RAPPORT 2020

Målbillede for sammenhængende brugerstyring

Beskrivelse af tillidstjenester og tillidsrelationer

SUNDHEDSDATA-
STYRELSEN

Resumé

Sundhedsdatastyrelsen har i tæt samarbejde med parterne udarbejdet et målbillede for sammenhængende brugerstyring med det formål at skabe klarhed og enighed om rammerne for en sammenhængende brugerstyring på sundhedsområdet. Målbilledet præsenterer en mere tillidsbaseret og lettere administrerbar model for sammenhængende brugerstyring samt opstiller det nødvendige fælles grundlag for tillid mellem parterne.

Målbilledet beskriver, hvordan en national føderation på sundhedsområdet kan etableres med sammenhæng til fællesoffentlig samt til regionale og kommunale føderationer. Fødererede sikkerhedsløsninger indebærer, at organisationer har gensidig tillid til oplysninger om brugeres elektroniske identiteter, autentifikation af brugere, rettighedsoplysninger med videre ved anvendelse af digitale tjenester på tværs af organisationer. Målbilledet beskriver videre, hvordan infrastruktur på sundhedsområdet kan integreres med fællesoffentlig infrastruktur (NemLog-in), således at MitID vil kunne bringes til at give adgang til nationale tjenester på sundhedsområdet, hvilket imødekommer ønsker fra især praksissektoren.

Tilliden mellem parterne i en fødereret model baserer sig på et tillidsrammeværk bestående af politikker og aftaler. Målbilledet udpeger National standard for identiteters sikringsniveau (NSIS) som tillidsrammeværk i føderationen, og identificerer desuden en række politikker, som modsvarer specifikke krav for sundhedsområdet.

Målbilledet danner herefter ramme for det videre arbejde med brugerstyringsløsninger på sundhedsområdet.

Udgiver	Sundhedsdatastyrelsen
Ansvarlig institution	Sundhedsdatastyrelsen
Design	Sundhedsdatastyrelsen
Copyright	© Sundhedsdatastyrelsen
Version	1.1.1
Versionsdato	23. januar 2020
Web-adresse	www.sundhedsdata.dk
Titel	Målbillede for sammenhængende brugerstyring

Målbilledet er udarbejdet på en række workshops med deltagelse af repræsentanter for regioner, kommuner (Kombit) og lægepraksisleverandører. Rapporten er skrevet af Sundhedsdatastyrelsen med bistand fra Jan Riis (Lakeside).

Deltagere:

Kjeld Sørensen	Region Hovedstaden
Allan Hansen	Region Midt
Rasmus Halkjær Iversen	Kombit/kommuner
Allan Greis Eriksen	Novax/PL-Forum
Dennis Kirkeby	Novax/PL-Forum
Michael Due Madsen	Medcom
Thomas Holme	Sundhed.dk
Simon Bergholt Holmgaard	Digitaliseringsstyrelsen
Esben Dalsgaard	Sundhedsdatastyrelsen
Wasim Shaukat Chohan	Sundhedsdatastyrelsen
Kim Michael Mortensen	Sundhedsdatastyrelsen
Pia Jespersen	Sundhedsdatastyrelsen
Søren Nielsen	Sundhedsdatastyrelsen
Helle Mørch	Sundhedsdatastyrelsen
Jan Riis	Lakeside

Indhold

1. Indledning

Dette dokument opstiller et fælles målbillede for sammenhængende brugerstyring på sundhedsområdet. Målbilledet er blevet til i et samarbejde mellem de centrale parter på området, og vil herefter være retningsanvisende for realisering af en fødereret brugerstyring for sundhedsområdet. Parterne har med målbilledet skabt enighed om fælles, forpligtende rammer.

1.1 Formål

Dette dokument har til formål at opstille et målbilledet for sammenhængende brugerstyring, som sikrer parterne adgang til nationale tjenester inden for sundhedsdomænet via egne føderationer eller den fællesoffentlige føderation, og som samtidig sikrer overholdelse af gældende lov for adgang til sundhedsdata.

