RAPPORT

2023

Målbillede for meddelelses-kommunikation på sundhedsområdet

SUNDHEDSDATA-
STYRELSEN

Resumé:
Et arkitekturmålbillede for meddelelseskommunikation på sundhedsområdet præsenteres. Målbilledets kerne er eDelivery, der er en standardiseret domæneneutral infrastruktur for effektiv meddelelseskommunikation udviklet i EU regi, som allerede anvendes på andre områder end sundhedsområdet i EU og herunder også Danmark, hvor den også tiltænkes en større rolle fremadrettet inden for andre domæner. Denne eDelivery kerne suppleres med forskellige tiltag og komponenter til gavn på sundhedsområdet.

Der er i eDelivery indbygget en meget høj grad af sikkerhed omkring forsendelsen af meddelelser ved anvendelse af både signering og kryptering samt tekniske kvitteringer, som sikrer både autenticitet, integritet, fortrolighed, og uafviselighed out of the box. Denne høje sikkerhed udbygges yderligere ved at meddelelseskommunikationen på sundhedsområdet skal foregå via sundhedsdatanettet. Herved samles meddelelseskommunikation på sundhedsområdet også med andre typer af kommunikation på sundhedsområdet, som webservice request/response, der netop foregår via sundhedsdatanettet.

Arkitekturen for meddelelseskommunikationen er lagdelt med det basale eDelivery lag i bunden. Her ovenpå er placeret et robust meddelelseslag med ekstra kvitteringer, der sikrer en pålidelig meddelelseskommunikation hele vejen fra afsender til modtager og giver en meget høj grad af sporbarhed. Oven på dette ligger forretningslaget, som understøtter de forskellige forretningsmæssige arbejdsgange, som involverer meddelelseskommunikation af varierende kompleksitet.

En fælles, centralt standardiseret, konvolut til meddelelserne på sundhedsområdet, inspireret af konvolutter fra lignende situationer, introduceres til at indeholde de relevante metadata om en meddelelse.

Dokumentdeling af de sendte meddelelser realiseres via opsamling af de sendte meddelelser og efterfølgende udstilling af samme i den nationale infrastruktur til både sundhedspersoner og borgere til gavn for borgernes patientsikkerhed.

Kontrol af forsendelsesstatus for meddelelser introduceres via opsamling af forsendelsesstatus på udvalgte punkter langs en meddelelses forsendelsesvej og efterfølgende udstilling af forsendelsesstatus via en service til både sundhedspersoner og borgere, der derved i nær realtid kan følge en meddelelses status (igen til gavn for borgerens patientsikkerhed).

I den eksisterende meddelelseskommunikation på sundhedsområdet er der identificeret udfordringer for en afsender med at finde rette modtager. For at løse dette vigtige problem introduceres derfor en ny national sundhedsadresseringsservice, der skal trække nødvendige informationer fra de rette autoritative kilder og udstille disse samlet til anvenderne af meddelelseskommunikationen, som derved kan blive hjulpet i at fremsøge den rette modtager.

Endelig introduceres rammerne for en styringsmodel for meddelelseskommunikationen, hvor der kan sættes fælles krav til infrastrukturkomponenterne og de deltagende systemer via forpligtende aftaler og politikker, og hvor der følges op på overholdelse af disse fælles krav.

Den samlede moderniserede infrastruktur for meddelelseskommunikation, der præsenteres, benævnes EHMI for ”Enhanced Healthcare Messaging Infrastructure”.

Udgiver	[Tekst]
Ansvarlig institution	[Tekst]
Design	[Tekst]
Copyright	[Tekst]
Version	1.0
Versionsdato	3. februar 2023
Web-adresse	www.sundhedsdata.dk
Titel	Målbillede for meddelelseskommunikation på sundhedsområdet

Vælg (eller skriv) tekst vedr. reference

Indhold

1. Indledning

1.1 Formål

Udarbejdelsen af målbilledet for meddelelseskommunikation på sundhedsområdet i Danmark udspringer ultimativt af strategien for digital sundhed 2018-2022 [SFDS-18-22]. I initiativerne i strategien indgår både en modernisering af infrastrukturen for meddelelseskommunikation og større anvendelse af datadeling. Derfor blev der i 2018 under ledelse af MedCom foretaget et første proof of concept (POC), hvor begge disse aspekter blev afprøvet. Helt konkret afprøvede man "eDelivery" som underliggende ny infrastruktur til meddelelseskommunikation i POC. eDelivery er en teknologi-arkitektur udviklet og afprøvet i EU-regi med deltagelse af flere medlemslande (herunder Danmark), der løbende vedligeholdes og allerede i dag sikrer sikker udveksling af data på andre områder end sundhedsområdet (bl.a. e-handel). eDelivery forventes også blive anvendt i næste generation af offentlig digital post i Danmark og er en central byggeblok i forhold til to af EU's store kommende implementeringer "Single Digital Gateway" [SDG] og "European Health Data Space" [EHDS].

Kort fortalt var anbefalingen fra POC, at man arbejdede videre mod at implementere eDelivery som en modernisering af den eksisterende teknologiske infrastruktur for meddelelseskommunikation og at implementere datadeling i form af opsamling af de meddelelser som sendes imellem parterne på sundhedsområdet i repositorier med derfra efterfølgende deling. Herunder anbefaledes det både at foretage en udvidet pilotafprøvning med fokus på mere avancerede og komplicerede dele af de to aspekter end adresseret i POC og, særlig relevant i forhold til nærværende dokument, at udarbejde et målbillede for meddelelseskommunikation. For yderligere detaljer se evalueringsnotatet for POC i reference [POCEVAL].

Målbilledet for meddelelseskommunikation på sundhedsområdet er bestilt af MedComs styregruppe [MC11-SG-7] og den tidligere første version af målbilledet havde til formål:

- At afklare de vigtigste arkitektoniske udeståender fra den første POC.
- At fastlægge den overordnede arkitektur for meddelelseskommunikation via eDelivery på sundhedsområdet og for deling af meddelelser på sundhedsområdet via repositorier for meddelelser.
- At guide den efterfølgende nævnte pilotafprøvning.
- At tjene som redskab til kommunikation med sundhedsområdets parter i dialogen om hvorledes meddelelseskommunikationsinfrastrukturen skal udvikle sig.

Den første version blev udarbejdet gennem en række workshops hvortil de centrale parter, der anvender meddelelseskommunikation, var inviteret. På de enkelte workshops blev forskellige centrale aspekter af målbilledet diskuteret på baggrund af oplæg og konsensus omkring em-

nerne derved opnået mellem deltagerne fra parterne – i enkelte tilfælde med hjælp fra eksterne interessenter (som repræsentanter fra patientforeningen Danske Patienter) og eksperter (som sundhedsjurister og netværkseksperter) i forhold til deltagergruppen i workshoprækken.

Nærværende reviderede version af målbilledet indeholder kvalitetssikrende ændringer foranlediget dels af de erfaringer, der er blevet gjort i pilotafprøvningen og fastholdt i den dertilhørende evalueringsrapport [PILEVAL], og dels den dialog, der har været med it-arkitekturfora hos forskellige parter på sundhedsområdet med udgangspunkt i første version af målbilledet. Den nuværende version skal præsenteres for det rådgivende udvalg for standarder og arkitektur på sundhedsområdet (RUSA), der skal afgøre om det kan godkendes og publiceres umiddelbart eller skal sendes i offentlig høring. Sidstnævnte vil kunne give anledning til en yderligere revideret version og efterfølgende genbehandling i RUSA. Den reviderede version efter endt behandling i RUSA (af en eller to omgange) vil have til formål:

- At guide den efterfølgende implementering af meddelelseskommunikation på sundhedsområdet.
- At guide den efterfølgende implementering af deling af meddelelser på sundhedsområdet via repositorier for meddelelser.

Implementeringen planlægges at foregå trinvis startende med en produktionspilot, der alene omhandler en enkelt ny meddelelsestype med et begrænset sæt af deltagere. På den måde vil man uden at påvirke den eksisterende kritiske meddelelseskommunikation kunne gøre sig de første produktionserfaringer med den nye implementerede infrastruktur og dens muligheder samt etablere den nødvendige governance derom. Efter produktionspiloten følger en stor og langvarig trinvis migrering af den eksisterende meddelelseskommunikation til den nye infrastruktur meddelelsestype for meddelelsestype.

Dette motiverer udarbejdelsen af målbilledet for meddelelseskommunikation på sundhedsområdet og forklarer den proces, der har ligget til grund for udarbejdelsen. For yderligere detaljer se også reference [POCEVAL, MC11-SG-7, PILEVAL].

Resultaterne af hele arbejdet er udmøntet i dette dokument, der detaljeret beskriver de forskellige aspekter ved målbilledet. Da målbilledet er udarbejdet i samarbejde mellem de centrale parter på sundhedsområdet, der anvender meddelelseskommunikation, beskriver målbilledet fælles forpligtende retningsvisende rammer, som parterne skal følge i det videre arbejde med meddelelseskommunikation på sundhedsområdet.

I dette indledende kapitel præsenteres formålet med og baggrunden for udarbejdelsen af målbilledet – herunder sammenhængen med centrale strategier og øvrige målbilleder på sundhedsområdet [SFDS-18-22, MFDFS] samt definitionen af centrale begreber. Dernæst følger et kapitel med fokus på strategiske aspekter: Interessenter (og disses interesser), drivere, vision, mål og gevinster, samt kvaliteter og principper. Derefter følger først et kapitel om relevante juridiske

aspekter og dernæst et kapitel med forretningsmæssige aspekter – herunder særligt user stories. Herefter følger kapitler, der omhandler de øvrige arkitekturperspektiver information, applikationer, teknologi, og sikkerhed, samt et kapitel om governance. Endelig afsluttes dokumentet, på nær appendiks, med et kapitel, der beskriver den videre udvikling af målbilledet.

Teknisk orienterede læsere, som f.eks. it-arkitekter, anbefales at læse hele denne målbillederapport. Ikke-teknisk orienterede læsere, som f.eks. ledelsesrepræsentanter og projektledere, anbefales som minimum at læse kapitlerne 1-3 og 8, og derudover efter interesse udvalgte afsnit af kapitel 4. Såfremt læseren ikke er bekendt med strategien for digital sundhed 2018-2022 [SFDS-18-22], anbefales det at orientere sig i denne som yderligere baggrundslæsning.

1.2 Indhold og afgrænsning

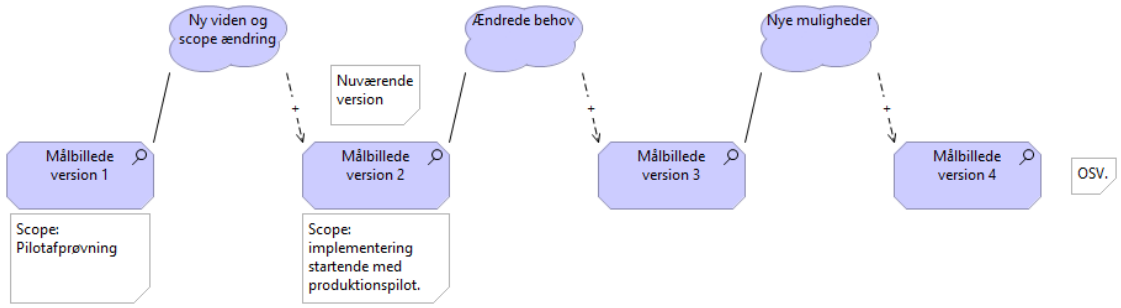
1.2.1 Hvad er et målbillede?

Et målbillede beskriver en ønsket fremtid. Målbilledet er en konkretisering af en overordnet vision. Emnerne, som behandles i målbilledet, er erfaringsmæssigt væsentlige at afdække i forbindelse med en digital transformation. Målbilledet giver et godt afsæt for en mere præcis beskrivelse af resultatet af transformationen (*target architecture*), der sammen med en beskrivelse af transformationens udgangspunkt (*baseline architecture*) og beskrivelser af mellemliggende "trædesten" (*transition architectures*), danner grundlaget for et professionelt styret arbejde med den digitale transformation. Målbilledet dækker ikke detaljeret arkitekturbeskrivelse, gapanalyse, roadmap, kravspecifikation, og implementering og test, men sætter rammerne for dette videre arbejde[1]. Hensigten med at udarbejde et målbillede er at sikre en fælles retning for den videre udvikling. Behandlingen af emner, hvis afklaring ikke har haft betydning for fastlæggelsen og forståelsen af den overordnede retning, er blevet udskudt til det efterfølgende arbejde. Det er således vigtigt at understrege, at arkitekturarbejdet med meddelelseskommunikation på sundhedsområdet ikke stopper med målbilledet. Der er dels et ikke-trivielt efterfølgende mere detaljeorienteret arbejde af betydeligt omfang, der skal udføres, og desuden en meget vigtig opgave med at sikre økonomisk opbakning til implementering af den arkitektur målbilledet rammesætter. Konkrete emneinput til dette efterfølgende arbejde er givet i bilag 1 *Kommende afklaringer*. Det betyder også, at man fortsat må forvente afklaring og specifikation i forbindelse med efterfølgende projekter (dette er ikke klaret med målbilledet alene).

Målbilledet præsenteret i dette dokument må ikke betragtes som statisk. Det skal genbesøges og justeres med jævne mellemrum, så det afspejler den aktuelle virkelighed og den viden man måtte have om denne. Eksempelvis vil arbejdet med at konkretisere arkitekturen og specificere, implementere og anvende løsninger bidrage med ny viden, der bør tages højde for i fremtidige versioner af målbilledet (herunder f.eks. også de erfaringer, der er blevet gjort i pilotafprøvningen). Desuden forandrer verden sig; nye muligheder opstår og behov ændres. Dette er illustreret

[1] Benytter man sig af den fællesoffentlige arkitekturmetode, baseret på det internationale TOGAF rammeværk [TOGAF] svarer dette til, at vi med målbillede-arbejdet udfører fase A og dermed lægger grunden for faserne B-G.

i følgende figur, hvor det samtidig er illustreret hvor den nuværende version af målbilledet befinder sig, jf. diskussionen ovenfor i afsnit 1.1:



Figur 1: Et målbilledes udvikling i takt med f.eks. ny viden, ændrede behov, og nye muligheder.

Det vil derfor være hensigtsmæssigt om man med mellemrum forholder sig til, om målbilledet fortsat har rette scope og peger i den ønskede retning[2]. Disse emner diskuteres yderligere i kapitel 8 i dette målbillede.

1.2.2 Hvad er meddelelseskommunikation?

Meddelelseskommunikation i titlen *Målbillede for meddelelseskommunikation på sundhedsområdet* skal i en vis forstand forstås bredt i overensstemmelse med formålsafsnittet ovenfor. Dvs., det dækker over begge følgende typer:

1. asynkron punkt til punkt kommunikation af strukturerede patient/borgercentrerede meddelelser fra afsender til af afsender kendt modtager (også kaldet meddelelseskommunikation ved videregivelse)
2. deling hvor de i punkt 1 sendte meddelelser opsamles i et repositorie, hvorfra andre modtagere kan hente meddelelsen enten efter at være blevet notificeret om dem eller på anfordring (også kendt som meddelelseskommunikation ved forespørgsel). Ved deling af meddelelser forstås således, at man i et repositorie kan hente de enkelte sendte meddelelser, præcis som de så ud, da de blev sendt.

Meddelelseskommunikation ved videregivelse er særlig relevant ved sektorovergange på sundhedsområdet og anvendes når en organisation (f.eks. et hospital) ønsker at starte en bestemt forretningsproces (f.eks. iværksæt genoptræning) hos en anden organisation (f.eks. en kommune).

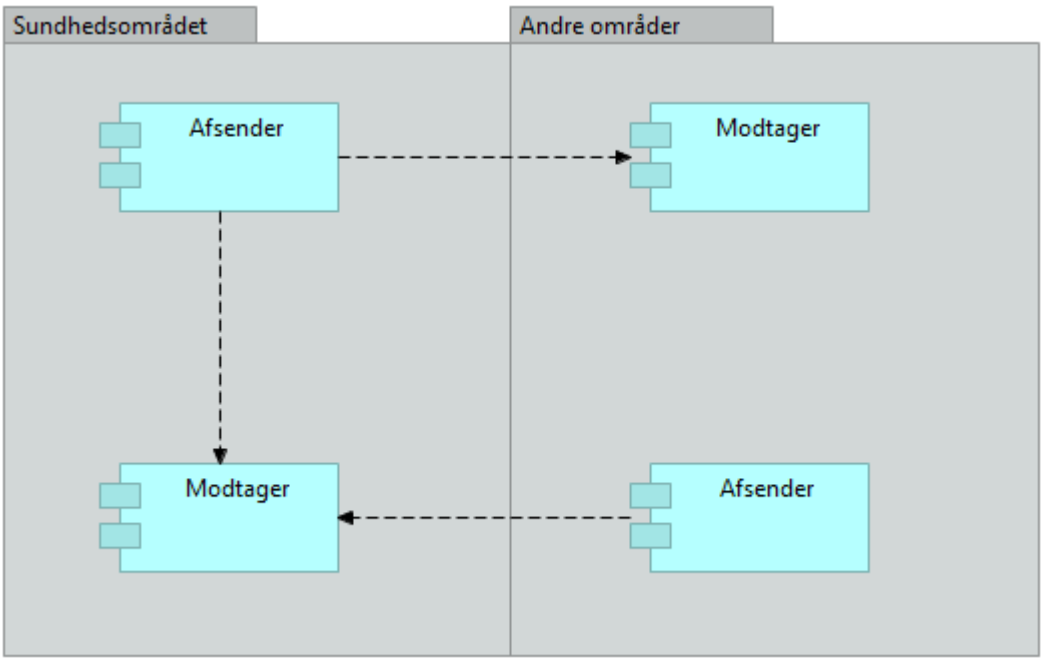
Meddelelseskommunikation ved forespørgsel og muligheden for at abonnere på meddelelser udsendt ved bestemte hændelser understøttes principielt allerede i dag. De foreslåede løsninger i dette målbillede moderniserer primært den infrastruktur, som i dag benyttes til forsendelse (meddelelseskommunikation ved videregivelse), og denne skal spille sammen med andre med-

[2] Igen, i TOGAF-termer [TOGAF] svarer dette til fase H, der kan udløse en ny fase A med et efterfølgende gennemløb af de øvrige faser B-G.

delelsesdistributionsløsninger. Et eksempel på dette er, at man kan benytte eksisterende infrastruktur til at give muligheder for at forespørge på meddelelser afsendt i infrastrukturen (og opsamlet i repositorier). Det er tilsvarende relevant, at man også kan benytte eksisterende mekanismer til at advisere relevante parter om, at bestemte meddelelser er blevet sendt og opsamlet (f.eks. at der er sendt en advisering om indlæggelse eller udskrivelse). Disse samspil behandles i målbilledet, men dog i mindre detalje end forsendelsesinfrastrukturen.

1.2.3 Afgrænsninger i forhold til sundhedsområdet

Sundhedsområdet er principielt defineret som det område, der er underlagt sundhedsloven, men meddelelseskommunikation på sundhedsområdet i titlen skal ligeledes forstås i bred forstand, og er derfor ikke udelukkende meddelelseskommunikation internt mellem de forskellige sektorer (som hospitaler, hjemmepleje, praktiserende læger, og speciallæger) på sundhedsområdet. Det inkluderer også meddelelseskommunikation mellem sundhedspersoner og borgerne, samt meddelelseskommunikation ind og ud af sundhedsområdet fra/til andre domæner (som f.eks. mellem jobcentre og praktiserende læger). Dette er illustreret i følgende overordnede figur, hvor kun de primære meddelelser (fra afsender til modtager) er medtaget, og alle detaljer angående f.eks. kvitteringer og eventuelle mellemstationer imellem en afsender og en modtager for overskuelighedens skyld er udeladt:



Figur 2: Meddelelseskommunikation på sundhedsområdet i scope for dette målbillede.

1.3 Baggrund

1.3.1 Eksisterende meddelelseskommunikation

Den eksisterende baseline arkitektur for meddelelseskommunikation på sundhedsområdet anvender VANS-nettet, som bygger på et koncept og et teknologisk fundament, der blev skabt omkring 1990 (Amagerprojektet 1989-1990, se [MC-S86]). Her bestyrer såkaldte VANS-leverandører elektroniske postkasser for parterne og VANS-leverandørerne udveksler meddelelser indbyrdes. Meddelelserne har et standardiseret indhold og meddelelsesformatet følger UN EDIFACT formatet. I 1994 blev MedCom etableret som et tværgående samarbejdsprojekt, der havde til formål at udvikle landsdækkende standarder for de hyppigst anvendte meddelelsestyper i sundhedssektoren.

Der er løbende sket teknologiske forbedringer af infrastrukturen (f.eks. er opkaldsforbindelser erstattet af VPN-forbindelser over Internet og EDIFACT-formatet er suppleret af et XML-baseret format), men det grundlæggende koncept er det samme. Der har periodevis været tilløb til en mere grundlæggende modernisering, men den er endnu ikke foretaget.

I 2003 etablerede MedCom det såkaldte Internetbaserede Sundhedsdatanet. Visionen bag dette var, at man skulle kunne imødekomme de væsentligste behov for elektronisk kommunikation og information i sundhedssektoren gennem anvendelse af standard-internetteknologi. Ud over at tilbyde nye muligheder for kommunikation (f.eks. Web opslag) tillod det Internetbaserede sundhedsdatanet også kommunikation af EDIFACT beskeder via SMTP (e-mail). Men der forelå ikke en klar beskrivelse af, hvad der samlet skulle til for at skabe sikker og troværdig kommunikation, og sundhedsvæsenets parter gik ikke denne vej.

I 2012-2013 blev projektet "Teknologisk fremtidssikring af MedCom-kommunikationen" gennemført [MC8-SG-4]. Projektet søgte indledningsvis at afdække de behov parterne så for forandring. Et af de væsentligste behov vedrørte hurtigere og mere stabil transport, hvor beskeder ikke bliver væk, og hvor der er bedre mulighed for fejlfinding. Et andet vigtigt behov vedrørte bedre ændrings- og versionsstyring ift. MedCom standarderne. Der blev også udtrykt en bekymring i forhold til, hvordan aldrende teknologi og anvendelsen af rent danske standarder påvirker konkurrencesituationen negativt med risiko for dårligere service og højere priser. Det blev kort bemærket, at VANS-leverandørerne autentificerer brugere ved en kombination af brugernavn, kodeord og lokationsnummer (og ikke med digitale certifikater), hvilket kun giver lav sikkerhed for at afsender og modtager er de rette, men ellers var parterne ikke fokuseret på de sikkerhedsmæssige aspekter.

Med inspiration fra NemHandelsløsningen, der netop havde afløst en VANS/EDIFACT-baseret løsning på handelsområdet, ønskede MedCom at gå i samme retning [MC8-SG-5, MC8-SG-6]. Parterne bag MedCom var imidlertid ikke overbevist om, at de væsentligste udfordringer ikke

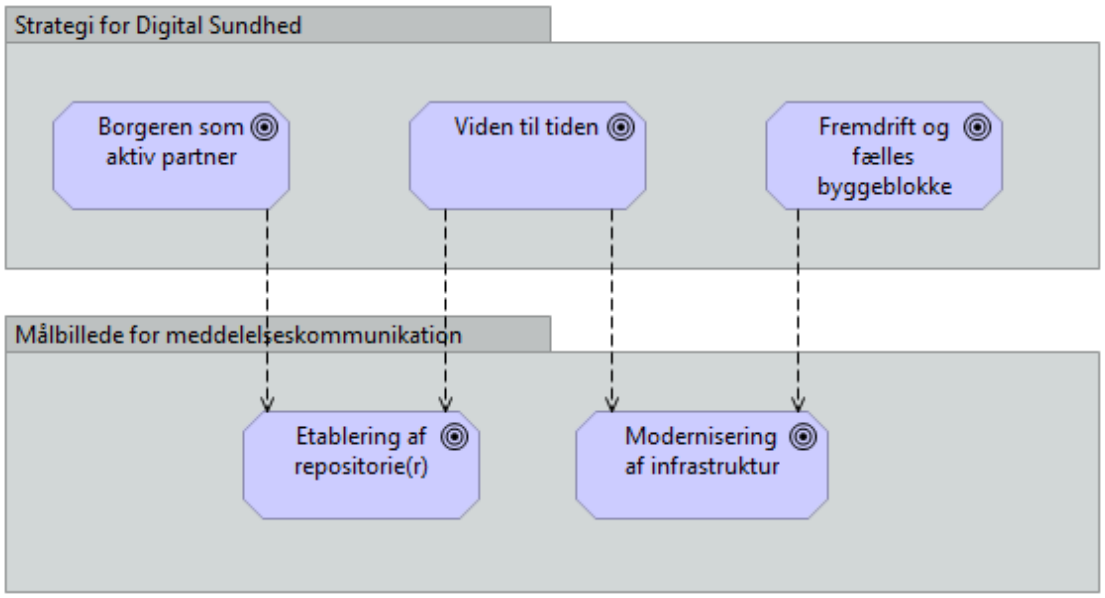
kunne løses ved optimering af infrastruktur og processer inden for det eksisterende setup. Efterfølgende har MedCom professionaliseret processer vedr. versions- og ændringsstyring, men etableringen af et samlet forpligtende SLA (Service Level Agreement) apparat, der dækker hele kommunikationen fra afsender til modtager, udestår stadig.

1.3.2 Sammenhæng med strategien for digital sundhed

Som nævnt ovenfor er målbilledet motiveret af og helt i tråd med strategien for digital sundhed 2018-2022 [SFDS-18-22]. Nærmere bestemt spiller målbilledet direkte ind i tre af de fem indsatsområder fra nævnte strategi:

- Borgeren som aktiv partner.
- Viden til tiden.
- Fremdrift og fælles byggeblokke.

Sammenhængen er illustreret i følgende figur:



Figur 3: Sammenhæng mellem Strategi for Digital Sundhed 2018-2022 [SFDS-18-22] og målbilledet for meddelelseskommunikation.

Etablering af services rettet mod borgere og sundhedspersoner baseret på et eller flere repositorie(r) for meddelelser vil dels kunne give borgeren adgang til meddelelser om sig selv (indsatsområdet *Borgeren som aktiv partner*), og dels kunne give bredere adgang for sundhedspersoner til meddelelser om borgeren (indsatsområdet *viden til tiden*).

Modernisering af infrastrukturen for meddelelseskommunikation vil dels bidrage direkte til *Bedre, hurtigere og mere sikker digital kommunikation mellem sektorer,* som er et initiativ under *Viden til tiden* [SFDS-18-22], hvori der eksplicit står:

”For at understøtte hurtigere, mere sikker og fleksibel kommunikation har initiativet til formål at gennemføre en modernisering af det tekniske grundlag for kommunikationen, så der frem

for punkt-til-punkt kommunikation, hvor kommunikationen sker fra én bestemt afsender til én bestemt modtager, igangsættes en omlægning til online deling af data og mere tidssvarende og mere sikre teknologiske platforme."

Desuden vil det bidrage direkte til initiativet om *Langsigtet målbillede for den fælles it-infrastruktur* under indsatsområdet *Fremdrift og fælles byggeblokke*, hvori der eksplicit står:

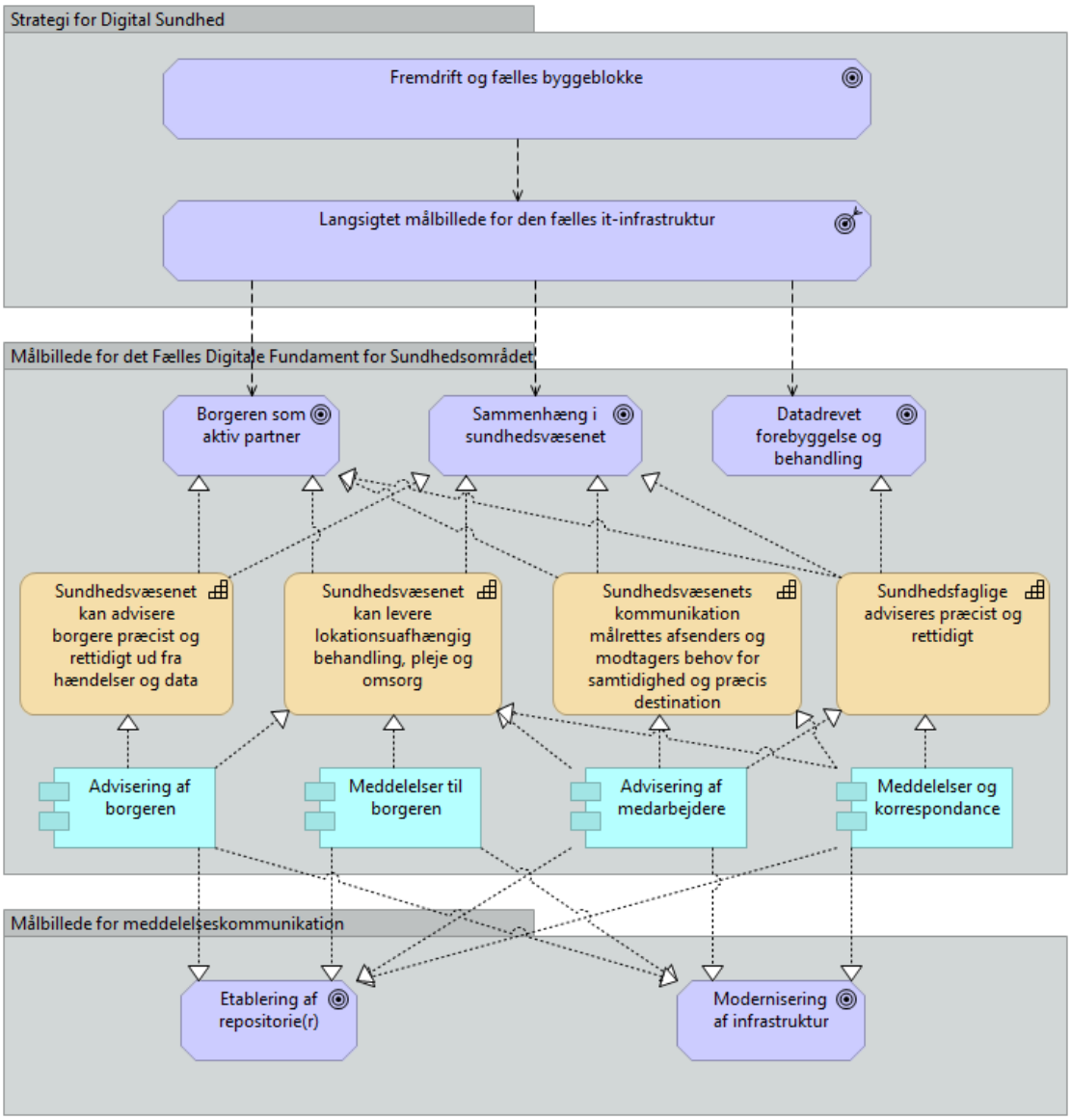
"Arbejdet med at binde it-systemerne på sundhedsområdet bedre sammen skal ske med udgangspunkt i en sikker, robust og skalerbar fælles infrastruktur, der er baseret på åbenhed og leverandøruafhængighed. Samtidig skal infrastrukturen også følge med udviklingen, så den understøtter løsninger, der bygger på nye teknologier."

1.3.3 Sammenhæng med målbilledet for det fælles digitale fundament på sundhedsområdet

Et hovedprodukt under initiativet *Langsigtet målbillede for den fælles it-infrastruktur* [SFDS-18-22] er *Målbilledet for det fælles digitale fundament på sundhedsområdet* [MFDFS]. I dette, i forhold til nærværende, mere overordnede målbillede, opereres med temaer på overordnet niveau. Der er tre temaer og nærværende målbillede spiller direkte ind i alle tre:

- Borgeren som aktiv partner.
- Sammenhæng i sundhedsvæsenet.
- Datadrevet forebyggelse og behandling.

I [MFDFS] opereres der under temaerne hierarkisk med mål, delmål, og evner (også kendt som kapabiliteter), hvor evnerne realiseres via byggeblokke. Målbilledet for meddelelseskommunikation er med til at definere fire af disse byggeblokke, som illustreret i følgende figur, hvor kun udvalgte kapabiliteter er medtaget og mål og delmål helt udeladt for overskuelighedens skyld:



Figur 4: Sammenhæng mellem Målbillede for det Fælles Digitale Fundament for Sundhedsområdet [MFDFS] og målbilledet for meddelelseskommunikation.

Som sådan er målbilledet for meddelelseskommunikation med til at definere fire af de fem byggeblokke inden for kommunikationsområdet i *Målbilledet for det fælles digitale fundament på sundhedsområdet* [MFDFS], og må derfor betegnes som centralt herfor.

1.4 Centrale begreber

Følgende tabel indeholder kun udvalgte centrale begreber, der anvendes ofte i målbilledet, og må således ikke opfattes som en udtømmende begrebsliste.

Foretrukken term	Accepteret term	Definition
Sundhedsområdet	Sundhedsdomænet	Det område, som er underlagt sundhedsloven

Foretrukken term	Accepteret term	Definition
Meddelelse	Besked	En unikt identificeret, velstruktureret og standardiseret samling af data relateret til en borger, der indpakket i en konvolut sendes elektronisk fra en afsender til en modtager
Konvolut		En unikt identificeret, velstruktureret og standardiseret samling af data, der indeholder metadata om den meddelelse konvolutten derudover indpakker
eDelivery		Standardiseret infrastruktur til forsendelse af meddelelser udviklet i EU regi
System		Centralt begreb i eDelivery arkitekturen for et IT-system, der enten afsender eller modtager meddelelser
Access-punkt	Access point	Andet centralt begreb i eDelivery arkitekturen for en komponent, der efter indgået aftale med et system agerer på systemets vegne i forbindelse med meddelelseskommunikation og dermed giver systemet adgang til eDelivery meddelelseskommunikationsnetværket
eDelivery Domæne	Domæne	Et velafgrænset område indenfor eDelivery med sine egne meddelelsestyper, egne SLA-krav, og egen governance
Governance	Styringsmodel	Fora, roller og ansvar, processer, aftaler, regler og praksis, der anvendes til at styre et område.
Pilotafprøvning		Afprøvning i testmiljø i meget lav skala. Afprøver arkitekturen og konfigurationen af de involverede komponenter med forskellige typiske forretningsrelevante flow af meddelelser.
Produktionspilot		Afprøvning i produktionsmiljø i lav skala med få aktører og begrænset antal meddelelser. Er med til at fange ”børnesygdomme” og giver læring ift. justering af initiel governance setup.

2. Strategisk

2.1 Interessenter og interesser

De vigtigste interessenter og deres overordnede interesser, hvoraf nogle går igen på tværs af de forskellige interessenter, er som følger:

- Parterne på sundhedsområdet, der anvender meddelelseskommunikation:
  - Er interesseret i at have en effektiv, standardiseret, sikker og robust infrastruktur til meddelelseskommunikation med høj oppetid og minimale udfald samt hurtig levering af meddelelser.
  - Er interesseret i at det er let at koble sig til infrastrukturen for meddelelseskommunikation og angive hvilke typer af meddelelser man understøtter.
  - Er interesseret i at have nogle klare og let anvendelige rammer for implementeringen af meddelelseskommunikation i deres applikationslandskab, eksempelvis til kravsætning over for leverandører.
- Borgere, der dels deltager direkte i meddelelseskommunikation og dels modtager behandling fra sundhedsvæsenet:
  - Er interesseret i let at kunne deltage som aktiv part i meddelelseskommunikationen omkring dem, enten på egne eller andres vegne (typisk pårørende), med parterne på sundhedsområdet.
  - Er interesseret i at have en effektiv, standardiseret, sikker og robust infrastruktur til meddelelseskommunikation med høj oppetid og minimale udfald samt hurtig levering af meddelelser af hensyn til deres behandlingsforløb og patientsikkerhed.
- Leverandører af komponenter til meddelelseskommunikation på sundhedsområdet
  - Er interesserede i at have klare specifikationer for deres udvikling og implementering til rådighed.
  - Er interesserede i at deres udviklede komponenter er så tilpas generiske, at de vil kunne genbruges i andre lignende sammenhænge.
- Parter, der grænser op til sundhedsområdet, i den forstand at de deltager i meddelelseskommunikation ind og ud af sundhedsområdet:
  - Er interesserede i let at kunne koble sig på og deltage i den standardiserede meddelelseskommunikation med parter fra sundhedsområdet.
  - Er interesseret i at have en effektiv, standardiseret, sikker og robust infrastruktur til meddelelseskommunikation med høj oppetid og minimale udfald samt hurtig levering af meddelelser.

2.2 Hvad driver udviklingen?

Arbejdet med dette målbillede er fortsat styret af behovet for at skabe en robust og effektiv infrastruktur til understøttelse af meddelelseskommunikation, men i forhold til tidligere er der i

dag større fokus på sikkerhed. Sundhedsområdet er udpeget som en særlig samfundskritisk sektor (sammen med finans-, tele-, søfarts-, transport- og energisektoren), hvorfor der er særlige krav til beskyttelse imod bl.a. cyber-angreb. Her er sikkerhedsniveauet i den nuværende infrastruktur problematisk.

Den aldrende teknologi og anvendelsen af rent danske standarder og den deraf følgende indsnævring af leverandørfeltet er heller ikke alene en risiko i forhold til dårligere service og højere priser. I dag er kritisk kommunikation på sundhedsområdet gjort afhængig af, om private leverandører ser en forretning i at drive kommunikationen. Og mulighederne for at skabe forretning på transport af asynkrone meddelelser bliver ikke bedre efterhånden som kommunikation på forskellige områder omlægges til andre kommunikationsmønstre (f.eks. ved opslag eller abonnerings- og publiceringsservices).

