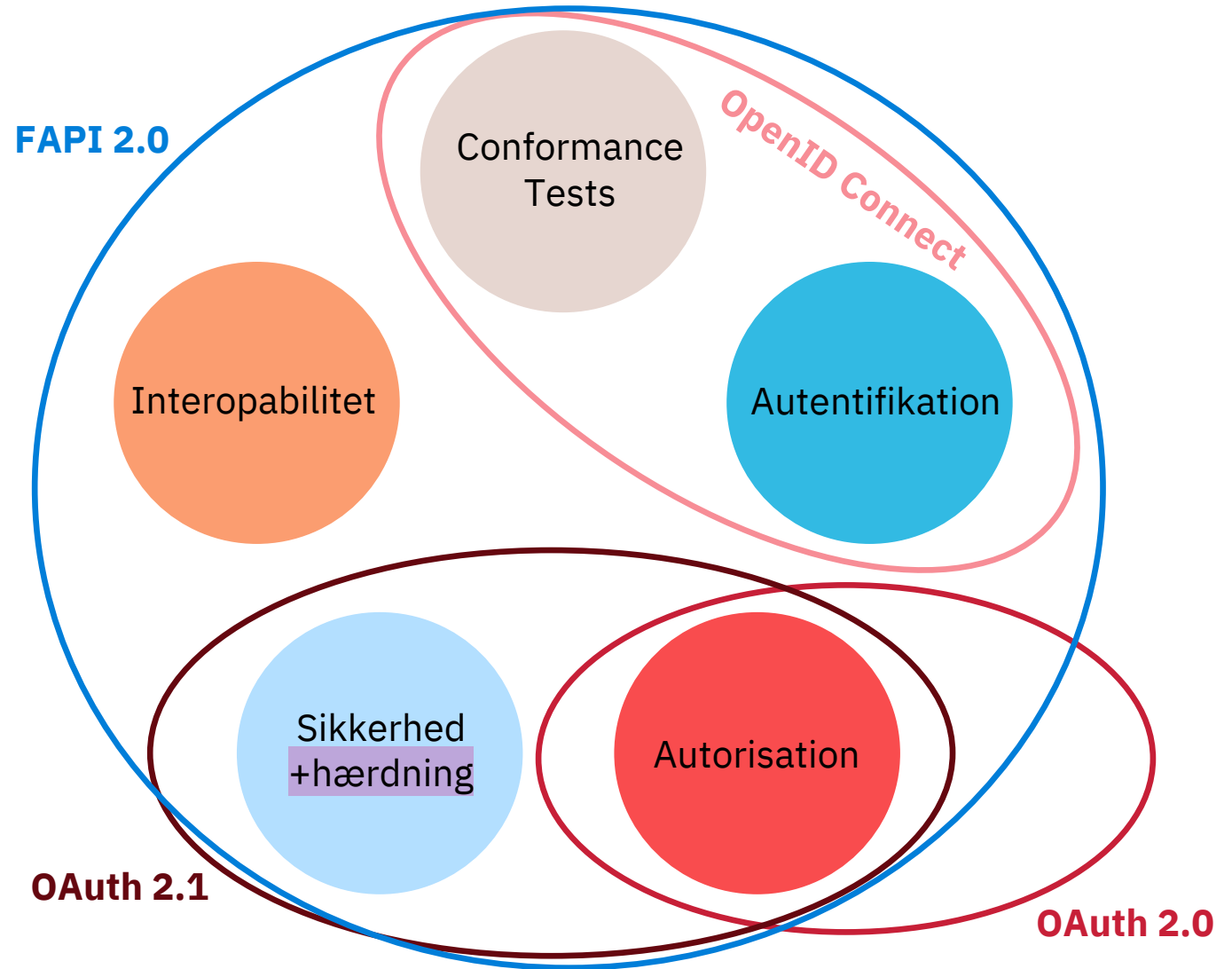
Derudover gælder FAPI 2.0 sikkerhedsprofilen for disse services i EHMI:

- EHMI Addressing Service
- EHMI Endpoint Register
- EHMI Delivery Service



OAuth sikkerhedsprofil: FAPI 2.0

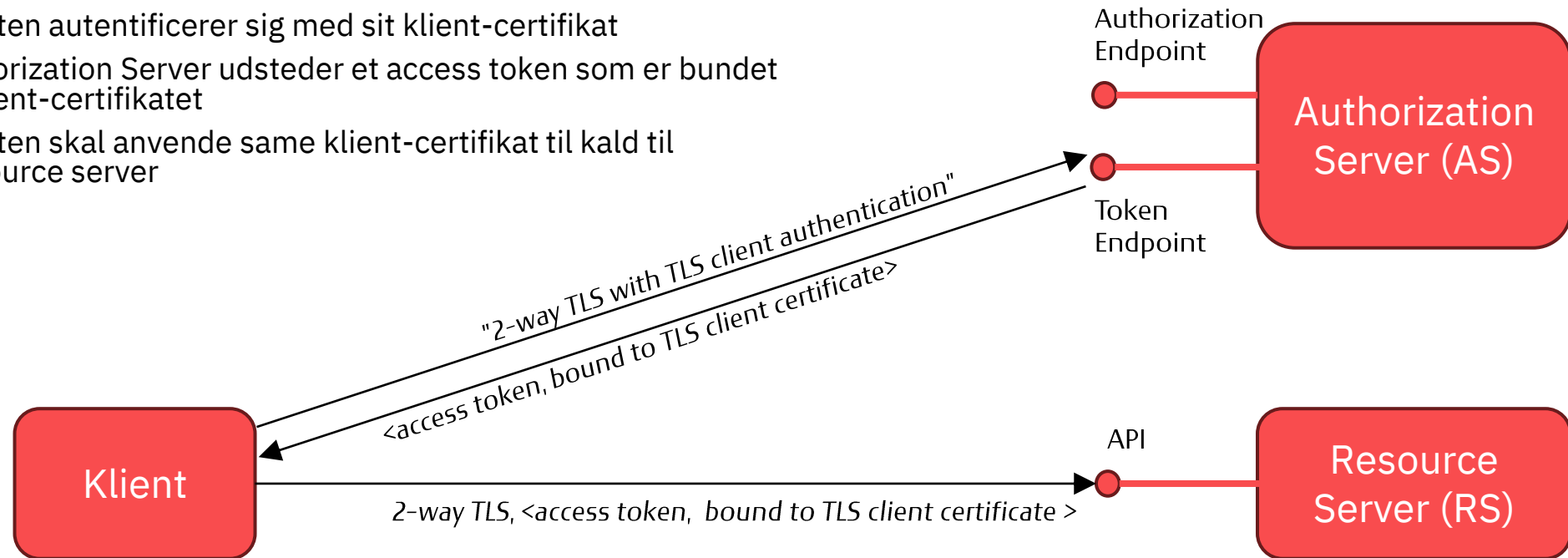
- Udgives af OpenID Foundation
- Generel sikkerhedsprofil til anvendelser med høje sikkerhedskrav (bank og finans, sundhedsvæsen etc.)
- Operationel profil, med klart definerede krav til de forskellige aktører
- Certificeringsprogram ved OpenID Foundation; katalog af certificerede produkter
- Sikkerhedsfeatures: Påkrævet klient-autentifikation, adgangsbilletter kryptografisk bundet til klienten
- Ikke bundet til FHIR, men kan anvendes sammen med FHIR (som i EHMI services), herunder SMART on FHIR





Sikkerhed i EHMI services – Systemkald til EER

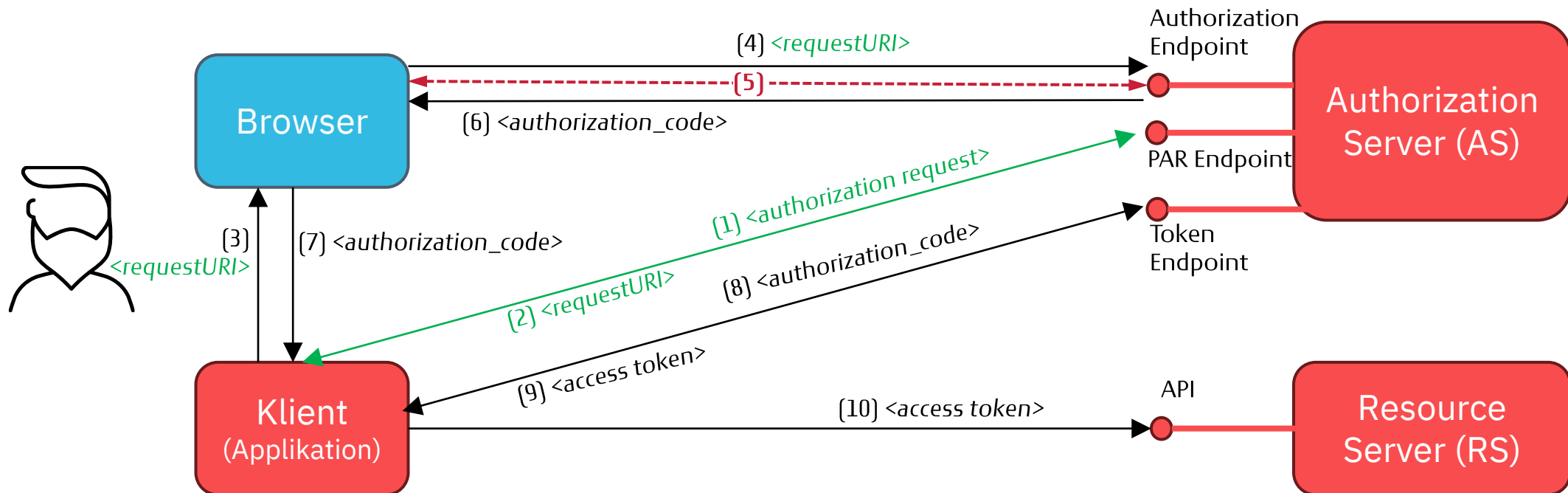
- Systemkald er baseret på mTLS (mutual TLS):
 - Klienten whitelistes i Authorization Server på forhånd
 - Klienten autentificerer sig med sit klient-certifikat
 - Authorization Server udsteder et access token som er bundet til klient-certifikatet
 - Klienten skal anvende same klient-certifikat til kald til ressource server