Målbilledet har konkret til opgave at gøre følgende:

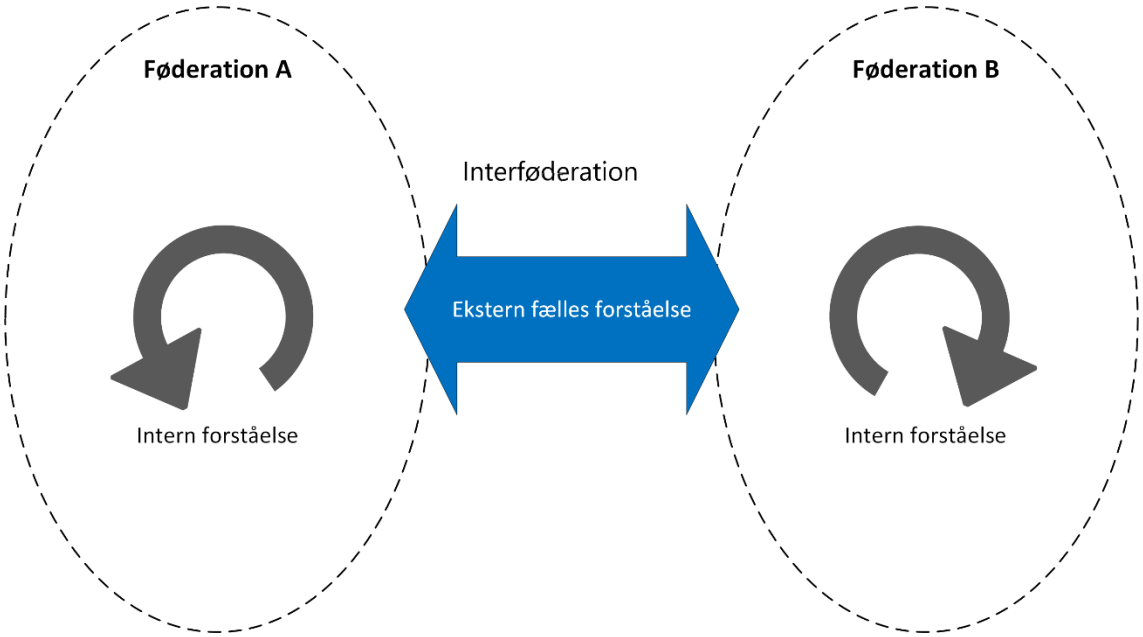
- At anvise hvorledes parternes egne autentifikations- og billetudstedelsestjenester kan tages i brug for at give borgere og medarbejdere mulighed for at tilgå nationale digitale tjenester på sundhedsområdet
- At bestemme hvilke tillidsforhold, de enkelte tjenester baseres på
- At identificere de tillidstjenester, der skal indgå i fremtidige føderationer
- At identificere nødvendige interføderale integrationer med tilhørende aftaler.

Målbilledet danner således afsæt for det videre arbejde med at specificere og etablere føderationerne.

1.2 Indhold

Målbilledet beskriver sammenhængende brugerstyring for sundhedsområdet. Brugerstyring anvendes her i samme betydning som i Den fællesoffentlige referencearkitektur for brugerstyring [Brugerstyring-referencearkitektur], og skal opfattes bredt omfattende autentifikation, adgangskontrol såvel som administration af brugere og adgangsrettigheder.

Målbilledet anviser, hvordan den nationale føderation på sundhedsområdet, den regionale, den kommunale samt den fællesoffentlige føderation sammenbindes i en føderation af føderationer, i målbilledet betegnet en interføderation. Parterne indgår i interføderationen ud fra en fælles forståelse, som respekterer parternes interne forståelse (se Figur 1). Målbilledet for sammenhængende brugerstyring sigter således på at skabe den fælles forståelse, som er nødvendig for, at de øvrige føderationer kan indgå i interføderation med den nationale føderation på sundhedsområdet.



Figur 1: Intern vs. ekstern forståelse af tekniske og organisatoriske procedurer, specifikationer og standarder [modificeret efter Analyse2014, s. 23]

Målbilledet angår både sundhedspersoner og borgeres adgang til sundhedsdata.

1.3 Afgrænsning

Målbilledet opstiller ikke konkrete løsninger for brugerstyring hos parterne, men overlader det til parterne selv at udforme lokale løsninger i overensstemmelse med målbilledet. Målbilledet forholder sig desuden kun til parternes adgang til fællesoffentlige tjenester i den udstrækning, at interføderationen påvirker parternes adgang til disse.

Endelig forholder målbilledet sig ikke til brugerstyring relateret til ikke-nationale tjenester såsom den fællesregionale præhospitale patientjournal eller tilsvarende fælleskommunale tjenester. Der opfordres i stedet til, at man ved udformning af nye tjenester tager højde for målbilledet, såfremt den pågældende tjeneste har potentiale til at blive en national sundhedstjeneste. Der opstilles ikke faste kriterier for, hvornår en tjeneste betragtes som national, det må i stedet bero på en vurdering i det konkrete tilfælde.