Der kan af hensyn til forsyningssikkerheden være behov for, at kritiske delløsninger kommer under offentlig kontrol og/eller, at der åbnes op for markedet igen ved at kunne invitere leverandører ind, der også leverer nogle af de samme ydelser til øvrige dele af den offentlige sektor (og den private sektor). Eller som leverer tilsvarende løsninger på et internationalt marked.

Sikkerhedsmæssige og markedsmæssige udfordringer vil ikke alene kunne løses som optimeringer inden for eksisterende rammer, men kræver modernisering af selve fundamentet for den meddelelsesbaserede kommunikation. Det skal i denne sammenhæng bemærkes, at der i dag benyttes et antal forskellige distributionsmekanismer til strukturerede meddelelser, der ikke alene tæller VANS-leverandører, men også blanket-løsninger, meddelelseshoteller mm. – med hver deres driftskvalitet, serviceniveau og sikkerhedsniveau. Der ligger et potentiale i at konsolidere disse løsninger eller dele heraf – ikke mindst, hvis man ønsker at sikre ensartede service- og sikkerhedsniveauer, der ville blive dyrt at gennemføre i flere løsninger og supportorganisationer.

Som beskrevet i afsnit 1.3 er der også nogle forretningsstrategiske grunde til at modernisere infrastrukturen. Opsamling og opbevaring af meddelelser vil medvirke til at styrke samarbejdet mellem sundhedspersoner, og det medvirker til at inddrage borgeren mere aktivt i egen behandling. Opsamlingen af oplysninger om den pågåede kommunikation kan være en vigtig kilde til at skabe mere ”intelligente” løsninger (f.eks. støtte til sundhedspersoners eller borgeres fremsøgning af parter og relevante tilbud) og analyser (der f.eks. kan give viden om hvorledes forskellige parter inddrages i de enkelte patientforløb).

Motivationen bag det forslag til rammer for modernisering, som udfoldes i dette målbillede, kan kort opsummeres ved nedenstående:

1. Der er fortsat brug for at nedbringe antallet af forsendelsesfejl, forsinkelser og fejlforsendelser og at øge hastigheden hvormed disse opdages og afhjælpes
2. Der er behov for at etablere en teknologisk tidssvarende infrastruktur, der kan leve op til den grad af beskyttelse overfor cyber-angreb, som er nødvendig for en samfundskritisk

sektor, og hvor der er høj sikkerhed for fremtidig drift, support, vedligehold og videre udvikling af infrastrukturen

3. Der er brug for at udbygge infrastrukturen, hvis man skal indfri nationale målsætninger om bedre sammenhæng i behandling, aktiv borgerinddragelse og datadrevet forebyggelse og behandling
4. Der er behov for at sikre, at der arbejdes med en økonomisk rationel infrastruktur – også på sigt

2.3 Vision

Arkitekturvisionen for målbilledet for meddelelseskommunikation er:

> *Effektiv digital meddelelseskommunikation på sundhedsområdet til gavn for borgere og sundhedspersoner via en sikker, robust, skalerbar generel infrastruktur baseret på velafprøvede åbne internationale standarder*

Betydningen af udvalgte nøgleord i visionen kan uddybes ved:

- Effektiv: Dækker over at meddelelser, der sendes via infrastrukturen ikke forekommer forsinket fra hverken afsenderens eller modtagerens perspektiv. En meddelelse bliver således afleveret til bestemmelsesstedet i infrastrukturen på det tidspunkt både afsenderen og modtageren af meddelelsen forventer det. Relaterer sig til punkt 1 i listen i afslutningen af driver afsnittet.
- Digital meddelelseskommunikation: Dækker både over meddelelseskommunikation ved videregivelse og meddelelseskommunikation ved forespørgsel (som i afsnit 1.2 ovenfor).
- Sundhedsområdet: Dækker meddelelseskommunikation både mellem forskellige sektorer inden for sundhedsområdet, mellem sundhedspersoner/instanser og borgere, samt ind/ud af sundhedsområdet fra/til andre domæner (som i afsnit 1.2 ovenfor).
- Sikker: Dækker over sikkerhed imod uvedkommendes læsning og manipulering af meddelelserne (og forsendelse af falske meddelelser) via indbygget kryptering og anvendelse af digitale certifikater i infrastrukturen. Relaterer sig til punkt 2 i listen i afslutningen af driver afsnittet.
- Robust: Dækker over meget høj grad af garanti for aflevering via kvitteringsflow og automatiske genforsendelsesmekanismer i infrastrukturen samt høj oppetid af infrastrukturen. Specifikt skal infrastrukturen beskyttes over for udfald forårsaget af angreb, hvor dele af infrastrukturen overbelastes (denial of service). Relaterer sig til punkterne 1 og 2 i listen i afslutningen af driver afsnittet.
- Skalerbar: Dækker over at infrastrukturen kan håndtere både mange anvendere, mange forskellige typer af meddelelser, og mange forsendelser af meddelelser (transaktioner).
- Generel infrastruktur: Dækker over at infrastrukturen hverken er specifik for sundhedsområdet eller for et givet sæt af meddelelsestyper. Infrastrukturen er fælles på tværs af sundhedsdomænet og de øvrige domæner, der kommunikeres med til/fra sundhedsområdet.

Enhver ny meddelelsestype, som det er aftalt skal sendes via infrastrukturen, og som pakkes ind i infrastrukturens standardiserede konvolut på den måde infrastrukturen kræver, vil kunne blive sendt via infrastrukturen udelukkende ved tilføjelse af den nye meddelelsestype i konfigurationen af infrastrukturen. Endvidere er der gode muligheder for på en agil måde at udvikle innovative forretningsservices oven på den generelle infrastruktur, f.eks. til at bidrage til mere aktiv inddragelse af borgeren og bedre sammenhæng i behandlingen, der jf. afsnit 1.3 er vigtige strategiske mål på sundhedsområdet. Relaterer sig til punkt 3 i listen i afslutningen af driver afsnittet.

2.4 Målsætninger

Med afsæt i de beskrevne motivationsgrunde for modernisering af den eksisterende forsendelsesinfrastruktur og den opstillede vision for en kommende infrastruktur er der formuleret følgende målsætninger for infrastrukturen med tilhørende gevinster:

Målsætning	**Gevinster**
Antallet af driftsproblemer er lavt. Når de opstår, opdages og afhjælpes de hurtigt.	Få og små forsinkelser ift. udredning og behandling af borgeren. En hurtig indsats gavner borgerens sundhedstilstand og reducerer eventuelle gener ved helbredsproblemer.
Antal fejlforsendelser er lavt.	Behandlerressourcer belastes ikke unødigt. Borgeren undgår forsinkelse i udredning og behandling.
Produkter og ydelser (vedr. meddelelseskommunikation) leveret af private udbydes på et marked præget af høj konkurrence.	Det er muligt at udskifte leverandører og løsninger og dermed sikre kontinuitet i leverance (forsyningssikkerhed). Endvidere vil konkurrencen sikre et optimalt forhold mellem kvalitet og pris.
Kommunikationen er beskyttet mod angreb fra aktører med høj angrebskapacitet (andre stater etc.).	Stat og borgere beskyttes mod udefra kommende trusler. Samfundskritiske funktioner kan opretholdes under kriser og der sikres et validt datagrundlag at styre ud fra.
Infrastrukturen understøtter udvikling af innovative forretningstjenester der deler information mellem parter involveret i en behandling (herunder borgeren selv og/eller dennes pårørende).	Meddelelsesinfrastrukturen styrer i retning af målbilledet for national infrastruktur, der sigter på at skabe sammenhæng i behandling og aktiv inddragelse af borgeren.
Infrastrukturen understøtter udvikling af innovative forretningstjenester baseret på beslutningsstøtte og anden kunstig intelligens (AI)	Meddelelsesinfrastrukturen styrer i retning af målbilledet for national infrastruktur, der sigter på at udnytte teknologiske muligheder til at skabe datadrevet forebyggelse og behandling.

Målsætning	Gevinster
Infrastrukturen understøtter hurtig agil transition fra udvikling til afprøvning og drift.	Infrastrukturen står ikke i vejen for udviklingen af forretningen. Gevinster ved digitalisering af sundhedsområdet kan høstes hurtigt.
At gå sammen fællesoffentligt og fælleseuropæisk ift. at bygge på samme teknologiske fundament.	Anvendelse af en infrastruktur baseret på tidssvarende teknologier og standarder er med til at sikre kvalitet og sikkerhed i forsendelse samt give god mulighed for udskiftning af leverandører og løsninger (og stimulere et konkurrencepræget marked). Infrastruktur forberedes til at kunne indgå i en fælleseuropæisk infrastruktur med henblik på understøttelse af grænseoverskridende sundhedsydelser. Deltagelse i den fælleseuropæiske infrastrukturs community sikrer dels mulighed for indflydelse på hvordan infrastrukturen udvikler sig over tid og dels erfaringsudveksling med andre anvendere af infrastrukturen.

Målbilledet peger på følgende leverancer for realisering af målsætningerne:

Leverance	Bidrag til realisering af målsætning
Etablering af en national forsendelsesinfrastruktur på sundhedsområdet baseret på sundhedsdatanettet og fællesoffentligt eDelivery-netværk.	Anvendelse af en infrastruktur baseret på tidssvarende teknologier og standarder (med bred markedsadoption og/eller understøttet af open-source communities). Dette giver en række sikkerhedsmæssige og vedligeholdelsesmæssige fordele. Da flere leverandører er kompetente til at anvende og/eller supportere (dele af) infrastrukturen, er der reel mulighed for leverandørskifte (eller "hjemtagning" af opgaver). Den standardiserede infrastruktur er åben for nye aktører. Bidrager derfor til sikring af kontinuitet og øget konkurrence mellem leverandører.
Etablering af gateway(s), der kan sikre kommunikation mellem sundhedsområdets parter og eksterne parter.	Bidrager til at beskytte kommunikation på sundhedsområdet mod angreb udefra.

Leverance	Bidrag til realisering af målsætning
Etablering af komponenter, der hjælper afsendere af meddelelser med at fremsøge rette modtager(e) af en meddelelse.	Bidrager til at holde antallet af fejlforsendelser nede, og dermed til både at undgå unødige forsinkelser i udredningen og behandlingen af borgerne, og undgå at forstyrre irrelevante sundhedspersoner.
Etablering af komponenter, der opsamler information om alle forsendelseshændelser i netværket.	Gør det muligt at opdage driftsproblemer hurtigt, hvis der f.eks. etableres en samlet overvågning, eller hvis borgere og/eller aktører, der deltager i kommunikationen kan følge status på forsendelser. Gør det muligt for sundhedspersoner at følge med i, hvad andre sundhedspersoner kommunikerer om borgeren. Hjælper derfor til at skabe sammenhæng i behandlingen.
Etablering af komponenter, der kan opsamle afsendte meddelelser og fremfinde disse igen	Gør det muligt for sundhedspersoner at se, hvad andre sundhedspersoner har skrevet om borgeren. Hjælper derfor til at skabe sammenhæng i behandlingen. Giver en borger og/eller dennes pårørende mulighed for at se meddelelser vedrørende dem selv og dermed forberede sig til møde med sundhedsaktører (samt evt. fange og rette op på fejl og misforståelser). Bidrager derfor til aktiv inddragelse af borgeren i behandlingen.
Etablering af konvolutstandarder i forsendelsesinfrastrukturen baseret på en åben international standard.	Konvolutten indeholder kryptografisk bevis for autenticitet af afsender samt integritet og fortrolighed af meddelelse. Dette bidrager til at beskytte kommunikation mod angreb fra aktører med betydelig eller høj angrebskapacitet. Nye meddelelsestyper og meddelelsesregimer kan understøttes uden ændring i den underliggende teknologiske infrastruktur. Dermed bidrager konvolutstandarderne til at understøtte hurtig transition fra udvikling til afprøvning og drift.

Leverance	Bidrag til realisering af målsætning
Etablering af en styringsmodel, hvor der kan sættes fælles krav til infrastrukturkomponenter og/eller systemer og services og hvor der følges op på overholdelsen af disse fælles krav.	Et samlet forpligtende SLA-apparat, der dækker hele kommunikationen fra afsender til modtager medvirker til at sikre pålidelig kommunikation med få driftsproblemer. Der er defineret roller med tværgående ansvar – f.eks. for sundhedsdomænet og for hele netværket. Dette medvirker til hurtig afhjælpning af driftsproblemer (reducerer "blaming games").

Infrastrukturen for meddelelseskommunikation, som præsenteres i målbilledet, sigter således efter at være en markant forbedring af den eksisterende infrastruktur, hvorfor den samlet set fremadrettet benævnes "EHMI" (forkortelse for det engelske "Enhanced Healthcare Messaging Infrastructure"). Oven på infrastrukturen vil der kunne etableres en række services:

Anvendelse	Services
Services der anvendes i forbindelse med styring og drift af infrastruktur	Services, der gør det muligt for supportere at følge meddelelser med henblik på afhjælpning af forsendelsesproblemer. Services, der leverer aggregeret information om antal og størrelse af forsendelser (evt. fordelt på systemer eller organisationer) med henblik på kapacitetsplanlægning, problemidentifikation m.v..

Anvendelse	Services
Etablering af services rettet mod aktører i behandlingen af en borger	Services der hjælper sundhedspersoner med at fremfinde relevante aktører at kommunikere med i forhold til behandling af en borger. Services, der giver den sundhedsperson, der sender en meddelelse mulighed for at kontrollere status på denne og dermed hurtigere følge op på eventuelle forsinkelser. Services, der giver sundhedspersoner (med behandlingsrelation til borgeren) mulighed for at se andre parters meddelelser om borgeren til gavn for borgerens behandling. Services, der giver en borger og/eller dennes pårørende mulighed for at kontrollere status af meddelelser vedrørende dem selv og dermed hurtigere kan følge op på eventuelle forsinkelser eller forsendelsesfejl. Services, der giver en borger og/eller dennes pårørende mulighed for at se meddelelser vedrørende dem selv og dermed forberede sig til møde med sundhedsaktører.
Services med sekundære formål	Services, der gør det lettere for en behandler af patientklager at danne sig et overblik over den samlede meddelelseskommunikation om patienten. Services, der udtaler sig om evidensen for, at der eksisterer en behandlingsrelation (f.eks. den nationale behandlingsrelationsservice) kan benytte forsendelsesinformation til forbedring af servicen. Udtræksservices, der kan levere aggregeret information (ikke personhenførbart) om aktivitet i sundhedsvæsenet til analytikere og beslutningstagere i sundhedsvæsenet.

Ovenstående liste er ikke udtømmende og vigtigheden af den enkelte service varierer i forhold til, om den er vigtig for drift af infrastrukturen, om den er vigtig i forhold til realisering af de opstillede målsætninger eller om den leverer værdi i forhold til andre parametre.

Da de forskellige services har forskellige formål, skal hjemmelsgrundlaget for de enkelte services også afklares, inden man eventuelt etablerer dem (som nævnt i nedenstående jura kapitel 3).

2.5 Kvaliteter

De centrale arkitekturkvaliteter, som målbilledet er bygget op omkring, er dels direkte udtrykt i visionens ordlyd:

- Sikkerhed.
- Robusthed.
- Skalerbarhed.
- Generalitet.
- Åbenhed.

Derudover er følgende arkitekturkvaliteter indirekte bygget ind i visionen og dermed centrale for målbilledet:

- Vedligeholdelsesvenlighed.
- Fleksibilitet.
- Pålidelighed.
- Tilgængelighed.

Vedligeholdelsesvenlighed hænger sammen med den generelle (meddelelsesagnostiske) infrastruktur: Det skal være nemt hurtigt og agilt at kunne tilføje aftalte meddelelsestyper og modtagere af meddelelser til konfigurationen af infrastrukturen. Fleksibilitet hænger også sammen med generalitet og dækker dels over høj fleksibilitet i tilslutningen til infrastrukturen, der kan tilpasses den enkelte deltagende organisation, og dels over dynamiske frem for statiske konfigurationer, der gør migreringer og andre ændringer lettere for de deltagende parter. Pålidelighed er indbygget i visionens ordlyd via effektiv og robust tilsammen og sigter til høj grad af garanti for rettidig aflevering af meddelelser til bestemmelsesstedet i infrastrukturen. Tilgængelighed er en anden del af visionens ordlyd om robust og sigter til høj grad af oppetid for infrastrukturen.

2.6 Principper

Følgende arkitekturprincipper ligger til grund for udformningen af målbilledet. Der er naturligvis dels stor overensstemmelse imellem principperne og de ovenstående formulerede vision, målsætninger, og arkitekturkvaliteter, og dels (i de fleste tilfælde) sammenhæng med de overordnede arkitekturprincipper for sundhedsområdet givet i reference [ARPRSU], som for størstedelen af tilfældene er afledt af principper fra hvidbogen om fællesoffentlig digital arkitektur [HVIDBOG]:

Id.	Princip	Reference
PF1	Anvend velafprøvede etablerede standarder og infrastruktur	F2 [ARPRSU]
PF2	Anvend driftsmodnede løsningskomponenter med gode referencer fra eksisterende anvendelser	F6 [ARPRSU]
PF3	Den fælles løsning for meddelelseskommunikation skal baseres på en fælles national governance	F1 [ARPRSU]
PF4	Den fælles løsning for meddelelseskommunikation skal give de enkelte parter tilpas frihedsgrad til, at de kan overholde deres egne interne regler, retningslinjer og processer	F3 [ARPRSU]
PF5	Den fælles løsning for meddelelseskommunikation med tilhørende governance skal kunne favne de store forskelle i organisationsstørrelse, der eksisterer på sundhedsområdet	PF3, PF4
PF6	Den fælles løsning for meddelelseskommunikation må ikke give anledning til unødige organisatoriske flaskehalse	
PF7	Meddelelseskommunikation imellem sundhedspersoner og borgere skal følge de fællesoffentlige retningslinjer for kommunikation med borgere	PF1, PF2
PI1	Ansvaret for dataindhold i en meddelelse ligger hos afsenderen af meddelelsen	I1 [ARPRSU]
PI2	Ansvaret for anvendelsen af en meddelelse ligger hos modtageren af meddelelsen	I1 [ARPRSU]
PI3	Meddelelser opsamles én gang i forbindelse med forsendelse og genanvendes herefter i relevante sammenhænge i overensstemmelse med regler for visning og anvendelse	I4 [ARPRSU]
PI4	Alle meddelelser der forsendes via infrastrukturen opsamles i overensstemmelse med regler for opsamling af information	PI3
PI5	Der skal være en 1:1 relation imellem en meddelelses indhold og unikke identifikation	
PI6	En meddelelseskonvolut må kun anvendes én gang og skal have en unik identifikation	
PI7	Metadata med oprindelse fra meddelelserne til anvendelse i forbindelse med fremsøgning af meddelelser ved meddelelseskommunikation ved forespørgsel, skal tages fra meddelelsernes konvolut	
PA1	Anvend velafprøvede driftsmodnede applikationer, der har gode referencer fra eksisterende anvendelser og baserer sig på etablerede standarder og infrastruktur	PF1, PF2
PT1	Anvend fælles teknologiske infrastrukturkomponenter til effektivt at sikre et højt ensartet sikkerhedsniveau i meddelelseskommunikationen	T1 [ARPRSU]

PT2	Anvend teknologisk standardiserede komponenter til at sikre interoperabilitet	T2 [ARPRSU], PF1
PT3	Anvend modne bredt understøttede teknologier og modne bredt adopterede standarder til at højne leverandøruafhængighed	T3 [ARPRSU], PF1, PF2, PA1
PT4	Den fælles løsning for meddelelseskommunikation er standardiseret på nationalt niveau og ansvaret for at integrere dertil ligger hos de enkelte parter	T5 [ARPRSU], PF3, PF4
PT5	Den fælles løsning for meddelelseskommunikation må ikke basere sig på unødige teknologiske potentielle flaskehalse	T4 [ARPRSU], PF6
PT6	De sikkerhedsmekanismer og sikringsniveauer, der anvendes ved meddelelseskommunikation på sundhedsområdet skal så vidt muligt være de samme som dem, der anvendes ved anden kommunikation på sundhedsområdet og meddelelseskommunikation på andre områder	PT1

Det andet tegn i id'et for et princip henviser til hvilket arkitekturniveau princippet opererer på (F for forretning, I for information, A for applikation, og T for teknologi), så princip PF1 er princip nummer 1 på forretningsniveauet etc. Principperne gennemgås enkeltvis i lidt større detalje i det følgende:

Princip PF1	Anvend velafprøvede etablerede standarder og infrastruktur
Rationale	Anvendelsen af velafprøvede etablerede standarder og infrastruktur øger konkurrencen, styrker leverandøruafhængigheden og letter interoperabiliteten
Implikationer	Der kan nemmere og mere effektivt etableres sammenhæng på sundhedsområdet via den standardiserede meddelelseskommunikation. Der sikres ensartethed i meddelelseskommunikationen. Ansvaret for standarderne og koordinationen af deres anvendelse er et fælles nationalt anliggende
Reference	F2 [ARPRSU]

Princip PF2	Anvend driftsmodnede løsningskomponenter med gode referencer fra eksisterende anvendelser
Rationale	Anvendelsen af driftsmodnede løsningskomponenter med gode referencer fra eksisterende anvendelser sikrer kvaliteten og giver større driftsstabilitet af meddelelseskommunikationen
Implikationer	Store dele af basissen for meddelelseskommunikationen er velafprøvet og stabil. Det er kun mindre dele til integration til infrastrukturen for meddelelseskommunikation, der skal udvikles
Reference	F6 [ARPRSU]

Princip PF3	Den fælles løsning for meddelelseskommunikation skal baseres på en fælles national governance
Rationale	Meddelelseskommunikation på sundhedsområdet er karakteriseret ved at mange forskellige parter er involveret, og det er derfor nødvendigt med en fælles national governance til at sikre helhedssynet og sikre at ukoordinerede løsninger udenom den fælles løsning undgås
Implikationer	Der skal etableres centrale forankringspunkter på nationalt niveau, der er ansvarlig for meddelelseskommunikationen. Der bliver behov for koordinerende samarbejde mellem de centrale instanser og parterne, der deltager i meddelelseskommunikationen
Reference	F1 [ARPRSU]

Princip PF4	Den fælles løsning for meddelelseskommunikation skal give de enkelte parter tilpas frihedsgrad til, at de kan overholde deres egne interne regler, retningslinjer og processer
Rationale	De enkelte parter skal have tilpas dispositionsfrihed til at kunne tilgodese lokale hensyn, som den fælles løsning for meddelelseskommunikation ikke må lægge unødige hindringer i vejen for
Implikationer	Regler, retningslinjer, og processer omkring den fælles løsning for meddelelseskommunikation må ikke være alt for rigide. Lokale processer og regler hos parterne skal omvendt tage behørigt hensyn til den fælles løsning for meddelelseskommunikation
Reference	F3 [ARPRSU]

Princip PF5	Den fælles løsning for meddelelseskommunikation med tilhørende governance skal kunne favne de store forskelle i organisationsstørrelse, der eksisterer på sundhedsområdet
Rationale	For at den fælles løsning for meddelelseskommunikation kan blive en succes, er det vigtigt at alle parter deltager, så løsningen inklusive dens governance skal være mulig at håndtere for organisationer af størrelse fra små lægehuse til store kommuner og regioner
Implikationer	Den fælles løsning for meddelelseskommunikation skal være økonomisk overkommelig at tilslutte sig til og efterfølgende anvende. Governance omkring den fælles løsning for meddelelseskommunikation skal være smidig og agil og ikke så rigid og omfangsrig, at den reelt set umuliggør små organisationers deltagelse i løsningen
Reference	PF3, PF4

Princip PF6	Den fælles løsning for meddelelseskommunikation må ikke give anledning til unødige organisatoriske flaskehalse

Rationale	Det må ikke være langsommeligt og usmidigt at tilslutte sig til, og i øvrigt anvende, den fælles løsning for meddelelseskommunikation, da man i givet fald ville risikere at miste opbakningen til samme
Implikationer	De enkelte niveauer, der eksisterer i den fælles løsning for meddelelseskommunikation skal hver især i så høj grad som muligt være ansvarlige for det, som logisk set tilhører dem, og hvor andre niveauer er afhængige af (og skal anvende) noget, skal dette være nemt og i så høj grad som muligt automatiseret
Reference	

Princip PF7	Meddelelseskommunikation imellem sundhedspersoner og borgere skal følge de fællesoffentlige retningslinjer for kommunikation med borgere
Rationale	Meddelelseskommunikation med borgere optræder på mange forskellige områder og er ikke specifikt for sundhedsområdet, hvorfor denne kommunikation skal følge ensartede fællesoffentlige retningslinjer
Implikationer	Der skal ikke udvikles sundhedsdomænespecifikke løsninger til meddelelseskommunikation imellem sundhedspersoner og borgere. Man skal i stedet anvende de udviklede fællesoffentlige løsninger til meddelelseskommunikation med borgere, som, om nødvendigt, skal udvides i konstruktivt fællesoffentligt samarbejde til at inkludere særlige behov fra sundhedsområdet
Reference	PF1, PF2

Princip PI1	Ansvaret for dataindhold i en meddelelse ligger hos afsenderen af meddelelsen
Rationale	En klar, logisk og ensartet ansvarsfordeling for de informationer, der sendes via meddelelseskommunikation, fastlægger de enkelte rollers forpligtelser entydigt og øger de enkelte deltagere i meddelelseskommunikationens tillid til både selve meddelelseskommunikationen og den sendte information. Da meddelelseskommunikationens indhold stammer fra det afsendende system er det eneste logiske, at det er afsenderen af en meddelelse, der har ansvaret for dens indhold
Implikationer	Afsenderen af en meddelelse har ansvaret for at al indholdet af en meddelelse dels er i overensstemmelse med det registrerede i det afsendende system og dels er tilstrækkeligt til at modtageren vil kunne anvende den. Indtil afsenderen af en meddelelse har modtaget en positiv kvittering fra modtageren af meddelelsen om, at meddelelsen er modtaget og teknisk forståelig, har afsenderen ansvaret for at de aktioner, som meddelelsens indhold indebærer, udføres
Reference	I1 [ARPRSU]

Princip PI2	Ansvaret for anvendelsen af en meddelelse ligger hos modtageren af meddelelsen
Rationale	En klar, logisk og ensartet ansvarsfordeling for de informationer, der sendes via meddelelseskommunikation, fastlægger de enkelte rollers forpligtelser entydigt og øger de enkelte deltagere i meddelelseskommunikationens tillid til både selve meddelelseskommunikationen og den sendte information. Da det er modtageren af en meddelelse, som skal agere på meddelelsens indhold, er det kun logisk, at det er modtageren, der har ansvaret for anvendelsen af en meddelelse
Implikationer	Det er modtagersystemets ansvar, når meddelelsen er modtaget og valideret teknisk forståelig, at sende en positiv kvittering til afsenderen der indikerer dette, og i modsat fald sende en tilsvarende negativ kvittering. Det er modtagersystemets ansvar at vise de modtagne informationer korrekt for slutbrugeren, så denne kan agere bedst muligt på indholdet af meddelelsen
Reference	I1 [ARPRSU]

Princip PI3	Meddelelser opsamles én gang i forbindelse med forsendelse og genanvendes herefter i relevante sammenhænge i overensstemmelse med regler for visning og anvendelse
Rationale	Det vil gøre opsamlingen af meddelelserne, der sendes, unødig kompleks og ekstra tidskrævende, hvis en given meddelelse samles op mere end én gang. Gældende lovgivning om deling af data, og herunder sendte meddelelser, skal naturligvis overholdes
Implikationer	Der skal formuleres klare fælles regler for hvordan konsistent opsamling af meddelelser skal foregå i forbindelse med forsendelsen af meddelelserne. Meddelelser må kun opsamles og efterfølgende genanvendes, såfremt der er lovmæssig hjemmel til dette
Reference	I4 [ARPRSU]

Princip PI4	Alle meddelelser der forsendes via infrastrukturen opsamles i overensstemmelse med regler for opsamling af information
Rationale	Som udgangspunkt ønskes alle sendte meddelelser opsamlet med henblik på deling, da det vil have væsentligt mindre værdi for anvenderne, hvis det kun er en (begrænset) delmængde af meddelelserne, der vil være til rådighed, men samtidig skal der naturligvis være lovmæssig hjemmel til opsamlingen af meddelelserne

Implikationer	Meddelelser må kun opsamles såfremt der er hjemmel til opsamling og deling af dem. Når hjemmel til opsamling og efterfølgende deling er etableret, må ingen bortfiltrering, f.eks. på baggrund af modtager eller andet lignende, ske i forbindelse med opsamling
Reference	PI3

Princip PI5	Der skal være en 1:1 relation imellem en meddelelses indhold og unikke identifikation
Rationale	Hvis ikke der for en given unik meddelelsesidentifikation svarer ét og kun ét meddelelsesindhold kan vi ikke identificere en given meddelelse unikt, hvilket vil umuliggøre effektiv deling, sporing, videreforsendelse, og support af meddelelser
Implikationer	Enhver afsender af meddelelser skal ved afsendelse af en meddelelse give denne en identifikation, der er unik globalt set. En identifikation for en meddelelse må aldrig genbruges til en anden meddelelse
Reference	

Princip PI6	En meddelelseskonvolut må kun anvendes én gang og skal have en unik identifikation
Rationale	En meddelelseskonvolut relaterer sig til en enkelt forsendelse af en meddelelse, og skal derfor kun anvendes én gang (helt analogt til papirkonvolutter (og deres indeholdte brev)). Unik identifikation af meddelelseskonvolutter effektiviserer sporing og support af meddelelser
Implikationer	Meddelelseskonvolutter er engangskonvolutter. Enhver afsender af meddelelser skal ved afsendelse af en meddelelse give meddelelsens konvolut en identifikation, der er unik globalt set. En identifikation for en meddelelseskonvolut må aldrig genbruges til en anden meddelelseskonvolut
Reference	

Princip PI7	Metadata med oprindelse fra meddelelserne til anvendelse i forbindelse med fremsøgning af meddelelser ved meddelelseskommunikation ved forespørgsel, skal tages fra meddelelsernes konvolut
Rationale	Når metadata udelukkende er placeret i meddelelsens konvolut, bliver udtrækningen/opsamlingen af metadata til efterfølgende fremsøgning af meddelelser forenklet betragteligt, da denne ikke behøver at kende til strukturen af de enkelte meddelelser men kun til strukturen af meddelelsernes konvolut

Implikationer	Alle relevante metadata oprindende fra en meddelelse skal placeres i pågældende meddelelses konvolut. Opsamlingen/udtrækningen af metadata til senere anvendelse ved deling af meddelelser må kun basere sig på meddelelseskonvolutten og ikke på selve meddelelsens body
Reference	

Princip PA1	Anvend velafprøvede driftsmodnede applikationer, der har gode referencer fra eksisterende anvendelser og baserer sig på etablerede standarder og infrastruktur
Rationale	Anvendelsen af velafprøvede driftsmodnede applikationer med gode referencer fra eksisterende anvendelser, som er baseret på etablerede standarder og infrastruktur, giver større driftsstabilitet, sikrer kvaliteten, letter interoperabiliteten, og styrker leverandøruafhængigheden af meddelelseskommunikationen
Implikationer	Der sikres applikationsmæssig ensartethed i meddelelseskommunikationen på sundhedsområdet. Store dele af den applikationsmæssige basis for meddelelseskommunikation er velafprøvet og stabil. Kun mindre applikationer, relateret til integration til infrastrukturen for meddelelseskommunikation, skal udvikles
Reference	PF1, PF2

Princip PT1	Anvend fælles teknologiske infrastrukturkomponenter til effektivt at sikre et højt ensartet sikkerhedsniveau i meddelelseskommunikationen
Rationale	En kæde er ikke stærkere end dens svageste led og anvendelsen af fælles teknologiske infrastrukturkomponenter med indbygget høj sikkerhed, sikrer at sikkerhedskæden for den fælles løsning for meddelelseskommunikation er stærk for alle anvenderne
Implikationer	Duplikering af ens sikkerhedsfunktionalitet mindskes. Auditlog og overvågning kan ske på en ens standardiseret måde. Ændringer i sikkerhedsfunktionaliteten skal kun foretages få steder, og kan derfor effektueres hurtigere
Reference	T1 [ARPRSU]

Princip PT2	Anvend teknologisk standardiserede komponenter til at sikre interoperabilitet
Rationale	Anvendelsen af teknologisk standardiserede komponenter giver større interoperabilitet, øger konkurrencen, styrker leverandøruafhængigheden, og fremtidssikrer løsningerne

Implikationer	Det bliver økonomisk billigere at tilslutte sig til den fælles løsning for meddelelseskommunikation. Det bliver økonomisk billigere at anvende den fælles løsning for meddelelseskommunikation på den lange bane, da standardiserede løsninger lever længere og følger bedre med den teknologiske udvikling
Reference	T2 [ARPRSU], PF1

Princip PT3	Anvend modne bredt understøttede teknologier og modne bredt adopterede standarder til at højne leverandøruafhængighed
Rationale	Anvendelsen af modne bredt understøttede teknologier og modne bredt adopterede standarder øger konkurrencen, styrker leverandøruafhængigheden og øger fleksibiliteten i forhold til fremtidige ændringer
Implikationer	Det bliver alt andet lige økonomisk billigere at tilslutte sig til og anvende den fælles løsning for meddelelseskommunikation. Det bliver nemmere at skifte tilslutningsleverandør til den fælles løsning for meddelelseskommunikation
Reference	T3 [ARPRSU], PF1, PF2, PA1

Princip PT4	Den fælles løsning for meddelelseskommunikation er standardiseret på nationalt niveau og ansvaret for at integrere dertil ligger hos de enkelte parter
Rationale	En klar ansvarsfordeling effektiviserer implementeringsforløbet for den fælles løsning for meddelelseskommunikation
Implikationer	Ansvaret for den fælles løsning for meddelelseskommunikation og dennes standardiserede basiskomponenter ligger centralt. Ansvaret for den lokale integration til den fælles løsning for meddelelseskommunikation ligger hos den enkelte anvendende part
Reference	T5 [ARPRSU], PF3, PF4

Princip PT5	Den fælles løsning for meddelelseskommunikation må ikke basere sig på unødige teknologiske potentielle flaskehalse
Rationale	Ved ikke at basere sig på unødige teknologiske flaskehalse sikres skalerbarheden og tilgængeligheden af den fælles løsning for meddelelseskommunikation
Implikationer	Der skal udarbejdes klare SLA for de forskellige komponenter i den fælles løsning for meddelelseskommunikation. Skalerbarhed skal tænkes ind i alle dele af løsningsarkitekturen
Reference	T4 [ARPRSU], PF6

Princip PT6	De sikkerhedsmekanismer og sikringsniveauer, der anvendes ved meddelelseskommunikation på sundhedsområdet skal så vidt muligt være de samme som dem, der anvendes ved anden kommunikation på sundhedsområdet og meddelelseskommunikation på andre områder
Rationale	Meddelelseskommunikation på sundhedsområdet skal ses som en integreret del af kommunikationen på sundhedsområdet, og ikke som sit eget parallelunivers med egne sikkerhedsregler og sikringsniveauer. Da meddelelseskommunikation ind og ud af sundhedsområdet også er i scope, skal sikkerhedsprincipper for meddelelseskommunikation for disse andre områder også tages i betragtning
Implikationer	Sikkerhedsmekanismer og sikringsniveauer, som defineret af NSIS, for punkt til punkt meddelelseskommunikation skal være sammenlignelige med (på samme niveau som) den øvrige kommunikation på sundhedsområdet. Sikkerhedsmekanismer og NSIS sikringsniveauer for punkt til punkt meddelelseskommunikation skal mindst være på samme niveau som den øvrige meddelelseskommunikation, som foregår via eDelivery. Deling af meddelelser skal anvende de samme sikkerhedsmekanismer og NSIS sikringsniveauer som deling af andre data på sundhedsområdet, herunder de nationale services MinSpærring, MinLog, og behandlingsrelationsservicen
Reference	PT1

Det ses, at principperne PF1, PF2, PT1, PT2, PT3, og PT5, der er afledt fra de overordnede arkitekturprincipper for sundhedsområdet [ARPRSU], samt PA1, der er direkte afledt af PF1 og PF2, alle ligger til grund for, og dermed er indbygget i, målbilledets vision.

3. Jura

Når man ønsker at anvende meddelelseskommunikation på sundhedsområdet, skal relevant lovgivning naturligvis overholdes, herunder databeskyttelsesforordning, databeskyttelseslov, sundhedslov med videre.

Databeskyttelsesretten fastsætter først og fremmest, at der skal være hjemmel til behandlingen af data, altså meddelelseskommunikationen, til indhentning, videregivelse og/eller deling. Hver databehandling skal vurderes selvstændigt, og skal i øvrigt opfylde de almindelige databeskyttelsesretlige regler om proportionalitet, dataminimering etc.

Sundhedsloven er særlovgivning ift. databeskyttelsesretten, og indeholder en række mere specifikke regler om indhentning, videregivelse og deling af oplysninger inden for sundhedsområdet, den venstre halvdel i Figur 2, i visse tilfælde også i forhold til meddelelseskommunikation, hvilket er særlig relevant i forhold til dette målbillede.