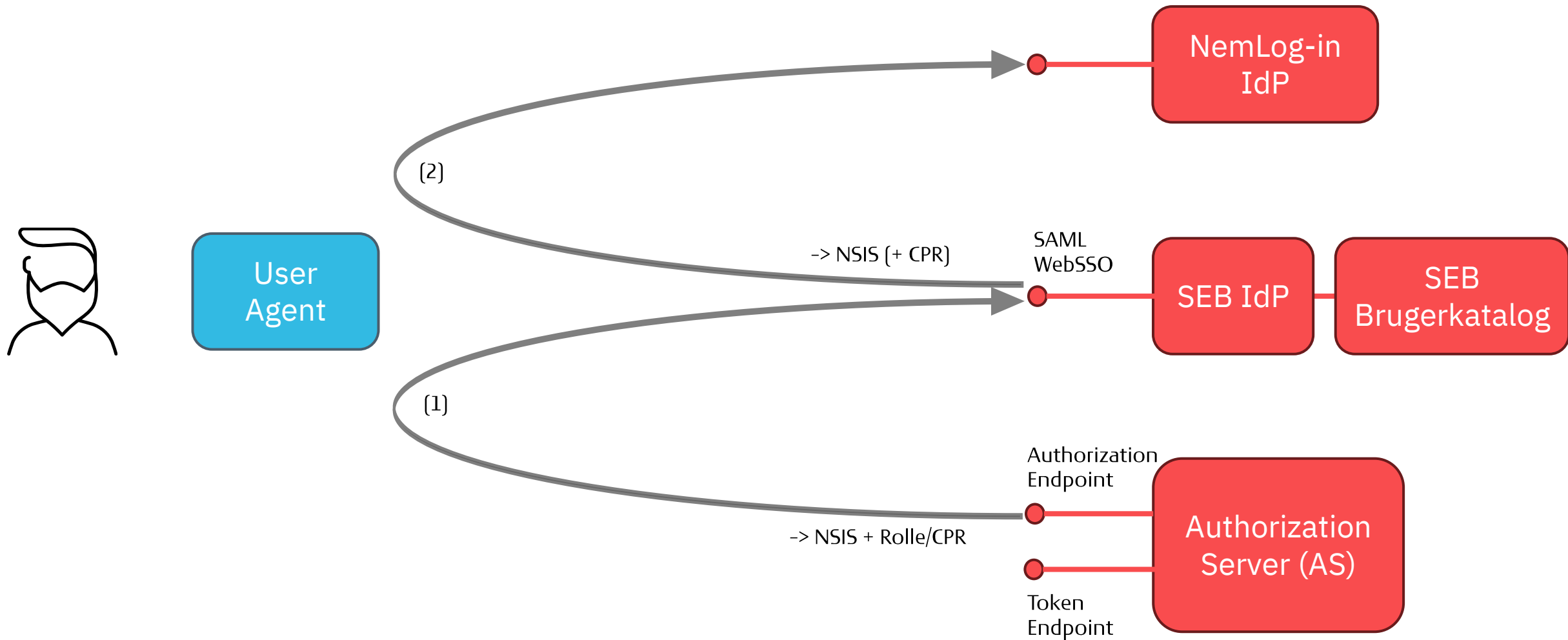
Sikkerhed i REST service – f.eks. EER Administration

- Udgangspunkt i OAuth 2.0 / OpenID Connect
- Behov for profilering: hvilke operationer skal man kunne udføre med en bestemt brugerprofil.





Bruger-autentifikation via SEB/NemLog-in – og rettigheder fra SEB brugerkataloget





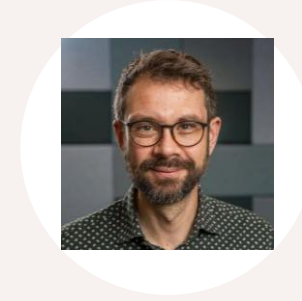
Tak!



Ole Vilstrup Møller

Standardiseringskonsulent
Digital Sundhed Danmark

ovi@medcom.dk



Christian Gasser

IT-arkitekt
Lakeside

chg@lakeside.dk