1.3.1 Afgrænsninger i denne version

Fokus med denne første version af målbilledet er at tilvejebringe det nødvendige grundlag for, at parterne inden for sundhedsområdet kan forberede overgangen til MitID og Nemlogin 3 på en måde som sikrer, at der ikke sker tab af substantiel funktionalitet. Der er allerede et kendt behov for at udvide målbilledet med yderligere elementer, hvorfor der inden for en kort tidshorisont vil blive igangsat udarbejdelse af en ny version af målbilledet. Følgende elementer vil ikke være omfattet af første version af målbilledet, men vil blive indarbejdet i en fremtidig version:

- EIDAS-forordningens krav om gensidig anerkendelse af elektroniske identiteter fra EU-borgere i forbindelse med tjenester af grænseoverskridende karakter. Målbilledet vil her skulle bero på elementer i den fællesoffentlige infrastruktur, som der endnu ikke er tegnet et klart billede af. Denne version af målbilledet afgrænser sig derfor fra denne problematik
- *Internet of things*, *devices* og borgerrapporterede data. Området forventes at få en større betydning inden for sundhedsvæsnet i fremtiden, men er dog endnu ikke tilstrækkelig modent i et nationalt sundhedsitperspektiv, og udskydes derfor til en senere version af målbilledet
- Borgerens egen kontrol over egne data

Målbilledet formuleres inden for rammerne af den fællesoffentlige referencearkitektur for brugerstyring [Brugerstyring-referencearkitektur] samt referencearkitekturen for informationssikkerhed for sundhedsområdet [INFSIK-REF]. Begge disse er under revision, og kan medføre behov for efterfølgende ændringer af målbilledet.

1.4 Terminologi

Centrale begreber forklares efterhånden som de behandles i dokumentet, og fremhæves med **fed**, første gang det sker. Der er desuden givet en samlet oversigt over disse termer i appendiks A. Indledningsvist er **brugerstyring** og **interføderation** introduceret ovenfor. Der tages udgangspunkt i det fællesoffentlige begrebsapparat for brugerstyring, først og fremmest udtrykt i [brugerstyring], samt i den nationale begrebsdatabase for sundhedsområdet [Nationale begrebsdatabase]. Centrale begreber, som det ikke skønnes nødvendige at forklare nærmere, fremhæves med *kursiv,* når de introduceres første gang. *Kursiv* anvendes også, når engelske termer optræder i rapporten.

1.5 Læsevejledning

Resumé
Giver en sammenfatning af målbilledet henvendt til beslutningstagere og andre interesserede.

Den øvrige del af dokumentet er primært rettet mod arkitekter og ansvarlige for udvikling af sammenhængende brugerstyring blandt parterne.

Afsnit 1: Indledning
Giver et samlet overblik over dokumentet.

Afsnit 2: Baggrund

Ridser historien op for udviklingen inden for området, herunder udviklingen frem mod den interføderale model.

Afsnit 3: Styring
Her introduceres målbilledets interessenter. Dernæst præsenteres den interføderale model, og herunder identificeres de forskellige tillidsbaserede elementer samt de tilhørende styringsredskaber.

Afsnit 4: Strategisk
Redegør for *drivere* bag målbilledet og rammerne, inden for hvilke målbilledet formuleres. Dette omfatter juridiske såvel som øvrige rammer. Afsnittet opstiller desuden vision og målsætning for målbilledet samt fastlægger principper for sammenhængende brugerstyring.

Afsnit 5: Jura
Giver et kort overblik over de juridiske rammer, som målbilledet er underlagt.

Afsnit 6: Forretningsmæssigt
Beskriver forretningsentiteter, brugsscenarier i form af *user stories* samt forretningsprocesser forbundet med sammenhængende brugerstyring.

Afsnit 7: Applikation og teknik
Beskriver applikationskomponenter, applikationsflows, identificerer attributindhold og –tjenester samt belyser rammer for *token*profiler.

2. Baggrund

Målbilledet opstillet i dette notat, er seneste led i en udvikling af infrastruktur- og sikkerhedsløsninger på sundhedsområdet. Gennem en årrække har man styret i retning af såkaldt føderative sikkerhedsmodeller, hvor sikkerhedsløsninger ved forskellige parter indgår i en samlet sikkerhedsmodel for sundhedsområdet.

Føderationsmodellen blev officielt lanceret på sundhedsområdet med referencearkitekturen for informationssikkerhed [INFSIK-REF] i 2013. Heri diskuteres forskellige typer sikkerhedsmodeller der varierer i forhold til hvordan forskellige parter har tillid til hinanden. Referencearkitekturen fastslår endvidere, at sikkerhedsniveauer og tillidsrelationer skal reguleres gennem klare politikker og aftaler, der kan gøres til genstand for opfølgning og styring [INFSIK-REF, princip S3].