Hvis der ønskes introduceret en ny type af meddelelse i punkt til punkt meddelelseskommunikation og/eller deling, skal lovhjemlen undersøges, og eventuelt etableres. Hertil kommer, at hver databehandling fra denne nye meddelelseskommunikation skal vurderes selvstændigt. Regler om indhentning, videregivelse og deling kan være forskellige (herunder også hvor længe meddelelser af den pågældende type må gemmes i forhold til deling) og kommer an på den kontekst meddelelsen skal anvendes i. På nogle områder, f.eks. i forbindelse med epikriser, er meddelelsen særskilt reguleret i forhold til, hvem der kan få videregivet meddelelsen (som udgangspunkt via punkt til punkt meddelelseskommunikation). En konkret stillingtagen i lovgivningen kan medføre, at det ikke vil være relevant og heller ikke lovmedholdeligt, at alle i sundhedsvæsenet kan se meddelelsen (deling). (I parentes bemærkes det, at et særligt interessant tilfælde i denne sammenhæng kan blive deling af korrespondance meddelelser, da denne meddelelsestype er mindre struktureret end de fleste andre (som f.eks. laboratoriesvar), i høj grad er domineret af fritekst, kan indeholde tekst fra flere forskellige sundhedspersoner, og denne tekst kan være af afklarende karakter, som tekstforfatterne ikke nødvendigvis ønsker skal kunne ses af andre end dem, som den pågældende korrespondance var imellem.)

Det er vigtigt, at allerede eksisterende komponenter, der implementerer håndhævelsen af forskellige dele af den relevante lovgivning i andre kontekster, som MinSpærring, MinLog, og Behandlingsrelationsservicen, også tages i betragtning i forhold til meddelelseskommunikation.

Når disse juridiske vurderinger er foretaget og lovhjemlen tilstede kan meddelelseskommunikationen påbegyndes.

For de øvrige services listet i ovenstående afsnit 2.4 skal en lignende undersøgelse og etablering af hjemmel naturligvis også foretages, inden de hver især kan tages i anvendelse.

For meddelelseskommunikation ind/ud af sundhedsområdet fra/til andre domæner (kommunikationen mellem de to halvdele i Figur 2), øges kompleksiteten ved, at hjemmelsgrundlaget for behandlingen skifter f.eks. fra sundhedsloven til socialloven. Begge lovgivninger skal overholdes. Her kan det således være meget komplekst at afdække det konkrete hjemmelsgrundlag for etablering af meddelelseskommunikationen. Hvis der findes ikke at være hjemmel til behandlingen i de forskellige lovgivninger i deres gældende form, vil der være behov for en strategisk harmonisering imellem de pågældende områder med etablering af hjemmel før pågældende meddelelseskommunikation kan begynde.

Det kan ikke udelukkes, at nogle former for meddelelseskommunikation kan puljes under samme hjemmelsgrundlag, f.eks. (men ikke udelukkende) meddelelser af lignende tekniske meddelelsestyper. Det kommer an på meddelelsens indholds fortrolige og følsomme karakter. Af denne grund må systemer heller ikke umiddelbart sættes op til automatisk at kommunikere oplysninger videre. Fra et strategisk synspunkt vil denne gruppering under sammen hjemmel, jf. princip PF6 være ønskværdig, så der ikke opstår en juridisk flaskehals i forhold til meddelelseskommunikation.

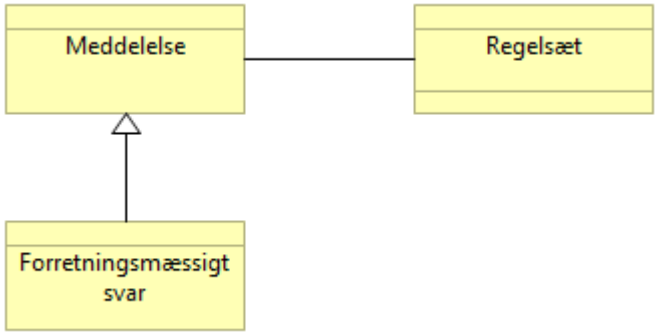
Supportfunktionerne for meddelelseskommunikation kan have adgang til data i bredere omfang, men det er stadig begrænset til det, der er nødvendigt for at supportfunktionerne kan udføre deres arbejde. Dette betyder, at såfremt de kan gøre deres arbejde uden at have adgang til hele indholdet af en meddelelse, men i stedet kun til et begrænset udsnit af metadata, skal dette etableres. Disse funktioner vil i øvrigt blive underlagt en fortrolighedsaftale med tavshedspligt.

Sikkerhedsmæssige juridiske krav, f.eks. med hensyn til kryptering af meddelelser og autentifikation af anvendere er beskrevet i sikkerhedskapitlet, kapitel 6, nedenfor.

4. Forretningsmæssigt

4.1 Modellering af forretningsobjekter

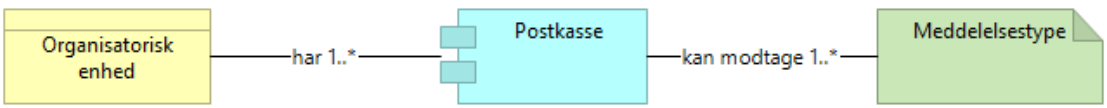
Det helt centrale forretningsobjekt i forhold til meddelelseskommunikation er en meddelelse som illustreret i følgende figur:



Figur 5: Forretningsobjekter.

En meddelelse har nogle helt centrale attributter som type (henvisning, epikrise, etc. inklusive version), afsender og modtager. En meddelelse er underlagt et regelsæt som kontrakt, som f.eks. et MedCom meddelelsesregelsæt eller en sundhedsaftale, som er indgået imellem de parter, som meddelelsen skal sendes imellem. Et forretningsmæssigt svar, som f.eks. et laboratoriesvar på en laboratorierekvisition, er ikke en separat type forretningsobjekt i sig selv, men i stedet en specialisering af en meddelelse. Disse svar benævnes sommetider "forretningsmæssige kvitteringer", men i dette målbillede anvender vi termen "forretningsmæssige svar", da dette er mere korrekt taget indholdet af meddelelsen i betragtning. Hvordan meddelelser realiseres i informations-, applikations- og teknologi-lagene vil blive gennemgået i kapitel 5.

En modtager er en organisatorisk enhed (eller en nærmere identificeret medarbejder ved samme), og en organisatorisk enhed kan have en eller flere postkasser, hvori de kan modtage meddelelser. Den enkelte postkasse kan håndtere en eller flere typer af meddelelser, hvilket kan illustreres på følgende vis:



Figur 6. Sammenhæng imellem organisatorisk enhed, postkasser, og understøttede meddelelsestyper.

Hvor mange postkasser en given organisatorisk enhed ønsker at have, og hvor mange meddelelsestyper disse hver især skal håndtere, er helt op til den organisatoriske enhed i overensstemmelse med principperne PF4, PF5, og PT4 i afsnit 2.6 og kan gå fra den ene yderlighed med en postkasse, der håndterer samtlige meddelelsestyper til den anden yderlighed med en postkasse per meddelelsestype. I dag håndteres relationen imellem organisatoriske enheder og postkasser

i Sundhedsvæsenets Organisationsregister (SOR), hvor der er en tæt kobling imellem de to, og der kun er mulighed for en 1 til 1 relation imellem dem.

4.2 User stories for meddelelseskommunikation

Der findes rigtig mange user stories for meddelelseskommunikation på sundhedsområdet. Et klassisk eksempel er, når en praktiserende læge har behov for at henvise en patient videre i systemet. Dette kan udtrykkes ved følgende user story:

Som en praktiserende læge
ønsker jeg at sende en henvisning til sygehus/speciallæge/fysioterapi m.fl.
når jeg har brug for at henvise en patient videre i systemet i forbindelse med patientens udredning/behandling

Et andet klassisk eksempel er, når en patient har behov for genoptræning efter et hospitalsbesøg, og en ergoterapeut eller fysioterapeut ved hospitalet derfor har behov for at sende en genoptræningsplan til forskellige relevante parter. Dette kan udtrykkes ved følgende user story:

Som en ergo- eller fysioterapeut ved et hospital
ønsker jeg at sende en genoptræningsplan til kommune/fysioterapeut/patientens egen læge
når patienten ved hjemsendelse fra hospitalet har behov for genoptræning

I forbindelse med målbillede workshop-arbejdet med de centrale parter på sundhedsområdet nævnt i afsnit 1.1 blev mere end 70 user stories i forhold til meddelelseskommunikation på sundhedsområdet identificeret, og af disse er mere end 60 vurderet som relevante i forhold til denne version af målbilledet. Den fulde liste over disse kan ses i Appendiks A sidst i dokumentet. På baggrund af listen er tre user story arketyper på et forholdsvis højt/generelt niveau identificeret. Hver af arketyperne relaterer sig til en af de tre overordnede typer af meddelelseskommunikation på sundhedsområdet introduceret i afsnit 1.2:

- Internt imellem sundhedspersoner inden for sundhedsområdet
- Imellem sundhedspersoner på sundhedsområdet og fagpersoner i andre domæner uden for sundhedsområdet
- Imellem sundhedspersoner på sundhedsområdet og borgeren

De tre identificerede user story arketyper er som følger:

Som en sundhedsperson
ønsker jeg at kunne sende/modtage en meddelelse til/fra en anden sundhedsperson
når jeg har behov for det i forbindelse med mit arbejde

Her kan sundhedsperson dække over: praktiserende læge/speciallæge, hospitalslæge, hospitalssygeplejeske, lægesekretær, laborant, hjemmesygeplejeske, sundhedsassistent, fysioterapeut, ergoterapeut, etc.; og meddelelse kan dække over typerne: henvisning, epikrise, korrespondance, advis, (genoptrænings)plan, (lab)rekvisition, (lab)svar, attest/blanket, etc.

Som en sundhedsperson
ønsker jeg at kunne sende/modtage en meddelelse til/fra en fagperson uden for sundhedsdomænet
når jeg har behov for det i forbindelse med mit arbejde

Her kan fagperson dække over en sagsbehandler ved et jobcenter, bosted, misbrugscenter, domstol, advokat, politi, forsikringsselskab etc., og meddelelse vil typisk være et journaludtræk eller en korrespondance.

Som en sundhedsperson
ønsker jeg at kunne sende/modtage en meddelelse til/fra en borger
når jeg har behov for det i forbindelse med mit arbejde

Her kan meddelelse dække over: spørgeskema og tilhørende svar, journaludtræk, indkaldelse, hjemmemålinger, etc.

I den fulde liste over user stories i Appendiks A er det et gennemgående ønske i flere, at det skal være nemmere som afsender at fremsøge den rette modtager af en meddelelse end det er i dag. Derfor er der identificeret følgende yderligere arketype:

Som en anvender af meddelelseskommunikation på sundhedsområdet
ønsker jeg at det er nemt at fremsøge den korrekte modtager af en meddelelse
når jeg skal sende en meddelelse

I det følgende afsnit 4.3 fokuseres der meget på forretningsprocesserne i forhold til denne. Som en afledt user story af denne kan følgende formuleres for situationen, hvor man skal sende en meddelelse, der er et svar på en tidligere modtaget meddelelse:

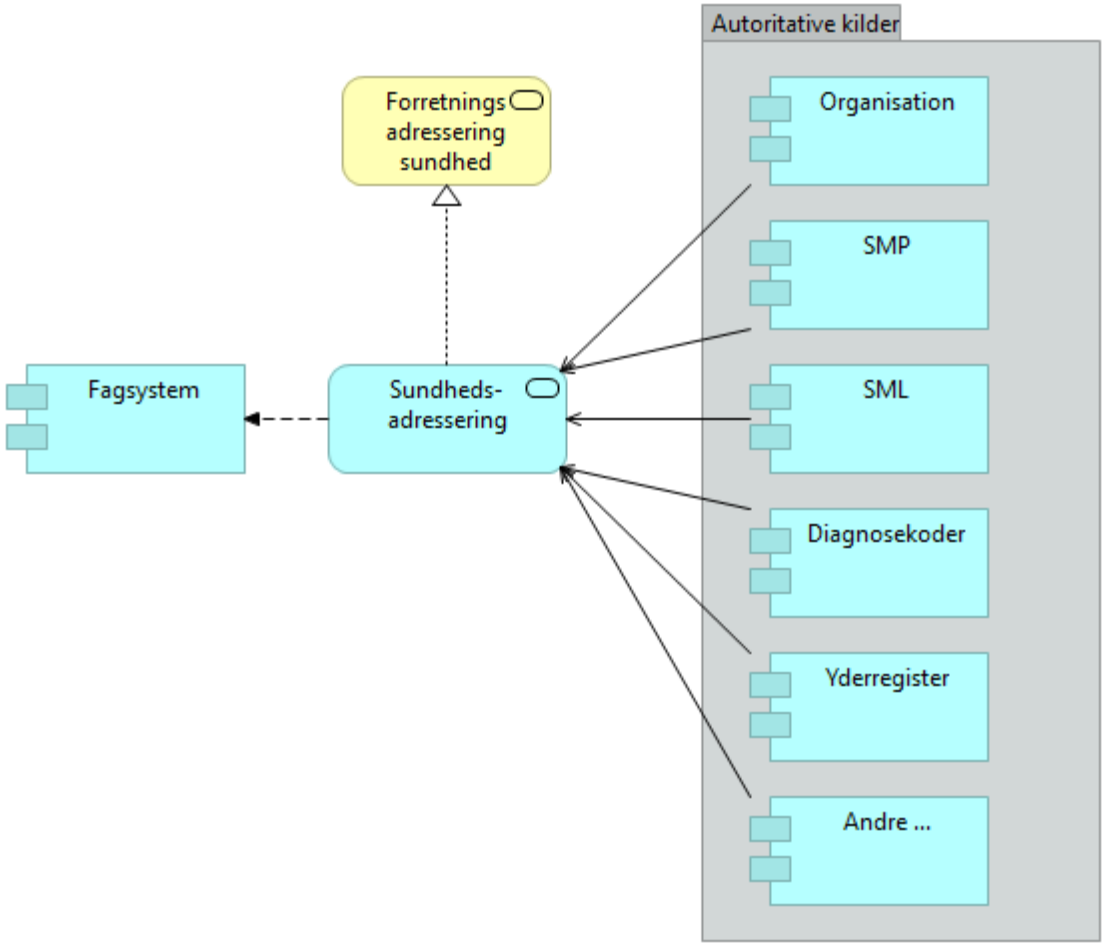
Som en anvender af meddelelseskommunikation på sundhedsområdet
ønsker jeg at jeg ikke skal fremsøge/angive modtager manuelt
når jeg skal sende et svar på en tidligere modtaget meddelelse

4.3 Forretningsadressering

Når en anvender af meddelelseskommunikation på sundhedsområdet gerne vil sende en meddelelse og i den forbindelse skal fremsøge modtageren for meddelelsen, så foregår dette via anvenderens fagsystem. Denne fremsøgningsfunktionalitet eksisterer allerede i varierende grad

i de forskellige fagsystemer, og alt efter hvor smidig denne funktionalitet er, er anvenderne mere eller mindre tilfredse. Som en mulig hjælp til fremsøgning af modtagere foreslås det derfor at introducere en fælles forretningsadresseringsservice på sundhedsområdet, som fagsystemer kan kalde, hvis de har behov for det i forbindelse med fremsøgning af modtagere – f.eks. når en modtager ikke entydigt kan identificeres ud fra en given klinisk kontekst. Denne forretningsadresseringsservice kalder videre til de relevante autoritative kilder, der måtte være behov for, for at kunne svare på forespørgslerne fra fagsystemerne. Dette vil dels hjælpe med at afkoble fagsystemerne fra de autoritative kilder og dels vil det betyde at den logik, der skal implementeres for at fremsøge modtagere i forskellige situationer, ultimativt kun behøver blive implementeret (og dermed vedligeholdt) et sted, nemlig i den nye sundhedsadresseringsservice.

Denne konstruktion er illustreret i følgende figur i forhold til modtagere inden for sundhedsområdet:



Figur 7: Forretningsadressering i forhold til meddelelseskommunikation imellem sundhedspersoner på sundhedsområdet.

I figuren er forskellige autoritative kilder nævnt, og herunder også muligheden for at udvide med andre alt efter præcist hvilke fremsøgninger sundhedsadresseringsservicen skal kunne håndtere. Diagnosekoder er medtaget, da sundhedsadresseringsservicen skal kunne være et fuldautomatisk alternativ til den nuværende i MedCom regi delvist manuelt opdaterede "Pakketabel".

Bemærk at på forretningsniveau i målbillede-sammenhæng arbejdes med en autoritativ kilde for organisation, der på det fysiske plan i skrivende stund vil være realiseret via SOR. SMP og SML er relateret til den underliggende eDelivery teknologiske infrastruktur og vil blive gennemgået i kapitel 5.

Da evnen at kunne finde rette modtager til en meddelelse må betragtes som værende helt fundamental i forhold til meddelelseskommunikation, må sundhedsadresseringsservicen tilsvarende betragtes som værende meget vigtig, hvilket også er blevet bekræftet i diverse fora (som eksempelvis E-sundhedsobservatoriets årskonference og Danske Regioners IT-arkitekturråd), når målbilledet i tidligere versioner er blevet præsenteret. Da kvaliteten af svarene fra sundhedsadresseringsservicen ikke vil være bedre end kvaliteten i de bagvedliggende autoritative kilder, vil det være meget vigtigt at sikre høj datakvalitet i disse bagvedliggende autoritative kilder, hvilket blandt andet kalder på en omhyggelig governance og test omkring disse. Dette gælder alle scenarier (og ikke kun solskinsscenarier) i forhold til alle de autoritative kilder – f.eks. også når en organisatorisk enhed nedlægges i organisationsregisteret.

Da sundhedsadresseringsservicen skal afkoble fagsystemerne fra de autoritative registre er det endvidere vigtigt, at fagsystemerne ikke skal tage hensyn til eventuel særlig eller forskellig registreringspraksis i de bagvedliggende autoritative kilder – eksempelvis forskellig regional og kommunal registreringspraksis i organisationsregisteret. Denne type kompleksitet skal sundhedsadresseringsservicen selv tage sig af og derved afskærme sine anvendere fra.

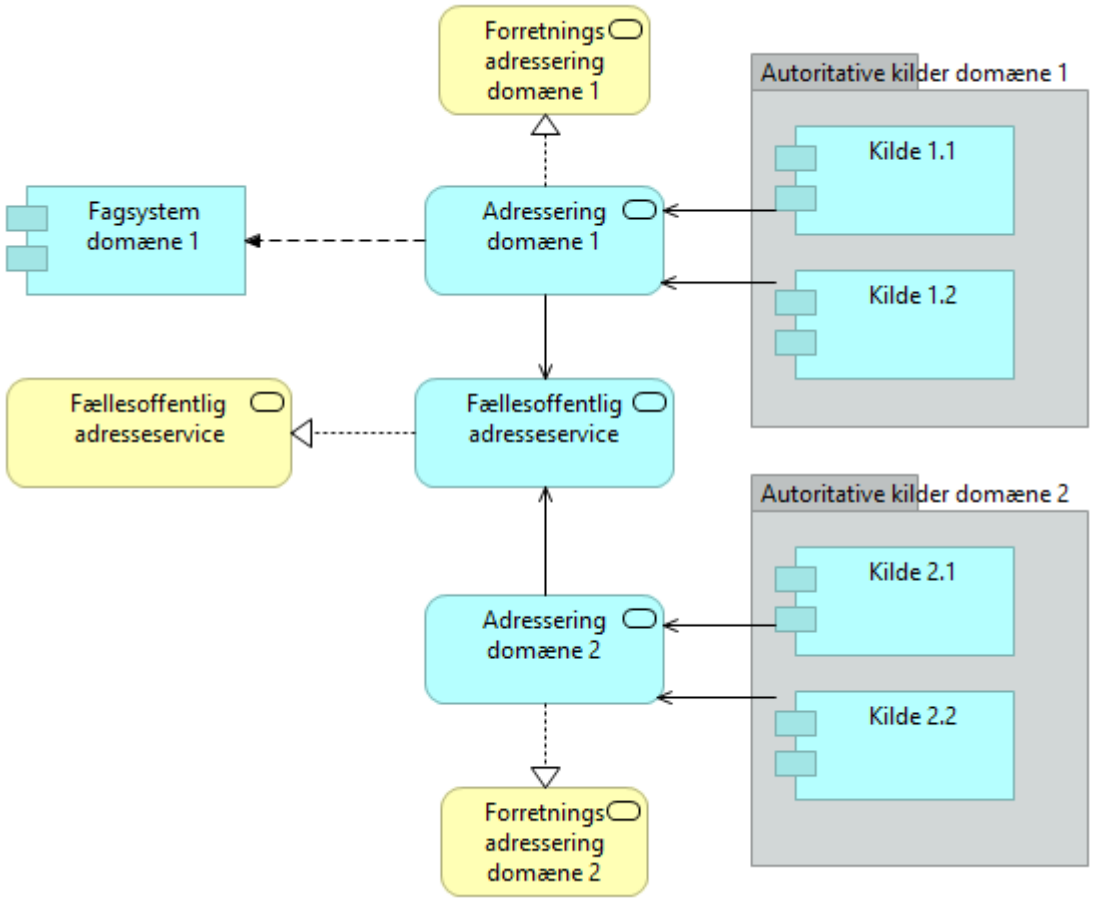
Fremsøgninger som sundhedsadresseringsservicen som udgangspunkt vil skulle understøtte (ud over det som i dag klares via pakketabellen) er:

- Fremsøg en patients praktiserende læge
- Fremsøg modtager via forskellige søgeparametre (som f.eks. adresse, ydernummer, etc. alt efter hvilken kontekst man arbejder i)
- Fremsøg modtager ud fra behandler uden ydernummer – særlig relevant for fremsøgning af f.eks. fysioterapeuter og fodterapeuter, hvor flere ofte er sammen under et (klinikkens ejers) ydernummer
- Fremsøg hvilke modtagere kan modtage specifikke typer af meddelelser (inklusive version af meddelelsestypen) – f.eks. relevant i forhold til henvisninger til røntgenundersøgelser, der kræver særligt udstyr ikke alle røntgenafdelinger har. I en senere kommende version gerne udbygget med de geografisk afgrænsede/nærmeste modtagere i forhold til et postnummer, kommunekode, regionskode (eller lignende)
- Hent liste over sidste udførte egne søgninger
- Hent liste over populære søgninger af andre

Denne liste må ikke betragtes som udtømmende og skal kvalificeres i det kommende arkitektur- og implementeringsarbejde.

Når vi vender os imod kommunikationen imellem sundhedspersoner på sundhedsområdet og fagpersoner uden for sundhedsområdet, bliver situationen lidt mere kompleks. Her vil vi gerne afkoble fagsystemerne i det enkelte domæne fra de øvrige domæner, man måtte have behov for at kommunikere med, så fagsystemer i et domæne skal vide mindst muligt om detaljer i de øvrige domæner. En opbygning med en forretningsadresseringsservice inden for de øvrige domæner a la den ovenfor illustrerede for sundhedsområdet foreslås derfor. Et målbillede på sundhedsområdet kan naturligvis ikke definere, hvordan arkitekturen i et andet domæne skal se ud, men forventningen er, at de øvrige domæner vil have de samme sunde ønsker om afkobling, samt at der fra fællesoffentlig side vil være et ønske om en overordnet grad af ensartethed på tværs af domænerne. Derfor er det for nemheds skyld valgt at illustrere de øvrige domæner på samme vis som sundhedsdomænet.

Da den underliggende eDelivery teknologiske infrastruktur for alle de involverede domæner er fælles, og vi yderligere gerne vil afkoble adresseringsservicerne i de forskellige domæner fra hinanden foreslås det derfor at modtagerfremsøgningen på tværs af domænerne går via en fællesoffentlig adresseservice, som illustreret i følgende generelle figur:

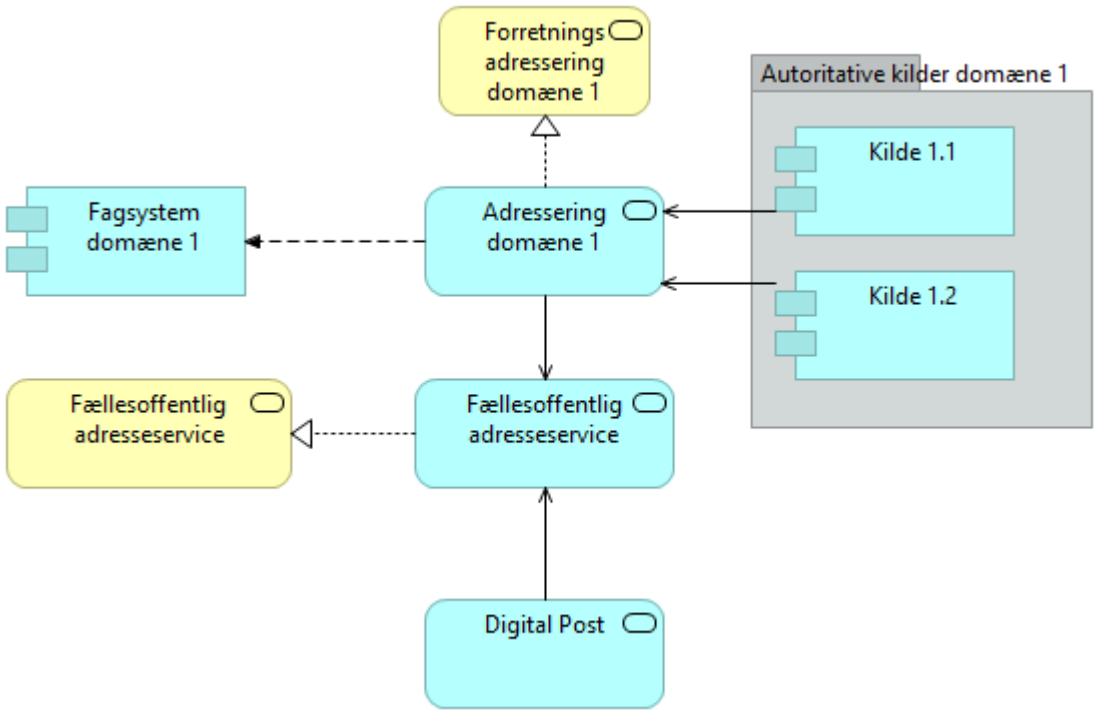


Figur 8: Forretningsadressering på tværs af domæner via fællesoffentlig adresseservice. Bemærk at de autoritative kilder ikke er de samme i de forskellige domæner.

På denne måde opnås dels den ønskede afkobling af systemerne i de forskellige domæner, og dels giver det muligheden for at ensrette funktionaliteten på tværs af domænerne og håndhæve de fællesoffentlige retningslinjer for samme, som i stigende grad forventes at komme i takt med at flere og flere får behov for at kommunikere med hinanden på tværs af domænerne via punkt til punkt meddelelseskommunikation. Dette er ikke mindst relevant for domæner, der kommunikerer meget med hinanden, som f.eks. social og sundhedsdomænerne.

Et eksempel på anvendelse af kommunikation på tværs af to domæner er en sagsbehandler på et jobcenter, der har behov for at sende en meddelelse til en borgers praktiserende læge, når en arbejdsløs borger bliver syg. I dette tilfælde er sundhedsdomænet domæne 2, og den service som kaldes i sundhedsadresseringsservicen (Adressering domæne 2 i figuren) er "Fremsøg en patients praktiserende læge", som allerede er identificeret ovenfor som nødvendig i forhold til modtagerfremsøgning i forbindelse med meddelelseskommunikation imellem sundhedspersoner internt på sundhedsområdet. Fagsystemet i jobcenteret sender sin modtagerfremsøgning afsted til sit eget domænes adresseringsservice. Denne kan ikke selv svare på forespørgslen og sender den videre til den fællesoffentlige adresseservice, der dirigerer videre til sundhedsdomænets sundhedsadresseringsservice, som svarer på forespørgslen, og svaret dirigeres tilbage den modsatte vej i kæden til fagsystemet i jobcenteret.

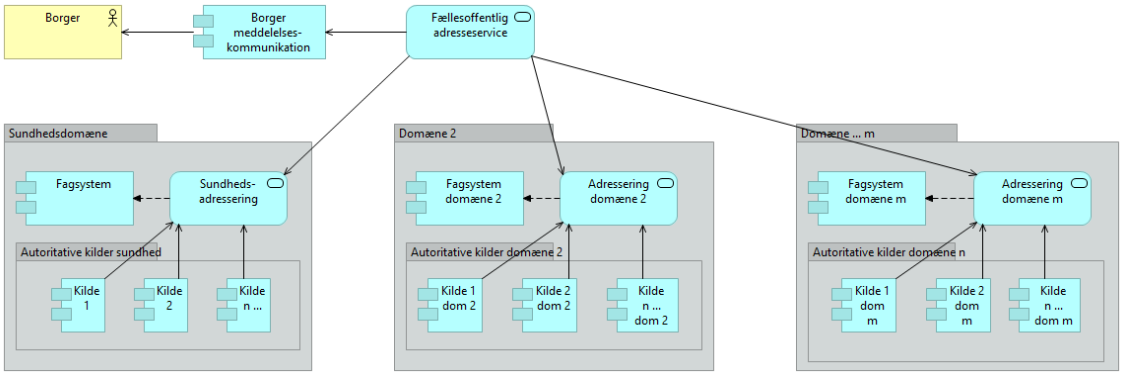
Tilsvarende bør kommunikation mellem sundhedspersoner og borgere, jf. princip PF7, følge de fællesoffentlige regler, retningslinjer, og formater for kommunikation med borgeren, og herunder borgerrettet digital post, hvis næstkommende generation kommer til at understøtte eDelivery. I forhold til fremsøgning af modtageren af meddelelsen i dette tilfælde, foreslås, igen af afkoblingshensyn og hensyn til de fællesoffentlige regler, at gå via sundhedsadresseringsservicen og den fællesoffentlige adresseservice som illustreret ved:



Figur 9: Forretningsadressering i forhold til meddelelseskommunikation imellem sundhedspersoner og borgere.

Præcis hvordan den fællesoffentlige adresseservice og borgerrettet meddelelseskommunikation (og herunder Digital Post) spiller sammen er ikke i scope for dette målbillede, da vi har lagt os fast på, at vi vil anvende de fællesoffentlige regler og retningslinjer for dette, hvorfor illustrationen for nemheds skyld blot har en applikationsservice kaldet Digital Post.

Som afslutning på diskussionen af forretningsadressering kan vi samle de tre figurer fra dette afsnit i en fælles generel illustration, der ser ud som følger:



Figur 10: Forretningsadressering samlet overblik.

Når et fagsystem har behov for hjælp til at udsøge den rette modtager af en meddelelse, går forretningsadresseringen i forhold til meddelelseskommunikation internt i sundhedsdomænet via sundhedsadresseringsservicen. Når kommunikationen er rettet ud af sundhedsdomænet

(enten til et andet domæne eller borgeren) går forretningsadresseringen fra afsenderdomænets adresseringsservice til rette anden adresseringsservice via den fællesoffentlige adresseservice.

I forhold til de fremsøgningsmuligheder af modtagere af meddelelser, der eksisterer i dag, er både sundhedsadresseringsservicen og den fællesoffentlige adresseservice nye. De nærmere detaljerede krav til sundhedsadresseringsservicen og den fællesoffentlige adresseservice og det roadmap, der skal etableres i forhold til deres implementering er, som nævnt i begyndelsen af afsnit 1.2.1, ikke en del af målbilledet, og de to komponenter ligger også i to forskellige domæner (sundhed og fællesoffentligt), med forskellige ansvarlige parter. Det nævnes derfor blot som kort input til det videre arbejde i forlængelse af dette målbillede, at den største del af den meddelelseskommunikation, som målbilledet dækker, er meddelelseskommunikationen imellem sundhedspersoner internt på sundhedsområdet, og sundhedsadresseringsservicen er bindeled mellem fagsystemerne på sundhedsområdet og alle de øvrige domæner (igennem den fællesoffentlige adresseservice).

4.4 Services baseret på et eller flere meddelelsesrepositorie(r)

I forbindelse med workshop-arbejdet er små 20 user stories relateret til services baseret på et eller flere repositorie(r) for meddelelser blevet identificeret. Disse er angivet i Appendiks B sidst i dokumentet, og omdrejningspunktet for dem er specielt to forretningsservices, der er indikeret i målsætningsafsnittet ovenfor (2.4):

- En service til at hente meddelelser, som er blevet sendt via meddelelsesinfrastrukturen
- En service til at hente forsendelsesstatus for afsendte meddelelser via meddelelsesinfrastrukturen

Af de listede user stories er de ca. 2/3 relateret til borgere (inklusive scenarier hvor en borger agerer på vegne af en pårørende), og disse borgerorienterede user stories er blevet præsenteret for repræsentanter fra patientforeningen Danske Patienter, der fandt dem relevante og dækkende fra et borger/patientperspektiv. Særligt blev servicen til forsendelsesstatus fremhævet sammen med vigtigheden af muligheden for at kunne spærre for adgang til at hente meddelelser og kontrollere hvem, der har tilgået meddelelser, via de velkendte MinSpærring og MinLog. Servicen til at hente meddelelser blev også vurderet relevant for borgeren, og det blev understreget, at det var uhyre vigtigt at have en brugervenlig præsentation for borgeren af meddelelser og forsendelsesstatus, og at denne præsentation var et sted, hvor borgeren var vant til at se sine øvrige sundhedsdata. Denne præsentation er ikke en del af dette målbillede, men er til gengæld vigtigt input i forhold til det efterfølgende implementeringsarbejde, hvis hovedlinjer inklusiv særlige opmærksomhedspunkter er overordnet skitseret i vedhæftede bilag 1.

Blandt de listede user stories rettet imod sundhedspersoner er servicen til at hente meddelelser, der er blevet sendt, særligt efterspurgt i forbindelse med etablering af overblik i forhold til

behandling af diabetes, og servicen til at hente forsendelsesstatus er specielt efterspurgt af praktiserende læger.

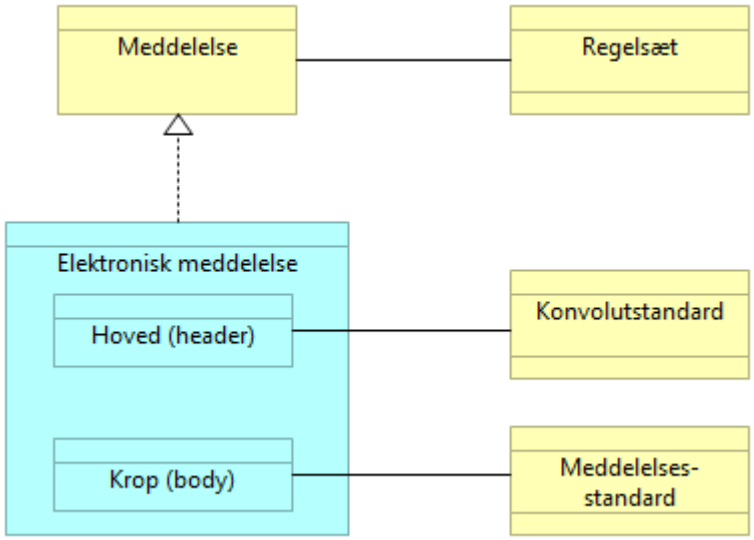
Som det fremgår af målsætningsafsnittet (2.4) og de formulerede user stories i Appendiks B, så er der flere forskellige anvendere af servicen til at hente meddelelser, som er blevet sendt via infrastrukturen, spændende fra sundhedspersoner over borgere til patientklagesagsbehandlere. Disse forskellige anvendere kan have forskellige behov for, hvor længe de skal kunne hente meddelelserne efter de er blevet sendt, og dermed hvor længe meddelelserne skal gemmes. En afklaring af denne tidsgrænse er dog også ikke mindst et juridisk spørgsmål og afhænger som nævnt i kapitel 3 af typen af meddelelse og skal derfor foretages i forbindelse med den juridiske behandling af den pågældende type af meddelelsestype, som omvendt skal tage de forskellige anvenderes behov i betragtning.

5. Information, applikationer og teknologi

I dette kapitel præsenteres de forskellige dele af informations-, applikations-, og teknologiarkitekturen, der skal realisere strategi- og forretningsarkitekturen beskrevet i de ovenstående kapitler. De forskellige dele introduceres løbende enkeltvis, og et samlet overblik gives til sidst i afsnit 5.4. Man kan således altid referere dertil for at se den samlede arkitektur den enkelte del/komponent er i kontekst af.

5.1 Overordnet modellering af meddelelse

Det centrale forretningsobjekt "Meddelelse" fra Figur 5 kan applikationsmæssigt foldes ud som:



Figur 11: Applikationsperspektiv på meddelelse.

En elektronisk meddelelse består på applikationsniveau af en header og body, eller sagt på en anden måde, med analogi til et almindeligt papirbrev man sender med posten, er meddelelsen pakket ind i en konvolut. I det følgende vil der kun blive refereret til konvolutten, når det er nødvendigt for sammenhængen, og ellers bare til meddelelse.

Ligesom forretningsobjektet "Meddelelse" er underlagt et regelsæt, er både en elektronisk meddelelses header og body underlagt regelsæt i form af standarder, henholdsvis en konvolutstandard og en meddelelsesstandard.

En meddelelse og en konvolut har hver deres unikke identifikation, jf. principperne PI5 og PI6, og normalt vil der i meddelelsen være et hovedobjekt, der i sig selv også har et unikt id – f.eks. et laboratorieprøvenummer eller et henvisnings-id.

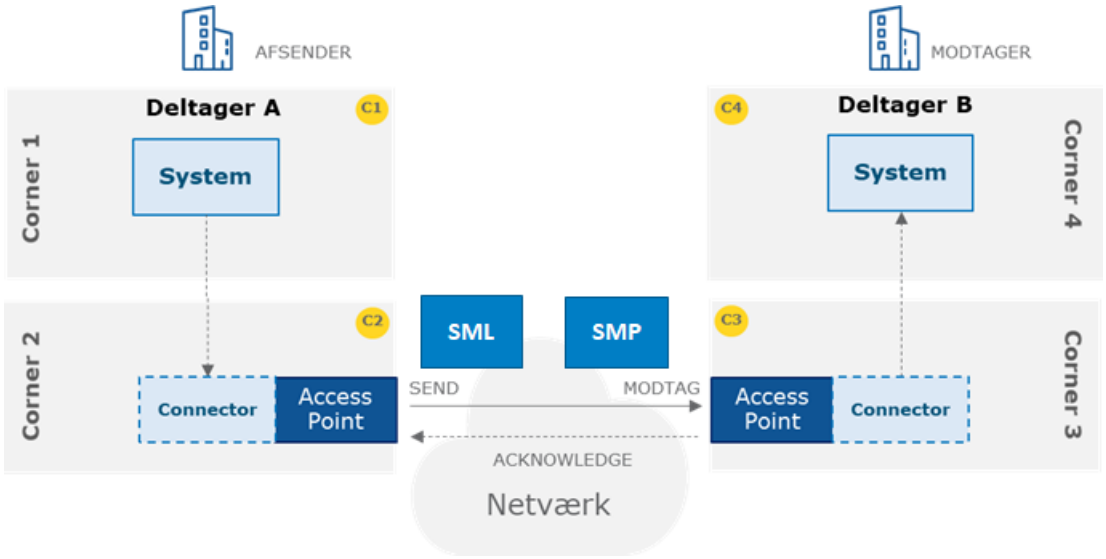
Ligesom et givet papirbrev ved modtagelse kan tages ud af en konvolut og videresendes ved at putte det i en anden konvolut, så kan en given meddelelse videresendes, men konvolutten i videreforsendelsen har et andet id end den oprindelige konvolut – mere om dette i afsnit 5.2.9.

5.2 Punkt til punkt kommunikation

Fra afsnit 1.2.2 erindrer vi først, at punkt til punkt meddelelseskommunikation anvendes, når en organisation ønsker at starte en bestemt forretningsproces hos en anden organisation, hvilket sker rigtig mange gange dagligt ved sektorovergange på sundhedsområdet.

5.2.1 Introduktion til eDelivery punkt til punkt kommunikation

Punkt til punkt meddelelseskommunikation i eDelivery kan, jf. reference [EDELDIGSTANRAP], illustreres ved følgende figur:



Figur 12: Punkt til punkt kommunikation i eDelivery.

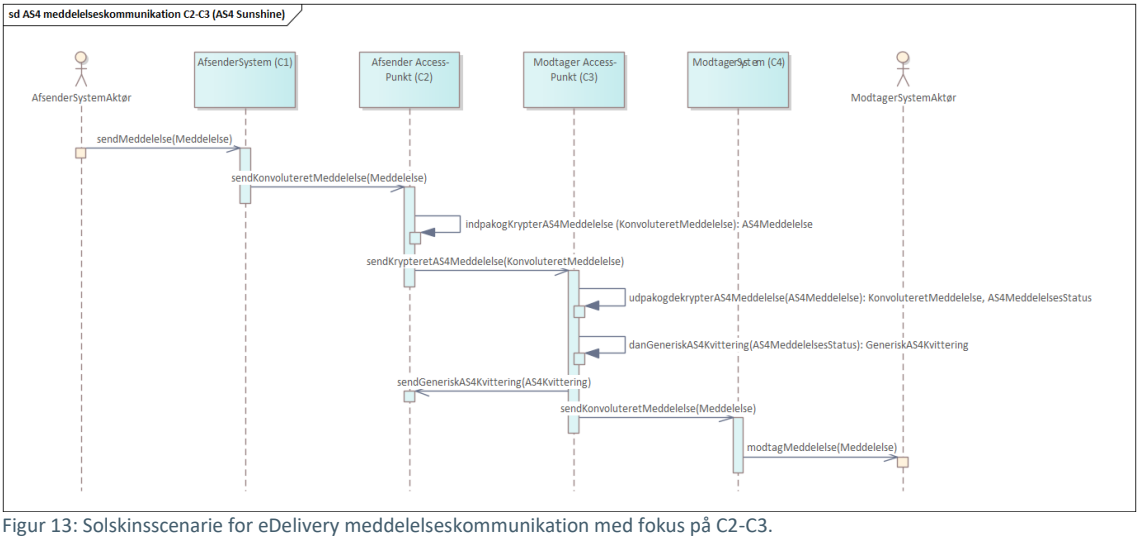
Adgang til eDelivery netværket foregår via access-punkter, der indgår aftaler om forsendelse af meddelelser med systemejere, og som agerer på systemernes vegne i forbindelse med meddelelseskommunikation via eDelivery netværket. Når en afsender A ønsker at sende en meddelelse til en modtager B, foregår dette overordnet ved, at meddelelsen først sendes fra deltager A's system til dets agerende access-punkt, hvorfra meddelelsen via eDelivery netværket sendes til access-punktet, der agerer på vegne af deltager B's system, og endelig sendes meddelelsen videre herfra til deltager B's system. Der er således fire "stop" på meddelelsens vej fra afsender til modtager. Disse stop benævnes corners i eDelivery terminologi, og modellen for den beskrevne meddelelseskommunikation kaldes derfor også "fire-corner modellen". Corner 1, eller kort C1, er det afsendende system, C2 dette systems access-punkt, C3 modtagerens access-punkt, og C4 endelig det modtagende system. Modtagerens access-punkt er således realiseringen i eDelivery-sammenhæng af postkassebegrebet fra Figur 6 i afsnit 4.1.

Kommunikationen imellem C1 og C2 foregår via en såkaldt connector og ligeså imellem C3 og C4, og et typisk eksempel på en connector er en integrationsplatform. En connectors implementering er selvsagt meget afhængig af det konkrete C1-C2 (eller C3-C4) par, og detaljer omkring dem er derfor ikke en del af dette målbillede. Der er således frihedsgrader i forhold til connectorerne, men da de, sammen med C1 og C4 selv, er vigtige brikker i forhold til den komplette kommunikation, nævnes krav til dem dog løbende, når det er relevant i de kommende afsnit. For eksempel er det et vigtigt krav, at connectorerne overholder SLA og ikke bliver forsinkende led i kommunikationen, men derimod er med til at sikre tilpas hurtig og kronologisk korrekt forsendelse af meddelelserne. Lidt mere om connectorer følger i afsnit 5.2.2.

Når C2 skal sende en meddelelse af en given type, skal den omsætte den i meddelelsen angive modtager (C4) til netværksadressen på modtagerens access-punkt (C3) for den givne type af meddelelse. Dette foregår via de to eDelivery service metadata komponenter SML (service metadata locator) og SMP (service metadata publisher) – der kan i eDelivery være mere end én SMP, men for overskuelighedens skyld er der kun angivet én i figuren. Først kalder C2 SML for at få information om hvilken SMP, der har information om C4 og dettes access-punkt (C3), og derefter kaldes den angivne SMP for at hente informationen om C4 og C3, der ud over netværksadressen for C3 også indeholder C3's offentlige digitale certifikat til kryptering og i øvrigt kapabiliteter som modtager (dvs. hvilke typer af meddelelser, der kan modtages).

Meddelelseskommunikationen imellem C2 og C3 på eDelivery netværket foregår via AS4 protokollen og er sikret via både kryptering og signering i C2, som beskrevet i afsnit 6.1 om sikkerhed. AS4 er en profilering af ebXML Messaging Service 3.0, der i mange år har været en standard under OASIS [OASIS], og som bliver en del af den kommende ISO-15000 standard, hvilket korresponderer glimrende med princip PF1.

Når C3 modtager en meddelelse, sender det en teknisk kvittering tilbage til C2, der, såfremt alt er gået godt, signalerer, at meddelelsen er modtaget og forstået rent teknisk, og at C3 tager ansvaret for at sende meddelelsen videre til C4. Dette er illustreret i følgende figur:

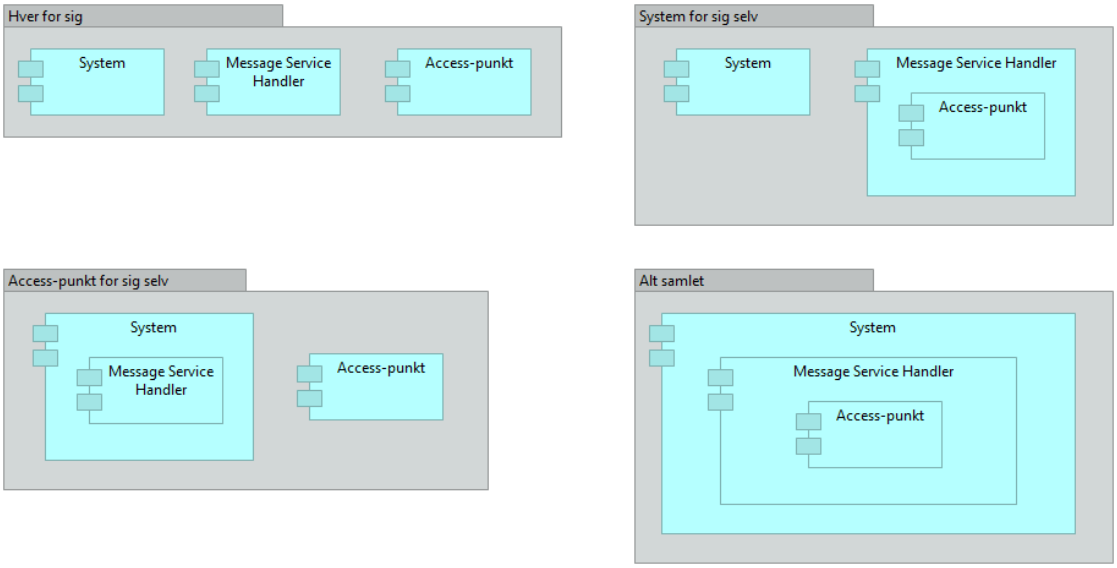


Figur 13: Solskinsscenarie for eDelivery meddelelseskommunikation med fokus på C2-C3.

Figuren illustrerer også anvendelsen af konvolutten introduceret ovenfor. Konvolutter, som kan anvendes i relation til eDelivery hedder henholdsvis ”Standard Business Document Header” (SBDH) [SBDH] og ”Exchange Header Envelope” (XHE) [XHE]. Begge kan indeholde vilkårlige overordnede meddelelsesformattyper såsom EDIFACT, OIO-XML og FHIR, og deres opgave er bl.a. at sikre en for netværket meddelelsestypeagnostisk kommunikation i netværket, så netværksnoderne ikke skal forholde sig til andet end en generisk konvolut. Man kan læse mere i Appendiks C om de to typer af konvoluts anvendelighed, samt fordele og ulemper. Konvolutter skal anvendes hele vejen fra C1 til C4, og det er heri, at relevante metadata, jf. princip PI7, skal placeres. Uanset hvilken konvolut, der ender med at blive valgt til implementeringsfasen, kaldes den i det følgende blot for konvolut.

5.2.2 Message Service Handlers

Connector er eDelivery termen for det generelle begreb ”Message Service Handler” inden for meddelelseskommunikation, der dækker over den logiske komponent, der håndterer klargøring, afsendelse, modtagelse, processering, kvittering etc. af meddelelser på vegne af systemet. I eDelivery fire-corner modellen er der stor fleksibilitet i forhold til hvor tæt system, message service handler, og access-punkt er integreret med hinanden, hvilket er illustreret i følgende figur:



Figur 14: Fleksibilitet ved tilslutning til eDelivery netværket i fire-corner modellen.

Mulighederne spænder lige fra at de tre komponenter eksisterer hver for sig, til at access-punktet er indeholdt i message service handleren, der igen er indeholdt i systemet. Der er således gode muligheder for at tilpasse anvendelsen af eDelivery fire-corner modellen. Denne fleksibilitet er vigtig, da det giver anvenderne mulighed for at vælge det set-up, der måtte passe bedst til deres behov og eksisterende systemlandskab. Har man f.eks. allerede en velfungerende message service handler, enten separat eller embedded i sit fagsystem, kan man nøjes med at anskaffe sig (eller etablere) et access-punkt og etablere kommunikationen imellem message service handleren og access-punktet. Eller hvis man ikke allerede har meddelelseskommunikation, eller i det hele taget gerne så vidt muligt vil afskærme sine systemer fra netværks-integrationerne med meddelelseskommunikation, kan man anskaffe sig en message service handler med et embedded access-punkt og skal så "blot" etablere kommunikation imellem sit system og message service handleren. Dette understøtter EHMI arkitekturkvaliteten "Fleksibilitet" nævnt i afsnit 2.5.

5.2.3 Kvitteringer, ansvarsoverdragelse, og lag

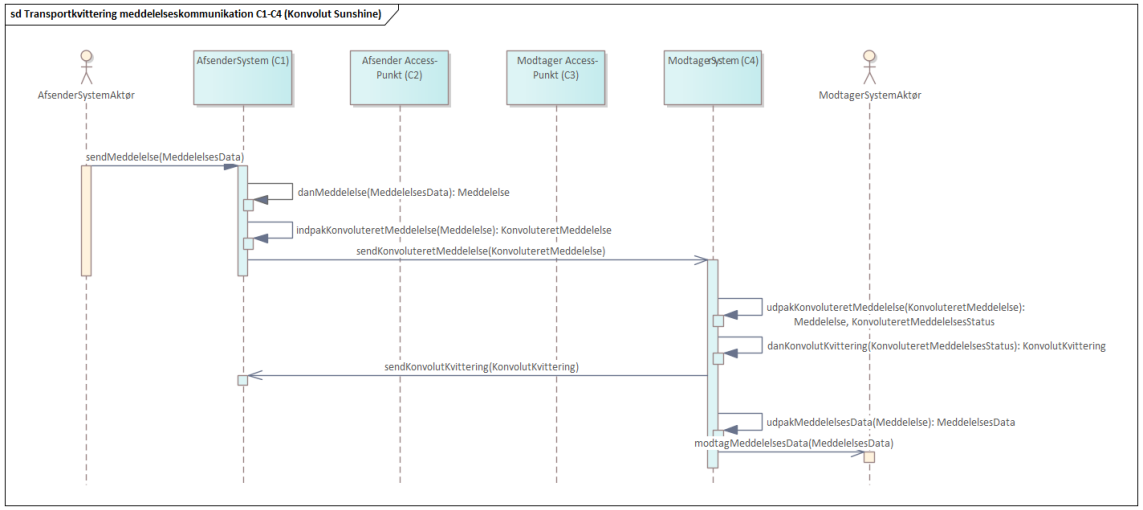
I afsnit 5.2.1 så vi, at der er indbygget en kvitteringsmekanisme i eDelivery imellem de to access-punkter. Når C2 modtager en positiv kvittering fra C3 angående en meddelelse, betyder det, at C3 tager ansvaret for den videre transport af meddelelsen i fire-corner modellen, og C2 behøver således ikke længere at bekymre sig om at få beskeden frem til C3. Men indtil denne positive kvittering er modtaget, er det fortsat C2's ansvar at sikre sig, at meddelelsen når frem til C3, hvilket kan indebære at gensende meddelelsen til C3 en eller flere gange, således at en pålidelig meddelelseskommunikation imellem de to access-punkter opnås. Hvor mange gange og hvor ofte en meddelelse skal forsøges gensendt i disse tilfælde kan variere og i nogle tilfælde endda afhænge af lovgivningen, så denne variation skal C2 kunne håndtere på en fleksibel måde. Såfremt C2 modtager en negativ teknisk kvittering fra C3, hvilket i produktionssammenhæng sker

yderst sjældent, betyder det, at der er noget teknisk galt med meddelelsen – f.eks. at den ikke er i overensstemmelse med det gældende meddelelsesdefinitionsskema. Tilsvarende tekniske kvitteringer skal også være en del af kommunikationen imellem C1 og C2 (og C3 og C4), da de også er vigtige i disse led i kommunikationen, men detaljerne omkring disse er (igen) ikke en del af målbilledet.

Den indbyggede pålidelige meddelelseskommunikation i eDelivery er imellem de to accesspunkter, men på sundhedsområdet ønsker vi dels at udvide denne til at strække sig hele vejen imellem C1 og C4, så C1 får at vide, at meddelelsen transportmæssigt er kommet hele vejen frem og afleveret til modtageren (C4), og dels at sørge for at C1 får at vide, hvorvidt modtageren rent faktisk overordnet også kan forstå og potentielt agere på indholdet af meddelelsen. Derfor introduceres to yderligere kvitteringstyper, som C4 automatisk skal sende tilbage til C1 i forbindelse med, at en meddelelse modtages i C4: En transportkvittering og en forståelseskvittering, der begge kan være positive eller negative. To yderligere kvitteringer kan måske virke lidt voldsomt, men det er faktisk det anbefalede fra f.eks. HL7, der er en international organisation grundlagt i 1987, der fastlægger rammer og standarder for udveksling og deling af elektroniske sundhedsdata, hvis udbredelse og anvendelse er meget stor inden for sundhedsområdet internationalt set. HL7 introducerede anvendelsen af begge disse kvitteringer i deres meddelelsesstandarder allerede for over 20 år siden, fordi det giver fleksibilitet til at separere den type ansvarsoverdragelse, som henholdsvis meddelelsestransport og meddelelsesforståelse indebærer – mere om dette nedenfor i dette afsnit.

Inden vi vender os imod de to kvitteringer i større detaljer, husker vi fra afsnit 5.1 og 5.2.1, at en meddelelse altid optræder i en konvolut (SBDH eller XHE), og det er denne konvoluterede meddelelse, der sendes fra C1 til C4 (og undervejs imellem C2 og C3 krypteres og pakkes yderligere ind som påkrævet af AS4 protokollen). Det naturlige valg af konvolut for vores yderligere kvitteringer på sundhedsområdet tilbage fra C4 til C1 er derfor også XHE eller SBDH, hvilket i øvrigt også er i overensstemmelse med andre domæners anvendelse af eDelivery, hvor konvoluterede kvitteringer allerede i dag sendes hele vejen fra C4 til C1.

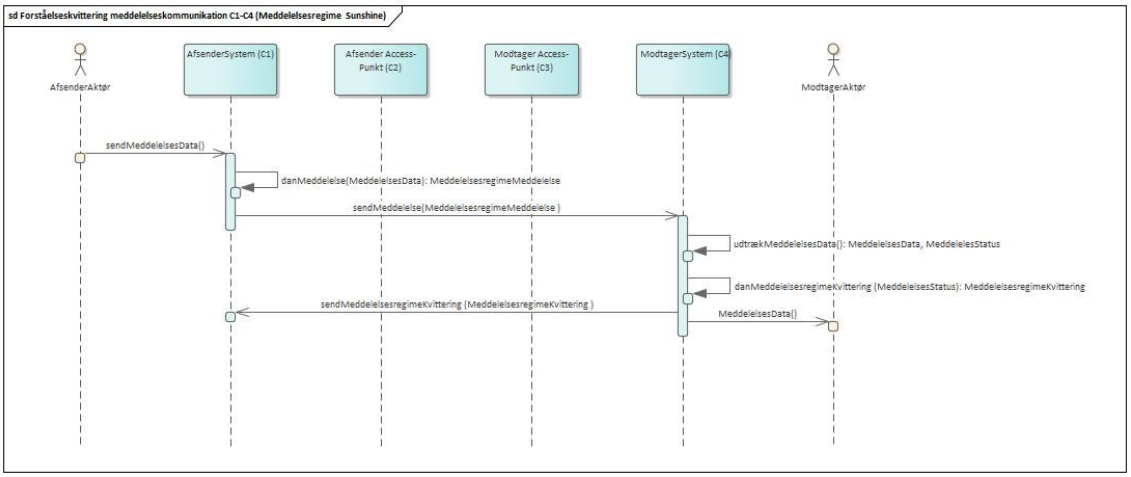
Transportkvitteringen fra C4 til C1 er yderst simpel af indhold og helt generisk og meddelelsesagnostisk og derfor den samme for samtlige meddelelsestyper på tværs af meddelelsesregimerne (OIO-XML, FHIR etc.), der sendes på sundhedsområdet, og skal sendes konvoluteret fra C4 til C1 via fire-corner modellen præcis som den meddelelse, den er kvittering for, blot den modsatte vej, som illustreret ved:



Figur 15: Solskinsscenarie for transportkvittering imellem C4 og C1.

Når C1 modtager en positiv transportkvittering fra C4 angående en meddelelse, betyder det, at C1 ikke længere behøver at bekymre sig om at få meddelelsen frem til C4. Men indtil denne positive kvittering er modtaget, er det fortsat C1's ansvar at sikre sig, at meddelelsen når frem til C4, hvilket kan indebære at gensende meddelelsen til C4 en eller flere gange (tilsvarende som beskrevet ovenfor imellem C2 og C3) – noget som ofte varetages af message service handleren imellem C1 og C2.

Forståelseskvitteringen fra C4 til C1 er ligeledes simpel af indhold, men ikke helt så generisk som transportkvitteringen, da den netop omhandler forståelse af meddelelsens indhold, og derfor bliver nødt til at være af samme meddelelsesregime (OIO-XML, FHIR etc.) som den oprindelige meddelelse, kvitteringen omhandler. Inden for hvert regime er meddelelseskvitteringen dog generisk, så den samme type meddelelseskvittering anvendes for alle meddelelser inden for et regime – f.eks. en for alle OIO-XML meddelelser, så en forståelseskvittering for et OIO-XML laboratoriesvar vil eksempelvis være af samme type som for en OIO-XML epikrise osv. Ligesom transportkvitteringen sendes forståelseskvitteringen konvoluteret fra C4 til C1 via fire-corner modellen den modsatte vej af den meddelelse, den er kvittering for, som illustreret ved:

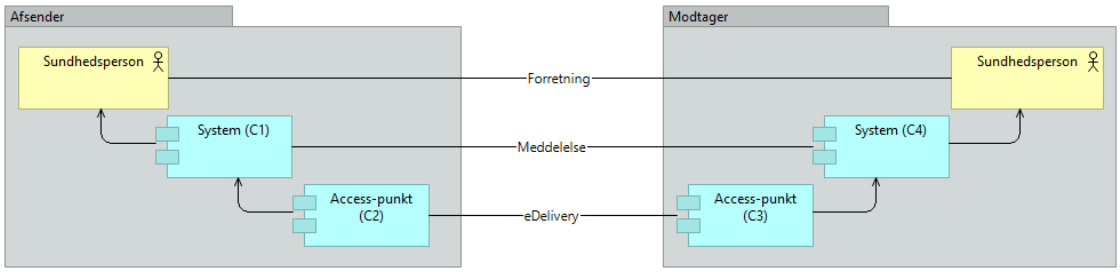


Figur 16: Solskinsscenarie for forståelseskvittering imellem C4 og C1.

Betydningen af forståelseskvitteringen er, hvorvidt C4 har forstået meddelelsen, igennem en automatiseret validering af meddelelsens struktur, format og syntaks, og dermed potentielt har mulighed for at agere på meddelelsens indhold eller ej. Derfor bliver forståelseskvitteringen nødvendigvis sendt efter transportkvitteringen for samme meddelelse. Dvs. først når C1 har modtaget en positiv forståelseskvittering fra C4, kan C1 være sikker på, at C4 potentielt vil kunne agere på og tage ansvar for det, som meddelelsens indhold indebærer – f.eks. udføre nogle laboratorieanalyser på givne identificerede blodprøver, når disse prøver ankommer til modtageren. Indtil C1 modtager en positiv forståelseskvittering fra C4, er C1 derfor forsat ansvarlig for det, som meddelelsens indhold indebærer (også i overensstemmelse med principperne PI1 og PI2).

På baggrund af ovenstående udbyggede pålidelige meddelelseskommunikation kan vi definere en forsendelsestransaktion, som dækker over forsendelsen af en meddelelse fra en afsender (C1) til en modtager (C4), og som inkorporerer alle de hertil nødvendige forsendelser af korrekt konvoluterede meddelelser og kvitteringer herpå, indtil den oprindelige afsender (C1) har modtaget en forståelseskvittering fra modtageren (C4) på sin oprindeligt afsendte meddelelse.

Ud over det nederste (AS4) lag med pålidelig meddelelseskommunikation imellem access-punkterne, som eDelivery kommer med out of the box, har vi på sundhedsområdet således der ovenpå introduceret ”kvitteringslag”, som udbygger den pålidelige meddelelseskommunikation til at strække sig hele vejen fra C1 til C4. Disse lag danner basis for hele den pålidelige punkt til punkt meddelelseskommunikation på sundhedsområdet, og er meget statiske efter de initielt er blevet etableret. Oven på disse ligger forretningslaget, hvor vi kan bygge vores forskellige forretningsmæssige arbejdsgange involverende meddelelseskommunikation, der kan være mere eller mindre komplekse, fra de simpleste tilfælde, hvor modtageren ikke skal sende et svar til afsenderen, til mere komplekse scenarier, hvor afsenderen skal sende svar tilbage (f.eks. laboratoriesvar som svar på en laboratorierekvisition, bookingsvar som svar på en henvisning, eller korrespondance meddelelser (der kan blive en længere kæde af på hinanden følgende meddelelser frem og tilbage imellem de to parter)). Dette kan illustreres ved følgende figur:



Figur 17: Lag i meddelelseskommunikationen.

5.2.4 SMP, postkasser og SOR

Information om en organisatorisk enheds postkasse er jf. afsnit 5.2.1 tilgængelig i SMP, hvilket åbner en vigtig diskussion. På den ene side er en postkasse relateret til den organisatoriske enhed, den modtager meddelelser for, og på den anden side er en postkasse også relateret til selve den meddelelsesinfrastruktur, som meddelelserne sendes via. SMP er en del af sidstnævnte, men i dag findes postkasseinformationen, som nævnt i afsnit 4.1, i SOR, altså meget tæt koblet til førstnævnte. For at tilgodese begge sider, og gøre den eksisterende kobling til SOR mindre tæt samt give mulighed for en-til-mange-relationen imellem en organisatorisk enhed og dens postkasser illustreret i Figur 6, foreslås det derfor, at postkasseinformationen flyttes til et selvstændigt register over postkasser udenfor SOR. På den måde separeres de tre forretningsmæssige forskellige begreber organisatorisk enhed, postkasse, og meddelelsestyper ud på tre separate, om end relaterede, registre SOR, "nye register over postkasseinformation", og SMP i logisk overensstemmelse med Figur 6. Det detaljerede samspil mellem de tre registre, samt præcis hvor, og dermed også under hvis governance, det nye register over postkasseinformation skal placeres er ikke en del af dette målbillede men i stedet noget, der skal besluttes i begyndelsen af den efterfølgende implementering af målbilledet. I samme ombæring skal man også beslutte et standardformat som registreringerne i SMP skal følge og på den måde profilere registreringerne i SMP.

5.2.5 Kopimodtagere

En kopimodtager af en meddelelse er i traditionel forstand, helt analogt til en kopimodtager af en e-mail (CC), en yderligere modtager af meddelelsen, som afsenderen angiver, ud over den primære modtager, og det er afsenderens ansvar at alle rette kopimodtagere (ligesom den primære modtager) modtager meddelelsen. Kopimodtagerfunktionalitet ligger i forretningslaget og er en del af *services rettet mod aktører i behandlingen af en borger* (jf. afsnit 2.4), der etableres på EHMI.

Kopimodtagere håndteres simpelt i eDelivery fire-corner modellen ved at C1, gennem sin message service handler, sender ens indholdsmæssige meddelelser til samtlige C4 hver især (primær modtager og hver og en af kopimodtagerne) via sit eget C2 og de respektive C3 for hver C4. Den eneste forskel på de enkelte meddelelser er den unikke identifikation af meddelelserne (og deres konvolutter). Det skal af meddelelsen fremgå klart, hvem der er primær modtager, og hvem

der er kopimodtager, da det ansvar disse to forskellige typer af modtager har ved modtagelse af en meddelelse er forskelligt. Diskussionen af det tilfælde, hvor der er flere interessenter, der har en interesse i en meddelelse, men disse er ukendte for afsenderen, følger i et senere afsnit.

5.2.6 Sundhedsadressering

Sundhedsadresseringsservicen ligger ligeledes i forretningslaget som en del af *services rettet mod aktører i behandlingen af en borger* (jf. afsnit 2.4), der etableres på EHMI. Da sundhedsadresseringsservicen skal være en hjælp til adressering for parterne, der anvender meddelelseskommunikation på sundhedsområdet, er det vigtigt at denne service er let tilgængelig for alle disse parter – for mere om dette (og andre sikkerhedsmæssige aspekter) se afsnit 6.4. Derfor vil det være oplagt at udstille denne service på en allerede eksisterende centralt placeret national platform på sundhedsområdet, da alle parter allerede har adgang til en sådan og implementeringsarbejdet må forventes at blive mindre, da mange krav f.eks. til skalering og oppetid allerede automatisk vil være opfyldt.

Sundhedsadresseringsservicen består jf. afsnit 4.3 af flere mindre services, og det er et krav at disse holdes klart afgrænset fra hinanden, da dette vil gøre både ændringer, udvidelser, og andet vedligehold af de enkelte services lettere. Endelig skal det være fleksibelt og nemt at tilføje yderligere relevante autoritative kilder til den samling, som sundhedsadresseringsservicen på et givet tidspunkt trækker på, så udvidelse med nye enkelte mindre services, i takt med at behovene for disse identificeres, er nemt.

Princip PT3 om anvendelse af modne bredt understøttede teknologier og modne bredt adopterede standarder til at højne leverandøruafhængighed gælder naturligvis også Sundhedsadresseringsservicen. Der kan her peges på standarder i Digital Europe's eDelivery byggeblok, som kan indbygge ”Collaboration Protocol Profile and Agreement” specifikationen [CPPA] fra OASIS [OASIS] således, at opslag i SMP og SML vil kunne beriges med yderligere metadata til gavn for forretningsadressering. Andre væsentlige eksisterende standarder, der er relevante ift. sundhedsområdet, er IHE’s (Integrating the Heathcare Enterprise) adressekatalogsstandarder: Health Provider Directory [HPD] og Mobile Care Services Discovery [MCSD]. Læs mere om alle tre standarders anvendelighed inklusive fordele og ulemper i Appendiks D. Valget blandt disse standarder betragtes som et implementeringsanliggende og derfor ikke som en del af målbilledet.

5.2.7 Forsendelsesmetadata

Ved forsendelse af meddelelser er der brug for at placere forskellige typer metadata i konvolutten. Metadata, som relaterer sig til eDelivery, skal konfigureres korrekt i de eDelivery kompatible konvolutter. Dette er basale informationer om meddelelserne og de håndteres jf. Digital Europe's eDelivery specifikationer. Metadata, som relaterer sig til MedComs meddelelsesregimer, skal ligeledes konfigureres korrekt i konvolutterne. Disse informationer relaterer sig f.eks. til statistik, og dette sker efter MedComs specifikationer.

Metadata, som relaterer sig til datadeling af meddelelser i repositorier, sendes normalt ikke med i den almindelige punkt-til-punkt kommunikation mellem C1 og C4. Mere om deling af meddelelser i afsnit 5.3, og i særdeleshed om metadata i forbindelse hermed i afsnit 5.3.2.

5.2.8 Forsendelsesstatus af meddelelser

Forsendelsesstatus af meddelelser kan overordnet betragtes som bestående af de tre trin opsamling, opbevaring, og udstilling. Her fokuseres på det første og sidste trin, da det mellemste trin er udpræget statisk og mest interessant i forhold til sikkerhed (i hvis sammenhæng det naturligvis diskuteres i kapitel 6). Her er vi dels (ved opsamling) nede i en af selve kernekomponenterne i EHMI og dels (ved udstilling) i forretningslaget som en del af *services rettet mod aktører i behandlingen af en borger* (jf. afsnit 2.4), der etableres på EHMI.

Opsamling til forsendelsesstatus for en meddelelse skal altid foregå, når en meddelelse passerer et access-punkt (både C2 og C3) af det pågældende access-punkt. Derudover skal det også foregå, når meddelelsen er leveret til modtagersystemet (C4). Om dette foretages af C4 selv, af C4's message service handler, eller af C3, når den modtager den tekniske kvittering fra C4, afhænger af hvilket af de setups beskrevet i afsnit 5.2.2 der eksisterer på modtagersiden, og aftales imellem C3 og C4 og er en del af tilslutningsaftalen herimellem (se kapitel 7 om governance). Endelig skal der også foregå opsamling til forsendelsesstatus, når meddelelsen afsendes fra C1. Alt efter hvilket setup beskrevet i afsnit 5.2.2, der eksisterer hos afsenderen, kan dette foregå i C1 eller dets message service handler. Det er essentielt, at de tidsstempler, som anvendes i forbindelse med opsamlingen af forsendelsesstatus for en given meddelelse, er konsistente med hinanden, men hvordan dette sikres i detaljer er et implementeringsanliggende.

Da det er en meddelelses vej fra afsender til modtager vi samler op, peger målbilledet på, at forsendelsesstatus for en meddelelse konsolideres i en centralt placeret komponent med et tilpas stort lager (f.eks. i form af en database) til at gemme forsendelsesstatusserne, hvorfra man nemt vil kunne etablere et overblik over den samlede status for en meddelelse. Uden denne konsolidering vil servicen, der skal svare på forsendelsesstatus blive mere (og unødig) kompliceret og performancetung. Samtidig er der ikke noget krav om, at denne komponent behøver at ligge sammen med (et) repositorie(t) for meddelelser, og faktisk vil det være at foretrække, at disse komponenter ligger hver for sig, for derved på en nem måde at mindske risikoen for at der implementeringsmæssigt opstår en uhensigtsmæssig tæt kobling imellem dem.

Naturen af forsendelsesstatus og anvendernes erfaringer med tilsvarende services fra andre domæner fordrer et serviceniveau, der er tæt på at være realtidstro, fordi ellers mister anvenderne tiltroen til forsendelsesstatusservicen – f.eks. hvis en borger på vej hjem i bussen efter et besøg hos sin praktiserende læge undersøger status for den henvisning lægen skulle sende, dur det ikke, hvis forsendelsesstatussen endnu ikke er blevet opsamlet, da informationen til borgeren så ikke er retvisende.

Princip PT5 om at undgå unødige teknologiske flaskehalse gælder naturligvis også for opsamlingen af forsendelsesstatus, men nærmere detaljer om hvortil og hvordan den opsamlede information gemmes betragtes som et implementeringsanliggende og derfor ikke som en del af målbilledet.

Ligeledes gælder princip PT3 om at anvende modne bredt understøttede teknologier og modne bredt adopterede standarder til at højne leverandøruafhængighed selvfølgelig også for opsamlingen af forsendelsesstatus. Der kan her peges på standarder i Digital Europe's andre byggeblokke, som f.eks. Blockchain teknologien, eller i e-handels eDelivery relaterede specifikationer for tilsvarende håndteringer. Førstnævnte er dog ikke på samme modenhedsniveau som de øvrige standarder og komponenter målbilledet peger på, og i øvrigt fokuserer de to standarder mest på selve datatransporten, og de dækker derfor ikke nærværende målbilledes fulde behov. De kan derfor kun benyttes til inspiration, og en (lokal dansk) standard, udviklet som udløber af dette målbillede, er derfor på dette punkt mest på sin plads. Det endelige valg betragtes dog, igen, som et implementeringsanliggende og derfor ikke som en del af dette målbillede.

I forbindelse med udstillingen af forsendelsesstatus for meddelelser er det uhyre vigtigt, at der anvendes letforståelige almene termer som langt de fleste anvendere vil kunne forstå umiddelbart, og tekniske termer som ”access-punkt”, ”corner” eller lignende må derfor ikke anvendes i præsentationen.

Forsendelsesstatusservicen er jf. diskussionen i kapitel 2 relevant for både borgere og sundhedspersoner. Servicen vil kunne bidrage til at inddrage borgeren som aktiv partner (jf. afsnit 1.3) og vil kunne gøre det lettere for sundhedspersoner at udvise rettidig omhu for sine patienter. Borgere skal kun kunne hente forsendelsesstatus for meddelelser angående dem selv (eller en pårørende man agerer på vegne af) angivet via unik borgeridentifikation inden for en angivet tidsperiode. Sundhedspersoner skal primært kunne hente forsendelsesstatus for meddelelser de selv har afsendt inden for en angivet tidsperiode, eventuelt yderligere indsnævret med typen af meddelelse og/eller unik borgeridentifikation, men de kan også have behov for at se forsendelsesstatus for meddelelser angående en given borger (angivet via unik borgeridentifikation) inden for en angivet tidsperiode i forbindelse med videreforsendelsesscenarier (se det følgende afsnit 5.2.9 for flere detaljer). Det er således som minimum nødvendigt, at unik borgeridentifikation (i form af id og type af id, som i langt de fleste tilfælde vil være et CPR-nummer), tidsangivelse, og afsender- og modtager-identifikation opsamles sammen med den unikke identifikation af meddelelsen og dens konvolut samt hvor langt meddelelsen er på sin forsendelsesvej, for at kunne tilgodese de opremsede anvendelsesscenarier af forsendelsesstatusservicen. De her opremsede scenarier må ikke ses som en udtømmende liste og flere vil ganske givet blive identificeret i forbindelse med det efterfølgende videre arkitektur og implementeringsarbejde.

5.2.9 Videreforsendelse af meddelelser

En særlig forretningsproces, videreforsendelse, skal diskuteres, da denne involverer nogle særlige problemstillinger. Vi er således atter i forretningslaget som en del af *services rettet mod aktører i behandlingen af en borger* (jf. afsnit 2.4), der etableres på EHMI.

Videreforsendelse af meddelelser er en ofte forekommende proces på sundhedsområdet, som foregår i udstrakt omfang dagligt på landets sygehuse, ikke mindst ved om-visitering af henvisninger, hvor en henvisning videresendes fra centralvisiteringen til den relevante modtager.

I denne sammenhæng kan det i nogle situationer være relevant for den oprindelige afsender at vide, hvor meddelelsen er blevet videresendt hen. Når den oprindelige meddelelse er mellem to forskellige afdelinger på sygehuse inden for samme region, er der ikke et særligt behov for dette, da man i stedet kan følge status i regionens elektroniske patient journal (EPJ) system. Men når den oprindelige meddelelse er mellem forskellige parter på sundhedsområdet, og ikke mindst i forbindelse med henvisninger fra lægepraksis til sygehus, kan der være et behov. Behovet opstår oftest, når det tager længere tid end forventet at få det forretningsmæssige svar, bookingsvaret, på den oprindelige meddelelse, henvisningen. Der er det ikke mindst lægefagligt vigtigt for den praktiserende læge at kunne udvise rettidig omhu for sin patient og kontakte rette instans for at forhøre sig om grunden til den tilsyneladende forsinkelse.

Dette kunne man forsøge at adressere rent punkt til punkt meddelelseskommunikationsmæssigt ved at kræve at en modtager ved en modtagelse af en videreforsendt meddelelse ikke blot skulle sende den obligatoriske meddelelseskvittering til den umiddelbare afsender, men også sende én til den oprindelige afsender, der således ville få besked om, at meddelelsen nu var afleveret til den nye modtager. Denne løsning er dog ikke at foretrække, da den dels ville komplicere håndteringen af kvitteringer for et begrænset sæt af særtilfælde, og det dels langt fra er alle videreforsendelsessituationer, hvor det er nødvendigt for den oprindelige modtager at vide, hvor meddelelsen er videresendt hen, før det forretningsmæssige svar modtages.

En anden løsning er at anvende forsendelsesstatusservicen introduceret ovenfor i afsnit 5.2.8. Afsenderen skal blot kalde forsendelsesstatusservicen, først via et kald for at få vished for om den oprindelige meddelelse er kommet frem, og dernæst via et andet kald for at finde ud af om, og i givet fald hvor, meddelelsen er (forsøgt) videresendt hen. På denne måde bliver det tydeligt for afsenderen, hvor meddelelsen er henne, og dermed hvem man eventuelt skal kontakte. Denne løsning introducerer ikke yderligere krav til punkt til punkt meddelelseskommunikation, bygger kun på services, der alligevel skal etableres, og involverer udelukkende de relevante parter, når der virkelig er behov for det, i stedet for at kræve at der ofte sendes information, der reelt ikke kommer til anvendelse. Derfor er denne løsning den foretrukne som målbilledet peger på.

Som et sidste twist på videreforsendelse er det for henvisninger muligt at tilføje supplerende oplysninger til meddelelsen i forbindelse med videreforsendelse. Dette skal betragtes som en ny

meddelelse, da meddelelsens indhold er ændret med den supplerende information, og fordi meddelelsens indhold er ændret fra det oprindelige, er det jf. princip PI5 påkrævet, at meddelelsens unikke identifikation også ændres, og her bliver begrundelsen særlig tydelig: Hvis identifikationen var den samme, hvilken af de to meddelelser (med eller uden de supplerende oplysninger) er der så tale om? Situationen i dag er desværre sådan, at der ved videreforsendelse af henvisninger med supplerende oplysninger i mange tilfælde godt nok anvendes et nyt konvolut-id (som påkrævet jf. afsnit 5.1 og princip PI6) men det samme id genanvendes for meddelelsen, så her bliver en ændring af den eksisterende håndtering påkrævet. Ved ren videreforsendelse uden supplerende oplysningerne er det nok at konvoluttens unikke identifikation ændres, men ved videreforsendelse med supplerende oplysninger skal både konvoluttens og meddelelsens unikke identifikationer ændres hver især.

5.2.10 Sammenfald af access-punkter

Her er vi nede ved en del af eDelivery kernen i EHMI fra afsnit 2.4. I eDelivery er der mulighed for at et givet fysisk access-punkt kan servicere mere end ét system, og det er op til en given organisation at beslutte sig for, hvordan sammenhængen imellem access-punkter og systemer skal være. Det kan derfor ske, at afsender access-punktet og modtager access-punktet for en meddelelse er fysisk ens. I dette ene særlige tilfælde er der ikke krav om, at meddelelsen skal sendes ud over eDelivery netværket, men alle de øvrige krav vi har i forbindelse med forsendelse af meddelelser er fortsat gældende, og kvitteringsflow, opsamling af meddelelsen (se næstfølgende afsnit), og opsamling af forsendelsesstatus skal derfor fortsat udføres som ellers.

Det er meget vigtigt at understrege, at dette kun gælder, når afsendende og modtagende access-punkter er fysisk ens. Det gælder således ikke, når de to access-punkter "ligger tæt ved hinanden", som f.eks. hører til den samme organisation (som samme region eller kommune) eller stammer fra den samme leverandør, da det i så fald ville bryde med den høje grad af standardisering, der ønskes, og de fordele, som derved opnås jf. principperne PF1, PA1, PT2, og PT3.

5.3 Deling af meddelelser

I forbindelse med opsamlingen af patient/borgercentrerede meddelelser til et repositorie, husker vi allerførst fra afsnit 1.2, at der er tale om deling af meddelelser, præcis som de så ud, da de blev sendt i punkt til punkt kommunikationen.

Derefter erindrer vi fra kapitel 3, at hvorvidt der er lovhjemmel til at opsamle og dele en meddelelse kan afhænge af den givne type af meddelelse, så i forhold til opsamlingen er det, jf. princip PI4, vigtigt at sikre sig, at der er hjemmel til at opsamle den pågældende type meddelelse, hvilket skal undersøges inden, meddelelsestypen begyndes at opsamles i forbindelse med forsendelse via eDelivery netværket.

Under forudsætning af, at det er lovligt at opsamle og dele meddelelserne, er det dernæst vigtigt jf. princip PI5, at meddelelserne har en unik identifikation, således at der for en given unik meddelelsesidentifikation svarer ét og kun ét meddelelsesindhold – hvis dette ikke var tilfældet ville man ikke kunne holde styr på de enkelte meddelelser i forhold til hinanden i forbindelse med deling eller i supportsammenhæng.

Endelig skal man være opmærksom på, at alt efter om der anvendes ét centralt repositorie eller flere decentrale repositorier placeret hos forskellige parter, så vil det være forskellige databehandlingsaftaler, der skal indgås – se også afsnit 7.2 om governance desangående.

Når alt dette indledningsvist er fastslået kan deling af meddelelser overordnet set, ligesom forsendelsesstatus for meddelelser, betragtes som bestående af følgende tre trin:

1. Meddelelserne opsamles og gemmes i et repositorie
2. Meddelelserne opbevares i repositoriet
3. Meddelelserne hentes af anvendere via udstillede services

I førstkommende underafsnit fokuseres, igen ligesom for forsendelsesstatus for meddelelser, på det første og sidste trin om henholdsvis opsamling og udstilling. Her er vi atter dels (ved opsamling) nede i en af selve kernekomponenterne i EHMI og dels (ved udstilling) i forretningslaget som en del af *services rettet mod aktører i behandlingen af en borger* (jf. afsnit 2.4), der etableres på EHMI.

5.3.1 Opsamling og udstilling

I forhold til opsamlingen er det vigtigt jf. princip PT5 ikke at introducere unødvendige teknologiske flaskehalse og deraf afledte performanceproblemer, men dette målbillede dikterer ikke en metode til opsamlingen af meddelelser – dette betragtes som et implementeringsanliggende – ligesom det heller ikke peger på, om der skal anvendes ét centralt eller flere decentrale repositorier.

Der er ikke, som for forsendelsesstatus i afsnit 5.2.8, krav om at opsamlingen er tæt på at være realtidstro, men omvendt må der ikke være en stor forsinkelse fra meddelelsen er blevet afleveret til C4 til den også er tilgængelig for deling. En opsamlingsmekanisme, der involverer at samle afsendte meddelelser sammen hos en afsender for efterfølgende én gang i døgnet at gemme alle disse i et repositorie, er således ikke en acceptabel løsning. Tilsvarende må meddelelserne heller ikke opsamles før de er blevet afleveret til C4.

Det er ligeledes i forhold til opsamlingen, jf. princip PI3, vigtigt, at opsamling af en given meddelelse kun foregår én gang i forbindelse med forsendelsen af meddelelsen, da det ellers vil gøre opsamlingen unødigt både kompliceret og performancetung.

Endelig er det også vigtigt at fastlægge ansvaret for opsamlingen klart, så dette er veldefineret, og der ikke kan være tvivl om det.

I forbindelse med diskussionen af sikkerhed i afsnit 6.2.1 skitseres en metode til opsamlingen, der er tæt på realtidstro, ikke sker inden meddelelsen er afleveret til C4, ikke giver anledning til nogle flaskehalse, fastlægger ansvaret klart, og ydermere fra et sikkerhedsperspektiv vil være fordelagtig. Denne anbefalede opsamlingsmetode går kort fortalt ud på, at det afsendende systems message service handler via sit access-punkt sender en tro kopi af meddelelsen til et access-punkt dedikeret til et meddelelsesrepositorie, når den positive transportkvittering for meddelelsen modtages. Andre metoder, der lever tilsvarende op til sikkerhedskravene, ikke går imod principperne PI3 og PT5, ikke sker før meddelelsen er afleveret til C4, og ikke involverer en stor forsinkelse i hvornår meddelelsen er tilgængelig for deling i forhold til hvornår den er blevet leveret til C4, vil dog også være acceptable.

Udstillingen af de sendte meddelelser via en service er både interessant for sundhedspersoner og borgere, da den, jf. diskussionen i kapitlerne 1.3, 2 og 4, bidrager til at realisere strategiske mål om at skabe sammenhæng i sundhedsvæsenet og inddrage borgeren som aktiv partner. Der eksisterer allerede en national infrastruktur for dokumentdeling med underliggende repositoriestruktur baseret på IHE-XDS. Til denne hører også en dokumentdelingsservice på den nationale service platform for sundhedsområdet, der netop kan kaldes af både sundhedspersoner og borgere (via websites, app's etc.). Anvendelse af denne, eller dele af denne, eksisterende dokumentdelingsinfrastruktur, vil derfor forventeligt kunne nedbringe det arbejde, der skal udføres for at implementere deling af meddelelser, men det er ikke et eksplicit krav at anvende den. Hvad der imidlertid er krav om er, at servicen til deling af meddelelser opfylder de samme krav og regler som dokumentdelingsservicen og den underliggende XDS infrastruktur gør, inklusive valideringsregler for data ved registrering, regler for anvendelse af delte data, jf. princip PI3, og sikkerhedsmæssige krav og regler, hvilket vil sige krav til autentifikation af anvenderne af servicen via digitale certifikater, krav til oppetid og svartider for servicen og repositorierne, samt at servicen integrerer med MinSpærring og MinLog – mere om dette i kapitel 6 om sikkerhed. Derudover skal servicen via tilpas fleksible kaldeparametre muliggøre de forskellige anvendelsesscenarier. Borgere skal kun kunne hente meddelelser angående dem selv (eller en pårørende man agerer på vegne af) angivet via unik borgeridentifikation inden for en angivet tidsperiode. Sundhedspersoner skal som minimum kunne hente meddelelser for en angivet borger (via unik borgeridentifikation) inden for en angivet tidsperiode, eventuelt yderligere indsnævret med type af meddelelse, samt for et angivet unikt meddelelses id (relevant i forhold til notifikationer (se næste afsnit 5.3.2)).

5.3.2 Metadata

Der skal foretages en klar udpegning af hvilke metadata angående meddelelserne, der er nødvendige for at muliggøre de forskellige relevante anvendelsesscenarier, i forbindelse med etableringen af deling af meddelelser, hvor metadata netop er særlig vigtige, da det er dem, som definerer hvilke søgninger på meddelelser, der kan foretages. Denne udvælgelse må derfor ikke

være så snæver, at den udelukkende fokuserer på de data, som anvendelserne nævnt i slutningen af det foregående afsnit 5.3.1 kræver til den første generation af anvendelsesscenarier. De metadata, der defineres i forbindelse hermed, skal endvidere kunne indgå i det sæt af metadata, der anvendes til deling af andre dokumenter end meddelelser.

Det skal også afgøres, hvorfra metadata skal tages i meddelelserne. Hvis alle relevante metadata er tilstede i meddelelsens konvolut, bliver opsamlingen af metadata agnostisk i forhold til typen af meddelelse og samtidig særlig simpel, da konvolutten er ens for samtlige meddelelser på tværs af de enkelte meddelelsesregimer, hvilket også er baggrunden for princip PI7 og hænger sammen med visionens generelle infrastruktur. Selvfølgelig skal afsenderen udføre et mindre ekstra arbejde ved at udfylde konvolutten med disse metadata, men afsenderen står alligevel med alle disse data på hånden i forbindelse med genereringen af meddelelsen, så dette er at foretrække, fremfor at de skal tages fra forskellige steder i de forskellige typer af meddelelser. Endelig betyder det også, at ændringer i metadata bliver væsentligt nemmere at håndtere, da det kun er ét og samme sted, der er ændringer for samtlige meddelelsestyper. Følgelig peger dette målbillede på, at metadata til anvendelse af deling af meddelelser skal være tilstede i konvolutten for meddelelserne, når disse opsamles til deling. Jf. afsnit 5.2.7 er disse metadata dog ikke nødvendige i forhold til punkt til punkt kommunikationen fra C1 til C4, og i forbindelse med det efterfølgende videre arkitektur og implementeringsarbejde skal det derfor afgøres, om disse to kategorier af metadata på en eller anden vis skal holdes separat fra hinanden for at gøre konvolutterne så slanke og dedikerede som muligt.

Når alle relevante metadata placeres i meddelelsens konvolut, betyder det, at f.eks. den unikke borgeridentifikation også trækkes ud i konvolutten. Dette udgør imidlertid ikke et yderligere sikkerhedsproblem, da hele meddelelsen, inklusive konvolut, er krypteret imellem access-punkterne.

Metadata for meddelelserne skal endvidere kunne virke i samspil med, og dermed tilgodese, de vigtigste allerede eksisterende danske standarder for metadata:

- Den danske XDS metadata profil for dokumentdeling
- Det fællesoffentlige metadataformat, der anvendes af både den fællesoffentlige dataforddeler og den kommunale beskedfordeler

Endelig skal det være nemt at vedligeholde standarden for metadata for meddelelser, da metadata, præcis ligesom resten af verden og dette målbillede selv, ikke er statiske.

5.3.3 Notifikationer

Her er vi atter i forretningslaget som en del af *services rettet mod aktører i behandlingen af en borger* (jf. afsnit 2.4), der etableres på EHMI. Det vil være fordelagtigt for en sundhedsperson at kunne modtage en notifikation, når en meddelelse angående en borger, som sundhedspersonen har en behandlingsrelation til, er tilgængelig via deling. Dette betyder, at sundhedspersonen i

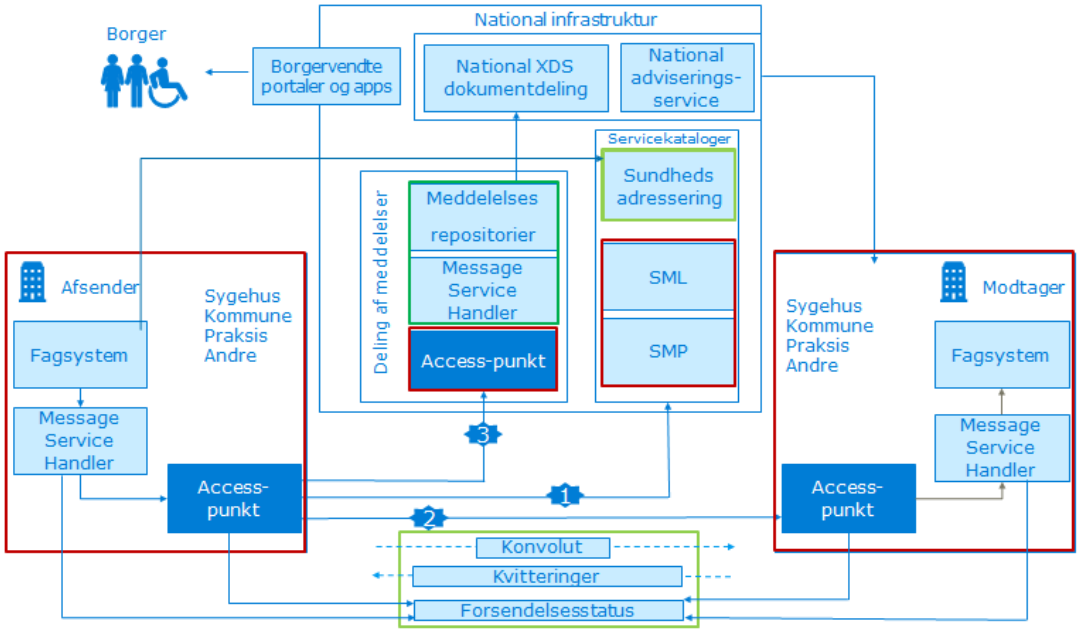
forhold til notifikationssystemet skal kunne angive, hvilke unikt identificerede borgere man er interesseret i at abonnere på notifikationer for, så der skal være en sådan tilmeldings- og afmeldings-mekanisme. Notifikationen angående meddelelser skal ligesom de øvrige notifikationer på sundhedsområdet indeholde så få informationer som muligt og ingen personoplysninger ud over den unikke borgeridentifikation (i langt de fleste tilfælde CPR nummeret), som er nødvendigt for at indikere hvilken konkret borger, notifikationen omhandler. Notifikationen skal således ikke indeholde selve meddelelsen, men i stedet blot den unikke identifikation af meddelelsen og meddelelsestypen (laboratoriesvar, epikrise, etc.) samt identifikationen på borgeren, så sundhedspersonen efterfølgende kan hente meddelelsen ud fra den unikke meddelelsesidentifikation via servicen beskrevet ovenfor i afsnit 5.3.1, såfremt sundhedspersonen ud fra meddelelsestypen vurderer det relevant. Der eksisterer allerede den nationale adviseringsservice på sundhedsområdet på den nationale service platform for sundhedsområdet, som hvis anvendt forventes, ligesom ovenfor, at kunne nedbringe det arbejde, som skal udføres for at implementere denne nye type notifikation.

5.3.4 Konvertering mellem meddelelsesformater

Som nævnt flere gange er det meddelelserne, som de blev sendt, der skal deles. Dvs., der foregår ingen konvertering i infrastrukturen fra et meddelelsesformat til et andet – f.eks. et kanonisk format – i forbindelse med deling af meddelelser. Så hvis f.eks. et laboratoriesvar er sendt fra afsender til modtager via punkt til punkt kommunikation i XRPT01 XML-formatet, så bliver selvsamme laboratoriesvar også gjort genstand for deling i XRPT01 XML-formatet. Hvis en anvender af delingsservicen for meddelelser ikke understøtter et givet meddelelsesformat, er det således anvenderens eget ansvar at få konverteret til et understøttet format jf. princip PT4 om, at den fælles løsning for meddelelseskommunikation er standardiseret på nationalt niveau og ansvaret for at integrere dertil ligger hos de enkelte parter. En sådan konvertering kan ske enten via en lokal konverteringskomponent, som en integrationsplatform, ejet af (eller i samme lokale infrastruktur som) anvenderen eller via en mere centralt placeret, men uafhængigt af meddelelsesrepositorierne, konverteringskomponent, certificeret til formålet af en passende instans (se kapitel 7 om governance), som der på denne måde kan opstå et marked for interesserede leverandører at byde ind på. Sidstnævnte kan således betragtes som en servicekomponent, der er en del af *services rettet mod aktører i behandlingen af en borger* (jf. afsnit 2.4), der etableres på EHMI.

5.4 Samlet overblik

Den samlede logiske arkitektur for EHMI beskrevet i dette kapitel, som realiserer strategi- og forretningsarkitekturen fra kapitlerne 2 og 4, kan illustreres ved:



Figur 18: Samlet logisk arkitektur for EHMI.

De med rødt markerede dele repræsenterer kerne eDelivery delen af arkitekturen, og de grønt-markerede dele er de yderligere komponenter og kapabiliteter, som målbilledet introducerer til EHMI – de mørkegrønne er særligt i forhold til deling af meddelelser. Endvidere er rækkefølgen af kald som det afsendende access-punkt udfører i forbindelse med afsendelse af en meddelelse indikeret ved nummerering.

Den samlede arkitektur i Figur 18 blev afprøvet med konkrete komponenter i pilotafprøvningen, og i evalueringsrapporten for pilotafprøvningen blev det konkluderet, at pilotafprøvningen ”sammen med erfaringer fra andre domæner, hvor tilsvarende IT-arkitekturer er implementeret, giver stærke argumenter for, at IT-arkitekturen lever op til målbilledets vision, mål og arkitekturkvalitetsegenskaber” [PILEVAL].

6. Sikkerhed

Diskussionen af sikkerhed tager udgangspunkt i referencearkitekturen for informationssikkerhed på sundhedsområdet [REFARKINFSIK]. I denne opereres med fem dimensioner ved sikkerhed, der overordnet dækker som følger:

Dimension	**Uddybning**
Autenticitet	Egenskab, der beskriver, om noget er, hvad det giver sig ud for at være (om det er autentisk/ægte). Gennem autenticitetssikring/autentifikation sikres, at en ressource eller person er den påståede
Tilgængelighed	Egenskab ved service der sikrer, at servicen er til rådighed for en bruger i henhold til fastlagte rammer
Integritet	Egenskab ved et informationsaktiv, der sikrer dettes nøjagtighed og fuldstændighed. Integritet sikrer fx kommunikation, således at en serviceudbyder og en serviceaftager er garanteret, at beskederne ikke ændres mellem afsender og modtager uden at én af parterne opdager det
Uafviselighed	Egenskab ved information der gør det muligt at bevise, at en given bruger har udført en given handling på et givet tidspunkt
Fortrolighed	Egenskab ved informationssystem der medfører, at kun bestemte brugere har adgang til bestemte data eller bestemt information

Sikkerhedsdimensionerne adresseres både ad tekniske veje og organisatoriske veje. Dette kapitel omhandler de tekniske, og de organisatoriske følger i nedenstående governance kapitel 7.

Integritet i forbindelse med meddelelseskommunikation handler i dette kapitel om integritet af den sendte meddelelse, som den er. Hvorvidt al den relevante information, der vises for slutbrugeren i det afsendende system (C1), bliver retvisende sendt i en meddelelse, er, jf. princip PI1, det afsendende systems ansvar og ikke infrastrukturens. Tilsvarende om al den information, der modtages i en meddelelse i det modtagende system (C4), vises korrekt for slutbrugeren af systemet, er, jf. princip PI2, det modtagende systems og ikke infrastrukturens ansvar. Hvorledes dette, der kunne benævnes forretningsmæssig integritetssikring, sikres i detaljer, er ikke en del af dette målbillede, men der stilles naturligvis krav om at principperne PI1 og PI2 skal overholdes af de involverede systemer i den forbindelse.

I de følgende fire afsnit gennemgås de fem dimensioner for henholdsvis punkt til punkt kommunikation, deling af meddelelser, forsendelsesstatus af meddelelser, og sundhedsadresseringsservicen.

6.1 Punkt til punkt kommunikation

eDelivery har indbygget mekanismer imellem access-punkterne (C2 og C3 i fire-corner modellen) i forhold til de fleste af de fem dimensioner [EDELSIK]:

Dimension	Uddybning
Autenticitet	Sikres via signering af meddelelse i afsendende access-punkt med efterfølgende verifikation af signaturen i modtagende access-punkt
Integritet	Sikres dels via den underliggende protokol (AS4) og yderligere via signeringsmekanismen beskrevet under autenticitet
Uafviselighed	Sikres ved at teknisk kvittering for modtagelse af meddelelse sendes fra modtagende access-punkt til afsendende access-punkt signeret på tilsvarende vis som en almindelig meddelelse
Fortrolighed	Sikres via kryptering af meddelelsens body i afsendende access-punkt med efterfølgende dekryptering i modtagende access-punkt

Der er således klare og effektive sikkerhedsmekanismer for fire af de fem sikkerhedsdimensioner, og det er kun tilgængelighedsdimensionen, som eDelivery ikke har indbygget en eksplicit håndtering af. Dog kan man sige, at der i eDeliverys fire-corner model ligger en implicit håndtering af tilgængelighed by design, i det meddelelserne sendes direkte imellem de relevante parters access-punkter uden at skulle routes gennem det samme punkt på forsendelsesnetværket i overensstemmelse med princip PT5 om at undgå potentielle teknologiske flaskehalse. Da eDelivery dels anvendes til meddelelseskommunikation på flere andre områder end sundhedsområdet i EU og Danmark og dels er baseret på underliggende protokoller og sikkerhedsmekanismer, der også anvendes i andre meddelelseskommunikationssammenhænge, er anvendelsen af eDelivery som underliggende fundament til meddelelseskommunikation på sundhedsområdet også implicit i overensstemmelse med princip PT6.

Der er derfor et rigtig godt udgangspunkt for sikkerhed i form af hvad eDelivery stiller til rådighed imellem C2 og C3, og det er vigtigt at denne suppleres med tilsvarende gode sikkerhedsmekanismer imellem henholdsvis C1 og C2 og C3 og C4, så meddelelseskommunikationen er dækket sikkert ind hele vejen fra C1 til C4. Når man udvider analysen til den komplette punkt til punkt kommunikation og indbefatter afsender- og modtager-systemerne (C1 og C4 i fire-corner modellen), og samtidig supplerer det som eDelivery lægger op til out of the box med vores egne tiltag på sundhedsdomænet, ser situationen ud som beskrevet i de følgende fem underafsnit.

6.1.1 Autenticitet

Ud over den beskrevne native eDelivery sikring imellem access-punkterne, stiller vi på sundhedsområdet krav om, at meddelelseskonvolutten signeres i C1 og at denne signatur efterfølgende verificeres i C2. På denne måde sikrer vi autentifikation af C1 i C2 (og helt tilsvarende

imellem C3 og C4), hvilket også er helt i overensstemmelse med anbefalingen fra organisationen bag eDelivery. Denne autentifikation vil være en del af den aftale, der indgås imellem access-punktet og det system access-punktet agerer på vegne af.

Autentifikation kan foregå enten via system-beviser eller bruger-beviser. I forhold til meddelelseskommunikation vurderes autentifikation via system-beviser generelt at ville være tilstrækkeligt. Det er dette "system-bevis niveau", der anvendes i meddelelseskommunikation i dag, og det forventes at være tilstrækkeligt også i de kommende år.

6.1.2 Integritet

Sikres ud over den beskrevne native eDelivery sikring imellem access-punkterne også af den under autenticitet (afsnit 6.1.1) just beskrevne konvolutsignering, samt via de protokoller, der anvendes imellem access-punkterne og de systemer access-punkterne agerer på vegne af – f.eks. TLS (Transport Layer Security), der også anbefales af organisationen bag eDelivery.

6.1.3 Uafviselighed

Sikres ud over den beskrevne native eDelivery sikring imellem access-punkterne også af det obligatoriske meddelelseskvitterings-flow på sundhedsdomænet fra modtageren tilbage til afsenderen beskrevet ovenfor i afsnit 5.2.3, hvor generiske meddelelseskvitteringer sendes (som meddelelser) fra C4 til C1, når C4 modtager en meddelelse fra C1. Sikres endvidere af opsamlingen af forsendelsesstatus for meddelelserne på deres vej fra afsenderen til modtageren til forsendelsesstatusservicen, som også beskrevet i afsnit 5.2.8.

6.1.4 Fortrolighed

Da alle meddelelser under sundhedsdomænet som udgangspunkt indeholder følsomme personoplysninger skal kryptering anvendes i så vid udstrækning som muligt. Ud over den beskrevne native eDelivery kryptering af meddelelserne imellem access-punkterne, skal meddelelsen derfor også krypteres imellem afsender og afsendende access-punkt (C1 og C2) samt imellem modtagende access-punkt og modtager (C3 og C4). Anvendelse af denne kryptering vil være en del af den aftale, der indgås imellem access-punktet og det system access-punktet agerer på vegne af. Når kryptering anvendes disse to steder opnås kryptering af meddelelsen hele vejen fra afsender til modtager, men det er dog en leddelt kryptering, i det der "omkrypteres" (dekrypteres og efterfølgende krypteres igen) i begge de to access-punkter. Den leddelte kryptering er ikke det samme som end to end kryptering, da access-punkterne i forbindelse med deres omkryptering har adgang til den ukrypterede meddelelse-body.

Såfremt man insisterer på at anvende ægte end to end kryptering af meddelelsens body fra C1 til C4 (med kryptering i C1 med C4's offentlige nøgle), betyder det, at meddelelsen godt nok kan samles op i et repositorie og efterfølgende udstilles til anvendere, men ingen andre end den oprindelige C4 vil kunne læse den (efter at have dekrypteret den med sin private nøgle).

Da dette er i modstrid med en af målbilledets helt fundamentale målsætninger skal man anvende noget andet til denne slags meddelelseskommunikation end eDelivery på sundhedsområdet. I praksis vil noget lignende end to end kryptering af meddelelseskommunikationen kunne opnås, såfremt dette ønskes, hvis C2 tages under fuld kontrol af C1 og integreres meget tæt hermed og tilsvarende for C3 af C4, jf. muligheden "Alt samlet" i Figur 14.

6.1.5 Tilgængelighed

I forhold til tilgængelighed er de helt overordnede krav til infrastrukturen for punkt til punkt meddelelseskommunikation, at den skal være til rådighed med aftalt oppetid og effektueringshastighed, der skal være tilpas henholdsvis høj og hurtig. Meddelelseskommunikation inden for sundhedsdomænet er en af hjørnestenene i sundhedsvæsenet, og sundhedsområdet er, som nævnt i afsnit 2.2, udnævnt som en af de særlig samfundskritiske sektorer. Derfor er tilgængelighed en meget vigtig dimension i sikkerhedsdiskussionen i dette målbillede, som det også fremgår af arkitekturkvalitetsafsnittet 2.5.

I forhold til en tilpas hurtig effektueringshastighed skal der via aftaler med leverandøren af det underliggende netværk sikres tilstrækkelig båndbredde til at kunne sende meddelelserne på sundhedsområdet. Derudover skal vi jf. princip PT5 undgå at introducere potentielle teknologiske flaskehalse, så for eksempel skal vi ikke lede samtlige meddelelser på sundhedsområdet gennem det samme access-punkt. Endvidere er der performance-, robustheds- og skaleringskrav til de enkelte access-punkter, jf. princip PT5, hvilket udtrykkes i tilslutningsaftalen for access-punktet (se kapitel 7 om governance).

I forhold til tilpas høj oppetid er der flere forskellige aspekter, der skal adresseres. I strategien for cyber- og informationssikkerhed i sundhedssektoren [CYBERSTRAT] opereres med fire spor i forhold til at skabe tryghed i forhold til cyber-angreb. Disse er "forudse", "forebygge", "opdage", og "håndtere", og i den følgende tabel anvendes disse som grupperinger for de mekanismer målbilledet peger på i forhold til at sikre tilpas høj oppetid:

Spor	**Mekanismer**
Forudse	**Sikkerhedsaudits**: Regelmæssige sikkerhedsaudits af de forskellige komponenter, der udgør infrastrukturen for meddelelseskommunikation, skal afholdes, f.eks. med penetrationstest

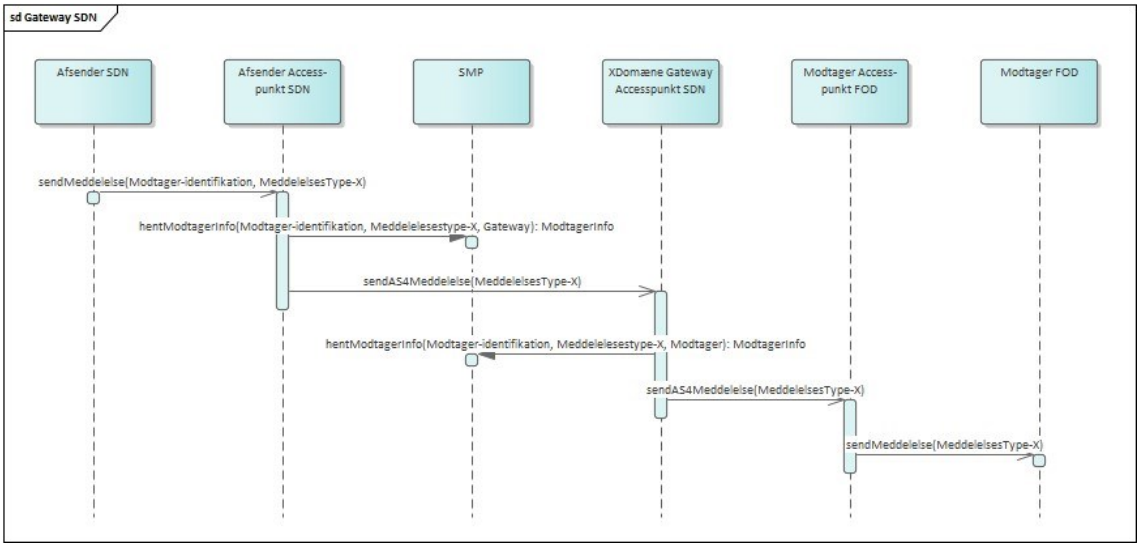
Spor	Mekanismer
Forebygge	**Beskyttelse af infrastrukturens centrale komponenter**: For at minimere risikoen for at infrastrukturen for meddelelseskommunikation tvinges ned af et cyber-angreb, skal der tages tilstrækkelige beskyttelsesmetoder i brug for i høj grad at sikre sig imod dette (100% sikkert er ikke realistisk). Det skal være meget svært at gøre (dele af) infrastrukturen til meddelelseskommunikation på sundhedsområdet utilgængelig i kortere eller længere tid, f.eks. via et denial of service angreb ved udefra at spamme et access-punkt med masser af meddelelser eller et hijacking angreb af et access-punkt eller SMP endda med muligt efterfølgende ransom-krav. Der skal derfor fokuseres på at sikre de centrale dele af infrastrukturen til punkt til punkt meddelelseskommunikation, som består af SML, SMP, trust store, og access-punkterne: - Access-punkter: Access-punkterne placeres i et beskyttet netværk med kontrolleret, sikret, og begrænset adgang, da angrebsvektoren så mindskes betragteligt i forhold til hvis access-punkterne lå med adgang til det åbne internet – uddybes og konkretiseres i teksten neden for tabellen. Dette vil i øvrigt også være med til yderligere at sikre imod cyber-angreb rettet imod integriteten (injection i meddelelser inden afsendelse i C2) eller uafviseligheden (afsende falske kvitteringer fra C3) - Øvrige centrale komponenter: SML, SMP, og trust store skal sikres med avancerede beskyttelsesmetoder som intrusion detection etc.
Opdage	**Effektiv overvågning**: Det skal være nemt at overvåge meddelelseskommunikationen, så eventuelle problemer hurtigt kan detekteres og efterfølgende tages hånd om
Håndtere	**Hurtig reetablering**: Hvis ulykken er ude, er det meget vigtigt, at meddelelseskommunikationen hurtigt og effektivt kan reetableres, såfremt den tvinges ned enten af almindelige driftsmæssige problemer, såsom defekt hardware, eller af ondsindede cyber-angreb, da det er med til at sikre den robusthed, som formuleret i visionen, der er nødvendig for at kunne sikre den ønskede høje oppetid. Præcis hvor hurtigt reetableringen skal være vil være udtrykt igennem de indgåede SLA aftaler (se kapitel 7 om governance)

I forhold til uddybning og konkretisering af forebyggelse imod cyber-angreb for access-punkter, så findes der allerede et beskyttet netværk på sundhedsområdet, nemlig Sundhedsdatanettet (SDN), og målbilledet peger på at anvende dette, så access-punkterne placeres på det. Dette vil ikke bare give de beskrevne sikkerhedsmæssige fordele, men vil også give et godt udgangspunkt for den kommende implementering, da SDN allerede er veletableret, og langt de fleste af parterne, der anvender meddelelseskommunikation har allerede sikrede tilslutninger

dertil (såsom via MPLS og VPN). Endvidere bør det nævnes, at anvendelsen af SDN til meddelelseskommunikation på sundhedsområdet på sin vis er et logisk valg, fordi andre typer af kommunikation på sundhedsområdet, som request/response via webservices, allerede anvender SDN – eDelivery meddelelseskommunikationens anvendelse af SDN kan således betragtes som en konsoliderende samling af de forskellige typer af kommunikation på sundhedsområdet til SDN.

Da de øvrige dele af eDelivery (SML, SMP, etc.) og de øvrige domæner under eDelivery anvender det åbne internet, giver anvendelsen af SDN på sundhedsområdet dog anledning til at meddelelseskommunikationen ind og ud af sundhedsområdet samt anvendelsen af SML og SMP fra sundhedsområdet kompliceres. Dette er dog ikke en uoverstigelig komplikation og kan løses via introduktionen af en gateway til sundhedsområdet, der har adgang både til SDN og det åbne internet, og som derfor også skal have høj beskyttelse imod cyber-angreb (ligesom SMP etc.).

På gateway'en placeres et access-punkt, der anvendes som intermediært i forhold til kommunikationen ind og ud af sundhedsområdet, der således kommer til at bestå af to på hinanden umiddelbart følgende meddelelseskommunikationer. For meddelelseskommunikation ud af sundhedsområdet først fra afsender på sundhedsområdet på SDN til gateway og derefter fra gateway til modtager uden for sundhedsområdet som illustreret ved følgende figur:



Figur 19: Meddelelseskommunikation ud af sundhedsområdet via gateway.

Helt tilsvarende vil meddelelseskommunikation ind til sundhedsområdet først være fra afsender uden for sundhedsområdet til gateway og derefter fra gateway til modtager på sundhedsområdet. Konstruktionen med to på hinanden direkte følgende kommunikationer via et centralt access-punkt er ikke opfundet til lejligheden, men er en eksisterende standardkonstruktion i eDelivery (desværre lidt inkonsistent) kaldet tre-corner modellen.

Kald til SML fra et access-punkt på sundhedsområdet på SDN kan relativt simpelt realiseres via en viderestillende proxy SML service på gateway'en. I SMP skal der registreres mere end én netværksadresse med sigende label for hvert access-punkt, så et givet access-punkt, der deltager i meddelelseskommunikationen alt efter situationen altid vil kunne slå den korrekte netværksadresse på den umiddelbare modtager op (internt på SDN eller gateway), men også dette er der allerede mulighed for i eDeliverys standard SMP.

6.2 Deling af meddelelser

Som i afsnit 5.3 er der flere forskellige trin ved deling af meddelelser, som diskussionen af sikkerhed med fordel kan deles op i:

1. Meddelelserne opsamles og gemmes i et repositorie
2. Meddelelserne opbevares i repositoriet
3. Meddelelserne hentes af anvendere via udstillede services

I det følgende diskuteres de fem sikkerhedsdimensioner for hver af de tre trin under behørig hensyntagen til at deling af meddelelser, jf. princip PT6, bør overholde de samme sikkerhedskrav og -regler som deling af øvrige data på sundhedsområdet.

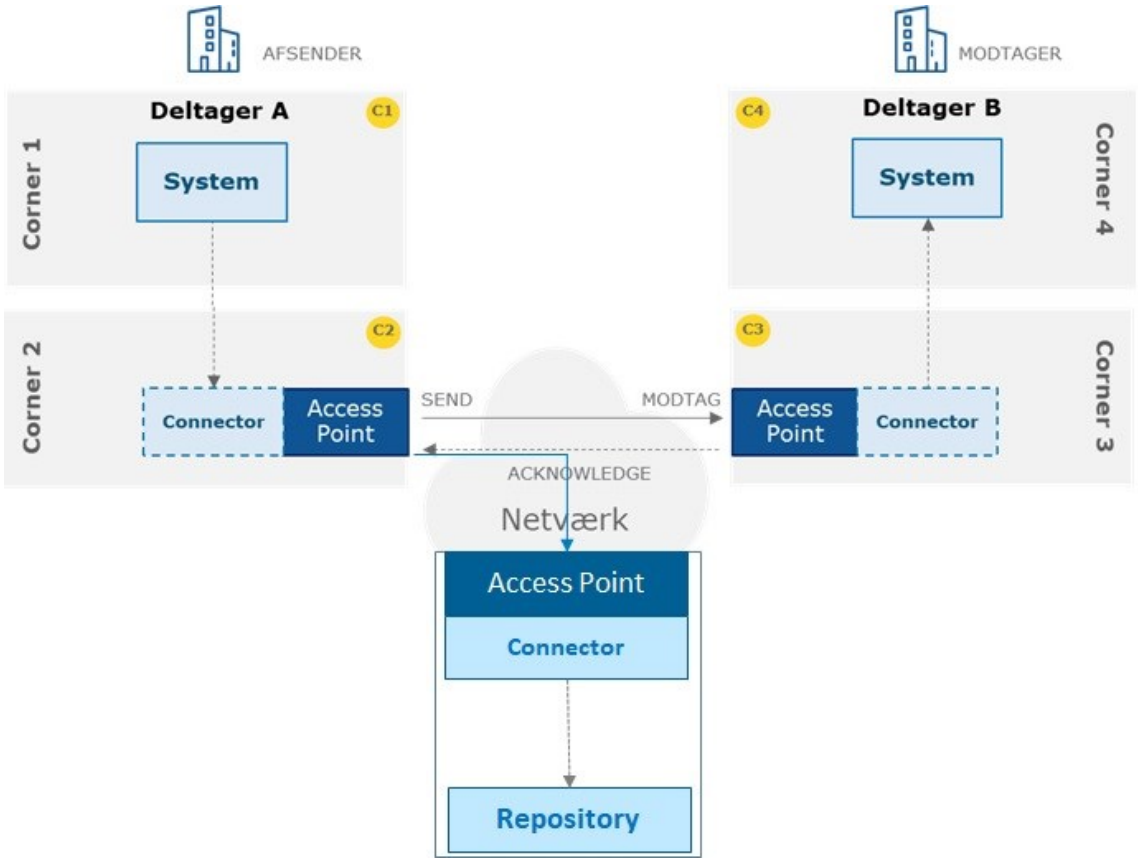
6.2.1 Opsamling til repositorie

Overordnet set ønskes en sikkerhedshåndtering på samme niveau, som den beskrevne ovenfor for punkt til punkt meddelelseskommunikation. Efter at have adresseret sikkerhedsdimensionerne så effektivt i forbindelse med punkt til punkt kommunikationen, ønsker vi naturligvis ikke at slække på kravene, og derfor kræves det, at opsamlingen foregår på en måde, hvor:

- der er autentifikation af den komponent, der gemmer den opsamlede meddelelse i repositoriet
- der er integritetssikring af at det som gemmes i repositoriet faktisk var den meddelelse, som blev sendt
- der er kvitteringer og/eller standardiserede audit logs til at sikre uafviselighed
- der er fortrolighedssikring via eksplicit kryptering eller implicit kryptering på infrastrukturniveau
- der er sikring af tilgængeligheden af opsamlingen

Ellers ville hvem som helst i princippet kunne gemme hvad som helst, uden at der var nogen som helst dokumentation for det, og de ægte meddelelser ville nemt kunne blive opsamlet af uvedkommende undervejs, og opsamlingen kunne nemt stoppes ved cyber-angreb.

Den metode, som målbilledet peger på, er at lade opsamlingen foregå ved, at det afsendende system (C1 i bred forstand i fire-corner modellen (typisk message service handleren)) ved modtagelse af en positiv transportkvittering for en meddelelse fra det modtagende system (C4 i bred forstand i fire-corner modellen) sender en tro kopi af meddelelsen til et repositorie via de sædvanlige eDelivery-mekanismer (dvs. via dets eget access-punkt og et access-punkt dedikeret til repositoriet), som illustreret i følgende figur:



Figur 20: Opsamling af meddelelser via standard eDelivery kommunikation.

På den måde vil opsamlingen af meddelelserne nemt og elegant blive sikret af de selvsamme mekanismer som punkt til punkt kommunikationen af meddelelserne, og en meddelelse vil først blive sendt til repositoriet, efter den er nået frem til den oprindelige punkt til punkt modtager. Da dette naturligvis også indebærer, at de samme kvitteringsflows skal anvendes i forhold til opsamlingen af meddelelserne som til punkt til punkt kommunikationen af meddelelserne, betyder det, at den afsendende message service handler skal holde styr på kvitteringerne både overfor den oprindelige punkt til punkt kommunikation og overfor opsamlingen til deling.

6.2.2 Opbevaring i repositorie

Dette er i sagens natur det mest statiske af de tre trin. Generelt ønskes det at repositoriet, hvori de sendte meddelelser er gemt, skal overholde de samme sikkerhedskrav og -regler som øvrige tilsvarende repositorier på sundhedsområdet. Derfor ønskes sikkerhedsmekanismer tilsvarende dem for disse andre repositorier anvendt:

- **Autenticitet:** Både servicen, der udstiller meddelelser, og supportmedarbejdere skal autentificere sig, når de tilgår repositoriet.

- **Tilgængelighed:** Aftalt oppetid og svartid skal sikres via standard driftsmekanismer som f.eks. load-balancere og fail-over.
- **Integritet:** Sikres på low level niveau af den protokol, som repositoriet er implementeret med. Sikres på logisk niveau ved at det kun er i forbindelse med opsamlingen, at meddelelser gemmes i repositoriet. Efterfølgende må meddelelserne i repositoriet ikke ændres.
- **Uafviselighed:** Repositoriet skal audit logge alle kald til sig på en standardiseret måde.
- **Fortrolighed:** Meddelelserne i repositoriet kan kun tilgås via servicen, der har sin egen sikring af fortrolighed af de hentede data, samt af supportfunktionen for repositoriet, der kun har adgang i det omfang, det er nødvendigt for at udføre deres supportarbejde, og i øvrigt er underlagt en fortrolighedsaftale. Der er ikke på nuværende tidspunkt et strengt krav om kryptering af "data at rest" i repositoriet, men da dette princip vinder mere og mere indpas i mange IT-sammenhænge i disse år, og efterhånden er at betragte som best practice, må det forventes at blive et krav inden for en overskuelig fremtid. Det forventes dog, at indfrielsen til den tid vil kunne realiseres via det produkt, som repositoriet er realiseret med.

6.2.3 Udstilling via service

Generelt ønskes det at servicen, der udstiller sendte meddelelser, som minimum skal overholde de samme sikkerhedskrav og -regler som øvrige tilsvarende services på sundhedsområdet. Derfor bør flere af de samme allerede eksisterende sikkerhedsmekanismer fra disse andre services anvendes:

- **Autenticitet:** Servicen skal udstilles som en DGWS/IDWS service, og anvenderne (både sundhedspersoner og borgere) skal anvende digitale certifikater i forbindelse med kald til servicen på samme måde som for andre tilsvarende services, og det er et krav, at de anvendte certifikater er på personbevisniveau og ikke systembevisniveau.
- **Tilgængelighed:** Aftalt oppetid og svartid skal sikres via den platform, som servicen afvikles på – f.eks. via standard driftsmekanismer som fail-over og load-balancere.
- **Integritet:** Sikres på low level niveau af den protokol, som servicen er implementeret med. Sikres på logisk niveau ved at servicen skal hente meddelelsen som den er gemt i repositoriet og ikke må transformere denne til et andet format. Hvis det anvendende system ikke kan tolke og vise meddelelsen i dens oprindelige format, er det dets eget ansvar at transformere det til et format, det kan forstå og vise (evt. ved hjælp af en tredje parts komponent/service) jf. afsnit 5.3.4.
- **Uafviselighed:** Servicen skal implementere standardiseret audit log og skal endvidere logge til MinLog på samme måde som tilsvarende services, som f.eks. den nationale dokumentdelingsservice.
- **Fortrolighed:** Servicen skal aktivt anvende den identifikation af anvenderen (sundhedsperson eller borger) samt de søgeparametre, der er en del af kaldet af servicen. Endvidere skal nationale sikkerhedsløsninger som MinSpærring (samtykke) og behandlingsrelationsservicen anvendes aktivt af servicen, og denne anvendelse må, ligesom et målbillede, ikke betragtes som statisk, da disse komponenter også udvikler sig i takt med lovgivning og initiativer både indenfor sundhedsdomænet og i fællesoffentligt regi.

Da servicen udstilles og afvikles på en platform, der kan have sine egne mere strikse sikkerhedspolitikker end de generelle på sundhedsområdet, skal disse i givet fald også overholdes.

6.3 Forsendelsesstatus af meddelelser

Ligesom for deling af meddelelser opdeles diskussionen af sikkerhed i forhold til forsendelsesstatus i de forskellige trin:

1. Forsendelsesstatus opsamles og gemmes i et repositorie
2. Forsendelsesstatus opbevares i repositoriet
3. Forsendelsesstatus hentes af anvendere via udstillede services

Mange aspekter af sikkerhedsdiskussionen er helt de samme som for servicen til deling af sendte meddelelser, og disse er derfor kun opsummeret i de følgende tre underafsnit. Bemærk dog at repositorie i dette afsnit betyder repositorie over forsendelsesstatus, der ikke må forveksles med repositorie over meddelelser i afsnit 6.2.

6.3.1 Opsamling til repositorie

Diskussionen af sikkerhed for opsamlingen af forsendelsesstatus for meddelelser er ikke uvæsentlig. Dels er en tilpas sikkerhed omkring dette nødvendigt for at anvenderne vil anse servicen baseret på de opsamlede data for troværdig, og dels opsamles personoplysninger, da unik borgeridentifikation (oftest CPR-nummeret), for den borger meddelelsen omhandler, er en del af den opsamlede information:

- **Autenticitet:** En komponent, der gemmer forsendelsesstatus for meddelelser, skal autentificere sig når den tilgår repositoriet.
- **Tilgængelighed:** Aftalt oppetid og svartid skal sikres via standard driftsmekanismer. Dette er særlig vigtigt her, da forsendelsesstatus, jf. afsnit 5.2.8, skal være tæt på realtidsopdateret.
- **Integritet:** Sikres af den protokol, som opsamlingen implementeres via.
- **Uafviselighed:** En komponent, der gemmer forsendelsesstatus, skal audit logge opsamlingen på en standardiseret måde.
- **Fortrolighed:** Når den opsamlede forsendelsesstatus kommunikeres til repositoriet, sikres den enten via eksplicit kryptering eller implicit kryptering på det underliggende infrastruktur niveau.

6.3.2 Opbevaring i repositorie

- **Autenticitet:** Både servicen, der udstiller forsendelsesstatus for meddelelser, og supportmedarbejdere skal autentificere sig, når de tilgår repositoriet.
- **Tilgængelighed:** Aftalt oppetid og svartid skal sikres via standard driftsmekanismer som load-balancere og fail-over.

- **Integritet:** Sikres på low level niveau af den protokol, som repositoriet er implementeret med. Sikres på logisk niveau ved at det kun er i forbindelse med opsamlingen, at forsendelsesstatus for meddelelser gemmes i repositoriet. Efterfølgende må disse data i repositoriet ikke ændres.
- **Uafviselighed:** Repositoriet skal audit logge alle kald til sig på en standardiseret måde.
- **Fortrolighed:** Data i repositoriet kan kun tilgås via servicen, der har sin egen sikring af fortrolighed af de hentede data, samt af supportfunktionen for repositoriet, der er underlagt en fortrolighedsaftale, og som kun har adgang i det omfang, det er nødvendigt for at udføre deres supportarbejde.

6.3.3 Udstilling via service

Servicen, der udstiller forsendelsesstatus for meddelelser, skal overholde de samme sikkerhedskrav og -regler som øvrige services på sundhedsområdet, jf. princip PT6. Derfor bør flere af de samme allerede eksisterende sikkerhedsmekanismer fra disse andre services anvendes:

- **Autenticitet:** Servicen skal udstilles som en DGWS/IDWS service, og anvenderne (både sundhedspersoner og borgere) skal anvende digitale certifikater i forbindelse med kald til servicen på samme måde som for andre services på sundhedsområdet, og det er (igen) et krav, at de anvendte certifikater er på personbevisniveau og ikke systembevisniveau.
- **Tilgængelighed:** Aftalt oppetid og svartid skal sikres via den platform, som servicen afvikles på – f.eks. via standard driftsmekanismer som fail-over og load-balancere.
- **Integritet:** Sikres af den protokol, som servicen er implementeret med.
- **Uafviselighed:** Servicen skal implementere standardiseret audit log. Logning til MinLog er påkrævet i tilfældene hvor en borger henter forsendelsesstatus for meddelelser angående en anden borger end sig selv, og hvor en sundhedsperson henter forsendelsesstatus specifikt for en borger.
- **Fortrolighed:** Servicen skal aktivt anvende den identifikation af anvenderen (sundhedsperson eller borger) samt de søgeparametre, der er en del af kaldet af servicen.

Da servicen udstilles og afvikles på en platform, der kan have sine egne mere strikse sikkerhedspolitikker end de generelle på sundhedsområdet, skal disse i givet fald også overholdes.

6.4 Sundhedsadressering

Sundhedsadresseringsservicen skal, ligesom de to øvrige services diskuteret i de umiddelbart ovenstående to afsnit, overholde de samme sikkerhedskrav og -regler som tilsvarende services på sundhedsområdet, og derfor bør flere af de samme allerede eksisterende sikkerhedsmekanismer anvendes:

- **Autenticitet:** Servicen skal udstilles som en DGWS/IDWS service, og anvenderne skal anvende digitale certifikater i forbindelse med kald til servicen på samme måde som for tilsvarende services på sundhedsområdet. På grund af denne service' natur er det imidlertid i dette tilfælde tilstrækkeligt, at de anvendte certifikater er på systembevisniveau.

- **Tilgængelighed:** Aftalt oppetid og svartid skal sikres via den platform, som servicen afvikles på – f.eks. via standard driftsmekanismer som fail-over og load-balancere.
- **Integritet:** Sikres af den protokol, som servicen er implementeret med.
- **Uafviselighed:** Servicen skal implementere standardiseret audit log.
- **Fortrolighed:** Servicen skal anvende den identifikation af anvenderen samt de søgeparametre, der er en del af kaldet af servicen, men en egentlig brugerstyring i forhold til hvem, der kalder servicen, antages håndhævet af de kaldende systemer, så når et anvendersystem er korrekt autentificeret, er der adgang til servicen.

Da servicen udstilles og afvikles på en platform, der kan have sine egne mere strikse sikkerhedspolitikker end de generelle på sundhedsområdet, skal disse i givet fald også overholdes.

7. Governance

Der er allerede i fællesoffentligt regi under ledelse af digitaliseringsstyrelsen (DIGST) udarbejdet en analyserapport om etablering af et fællesoffentligt dansk eDelivery netværk [EDELDIGSTAN-RAP], som også inkluderer et kapitel om governance. Dette rapportkapitel er bl.a. sammen med den fællesoffentlige systemforvaltning af sundheds-IT (FSI) udgangspunkter for nærværende kapitel, som sætter grundige overordnede rammer for governance for meddelelseskommunikation på sundhedsområdet baseret på best practises. Denne skal, som også nævnt i bilag 1, uddybes og konkretiseres i det efterfølgende arkitektur- og implementeringsarbejde og produktionspilotprojektet. Bemærk at der ikke vil være fokus på governance af den detaljerede indholdsmæssige standardisering af meddelelserne, der sendes, i det meddelelsesinfrastrukturen netop er meddelelsesagnostisk, hvorfor dette emne kun nævnes ganske kort et enkelt sted.

7.1 Punkt til punkt kommunikation med eDelivery

7.1.1 Niveauer

Med udgangspunkt i hvordan meddelelseskommunikation i eDelivery fungerer, som beskrevet i afsnit 5.2, samt den allerede eksisterende og snarligt kommende anvendelse af eDelivery i Danmark (henholdsvis e-handel og næste generation af offentlig digital post), og i overensstemmelse med principperne PF3 og PF6, der omhandler fælles transparent national governance med centrale forankringspunkter og lokalt ansvar for det, som logisk hører til lokalt, og dermed en tydelig ansvarsfordeling, er fire forskellige ansvarsområder identificeret, hvorpå governance skal håndteres:

- eDelivery netværk (fællesoffentligt på tværs af domæner)
- eDelivery sundhedsdomæne
- Access-punkt (C2/C3)
- System (C1/C4 i bred forstand)

Disse ansvarsområder vil igennem hele dette governance afsnit blive omtalt som niveauer, og de er helt centrale omdrejningspunkter for diskussionen i resten af dette afsnit.

Et målbillede på sundhedsområdet (et domæne) kan selvfølgelig ikke bestemme, hvordan governance på det fællesoffentlige niveau på tværs af domænerne skal være, men dette afsnit beskriver de forslag, der var enighed om i målbillede-workshoparbejdet, hvor der også deltog repræsentanter for det fællesoffentlige niveau. I det kommende arkitektur- og implementeringsarbejde og produktionspilotprojektet, skal det afklares, hvor meget af det foreslåede for eDelivery netværk niveauet, som skal realiseres på det niveau. Såfremt det bliver mindre end det foreslåede, vil noget af det, der ellers var tiltænkt eDelivery netværk niveauet, skulle varetages af eDelivery sundhedsdomæne niveauet. For et stort domæne, som sundhedsdomænet,

vil dette godt kunne løftes, og i en vis forstand giver det også lidt større frihedsgrader for domænet. Til gengæld introducerer det også større omkostninger og risiko, der skal mitigeres, for domænet, og det er derfor en vigtig afklaring.

7.1.2 Fora

Der er flere forskellige fora i forhold til governance:

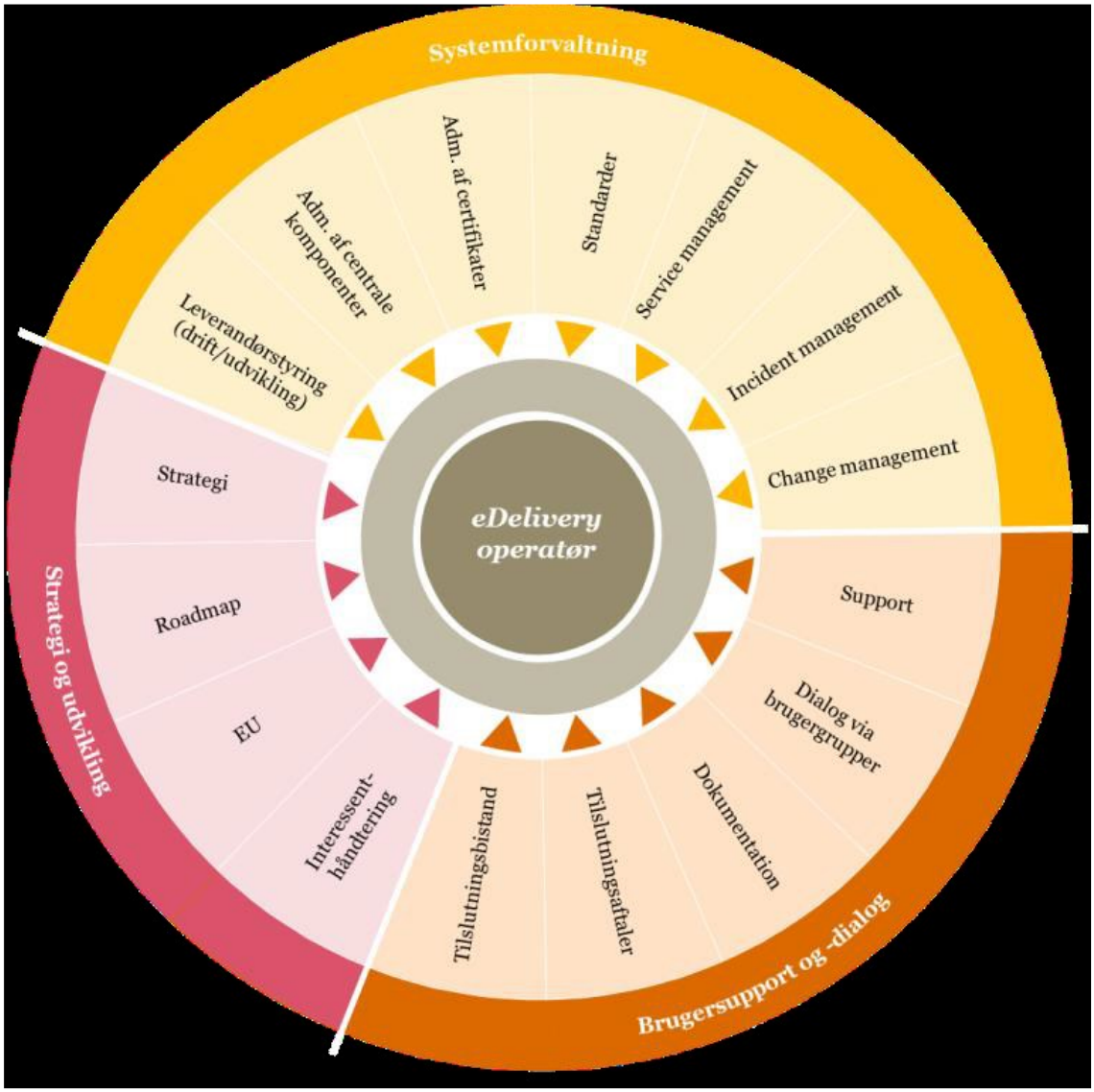
Forum	Beskrivelse
Forretningsstyregruppe	En sådan bør eksistere både på eDelivery netværk niveauet og på domæneniveau (i vores tilfælde sundhedsdomænet). Forretningsstyregruppen på et givet niveau er det øverste beslutningsorgan på dette niveau i forhold til funktionalitet, anvendelse, og økonomi, og det ejer strategien for det pågældende niveau, og agerer derfor også strategiforum. Deltagerne på sundhedsdomæne niveau er repræsentanter for parterne på sundhedsområdet, der anvender meddelelseskommunikation.
Faglig referencegruppe	En sådan bør ligeledes eksistere både på eDelivery netværk niveauet og på domæneniveau, og på sundhedsdomæne niveau er deltagerne igen repræsentanter for parterne på sundhedsområdet, som anvender meddelelseskommunikation. Den faglige referencegruppe på et givet niveau har til opgave at fagligt kvalitetssikre og teknisk vurdere vedligeholdelses- og udviklingstiltag for meddelelseskommunikation via eDelivery på det givne niveau.
Brugerforum	Der findes dels et EU brugerforum, hvori der bør være deltagere fra både eDelivery netværk niveauet og sundhedsdomæne niveauet. Endvidere bør der være et brugerforum på sundhedsdomæne niveau, hvor der er deltagere fra både access-punktleverandører (C2/C3) og systembrugere (C1/C4), hvor emner og problemstillinger som brugerne finder vigtige skal diskuteres. Hvorvidt et tilsvarende brugerforum skal etableres på eDelivery netværk niveauet er ikke op til dette sundhedsdomæne målbillede at afgøre.

Disse fora er vigtige, da det er her, repræsentanter for de enkelte parter, der anvender meddelelseskommunikation bliver sat om samme bord for at diskutere og videreudvikle forskellige aspekter ved meddelelseskommunikationen, og det således er her, at de enkelte parter har mulighed for at præge udviklingen af meddelelseskommunikation på sundhedsområdet. Præcis hvordan sammensætningen af disse fora skal være og hvilke sammenhænge, der skal være

mellem dem og de allerede eksisterende governance fora, skal besluttes i forbindelse med det videre implementeringsarbejde og produktionspilotprojektet.

7.1.3 Temaer

Der er mange temaer under governance som tydeligt illustreret i følgende figur, der stammer fra [EDELDIGSTANRAP]:



Figur 21: Forskellige governance temaer og deres gruppering.

Temaerne kan inddeles i tre grupper under overskrifterne *strategi og udvikling*, *systemforvaltning*, og *brugersupport og –dialog*. Det ses at temaerne ikke udelukkende handler om kontrol og forvaltning. Selvom dette naturligvis er en meget vigtig og central del af governance, er det også vigtigt at denne ikke er så rigid, at det gør udvikling af infrastrukturen for meddelelseskommunikation for langsommelig.

En opsummering af hvad der foregår på de enkelte fire governance niveauer hver især i forhold til de enkelte temaer er givet på tabelform i Appendiks E, hvor det meget generiske tema *service management* fra figuren er foldet lidt mere ud i nogle undertemaer.

For temaerne i *strategi og udvikling* gruppen er det overordnede billede, at de to øverste niveauer (eDelivery netværk og sundhedsdomæne) står som ansvarlige og med facilitatorrollen, og de to nederste niveauer (access-punkt (C2/C3) og system (C1/C4 i bred forstand)) står i deltagerrollen.

Dette overordnede billede gentager sig lidt i *brugersupport og –dialog* gruppen, hvor de to øverste niveauer primært har rollerne ansvarlig, facilitator, samt udgiver, og de to nederste niveauer rollerne deltager og anvender.

Dette overordnede billede gælder også for nogle af temaerne under *systemforvaltning* gruppen, men her er der også nogle temaer, specielt de klassiske ITIL temaer incident management, problem management, change management, og security management, hvor alle de enkelte niveauer hver især, næsten selvindlysende, selv er ansvarlig for det, der er logisk hjemmehørende på niveauet (f.eks. system (C1/C4 i bred forstand) for systemet, access-punkt (C2/C3) for access-punktet, sundhedsdomænet for sundhedsadresseringsservicen, og eDelivery netværk for SMP).

7.1.4 Processer

Der er også mange processer omkring temaerne under governance. I følgende tabel er de vigtigste af disse og deres væsentligste indhold præsenteret summarisk:

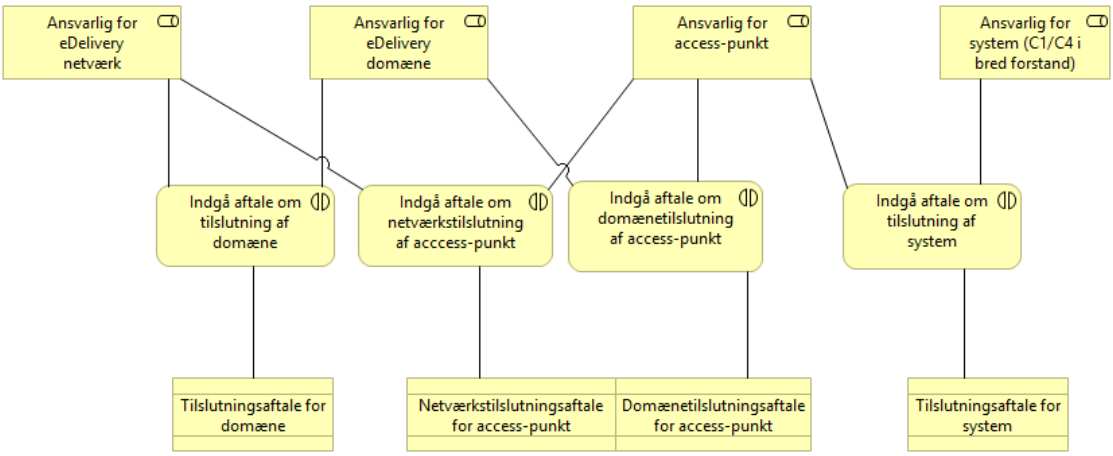
Proces	**Beskrivelse**
Tilslutning	Dette foregår mellem flere niveauer. Der er tilslutning af et system til et access-punkt, tilslutning af et domæne (eksempelvis relevant i vores kontekst sundhedsdomænet) til eDelivery netværket, og tilslutning af access-punkt til både eDelivery netværket og sundhedsdomænet. Disse tilslutninger styres af tilsvarende aftaler, som beskrevet i følgende afsnit 7.1.5. Som hjælp til tilslutningen af access-punkter stiller eDelivery netværket en startpakke (”getting started”) til rådighed, og denne suppleres med en domænestartpakke fra sundhedsdomænet i forhold til de yderligere krav fra sundhedsdomænet. Endvidere vil der på sundhedsdomænet blive udarbejdet vejledninger til korrekt anvendelse, herunder f.eks. i korrekt anvendelse af kvitteringer og fejlhåndtering. Endelig stiller eDelivery netværket et onboardingmiljø til rådighed, hvor det for et access-punkt er muligt at afprøve eDelivery meddelelseskommunikation og foretage basal connectivity og conformance test.

Proces	Beskrivelse
Certificering	Dette foregår på sundhedsdomæne niveau og er en forudsætning for, at et access-punkt agerende for et system kan blive tilsluttet sundhedsdomænet, og certificeringsprocessen kan derfor betragtes som værende relateret til tilslutningsprocessen. Certificering dækker eksplicit både korrekt anvendelse af standarderne for meddelelserne på sundhedsområdet og korrekte kvitteringsflows (både imellem C3-C2 og imellem C4-C1) og fejlhåndtering og dermed også implicit korrekt anvendelse af de underliggende eDelivery standarder. For at smidiggøre og lette certificeringsprocessen skal certificeringsinstansen, på samme måde som, og inspireret af, forberedelsesprocessen til IHE connectathons, stille en hjemmetestpakke til rådighed for systemer med agerende access-punkter, som skal dokumenteres passeret for at kvalificere sig til selve certificeringsprocessen med certificeringsinstansen. Certificeringsprocessen er yderst vigtig, da den sikrer både, at to parter, der kommunikerer med hinanden via punkt til punkt meddelelseskommunikation følger de samme standarder, og dernæst at alle, som efterfølgende henter meddelelserne via delingsservicen for meddelelser er sikret, at de hentede meddelelser følger de rette standarder.
Standardisering	De fælles eDelivery standarder styres af EU og processerne omkring disse er derfor ikke en del af dette målbillede. Standarderne for meddelelserne på sundhedsområdet inklusive disses konvolutter ejes og vedligeholdes på sundhedsdomæne niveau, og der er derfor en standardejer og en standardforvalter/vedligeholder rolle for disse sundhedsmeddelelsesstandarder – begge roller eksisterer allerede i dag og spilles af MedCom. Den overordnede proces for standarder for nye typer af meddelelser på sundhedsområdet vil fortsætte som i dag. Forslag til nye typer af meddelelser er behovsdrevet og kan fremsættes af enhver part (eller projekt) på sundhedsområdet. Standardforvalteren udarbejder detaljer for den nye standard i samarbejde med parterne, der ønsker den nye meddelelsestype. Afslutningsvis godkendes standarden for den nye type af meddelelse af RUSA.

Proces	Beskrivelse
"De klassiske ITIL inspirerede processer" om incident, problem, og change håndtering	På de enkelte niveauer håndteres, som nævnt i afsnit 7.1.3, de komponenter, hvis ansvar ligger på det pågældende niveau. Derudover er man ansvarlig for at holde de interessenter på andre niveauer, der er afhængige af den pågældende komponent, orienteret, så f.eks. skal sundhedsdomænet orientere systemerne (C1/C4 i bred forstand) angående sundhedsadresseringsservicen, og eDelivery netværket skal orientere sundhedsdomænet og access-punkterne (C2/C3) om SMP og SML. Derudover er det vigtigt, at sundhedsdomæne niveauet er eskaleringspunkt ved tvister systemer imellem angående indhold af meddelelser, og eDelivery netværk niveauet er tilsvarende eskaleringspunkt for tvister angående forbindelse imellem access-punkter.
Sikkerheds-håndtering	Dette foregår på flere niveauer og på et givet niveau (igen) for de komponenter niveauet har ansvar for. Hvor ofte sikkerhedsaudits skal foretages er en del af de tilslutningsaftaler, der indgås på det pågældende niveau, og resultatet af en audit skal afrapporteres til det andet niveau tilslutningsaftalen er indgået med. Endvidere er det naturligvis vigtigt, at relevant lovgivning, som eksempelvis NIS2 direktivet, overholdes.
SLA	Monitorering, opfølgning, og afrapportering i forhold til SLA eksisterer også på flere niveauer. Hvor detaljeret der skal monitoreres og hvor ofte, der skal følges op og afrapporteres er igen en del af de tilslutningsaftaler, der indgås på det givne niveau.

7.1.5 Aftaler

Aftaler er et helt centralt begreb i forhold til governance og taget i betragtning af, hvordan meddelelseskommunikation i eDelivery er, er de fleste af de centrale tilslutningsaftaler desangående imellem to på hinanden følgende niveauer. Dvs. imellem eDelivery netværket og sundhedsdomænet, imellem sundhedsdomænet og access-punktet (C2/C3), og endelig imellem access-punktet og systemet (C1/C4 i bred forstand). Den eneste undtagelse for dette er, at der også eksisterer en aftale imellem eDelivery netværket og access-punktet, som illustreret ved følgende figur:



Figur 22: Governance aftaler imellem de forskellige niveauer for punkt til punkt meddelelseskommunikation.

Bemærk at i figuren anvendes det generelle begreb eDelivery domæne, velvidende at i vores kontekst er det sundhedsdomænet, der er tale om.

At der er to tilslutningsaftaler for access-punktet (til henholdsvis netværket og domænet) skyldes, at der dels er nogle krav fra eDelivery netværket, f.eks. anvendelse af SMP, og dels er nogle krav fra sundhedsdomænet, f.eks. skærpede krav til tilgængelighed, overvågning og kvitteringer. Da der er meget store forskelle i størrelsen af de organisationer, der ejer et system (alt fra en hel region til en enkelt lægepraksis), er det vigtigt, at tilslutningsaftalen for et system, jf. princip PF5, tager højde for dette og ikke reelt umuliggør tilslutning af systemer fra de mindre organisationer.

Nogle dele af en aftale vedrører alene de to niveauer aftalen er indgået mellem, som f.eks. i domænetilslutningsaftalen for et access-punkt hvor det skal angives at et access-punkt med aftalte mellemrum skal udføre sikkerhedsaudits og afrapportere resultatet af disse audits til rette instans på sundhedsdomæne niveauet. Andre dele kan være krav til det nederste niveau i aftalen om at stille krav til det næstfølgende niveau, som f.eks. at der i tilslutningsaftalen for et access-punkt stilles krav om, at der i tilslutningsaftalen for et system skal stå, at systemets supportfunktion skal arbejde konstruktivt sammen med access-punktets supportfunktion, når udfordringer skal løses.

Der kan også være overordnede krav, der gør sig gældende på alle niveauer, som f.eks. at der på et givet niveau skal eksistere en supportfunktion med en nærmere specificeret minimumsåbningstid for henvendelser. Disse overordnede krav kan med fordel formuleres som politikker, så man i tilslutningsaftalerne kan skrive at den pågældende politik skal overholdes/implementeres – på denne måde behøver man ikke gentage den samme lange tekst i alle aftalerne, og såfremt der kommer ændringer skal man kun ændre et sted (nemlig i politikken) fremfor i samtlige aftaler.

Hovedoverskrifterne for de fire tilslutningsaftaler er som følger, hvor dog specielt netværkstilslutningsaftalen for access-punktet kun er indikativ, da indholdet af dette ikke er noget et målbillede på sundhedsområdet kan diktere:

Aftale	**Beskrivelse**
Tilslutningsaftale for domæne	▸ Vedligehold af meddelelsestyper inden for domæne ▸ vedligehold af standarder for meddelelser inden for domæne ▸ supportfunktion (kontaktdata, åbningstid, responstid, etc.) ▸ SLA (svartider, oppetid, driftstid (f.eks. 24/7), reetableringstid, servicevinduer, transaktionsmængder) ▸ miljøer ▸ varslingsfrister for ændringer ▸ eksistens af domænestartpakke ▸ domænekrav over for access-punkter formuleret (SLA, sikkerhed, supportfunktion, etc.)
Netværkstilslutningsaftale for access-punkt	▸ Supportfunktion (kontaktdata, åbningstid, responstid, etc.) ▸ SLA (svartider, oppetid, driftstid (f.eks. 24/7), reetableringstid, servicevinduer, transaktionsmængder) ▸ miljøer ▸ varslingsfrister for ændringer ▸ basale eDelivery meddelelseskommunikationskrav ▸ basale eDelivery sikkerhedskrav ▸ konstruktivt supportsamarbejde imellem access-punkter når nødvendigt ▸ krav om passus angående konstruktivt supportsamarbejde imellem access-punkt og system når nødvendigt indgår i tilslutningsaftale for system
Domænetilslutningsaftale for access-punkt	▸ Domænespecifikke krav til supportfunktion (kontaktdata, åbningstid, responstid, etc.) ▸ krav om passus angående supporterede meddelelsestyper indgår i tilslutningsaftale for system ▸ domænespecifikke krav til miljøer ▸ varslingsfrister for ændringer ▸ pålidelig meddelelseskommunikation ▸ supplerende domænespecifikke krav til sikkerhed og performance ▸ sikkerhedsaudit ▸ SLA (svartider, oppetid, driftstid (f.eks. 24/7), reetableringstid, servicevinduer, transaktionsmængder)

Aftale	Beskrivelse
Tilslutningsaftale for system	▸ Supportfunktion (kontaktdata, åbningstid, responstid, etc.) ▸ konstruktivt supportsamarbejde imellem access-punkt og system når nødvendigt ▸ SLA (svartider, oppetid, driftstid (f.eks. 24/7), reetableringstid, servicevinduer, transaktionsmængder) ▸ supporterede meddelelsestyper ▸ miljøer ▸ varslingsfrister for ændringer ▸ sikkerhedsmæssige aspekter (kryptering og autentifikation) ved kommunikationen imellem access-punkt og system ▸ håndtering af opsamling af forsendelsesstatus for meddelelser i system

Det er vigtigt at understrege, at de indgåede aftaler naturligvis er forpligtende, og at der fra de overordnede niveauers side følges løbende op på deres overholdelse, f.eks. jf. SLA-processen i afsnit 7.1.4., i overensstemmelse med dele af diskussionen i afsnit 2.4.

7.1.6 Afprøvningsdomæner

Ud over selve sundhedsdomænet som er blevet omtalt indtil nu, vil det også kunne være relevant parallelt hermed at have et sundhedsafprøvningsdomæne. De ansvarlige instanser for afprøvningsdomænet er de samme som for selve det rigtige "sundhedsproduktionsdomæne", og afprøvningsdomænet er, naturligvis, også underlagt eDelivery netværket og de krav, som følger heraf. Men da det, som navnet indikerer, er tænkt som et domæne, hvor et begrænset antal udvalgte anvendere kan prøve ting af, f.eks. en ny meddelelsestype, er der ikke behov for at have alle de yderligere skærpede krav, som sundhedsdomænet stiller til access-punkterne i sit rigtige produktionsdomæne. På den måde vil man have mulighed for at prøve forskellige ting af i et produktionslignende set-up, og for succesfuldt afprøvede features, som nye meddelelsestyper, vil det efterfølgende være nemmere at etablere det tilsvarende feature i det rigtige sundhedsproduktionsdomæne, end hvis man ikke havde afprøvningsdomænet.

Dette kan betragtes som et eksempel på, at governance for meddelelseskommunikation på sundhedsområdet ikke alene handler om kontrol og forvaltning, men også om at muliggøre udvikling af meddelelseskommunikationen på en smidig måde.

7.2 Services baseret på et eller flere meddelelsesrepositorie(r)

7.2.1 Niveauer

Deling af meddelelser på sundhedsområdet hører naturligt hjemme under sundhedsdomænet og dermed overordnet set under sundhedsdomænets governance, jf. princip PF3. Forsendelsesstatus af meddelelser er af så generel karakter, at det egentlig godt kunne høre hjemme under eDelivery netværket, men det er blevet vurderet, at behovet for forsendelsesstatus fra andre domæner end sundhedsdomænet ikke er stort, så dette kommer også i første omgang til overordnet at høre under sundhedsdomænets governance – hvor det så skal sikres, at det implementeres på en tilpas generisk måde, der vil gøre en eventuel senere generalisering til eDelivery netværk niveauet mulig.

Eftersom access-punkterne spiller en central rolle i opsamlingen af både meddelelser og forsendelsesstatus, så er disse et andet logisk governance niveau. Efter opsamlingen af meddelelserne og forsendelsesstatus gemmes disse i repositorier, hvorfra anvendersystemer henter dem via services, så på denne måde kommer vi frem til følgende fire governance niveauer i forhold til deling og forsendelsesstatus:

- eDelivery sundhedsdomæne
- Access-punkt (C2/C3)
- Repositorie/Service
- Anvendersystem

I forhold til niveauerne for punkt til punkt meddelelseskommunikation er sundhedsdomænet nu det overordnede niveau og det operationelle koblingspunkt er access-punkterne (C2/C3). Tilsvarende punkt til punkt kommunikation, hvor access-punkter indgik aftaler med både eDelivery netværket og sundhedsdomænet, så indgår repositorie/service her aftaler med både sundhedsdomænet og access-punktet.

Specielt i forhold til Repositorie/Service niveauet, så kommer de to typer services til at blive udstillet og afviklet på (ikke her nærmere angivne) platforme, og ligeledes for repositorierne for meddelelser og forsendelsesstatus. Disse platforme kan have sine egne skærpede governance krav og processer i forhold til de generelle på sundhedsområdet, og disse skal i givet fald naturligvis også efterfølges.

Derudover spiller distributionen af repositorier for meddelelser ind i forhold til hvilke databehandlingsaftaler, der skal indgås imellem hvem, i det der aftalemæssigt er forskel på om alle meddelelser fra alle afsendere opsamles i et centralt repositorie eller om meddelelser fra en samling afsendere opsamles i et decentralt repositorie tæt på dem selv eller en kombination af begge modeller anvendes.

7.2.2 Fora

Da deling af meddelelser og forsendelsesstatus på sundhedsområdet hører så tæt sammen med punkt til punkt meddelelseskommunikationen som det gør, bør de samme governance fora forankret på sundhedsdomæne niveau anvendes, dvs. den samme forretningsstyregruppe, den samme faglige referencegruppe, og det samme brugerforum.

7.2.3 Temaer

De relevante governance temaer er bortset fra EU temaet under gruppen *strategi og udvikling* de samme som for punkt til punkt meddelelseskommunikation. I det hele taget er den overordnede ansvarsdiskussion for temaerne niveauerne imellem meget lig den for punkt til punkt meddelelseskommunikationen. F.eks. ligger ansvaret for temaerne i gruppen *strategi og udvikling* på sundhedsdomæne niveau og de øvrige niveauer er deltagere, og for de klassiske ITIL temaer under *systemforvaltning* gruppen er det enkelte niveau hver især ansvarlig for det, der logisk hører hjemme på niveauet.

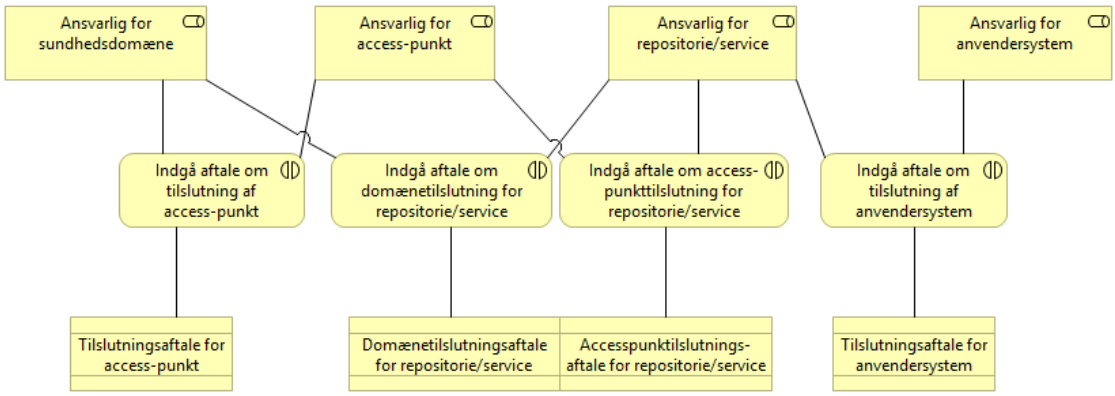
7.2.4 Processer

De relevante governance processer er ligeledes langt hen ad vejen analoge til de listede ovenfor for punkt til punkt meddelelseskommunikation, hvorfor udvalgte kun listes ganske kort:

- Tilslutning: Dette foregår mellem flere niveauer. Der er tilslutning af et anvendersystem til en repositoriebaseret service, tilslutning mellem repositorie og access-punkt, tilslutning af repositorie til sundhedsdomænet, og tilslutning af access-punkt til sundhedsdomænet. Disse tilslutninger styres af tilsvarende aftaler, som beskrevet i følgende afsnit 7.2.5
- ”De klassiske ITIL inspirerede processer” om incident, problem, og change håndtering: På de enkelte niveauer håndteres de komponenter, hvis ansvar ligger på det pågældende niveau. Derudover er man ansvarlig for at holde de interessenter på andre niveauer, der er afhængige af den pågældende komponent, orienteret.
- SLA: Monitorering, opfølgning, og afrapportering i forhold til SLA eksisterer også på flere niveauer. Hvor detaljeret der skal monitoreres og hvor ofte, der skal følges op og afrapporteres er igen en del af de tilslutningsaftaler, der indgås på det givne niveau.

7.2.5 Aftaler

Aftalestrukturen i forhold til deling af meddelelser og forsendelsesstatus kan illustreres ved:



Figur 23: Governance aftaler imellem de forskellige niveauer for deling af meddelelser og forsendelsesstatus.

Da deling af meddelelser og forsendelsesstatus på sundhedsområdet er en integreret del af meddelelseskommunikation på sundhedsområdet og hører tæt sammen med punkt til punkt meddelelseskommunikationen i dette målbillede, og der allerede i forbindelse med punkt til punkt meddelelseskommunikationen via eDelivery er blevet identificeret en domænetilslutningsaftale imellem sundhedsdomænet og access-punktet, er tilslutningsaftalen for access-punkt i Figur 23 en del af denne domænetilslutningsaftale fremfor en selvstående aftale. I det følgende er det derfor kun det relateret til opsamling af meddelelser/forsendelsesstatus i denne tilslutningsaftale, der omtales. Tilslutningsaftalen for anvendersystemet vil være meget lig tilsvarende aftaler for anvendersystemer af andre nationale services på sundhedsområdet.
Indholdet af de fire tilslutningsaftaler på hovedoverskriftniveau er som følger:

Aftale	**Beskrivelse**
Tilslutningsaftale for access-punkt	▸ Krav om opsamling af meddelelse til repositorie og sikkerhedsmæssige aspekter hertil ▸ krav om opsamling af forsendelsesstatus til repositorie og sikkerhedsmæssige aspekter hertil

Aftale	Beskrivelse
Domænetilslutningsaftale for repositorie/service	• Supportfunktion (kontaktdata, åbningstid, responstid, etc.) • SLA (svartider, oppetid, driftstid (f.eks. 24/7), reetableringstid, servicevinduer, transaktionsmængder) • miljøer • varslingsfrister for ændringer • krav om passus om konstruktivt supportsamarbejde imellem access-punkt og repositorie når nødvendigt • krav om passus om kommunikationsprotokol og sikkerhed i forhold til kommunikation imellem repositorie og access-punkt • krav om passus om tilslutningsaftale for anvendersystem til service
Access-punkttilslutningsaftale for repositorie/service	• Supportfunktion (kontaktdata, åbningstid, responstid, etc.) • SLA (svartider, oppetid, driftstid (f.eks. 24/7), reetableringstid, servicevinduer, transaktionsmængder) • miljøer • varslingsfrister for ændringer • konstruktivt supportsamarbejde imellem access-punkt og repositorie når nødvendigt • protokol for kommunikation af opsamlede data imellem access-punkt og repositorie • sikkerhedsmæssige aspekter (kryptering og autentifikation) ved kommunikationen imellem access-punkt og repositorie
Tilslutningsaftale for anvendersystem	• Supportfunktion (kontaktdata, åbningstid, responstid, etc.) • miljøer • varslingsfrister for ændringer • brugeradministration i anvendersystem • håndtering af de hentede data herunder personhenførbare data

8. Fremtidige versioner af målbilledet

Den nuværende version af målbilledet baserer sig, som beskrevet i afsnit 1.1, på den første version, der var rammesættende for pilotafprøvningen, efterfølgende revideret på baggrund af de erfaringer, der blev gjort i pilotafprøvningen, samt den dialog der har været med de forskellige parter på sundhedsområdet. Målbilledet vil blive præsenteret for RUSA, der vil tage stilling til, om det skal sendes i offentlig høring, med potentiel efterfølgende revidering og fornyet behandling i RUSA til følge, eller det kan godkendes og publiceres umiddelbart.

Der er, som nævnt i afsnit 1.1, aktuelt planlagt et produktionspilotprojekt med implementering af meddelelseskommunikation baseret på indeværende udgave af målbilledet for et mindre og meget velafgrænset scope. Det vil give en række erfaringer, ikke mindst i forhold til governance samt anvendelse og konfiguration af SMP, som næste udgave af målbilledet bør tage højde for.

Som beskrevet i det indledende afsnit 1.2.1, bør målbilledet dog derudover regelmæssigt justeres i takt med at viden øges og i takt med at nye behov afdækkes eller nye muligheder opstår. I forbindelse med udarbejdelsen af målbilledet er følgende potentielle udvidelser allerede blevet identificeret:

Målbilledet i nærværende version er som nævnt i det indledende afsnit 1.1 tænkt som gældende for meddelelseskommunikation på sundhedsområdet i Danmark. De øvrige dele af rigsfællesskabet Færøerne og Grønland er således ikke i scope i nærværende version af målbilledet. Men da borgere fra Færøerne og Grønland kommer til Rigshospitalet i forbindelse med udredning og behandling af visse sygdomme, vil det være en oplagt potentiel udvidelse af målbilledet. Håndtering af sundhedsmeddelelseskommunikation angående borgere fra Færøerne og Grønland, og de særlige problemstillinger, der i den sammenhæng skal adresseres, er derfor kandidat til en senere version af målbilledet.

Endvidere er håndtering af sundhed for ansatte i forsvaret anderledes end for andre borgere i landet. I forsvaret har lægerne f.eks. ikke egen adgang til patienternes (de ansattes) sundhedsoplysninger. For at få denne adgang logger lægen sammen med patienten på sundhed.dk med patientens login (NemId), hvilket patienten igennem sin ansættelseskontrakt med forsvaret har givet samtykke til. Situationen i forsvaret er således meget forskellig fra situationen uden for forsvaret, som er den beskrevne i dette målbillede. Håndtering af sundhedsmeddelelseskommunikation for ansatte i forsvaret er således ligeledes ikke i scope i nærværende version af målbilledet, men er en kandidat til en senere version af målbilledet.

Målbilledet i nærværende version fokuserer udelukkende, jf. afsnit 1.2.2, på patient/borgercentrerede meddelelser, og mere generelle meddelelser, der ikke omhandler en givet patient, har derfor ikke været i scope. En kommende version af målbilledet kunne inkludere behandling af disse typer af meddelelser, hvor en åbenbar forskel vil være, at de ikke skal opsamles til deling.

DIGST understøtter i første omgang eDelivery "out-of-the-box". Men løsningerne præsenteret i dette målbillede i det lag, der adresserer kvalitet og pålidelighed, kunne potentielt være relevante for parter uden for sundhedsområdet også. En fremtidig udgave af målbilledet kunne således beskrive ændringer (ikke mindst i governance), der gør det muligt at sætte lignende kvalitetskrav til meddelelseskommunikation uden for sundhedsområdet.

Efterhånden som der arbejdes på at implementere løsninger, der understøtter sundhedsydelser leveret på tværs af EU-medlemsstater, er der brug for at beskrive, hvordan dansk eDelivery infrastruktur hænger sammen med en europæisk infrastruktur (på sundhedsområdet og/eller generelt). En fremtidig udgave af målbilledet kunne således medvirke til at understøtte implementeringen af sammenhængende løsninger i Europa.

9. Appendiks A

Den konsoliderede liste af user stories i forhold til meddelelseskommunikation på sundhedsområdet er givet i følgende tabel. Den sidste kolonne indikerer, om meddelelseskommunikationen, som user storyen omhandler, i dag er via VANS – hvor dette ikke er tilfældet, er der i bemærkningskolonnen angivet, i hvilken grad user storyen er relevant for målbilledet. For nogle få user stories står der N/A i denne kolonne, fordi den omhandler adresseringsvenlighed i forbindelse med meddelelseskommunikation snarere end en egentlig type af meddelelseskommunikation. Bemærkningsfeltet er endvidere, af hensyn til at give en hurtigt overblik, farvelagt med en grøn, gul, rød farvemarkering, hvor grøn betyder relevant for målbilledet i nærværende version, gul betyder måske relevant for målbilledet i nærværende version, og rød betyder ikke relevant for målbilledet i nærværende version – i den sammenhæng betragtes alt, der kommunikeres via VANS i dag som relevant for målbilledet i nærværende version.

Id	Som en/et	Ønsker jeg	Når jeg	Bemærkning	VANS i dag?
P1	Praktiserende læge/speciallæge	At sende afregning til min region	Har afstemt mine regninger/ydelser		JA
P2	Praktiserende læge/speciallæge	At sende en korrespondance til en anden part i sundhedsvæsnet	Når jeg har behov for at udveksle generel info om en patient med f.eks. en speciallæge		JA
P3	Praktiserende læge/speciallæge	At sende en administrativ korrespondance til en anden part i sundhedsvæsnet	Når jeg har behov for at udveksle ikke patientspecifik info med en anden part		JA
P4	Praktiserende læge/speciallæge	At sende en henvisning til sygehus/speciallæge/fysioterapi m.fl.	Når jeg har brug for at henvise en patient videre i systemet	Der er tale om adskillige henvisningsstandarder	JA
P5	Praktiserende læge/speciallæge	At modtage en epikrise fra sygehus/speciallæge/fysioterapeut m.fl.			JA
P6	Praktiserende læge	At sende en patients fulde journal i	Skal sende en (eller flere) patients komplette		JA

Id	Som en/et	Ønsker jeg	Når jeg	Bemærkning	VANS i dag?
		forbindelse med lægeskift	data videre til en anden almen læge.		
P7	Praktiserende læge/special-læge	At se en oversigt over "dynamiske blanketter" sendt til mig fra f.eks. forsikringsselskaber	Når jeg er blevet adviseret om at der er nyt	Via blanketserver. Måske relevant for målbilledet i første version	NEJ
P8	Praktiserende læge/special-læge	At hente en dynamisk blanket stilet til mig	Når jeg skal udfylde den	Via blanketserver. Måske relevant for målbilledet i første version	NEJ
P9	Praktiserende læge/special-læge	At sende den udfyldte dynamiske blanket retur til rekvirenten	Når jeg er færdig med at udfylde den.	Via blanketserver. Måske relevant for målbilledet i første version	NEJ
P10	Praktiserende læge/special-læge	At modtage et spørgeskema	Når én af mine patienter har udfyldt et skema via WebPatient	PRO spørgeskemaer via Webpatient. Måske relevant for målbilledet i første version	NEJ
P11	Praktiserende læge/special-læge	At modtage laboratoriesvar fra interne	Når jeg har udført målinger på eget apparatur	Disse meddelelser kører ikke over VANS, men håndteres lokalt. Ikke relevant for målbillede i første version.	NEJ
P12	Praktiserende læge/special-læge	At modtage laboratoriesvar fra eksterne	Når jeg har rekvireret målinger hos eksternt laboratorie, eller jeg er kopimodtager	Typisk er egen læge kopimodtager på rekvisitioner fra lægevagten etc.	JA

Id	Som en/et	Ønsker jeg	Når jeg	Bemærkning	VANS i dag?
				Der er flere typer laboratoriesvar og også delvise svar	
P13	Praktiserende læge/speciallæge	At modtage en epikrise	Når én af mine patienter udskrives fra sygehus eller er færdigbehandlet hos speciallæge	Egen læge kan også være kopimodtager	JA
P14	Praktiserende speciallæge	At se og hente henvisninger på henvisningshotellet	Når en patient henvender sig	VANS og henvisningshotel	JA
P15	Praktiserende speciallæge	At afsende en speciallægeepikrise til henvisende læge	Når jeg har færdigbehandlet en patient		JA
P16	Praktiserende speciallæge	At sende en henvisning videre til en anden speciallæge	Når min patient skifter speciallæge eller jeg viderevisiterer		JA
P17	Ansat på et privathospital	At sende indlæggelses og udskrivnings advis til patientens hjem kommune	Når en patient indlægges eller udskrives hos os	Kommunikeres ikke i dag, men er relevant for målbilledet i første version	JA (når det kommer)
P18	Ansat på et privathospital	At sende en epikrise til egen læge	Når en patient udskrives		JA
P19	Praktiserende læge/speciallæge	At sende en OIO faktura	Når jeg har arbejdet for f.eks. en kommune eller en privat virksomhed	Her er ikke tale om sundhedsdatakommunikation. Ikke relevant for første version af målbillede.	NEJ
P20	Praktiserende læge	At når jeg besvarer en korrespondance fra en speciallæge, som har flere ydernumre, kan systemet finde ud af, til	besvarer en korrespondance fra en speciallæge	Relevant i forhold til adresseringsvenlighed. Oprindelig afsender skal	N/A

Id	Som en/et	Ønsker jeg	Når jeg	Bemærkning	VANS i dag?
		hvilken af disse ydernumre (og lokationsnumre) min besvarelse skal gå til		identificere sig mere præcist	
P21	Praktiserende læge	at en politiattest (f.eks. "Politiattest til brug ved friske skadetilfælde") kan sendes direkte til politiet	bliver anmodet fra politiet om at sende den pågældende politiattest	Via post og fax i dag. Relevant for målbillede i første version, men måske ikke del af første implementeringsbølge	NEJ
P22	Praktiserende læge	en ensartethed kommunerne imellem og en meget nem måde at finde den korrekte modtager på	Skal sende en meddelelse til en modtager ved en kommune	Relevant i forhold til adresseringsvenlighed. Mere specialiseret form af P2.	N/A
P23	Praktiserende læge	At kunne sende kopi af (udvalgte dele af) patientens journal fra mit fagsystem til patienten - gerne til patientens E-boks, som jeg formoder overholder GDPR-krav mv. - i stedet for som i dag papirudskrift eller overførsel til USB-stik	Får henvendelse fra patienten om at sende disse data	Digital post privat. Relevant for målbillede i første version	NEJ
P24	Praktiserende læge	At kunne sende kopi af (udvalgte dele af) patientens journal fra mit fagsystem til relevante parter (f.eks. advokater, domstole),	Får henvendelse derom	Almindelig post. Relevant for målbillede i første version	NEJ

Id	Som en/et	Ønsker jeg	Når jeg	Bemærkning	VANS i dag?
		der ønsker oplysninger fra patientens journal			
P25	Praktiserende læge	at kunne uploade patientens journal til et sikkert internetsted, hvor patienten alene har adgang - via sin NemID eller endnu mere sikker platform - men selv kan give adgang til advokater, forsikringsselskaber, pårørende mv.	Får henvendelse derom fra patienten	Ikke relevant for målbillede.	NEJ
P26	Praktiserende læge	At Arbejdsmarkedets Erhvervssikring kan anmode elektronisk og modtage elektronisk direkte fra vores fagsystem	skal korrespondere med Arbejdsmarkedets Erhvervssikring	Ikke relevant for første version af målbillede.	NEJ
P27	Praktiserende læge	at kunne kommunikere med de enkelte afdelinger (f.eks. familieafdeling eller jobcenter) i kommunen	Har en problemstilling med en borger, som hører under den pågældende afdeling	Relevant i forhold til adresseringsvenlighed	N/A
P28	Praktiserende læge	at det ikke er svært og tidskrævende at finde de korrekte modtager-adresser	når jeg skal kommunikere korrespondancer og henvisninger	Relevant i forhold til adresseringsvenlighed	N/A
P29	Praktiserende læge	at kunne sende underretninger til kommunen	skal underrette om fx omsorgssvigt	Måske relevant for målbilledet i første version	NEJ
P30	Praktiserende læge	at kunne sende en LÆ 165 med forslag om socialmedicinsk behandling	i mit lægesystem har udfyldt den attest, som	Via blanketserver. Måske rele-	NEJ

Id	Som en/et	Ønsker jeg	Når jeg	Bemærkning	VANS i dag?
			er aftalt vi skal benytte	vant for målbilledet i første version	
P31	Praktiserende læge	at kunne sende korrespondancemeddelelser til bosteder for udviklingshæmmede	i mit lægesystem har udfyldt en meddelelse som de behøver	Relevant for målbilledet i første version	NEJ
P32	Praktiserende læge	At kunne sende en henvisning til en borgers misbrugscenter	sidder med en borger som er misbruger (alkohol/hash/andet) som jeg vil henvise til behandling i borgers kommune, (som jo er dem der ved lov har behandlingsansvaret for misbrug og som jeg ikke kan henvise til elektronisk – men bare kan sige til borger, at de selv kan kontakte misbrugscenter)	XREF15	JA
P33	Praktiserende læge	At kunne sende/modtage elektroniske oplysninger til/fra kommunens Pædagogisk Psykologisk Rådgivning (PPR) direkte til/fra min journal	sidder med et barn/familie hvor kommunikation med PPR er påkrævet (PPR har lovmæssigt udrednings- og behandlingsansvar for børn med mindre psykiske vanskeligheder)	Relevant for målbilledet i første version	NEJ

Id	Som en/et	Ønsker jeg	Når jeg	Bemærkning	VANS i dag?
P34	Praktiserende læge	At kunne sende en elektronisk attest til patientforsikring/patienterstatning/STPS som svar på anmodning om journal materiale til en sag	modtager anmodning om oplysninger til en sag	Relevant for målbilledet i første version	NEJ
P35	Praktiserende læge	At det ikke er svært i forhold til hjemmepleje og hjemmesygepleje at overskue hvilket område patienten tilhører og hvem man i givet fald skal have fat i	Skal sende en meddelelse til hjemmepleje eller hjemmesygepleje	Relevant i forhold til adresseringsvenlighed	JA
K1	Hjemmesygeplejerske i akutfunktionen	At kunne sende en korrespondance faglig spørgsmål med vedhæftet skema med målinger til den sygehusafdeling/afsnit som er ansvarlig for borgers hjerteplan	I mit fagsystem opdaterer en borgers plejejournal ifm. forværring af ophobet væske i lungerne pga. hjerteinsufficiens	Relevant for målbilledet i første version	NEJ (dog under udvikling)
K2	Sygehus afdeling/afsnit	At kunne sende svar på faglig spørgsmål og behandlingsplan tilbage til en borgers akut hjemmesygeplejerske	I mit EPJ-system har lavet behandlingsplan		JA
K3	Hjemmesygeplejerske i akutfunktionen	At kunne vælge rette modtager på sygehuset	I mit fagsystem opdaterer en borgers plejejournal ifm. forværring af ophobet væske i	Relevant i forhold til adresseringsvenlighed	JA

Id	Som en/et	Ønsker jeg	Når jeg	Bemærkning	VANS i dag?
			lungerne pga. hjerteinsufficiens		
K4	Sygehus afdeling/afsnit	At kunne sende svar til rette modtager i det kommunale	I mit EPJ-system har lavet behandlingsplan	Relevant i forhold til adresseringsvenlighed	N/A
K5	Hjemmesygeplejerske i hjemmeplejen	At kunne sende en korrespondance til specifikt sygehusafsnit på sygehuset, men lokationsnumret er på sygehusafdelingsniveau og personalet på afsnittet ser ikke meddelelsen	I mit fagsystem opdaterer en borgers plejejournal	Relevant i forhold til adresseringsvenlighed	JA
K6	Sygehus afsnit	At kunne modtage korrespondance fra hjemmesygeplejersken	I mit EPJ-system skal dokumentere den tværsektorielle indsats	Relevant i forhold til adresseringsvenlighed	JA
K7	Hjemmesygeplejerske i akutfunktionen	At kunne sende en korrespondance faglig spørgsmål med vedhæftet skema med målinger til en borgers praktiserende læge	I mit fagsystem opdaterer en borgers plejejournal ifm. forværring af ophobet væske i lungerne pga. hjerteinsufficiens		JA
K8	Praktiserende læge	At kunne sende svar på faglig spørgsmål og behandlingsplan tilbage til en borgers akut hjemmesygeplejerske	I mit lægepraksissystem har lavet behandlingsplan		JA

Id	Som en/et	Ønsker jeg	Når jeg	Bemærkning	VANS i dag?
K9	Hjemmesygeplejerske i akutfunktionen	At få modtager indsat når der skal sendes en korrespondance til en borgers praktiserende læge	I mit fagsystem opdaterer en borgers plejejournal ifm. forværring af ophobet væske i lungerne pga. hjerteinsufficiens	Relevant i forhold til adresseringsvenlighed	JA
K10	Praktiserende læge	At kunne sende svar til rette kommunal modtager	I mit lægepraksissystem har lavet behandlingsplan	Relevant i forhold til adresseringsvenlighed	JA
K11	Misbrugscenter	At modtage relevant sundhedsfaglig information fra praktiserende læge eller hospital når borger henvises fra disse parter, eller efter behov fx ved multisygdom.	Igangsætter misbrugsbehandling	Gerne i en form, hvor helbredsoplysninger kan indgå direkte i borgerjournalen. Relevant for målbilledet i første version	NEJ
K12	Misbrugscenter	At have adgang til kommunal dokumentation fra andre faggrupper, hvis denne findes og borger giver samtykke.	Igangsætte misbrugsbehandling	Gerne i en form, hvor udredningens overlappende oplysninger kan genbruges fx ved problemer med personlig hygiejne. Er misbrugscenter inden for sundhedsområdet? Hvis ikke er dette kommunikation mellem to enheder uden for sundhedsområdet.	NEJ

Id	Som en/et	Ønsker jeg	Når jeg	Bemærkning	VANS i dag?
				Relevant for målbilledet i første version	
K13	Misbrugscenter	At have adgang til kommunal dokumentation fra tidligere fx hvis borger tidligere har været i et §119 forløb med fokus på misbrug, eller tidligere misbrugsforløb i denne eller andre kommuner. Hvis denne findes og borger giver samtykke.	Igangsætter misbrugsbehandling	Gerne i en form, der sparer tid ifm formulering af mål, indsatser, og planlægning af forløb. Er misbrugscenter inden for sundhedsområdet? Hvis ikke er dette kommunikation mellem to enheder uden for sundhedsområdet. Relevant for målbilledet i første version	NEJ
K14	Misbrugscenter	At kunne samarbejde/koordinere vedrørende patientens sideløbende behandling ved speciallæge eller egen læge	Ved anden sygdom, eller substitutionsbehandling	Relevant for målbilledet i første version	NEJ
K15	Misbrugscenter	At kunne koordinere substitutionsbehandling med behandlende læge	Oplever dårlig respons på nuværende eller ingen subsititutionsbehandling	Relevant for målbilledet i første version	NEJ
K16	Misbrugscenter	At kunne sende eller dele resultater fra urin, blodprøver og andre måleresultater til behandlende læge på syge-	Ifm. delegering af dette ansvar ifm. koordinering af behandling.	Også eksempelvis normalt EKG ved metadonbehandling. Relevant for målbilledet i første version	NEJ (højst som copy/pastet ustruktureret

Id	Som en/et	Ønsker jeg	Når jeg	Bemærkning	VANS i dag?
		hus, hjemmesygeplejerske eller praktiserende læge			tekst i en korrespondance)
K17	Kommunal akutfunktion	At have adgang til helbredoplysninger og behandlingsplaner fra behandlende læge (enten adgang til LPS, eller sendt)	Ifm igangsættelse af forløb	Gerne i en form der passer til borgerjournalen. Relevant for målbilledet i første version	NEJ
K18	Kommunal akutfunktion	At kunne dele indsatser og planer der igangsættes som respons på en behandlingsplan sendt fra lægen.	Ifm at lægen har sendt eller i telefonen specificeret en behandlingsplan eller en ændring til denne.	Så der ikke kun sendes en kvittering, men at lægen kan se hvad der specifikt er igangsat. Delingen kan ske i udvalg eller i helhed. lægen kan evt. forespørge på helheden hvis nødvendigt. Er en del af det samlede patientoverblik. Relevant for målbilledet i første version	NEJ
K19	Kommunal akutfunktion	At kunne dele observationer og måleresultater	Ifm at behandlende læge har efterspurgt informationen for at overvåge borgerens tilstand eller behandling.	Relevant for målbilledet i første version	NEJ

Id	Som en/et	Ønsker jeg	Når jeg	Bemærkning	VANS i dag?
K20	Kommunal akutfunktion	At kunne dele observationer og måleresultater	Ifm bekymring der kræver sparring med læge	Relevant for målbilledet i første version	NEJ
R1	Ansvarlig sundhedsaktør i centralvisitation eller på organisatorisk enhed	At kunne kunne modtage og registrer henvisninger (fra ekstern part) på relevant organisatorisk enhed		Modtag henvisning	JA
R2	Visiterende sundhedsaktør	At kunne omvisitere henvisning til anden organisatorisk enhed, både indenfor eget sygehus men også til andre samarbejdspartnere fx sygehuse, private behandlingstilbud		Omvisiter henvisning	JA
R3	Sundhedsaktør	At kunne hente relevante henvisninger fra Henvisningshotel		Hent henvisning fra Henvisningshotel	JA
R4	Ansvarlig sundhedsaktør	At kunne sende elektroniske henvisninger til en anden organisatorisk enhed indenfor eget sygehus eller til et andet offentligt sygehus, eller privathospital, en praktiserende speciallæge eller en kommune		Send henvisning	JA
R5	Sundhedsaktør	At kunne indkalde patient, således at patienten modtager dato, klokkeslæt og eventuelle		Indkald patient. Kører via digital post.	NEJ

Id	Som en/et	Ønsker jeg	Når jeg	Bemærkning	VANS i dag?
		vejledninger / informationer		Relevant for målbilledet i første version	
R6	Ansvarlig sundhedsaktør	At kunne sende fødselsanmeldelse til sundhedsplejersken		Send fødselsanmeldelse. Kører via VANS til relevante kommune	JA
R7	Ansvarlig sundhedsaktør	At kunne sende jordemoderanmeldelse til den elektroniske Kirkebog		Kører via Webservice. Måske relevant for målbilledet i første version	NEJ
R8	Ansvarlig sundhedsaktør	At kunne sende en af flere slags epikriser til interne/eksterne samarbejdspartnere, hvor eksterne samarbejdspartnere er alt sundhedsfagligt personale udenfor egen organisatorisk enhed, fx praktiserende læge, henvisende læge, modtagende organisatoriske enhed		Send epikrise	JA
R9	Sundhedsaktør	At kunne modtage og afsende elektronisk korrespondance i forhold til organisatoriske enheder og eksterne samarbejdspartnere, gennem en sikker postkasse, fx i forhold til prakti-		Afsendelse og modtagelse af elektronisk korrespondance	JA

Id	Som en/et	Ønsker jeg	Når jeg	Bemærkning	VANS i dag?
		serende læge/speciallæge/kommune, andre afdelinger internt i regionen/sygehuset og eksternt			
R10	Sundhedsaktør	At kunne sende en genoptræningsplan til fx kommune, fysioterapeut, anden organisatorisk enhed, samt kopi af genoptræningsplan til patientens egen læge, henvisende instans og patienten		Send genoptræningsplan	JA
R11	Sundhedsaktør	At kunne sende og modtage elektronisk post til/fra patient		Send brev til, og modtag brev fra patient. Relevant for målbilledet i første version	NEJ
R12	Sundhedsaktør	At kunne sende en rekvisition på fx genetisk, laboratorie eller billede diagnostisk undersøgelse hos ekstern part		Afsendelse af rekvisition på undersøgelse	JA
R13	Sundhedsaktør	At kunne modtage svar på fx genetisk, laboratorie eller billede diagnostisk undersøgelse hos ekstern part		Modtagelse af svar på rekvisition af undersøgelse	JA
R14	Sundhedsaktør	At kunne modtage målinger foretaget af patienten i dennes hjem		Modtagelse af hjemmemålinger. Kører som PHMR via KIH.	NEJ

Id	Som en/et	Ønsker jeg	Når jeg	Bemærkning	VANS i dag?
				Relevant for målbilledet i første version	
R15	Sundhedsaktør	At kunne afsende Indlæggelsesadvis og Udskrivningsadvis til ekstern part, herunder patientens kommune		Afsendelse af indlæggelsesadvis og udskrivningsadvis	JA
R16	Sundhedsaktør	At kunne sende spørgeskema til patient og modtage dette udfyldt af patienten		Afsendelse af, og modtagelse af udfyldt spørgeskema. Kører som QRD via KIH. Relevant for målbilledet i første version	NEJ
R17	Sundhedsaktør	At kunne modtage en indlæggelsesrapport fra ekstern part, herunder patientens kommune		Modtagelse af indlæggelsesrapport	JA
R18	Sundhedsaktør	af hensyn til patientinddragelse at patienten skal kunne få adgang til al relevant (ekstern meddelelsesbaseret) kommunikation vedrørende denne		Deling af kommunikation og patientinddragelse. Relevant for målbilledet i første version	NEJ

10. Appendiks B

Listen over identificerede user stories i forhold til services baseret på et eller flere repositorie(r) er givet i følgende tabel:

Id	Som en	Ønsker jeg	Når jeg	Bemærkning
S1	Borger	At kunne følge med i status for de meddelelser der sendes angående mig	Gerne vil orientere mig om hvor langt meddelelser om mig selv imellem forskellige sundhedspersoner er kommet	Hvis man f.eks. er blevet henvist fra egen læge til en røntgenundersøgelse, og man synes, der går lang tid inden man får besked fra røntgenafdelingen om tidspunktet for undersøgelsen, vil man gerne kontrollere om, og hvornår, den elektroniske henvisningsmeddelelse fra ens egen læge er kommet frem til røntgenafdelingen
S2	Borger	At kunne hente og gennemlæse de meddelelser der sendes angående mig	Har brug for den information, der findes i meddelelserne	På den måde slipper borgeren for selv at skulle opbevare disse informationer derhjemme i et papir- eller elektronisk kartotek
S3	Borger	At kunne se et overblik over de meddelelser der er blevet sendt angående mig i sammenhæng med visning af mine øvrige tilgængelige sundhedsdata	Gerne vil se et samlet overblik over mine sundhedsdata	På den måde kan borgeren danne sig et overblik over alle sine tilgængelige sundhedsdata ved at kigge et sted
S4	Borger	At kunne spærre for udvalgte sundhedspersoners	Ikke ønsker der skal være adgang til disse meddelelser	Dette er klassisk MinSpærring funktionalitet og helt ma-

Id	Som en	Ønsker jeg	Når jeg	Bemærkning
		adgang til (alle eller udvalgte) tidligere sendte meddelelser angående mig	for de(n) pågældende sundhedsperson(er)	gen til den tilsvarende funktionalitet for andre sundhedsdata end meddelelser
S5	Borger	At kunne se hvilke sundhedspersoner har tilgået sendte meddelelser angående mig	Undersøger hvem, der har tilgået sundhedsdata angående mig	Dette er klassisk MinLog funktionalitet og helt magen til den tilsvarende funktionalitet for andre sundhedsdata end meddelelser
S6	Borger	At relevante sundhedspersoner kan hente og gennemlæse tidligere sendte meddelelser til andre sundhedspersoner angående mig	Skal behandles af disse andre relevante sundhedspersoner og de tidligere sendte meddelelser er relevante for behandlingen	På den måde slipper borgeren for selv at skulle forklare indholdet af meddelelserne til de andre behandlere
S7	Borger	At jeg kan gøre på samme måde som for andre elektroniske meddelelser fra offentlige instanser	Skal modtage og læse elektronisk meddelelseskommunikation fra sundhedspersoner til mig selv	På den måde kan meddelelseskommunikation til borgeren fra sundhedsområdet sendes til digital post ligesom andre elektroniske meddelelser fra offentlige instanser, og vil kunne læses i e-boks
S8	Borger	At blive adviseret på samme måde som for andre elektroniske meddelelser fra offentlige instanser	Modtager elektronisk meddelelseskommunikation fra sundhedspersoner	På den måde vil en borger kunne modtage en advisering om, at der er ny elektronisk meddelelseskommunikation til borgeren fra en sundhedsperson, ligesom for andre elektroniske meddelelser fra offentlige

Id	Som en	Ønsker jeg	Når jeg	Bemærkning
				instanser, f.eks. via NemSMS eller via Apps på sundheds-området som f.eks. MinLæge
S9	Pårørende til en borger	At kunne følge med i status for de meddelelser der sendes angående den pårørende borger, som jeg agerer for/på vegne af	Gerne vil orientere mig om hvor langt meddelelser om min pårørende imellem forskellige sundhedspersoner er kommet	Dette er pårørende versionen af S1
S10	Pårørende til en borger	At kunne hente og gennemlæse de meddelelser der sendes angående den pårørende borger, som jeg agerer for/på vegne af	Har brug for den information, der findes i meddelelserne	Dette er pårørende versionen af S2
S11	Pårørende til en borger	At kunne se et overblik over de meddelelser der er blevet sendt angående den pårørende borger, som jeg agerer for/på vegne af i sammenhæng med visning af dennes øvrige tilgængelige sundhedsdata	Gerne vil se et samlet overblik over min pårørendes sundhedsdata	Dette er pårørende versionen af S3
S12	Pårørende til en borger	At kunne spærre for sundhedspersoners adgang til (alle eller udvalgte) tidligere sendte meddelelser angående den pårørende borger, som jeg agerer for/på vegne af	På vegne af min pårørende ikke ønsker der skal være adgang til disse meddelelser for de(n) pågældende sundhedsperson(er)	Dette er pårørende versionen af S4
S13	Pårørende til en borger	At kunne se hvilke sundhedspersoner har tilgået sendte meddelelser angående den pårørende borger, som jeg agerer for/på vegne af	Undersøger hvem, der har tilgået sundhedsdata angående min pårørende	Dette er pårørende versionen af S5
S14	Sundheds-person	At kunne hente og gennemlæse nyligt sendte meddelelser angående en borger	Har en aktiv behandlingsrelation til pågældende borger	På den måde kan sundhedspersonen proaktivt holde sig

Id	Som en	Ønsker jeg	Når jeg	Bemærkning
				ajour med hvad der måtte ske med sine patienter udenfor sit eget behandlingsregi til gavn for patientsikkerheden
S15	Sundhedsperson	At have mulighed for at modtage en notifikation når der er sendt en ny meddelelse angående en borger	Har en aktiv behandlingsrelation til pågældende borger	På den måde hjælpes sundhedspersonen til at holde sig proaktivt ajour og udføre rettidig omhu i forhold til borgeren til gavn for dennes patientsikkerhed
S16	Sundhedsperson	For en given borger at kunne hente og gennemlæse tidligere sendte meddelelser angående borgeren til andre sundhedspersoner/instanser/borgeren	Skal behandle den pågældende borger	På den måde kan sundhedspersonen blive hjulpet med at blive opdateret på, hvad der er sket med den pågældende borger udenfor sit eget behandlingsregi
S17	Sundhedsperson	At kunne følge med i status for de meddelelser jeg selv har sendt	Gerne vil orientere mig om hvor langt mine afsendte meddelelser er kommet	Er relateret til S1 – blot andre søgekriterier.
S18	Sagsbehandler af patientklagesager	At kunne hente og gennemlæse tidligere sendte meddelelser angående en borger	Undersøger en patientklagesag over et udrednings- eller behandlingsforløb	Dette kunne f.eks. være patientombudsmanden, der på denne måde nemt ville kunne få adgang til hvilken meddelelseskommunikation, der har været på hvilke tidspunkter angående borgeren

11. Appendiks C

I forhold til konvolutter er der som nævnt i afsnit 5.2.1 følgende to kandiderende standarder til konvolutten:

- Standard Business Document Header (SBDH) [SBDH]
- Exchange Header Envelope (XHE) Version 1.0 [XHE]

Kvaliteter, fordele og ulemper ved begge præsenteres i det følgende.

11.1 Standard Business Document Header

SBDH har følgende kvaliteter:

- Kompatibel med eDelivery og PEPPOL
- Kan bundte et indeholdt forretningsdokument (”business document”).

Fordele	**Ulemper**
Velafprøvet og udbredt brug i PEPPOL	Mangler kryptering af indeholdte dokumenter og/eller artefakter for øget sikkerhed og fortrolighed
Pt. de-facto standard i PEPPOL	Giver ikke i sig selv mulighed for at verificere integriteten af forretningsdokumenter
	SBDH specifikationen er en header teknologi ofte brugt i stedet for en konvolut. SBDH er ikke formelt optaget som en standard og kræver tilpasning forud for implementering
	Bliver ikke vedligeholdt af en standardiseringsorganisation

11.2 Exchange Header Envelope Version 1.0

XHE er en ny fælles OASIS- og UN/CEFACT-specifikation, som afløser de to gældende header/envelope-standarder (OASIS Business Document Envelope [BDE] og SBDH), og den har følgende kvaliteter:

- Kompatibel med eDelivery og PEPPOL
- Kan indeholde flere dokumenter og artefakter
- Understøtter kryptering af indeholdte dokumenter og/eller artefakter for øget sikkerhed og fortrolighed
- Giver mulighed for at verificere integriteten af forretningsdokumenter.

Fordele	Ulemper
XHE-konvolutten leverer funktionalitet, der ikke kan opnås ved hjælp af SBDH, såsom: - Kan indeholde flere dokumenter og artefakter - Understøtter kryptering af indeholdte dokumenter og/eller artefakter for øget sikkerhed og fortrolighed - Giver mulighed for at verificere integriteten af forretningsdokumenter	Endnu ikke bredt udbredt, men anvendes f.eks. i det svenske eDelivery initiativ [SVEDEL].
Der er udarbejdet migreringsguides: En SBDH-implementering kan migreres til XHE uden tab af data, mening eller kontekst. Uanset om SBDH bruges som header-teknologi eller som kuvert-teknologi, kan XHE problemfrit erstatte enhver forekomst af SBDH i nøjagtig samme position, kontekst og miljø, hvor den bruges, og uden behov for at ændre yderligere forretningsprocesser, dokumenter, konventioner eller andet relaterede systemer eller komponenter uden for selve SBDH	
Flere internationale PEPPOL organisationer anbefaler XHE, men tillader brugen af SBDH aktuelt, mens man bevæger sig mod den nye XHE-protokol (OpenPeppol [OPENPEPPOL], The Global In-teroperability Framework [GIF], The Business Payments Coalition [BPC])	

12. Appendiks D

I forbindelse med Sundhedsadressering er det interessant at undersøge følgende kandiderende internationale Standarder fra sundhedsdomænet:

- Healthcare Provider Directory (HPD) [HPD]
- Mobile Care Services Discovery (mCSD) [MCSD]

Derudover er der en yderligere kandiderende standard, som ikke udspringer af sundhedsdomænet og som er mere generisk:

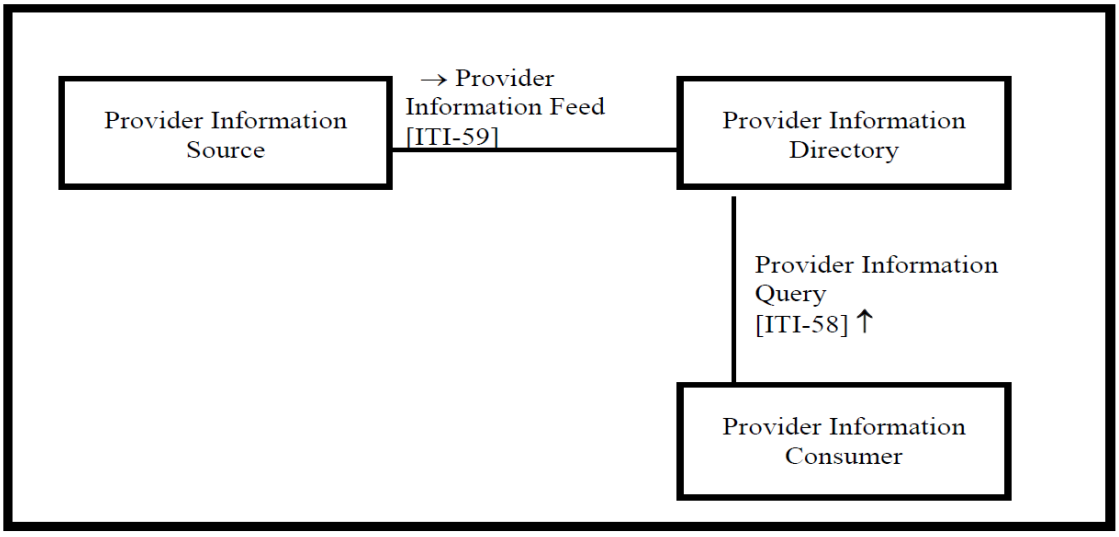
- Collaboration Protocol Profile and Agreement (CPPA) Version 3.0 [CPPA].

Sidstnævnte er bl.a. også interessant, da den vil kunne anvendes i forbindelse med et basisregister for de metadata, der skal populere SMP, således at SMP kan genskabes, om dette skulle blive nødvendigt – f.eks. i forbindelse med reetablering efter et alvorligt driftsnedbrud, jf. diskussionen i afsnit 6.1.5.

12.1 Healthcare Provider Directory

HPD er en IHE udviklet standard baseret på en udvidelse af Lightweight Directory Access Protocol (LDAP) standarden [LDAP]. Den udmærker sig, som alle IHE profiler, ved at være velbeskrevet efter IHE's sædvanlige regler med aktører og transaktioner mellem disse aktører.

LDAP er en moden, fleksibel og velunderstøttet standardbaseret mekanisme til interaktion med katalogservere. Det bruges ofte til godkendelse og lagring af oplysninger om brugere, grupper og applikationer, men en LDAP-katalogserver er i bund dog grund et datalager, der kan anvendes til forskellige formål og kan bruges i en lang række applikationer.



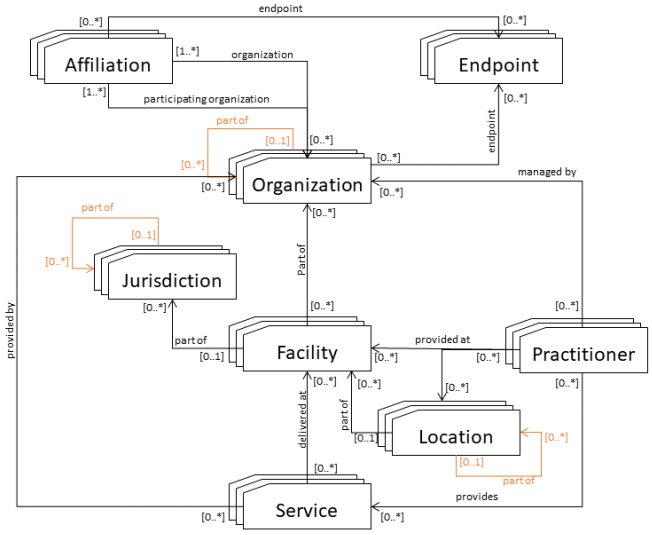
Figur 24: HPD profil aktør diagram.

HPD kan rumme alle de basale oplysninger i SOR, men forholder sig kun refererende til interoperabilitetsbegrebet, når vi snakker meddelelseskommunikation. Det betyder i princippet, at man kan benytte en standard som CPPA til at løfte denne sidste opgave.

Fordele	**Ulemper**
Baseret på LDAP	Kun en trial standard indtil videre
Fokuseret imod sundhedsdomænet	Mangler at forholde sig til meddelelseskommunikation
Kan udvides med extensions	

12.2 Mobile Care Services Discovery

mCSD er ligeledes en IHE udviklet standard men denne gang baseret på en udvidelse af HL7 FHIR standarden:



Figur 25: mCSD højniveau relationsdiagram imellem centrale entiteter.

Som for HPD, udmærker mCSD sig, som alle IHE profiler, ved at være velbeskrevet efter IHE's sædvanlige regler med aktører og transaktioner mellem disse aktører.

Fordele	**Ulemper**
Baseret på HL7 FHIR, som pt. er den sundhedsstandard, som har størst interesse og som er bedst værktøjsunderstøttet	Kun en trial standard indtil videre

Fokuseret imod sundhedsdomænet	Mangler at forholde sig til meddelelseskommunikation
Kan udvides med extensions	
Kan anvendes som ekstern snitfladespecifikation imod HPD	

12.3 Collaboration Protocol Profile and Agreement Version 3.0

CPPA anvendes til at definere hvordan meddelelsesprotokoller og kommunikationsnetværk bruges til at udveksle dokumenter eller data, og beskriver hvordan afsender- og modtagerparter konsekvent skal konfigurere deres kommunikationsparametrene for deres meddelelsessystemer og for deres netværk. Disse parametre kan grupperes i følgende kategorier:

- Parametre relateret til en afsender, såsom dens partidentifikator, signeringscertifikat(er) og IP-adressen (eller adresseområderne), hvorfra den forbinder og sender meddelelser.
- Parametre relateret til en modtager, såsom dens partidentifikator, krypteringscertifikat(er), server-URL og serverens IP-adresse(r), hvor den accepterer forbindelser og modtager meddelelser.
- Parametre relateret til den eller de understøttede forretningsprocesser, såsom processens navn, version og identifikator, partsroller, meddelelseskoreografier for tjenester og deres handlinger samt servicekvalitetsegenskaber for disse handlinger.
- Parametre relateret til den eller de anvendte meddelelsesprotokoller, såsom valg af (versioner af) konvolutformater, der skal bruges, sikkerhed og anden servicekvalitetskonfiguration, transmissionstilstand og fejlhåndtering.
- Parametre relateret til de data og/eller dokumenter, der udveksles, såsom (versioner af) XML-skemaet, der skal bruges til de udvekslede dokumenter, eventuelle egenskaber på meddelelsesniveau og den måde, dataene pakkes på.

Fordele	**Ulemper**
Baseret på ebXML, som også er den standard-familie, som AS4 og eDelivery er baseret på	Endnu en standard, der skal anvendes
Generisk, dvs. anvendelig i alle domæner	
Kan udvides med extensions	
Planlægges integreret ind i eDelivery's SMP/SML således, at disse kan populeres med de korrekte data fra CPPA	
Giver mulighed for at udstille og dokumentere en kommunikationsparts certificerede	

kapabiliteter i forhold til både afsendelse og modtagelse	

12.4 Diskussion

Alle tre standarder kan altså i virkeligheden bringes i spil for at understøtte sundhedsadressering. CPPA er dog den standard, der er mest generisk ift. brug i forskellige domæner, og den eneste, som forholder sig aktivt til meddelelseskommunikation og avancerede kommunikationsmønstre.

13. Appendiks E

I følgende tabel er forskellige temaer relateret til governance sammenholdt med de fire forskellige niveauer hvorpå governance for punkt til punkt meddelelseskommunikation tænkes håndteret. Disse fire niveauer er som nævnt i kapitel 7: eDelivery netværk, sundhedsdomæne, accesspunkt (C2/C3 i eDelivery's fire-corner model) og system (C1/C4 i bred forstand i eDelivery's fire-corner model). Temaerne i tabellen tager udgangspunkt i dem fra [EDELDIGSTANRAP], og en yderligere inspirationskilde er den fællesoffentlige systemforvaltning af sundheds-IT (FSI).

Gruppe	**Tema**	**eDelivery netværk**	**Sundhedsdomæne**	**Access-punkt**	**System (C1/C4 i bred forstand)**
Strategi og udvikling	Strategi	Vedligeholder overordnet strategi for eDelivery i Danmark. Ejes af forretningsstyregruppen for eDelivery i Danmark. Faciliterer strategiforum med deltagere fra samme parter som forretningsstyregruppen	Vedligeholder egen strategi for eDelivery internt på sundhedsdomænet. Deltager i eDelivery netværk strategiforum. Faciliterer strategiforum på sundhedsdomænet	Udvalgte deltager i eDelivery netværk strategiforum. Udvalgte deltager i strategiforum på sundhedsdomænet. Relevante brancheorganisationer udpeger deltagerne.	Udvalgte deltager i strategiforum på sundhedsdomænet.
	Roadmap	Aligned med strategien	Aligned med eDelivery netværk roadmap og egen interne strategi for eDelivery på sundhedsdomænet	Aligned med eDelivery netværk og sundhedsdomæne roadmaps for eDelivery.	Aligned med eDelivery netværk og sundhedsdomæne roadmaps for eDelivery.
	EU	Koordination med fælles EU regler for eDelivery.	Indirekte via forretningsstyregruppemedlem.	Indirekte via forretningsstyregruppemedlem	Indirekte via forretningsstyregruppemedlem

Gruppe	Tema	eDelivery netværk	Sundhedsdo-mæne	Access-punkt	System (C1/C4 i bred forstand)
		Deltagelse i diverse EU fora om eDelivery.	Deltagelse i udvalgte EU fora om eDelivery.		
	Interessenthåndtering	Faciliterer forretningsstyregruppe for eDelivery i Danmark, der har medlemmer fra de enkelte domæner under eDelivery og eventuelt (store) serviceudbydere. Faciliterer faglig referencegruppe for eDelivery i Danmark med deltagere fra samme parter som forretningsstyregruppen.	Deltager i eDelivery netværk forretningsstyregruppe. Faciliterer forretningsstyregruppe for eDelivery på sundhedsdomænet. Deltager i eDelivery netværk faglige referencegruppe. Faciliterer faglige referencegruppe for eDelivery på sundhedsdomænet.	Udvalgte deltager i fælles-offentlige forretningsstyregruppe. Udvalgte deltager i eDelivery netværk faglige referencegruppe. Udvalgte deltager i forretningsstyregruppen på sundhedsdomænet. Udvalgte deltager i den faglige referencegruppe på sundhedsdomænet. Relevante brancheorganisationer udpeger deltagerne.	Udvalgte deltager i forretningsstyregruppen på sundhedsdomænet. Udvalgte deltager i den faglige referencegruppe på sundhedsdomænet.
Systemforvaltning	Leverandør-styring	Aftale med leverandør af SMP. Aftaler med leverandører af accesspunkter.	Aftale med leverandør af sundhedsadresseringsservice. Domæneaftaler med leverandører af accesspunkter.	Efterlever aftaler med eDelivery netværk, sundhedsdomæne, og systemer.	Aftale med leverandør af access-punkt.

Gruppe	Tema	eDelivery netværk	Sundhedsdo-mæne	Access-punkt	System (C1/C4 i bred forstand)
	Adm. af centrale kompo-nenter	Vedligehol-delse og stabil drift af SMP.	Vedligeholdelse og stabil drift af sundhedsadres-seringsservice		
	Adm. af certifika-ter	Vedligehold certifikater – herunder trust list. Udstil "auto-matiserede" arbejdsgange i forhold til certifikater.	Anvender "auto-matiserede" eDe-livery netværk ar-bejdsgange for certifikater (her-under revoke)	Overvåg gyldig-hed af egne certifikater	Overvåg gyl-dighed af egne certifika-ter i det om-fang det måtte være relevant for meddelelses-kommunikati-onen.
	Standar-der	Sker i samar-bejde med EU. Vedligehold de fælles eDe-livery standar-der (som f.eks. under-liggende OASIS). Vedligehold metadata i forhold til de fælles eDeli-very standar-der. Giver access-punkter mu-lighed for ba-sal connecti-vity og confor-mance test i forhold til de	Vedligehold med-delelses-standar-der på sundheds-området (FHIR/OIO-XML/…). Vedligehold stan-darder for konvo-lutter på sund-hedsområdet. Vedligehold me-tadata i medde-lelsesstandarder på sundhedsom-rådet inklusiv re-levante metadata i forhold til efter-følgende deling af meddelelser. Certificerer ac-cess-punkter og systemer detalje-ret i forhold til eDelivery stan-	Holde sig ajour med og efter-leve ændringer i de fælles eDe-livery standar-der relevante for access-punkter	Holde sig ajour med og efterleve æn-dringer i stan-darder på sundhedsom-rådet.

Gruppe	Tema	eDelivery netværk	Sundhedsdomæne	Access-punkt	System (C1/C4 i bred forstand)
		fælles eDelivery standarder.	darder, kvitteringsflows, og meddelelsesstandarder på sundhedsområdet.		
	Incident management	Håndterer incidents i forhold til SMP. Holder for SMP relaterede incidents domæne og access-punkts incident managers informeret.	Håndterer incidents i forhold til sundhedsadresseringsservice. Orienterer systemer om sundhedsadresseringsservice relaterede incidents. Holdes orienteret om SMP relaterede incidents.	Håndterer incidents i forhold til access-punktet. Opdages enten internt i organisationen omkring access-punktet eller via henvendelse fra et system. Holdes orienteret om SMP relaterede incidents og system relaterede incidents.	Håndterer incidents angående eDelivery meddelelses-kommunikation i forhold til systemet. Holdes orienteret om access-punkt relaterede incidents og sundheds-adresseringsservice relaterede incidents.
	Problem management	Problem management angående SMP og SML opstået på baggrund af incidents. Orienterer sundhedsdomæne og access-punkt om SMP og SML relaterede problems.	Problem management angående sundheds-adresseringsservice opstået på baggrund af incidents. Orienterer systemer om sundhedsadresseringsservice relaterede problems. Orienteres om SMP og SML relaterede problems.	Problem management angående access-punktet. Orienteres om SMP og SML relaterede problems.	Problem management angående systemet. Orienteres om sundheds-adresseringsservice relaterede incidents.

Gruppe	Tema	eDelivery netværk	Sundhedsdomæne	Access-punkt	System (C1/C4 i bred forstand)
		Eskaleringspunkt for problemer med forbindelse mellem to access-punkter.	Eskaleringspunkt for problemer med indhold af meddelelser.		
	Change management	Er koordineret både i forhold til EU initiativer og domæneønsker til eDelivery netværk niveau og er prioriteret i roadmap. Ændringer til SMP opstået på baggrund af incidents.	Change management angående sundhedsadresseringsservice. Oprettelse af nye meddelelsestyper på sundhedsområdet (i SMP). Oprettelse af nye systemer modtagere (i SMP). Håndterer changes, der er gældende på sundhedsområdet, men ikke på eDelivery netværk niveau.	Håndterer changes for access-punktet, der kommer fra eDelivery netværk niveau og sundhedsdomæneniveauet. Håndterer changes i forhold til kommunikationen med systemer.	Håndterer changes i forhold til kommunikationen med access-punktet samt changes i forhold til sundhedsadresseringsservicen.
	Security management	Håndtering af SMP relaterede security incidents. Faciliterer audits af sikkerhed omkring SMP. Indarbejdelse af overordnede sikkerhedspolitikker for eDelivery i	Håndtering af security incidents relateret til sundhedsadresseringsservice. Faciliterer audits af sikkerhed omkring sundhedsadresseringsservice. Indarbejdelse af sikkerhedspolitikker specifikt for eDelivery på	Håndtering af access-punkt relaterede security incidents. Faciliterer audit af sikkerhed omkring access-punkt og rapporter til eDelivery netværk og sundhedsdomæne forretningsstyregrupper.	Håndtering af security incidents relateret til system.

Gruppe	Tema	eDelivery netværk	Sundhedsdomæne	Access-punkt	System (C1/C4 i bred forstand)
		Danmark i tilslutningsaftale.	sundhedsdomænet i domænetilslutningsaftale for access-punkter.		
	Service level management	Udarbejdning af overordnet SLA for eDelivery i Danmark. Opfølgning på overordnet SLA for eDelivery i Danmark. Afrapportering på overordnet SLA for eDelivery i Danmark til forretningsstyregruppe. Indarbejdelse af overordnet SLA for eDelivery i tilslutningsaftale.	Udarbejdning af SLA for eDelivery på sundhedsdomænet. Opfølgning på SLA for eDelivery på sundhedsdomænet. Afrapportering på SLA for eDelivery på sundhedsdomænet til forretningsstyregruppe for eDelivery på sundhedsområdet. Indarbejdelse af SLA for eDelivery på sundhedsdomænet i domænetilslutningsaftale for access-punkt. Udarbejdning af SLA for sundhedsadresseringsservice. Opfølgning på SLA for sundhedsadresseringsservice. Afrapportering på SLA for sund-	Udarbejdning af SLA imellem access-punkt og system. Opfølgning på SLA imellem access-punkt og system. Afrapportering på SLA imellem access-punkt og system til service level management hos system og sundhedsdomæne. Implementer forbedringer i access-punkt i forhold til SLA, når påkrævet.	Implementer forbedringer i system i forhold til SLA, når påkrævet.

Gruppe	Tema	eDelivery netværk	Sundhedsdomæne	Access-punkt	System (C1/C4 i bred forstand)
			hedsadresseringsservice til forretningsstyregruppe for eDelivery på sundhedsområdet. Implementer forbedringer i sundhedsadresseringsservice i forhold til SLA, når påkrævet.		
Brugersupport og -dialog	Support	Support af SMP – initieres enten internt eller via henvendelse fra et accesspunkt support.	Support i forhold til sundhedsadresseringsservice – initieres enten internt eller via henvendelse fra et access-punkts support eller et systems support.	Support af access-punkt – initieres enten internt eller via henvendelse fra et systems support eller via overvågningsinitieret henvendelse fra sundhedsdomæne support.	Support vedrørende eDelivery kommunikation for system – initieres oftest af slutbrugere af systemet.
	Dialog via brugergrupper	Deltager i EU eDelivery brugerforum.	Deltager i EU eDelivery brugerforum. Ansvarlig og facilitator for sundhedsdomæne eDelivery brugerforum.	Deltager i sundhedsdomæne eDelivery brugerfora.	Deltager i sundhedsdomæne eDelivery brugerfora.
	Dokumentation	Online dokumentation af al dokumentation relevant for eDelivery netværk	Online dokumentation af al dokumentation relevant for sundhedsdomæne niveau, herunder	Anvender online dokumentation fra eDelivery netværk	Anvender online dokumentation fra sundhedsdomæne niveau.

Gruppe	Tema	eDelivery netværk	Sundhedsdo-mæne	Access-punkt	System (C1/C4 i bred forstand)
		niveau, her-under tilslut-ningsvejled-ning, an-vendte fælles eDelivery standarder, service over-sigt, API doku-mentation, og kodeeksem-pler.	meddelelsesstan-darder på sund-hedsområdet, anvenderguide for sundheds-adresseringsser-vice, og "klar til certificering tjek-liste".	og sundheds-domæne ni-veau. Udveksler do-kumentation med system re-levant for kom-munikation med samme.	Udveksler do-kumentation med access-punkt rele-vant for kom-munikation med samme.
	Tilslut-ningsafta-ler	Netværkstil-slutningsafta-ler med ac-cess-punkter. Aftaler med domæner.	Domænetilslut-ningsaftaler med access-punkter for sundhedsdo-mænet.	Aftaler med sy-stemer.	Aftale med ac-cess-punkt.
	Tilslut-ningsbi-stand	"Startpakke". Udstil "auto-matiseret" ar-bejdsgang for tilslutning. Onboarding-miljø med mulighed for afprøvning og basal connec-tivity og con-formance test.	"Domænestart-pakke" for sund-hedsdomænet. Certificering af access-punkter. Certificering af systemer. White-lister ac-cess-punkter til tilslutning.	Hjælp til tilslut-ning til system. Anvender "au-tomatiseret" eDelivery net-værk arbejds-gang for tilslut-ning efter certi-ficering.	Hjælp til til-slutning til ac-cess-punkt.

Henvisning

[SFDS-18-22] Strategi for Digital Sundhed 2018-2022. https://sum.dk/~/media/Filer%20-%20Publikationer_i_pdf/2018/Strategi-for-digital-sundhed-januar-2018/Strategi%20for%20digital%20sundhed_Pages.pdf

[SDG] Single Digital Gateway. https://ec.europa.eu/growth/single-market/single-digital-gateway_en

[EHDS] European Health Data Space. https://ec.europa.eu/health/ehealth-digital-health-and-care/european-health-data-space_da

[POCEVAL] Evaluering af POC for modernisering af MedCom infrastruktur. https://www.medcom.dk/media/10151/bilag-3-evalueringsnotat-v1-3.pdf

[MC11-SG-7] Referat fra MedComs styregruppe d. 2. oktober 2019. https://www.medcom.dk/media/10683/endeligt-referat-af-7-moede-i-medcom11-styregruppen.pdf

[PILEVAL] Meddelelseskommunikation på Sundhedsområdet, Evaluering af Målbillede og Pilot. https://www.medcom.dk/media/13105/evaluering-af-maalbillede-og-pilot-for-meddelelseskommunikation-paa-sundhedsomraadet-100.pdf

[MFDFS] Målbillede for det Fælles Digitale Fundament for Sundhedsområdet. Er under publicering. Kan indtil videre fås ved henvendelse til SDS

[TOGAF] TOGAF®: https://www.opengroup.org/togaf

[MC-S86] MedCom - det danske sundhedsdatanet frem mod år 2000, MedCom, marts 1998. https://www.medcom.dk/media/1383/medcom-det-danske-sundhedsdatanet-frem-mod-aar-2000.pdf

[MC8-SG-4] Teknologisk fremtidssikring af MedCom-kommunikationen. Delprojekt 3 i MedCom8. Deloitte, 23. oktober 2012. Endelig afrapportering. Bilag til møde i MedComs styregruppe d. 15. november 2012. https://www.medcom.dk/media/4875/teknologisk-fremtidssikr.pdf

[MC8-SG-5] NemInfo. Teknologisk fremtidssikring af MedCom kommunikationen. SOA infrastruktur og Meddelelseshotel – teknologisk modernisering der rykker! MedCom, 12. december 2012. Bilag til møde i MedComs styregruppe d. 28. februar 2013. https://www.medcom.dk/media/4805/neminfo.pdf

[MC8-SG-6] Forslag til Teknologisk fremtidssikring af MedCom kommunikationen, Rambøll, 10. april 2013. Bilag til møde i MedComs styregruppe d. 25. juni 2013. https://www.medcom.dk/media/4831/teknologisk-fremtidssikr.pdf

[ARPRSU] Arkitekturprincipper for Sundhedsområdet. https://sundhedsdatastyrelsen.dk/-/media/sds/filer/rammer-og-retningslinjer/referenceaktitektur-og-it-standarder/arkitekturprincipper_version-2,-d-,0.pdf?la=da

[HVIDBOG] Hvidbog om fællesoffentlig digital arkitektur. https://arkitektur.digst.dk/sites/default/files/241_hvidbog_om_arkitektur_for_digitalisering_version_1.0_kolofon.pdf

[SBDH] Standard Business Document Header https://www.gs1.org/standards/edi/standard-business-document-header-sbdh

[XHE] Exchange Header Envelope (XHE) Version 1.0 https://docs.oasis-open.org/bdxr/xhe/v1.0/xhe-v1.0-oasis.html [CPPA] Collaboration Protocol Profile and Agreement. https://docs.oasis-open.org/ebcore/cppa/v3.0/cppa-v3.0.html

[OASIS] The Organization for the Advancement of Structured Information Standards. https://www.oasis-open.org/

[HPD] Health Provider Directory. https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_HPD.pdf

[MCSD] Mobile Care Services Discovery. https://profiles.ihe.net/ITI/mCSD/index.html

[REFARKINFSIK] Referencearkitektur for informationssikkerhed. https://sundhedsdatastyrelsen.dk/-/media/sds/filer/rammer-og-retningslinjer/referenceaktitektur-og-it-standarder/referencearkitektur/referencearkitektur-informationssikkerhed.pdf?la=da

[EDELDIGSTANRAP] Etablering af et fællesoffentligt dansk eDelivery netværk. Er under publicering. Kan indtil videre fås ved henvendelse til DIGST

[EDELSIK] CEF eDelivery Building Block. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Security+Controls+guidance?preview=/82773295/82802571/(CEFeDelivery).(SecurityControls).(v1.00).pdf

[CYBERSTRAT] Strategi for cyber- og informationssikkerhed i sundhedssektoren https://www.sum.dk/Aktuelt/Nyheder/Digitalisering/2019/Januar/~/media/Filer%20-%20dokumenter/2019/Cyberstrategi/SUM-Cyber-og-Informationssikkerhed_WEB_opsl.pdf

[LDAP] Lightweight Directory Access Protocol. https://ldap.com/

[BDE] OASIS Business Document Envelope. http://docs.oasis-open.org/bdxr/bdx-bde/v1.1/bdx-bde-v1.1.html

[SVEDEL] Svensk anvendelse af eDelivery. https://inera.atlassian.net/wiki/spaces/OISDK/pages/2879423212/Inneh+llsspecifikation-+Meddelande

[OPENPEPPOL] OpenPeppol. https://peppol.eu/

[GIF] The Global Interoperability Framework. http://gifworks.io/

[BPC] The Business Payments Coalition. https://businesspaymentscoalition.org/