I 2013 – 2014 blev der gennemført en fællesoffentlig analyse af sikkerhedsstandarder og –løsninger [Analyse2014]. Med denne ønskede man at give udviklingen af brugerstyring fællesoffentligt og på sundhedsområdet et serviceeftersyn. Analysen viste, at der er inden for det offentlige er udviklet fælles løsninger på en række områder, og at udviklingen af disse er foregået relativt ukoordineret. Men analysen viste også, at der - på trods af den forholdsvis ukoordinerede udvikling - var store lighedspunkter i den overordnede arkitektur (føderative, **billet**baserede teknologier) og anvendte standarder (*SAML 2*, *WSTrust* etc.). Det vurderedes derfor, at man med en relativ beskeden indsats kunne få de enkelte sikkerhedsløsninger til at hænge sammen. Til at underbygge dette beskriver analysen visionen om et såkaldt økosystem, hvor dele udvikles af forskellige offentlige og private parter, og hvor de udviklede dele bidrager til det samlede system[1]. Analysen skitserer, hvorledes et overordnet målbillede, der realiserer visionen, kunne se ud, og formuleringen af målbilledet i denne rapport kan ses som en konkretisering heraf.

Analysen kom også med en række konkrete anbefalinger. For det første burde visionen forankres i en fællesoffentlig strategi for brugerstyring, og denne burde underbygges af en fællesoffentlig referencearkitektur. For det andet burde en fællesoffentlig føderation understøttes af et såkaldt **trustrammeværk**, der udtrykker fælles krav til de parter, der indgår i en føderation, så disse kan have tillid til hinanden. Endelig blev der udtrykt behov for etablering af en fællesoffentlig styring af fællesoffentlige produkter i form af strategier, referencearkitekturer, standarder, værktøjer og infrastrukturkomponenter. I forhold til sundhedsområdet anbefalede analysen, at standarder på sundhedsområdet i højere grad bliver udarbejdet inden for rammerne af fællesoffentlige standarder; helt konkret blev det anbefalet at udarbejde en ny webservicestandard på sundhedsområdet ved at profilere den fællesoffentlige *IDWS*-standard (standard for

[1] Eksempelvis kan man forestille sig, at undervisningsområdet stiller Uni-login til rådighed for andre områder, således at børn og unge under 15 år kan benytte deres Uni-login til at få adgang til tjenester på forskellige fagområder (NemID udstedes kun til personer fra 15 år).

identitetsbaserede webservices) på en sådan måde, at denne også kom til at overholde den internationale *IHE XUA* standard. Denne nye webservicestandard (*IDWS XUA*) skulle så afløse den mere proprietære webservicestandard *DGWS* (Den Gode Web Service) på sundhedsområdet.

Samtidig med, at disse anbefalinger blev givet i 2014, var regioner og kommuner begyndt at etablere fællesregionale og fælleskommunale løsninger baseret på fødererede sikkerhedsmodeller, hvor brugerstyring og autentifikation skulle ske lokalt, og parterne udtrykte ønske om, at nationale løsninger på sundhedsområdet fulgte samme retning. Det førte til, at man i projektet vedrørende national sårjournal nedsatte en arbejdsgruppe, der kunne komme med forslag til en sikkerhedsløsning [Sårjournal-sikkerhed] [Sårjournal-løsning] baseret på anbefalingerne i den før omtalte analyse. Arbejdsgruppen var fokuseret på, at de infrastrukturkomponenter, der skulle indgå i løsningen blev tænkt som generelle sikkerhedskomponenter og ikke sikkerhedskomponenter specifikke for sårjournalen. I løsningen indgik således allerede etablerede fællesløsninger ved regioner og kommuner (den **fællesregionale ADFS**-løsning og Kombits **context handler**) og der blev peget på behovet for en national føderationsløsning. Denne funktionalitet blev etableret i den nationale SEB-løsning og lagt i drift i sommeren 2015. Forslaget til samlet sikkerhedsløsning blev forelagt såvel regionernes som kommunernes arkitekturråd. For at løsningen kommer til at fungere som tiltænkt, skal den nationale, den kommunale og den regionale fællesløsning integreres. Dette er endnu ikke sket (forventes gennemført ultimo 2019/primo 2020), men målbilledet er beskrevet i notatet [Interføderation]. Dette målbillede indgår som en del af det samlede målbillede beskrevet i denne rapport.

Et andet initiativ, der har bidraget til målbilledet i denne rapport, er det såkaldte IDWS-projekt på sundhedsområdet. Dette har fra 2017 til 2019 været med til at realisere anbefalingerne fra 2014-analysen [Analyse2014] om etablering af en ny webservicestandard/-profil (IDWS-XUA), understøttelsen af denne med værktøjer og infrastrukturkomponenter og afprøvning af disse i pilotprojekter. IDWS-projektet har kunnet bidrage såvel med anvendelsesscenarier [IDWS-anvendelsesscenarier] som med mere tekniske flows [IDWS-målbilleder] [IDWS-målarkitektur].

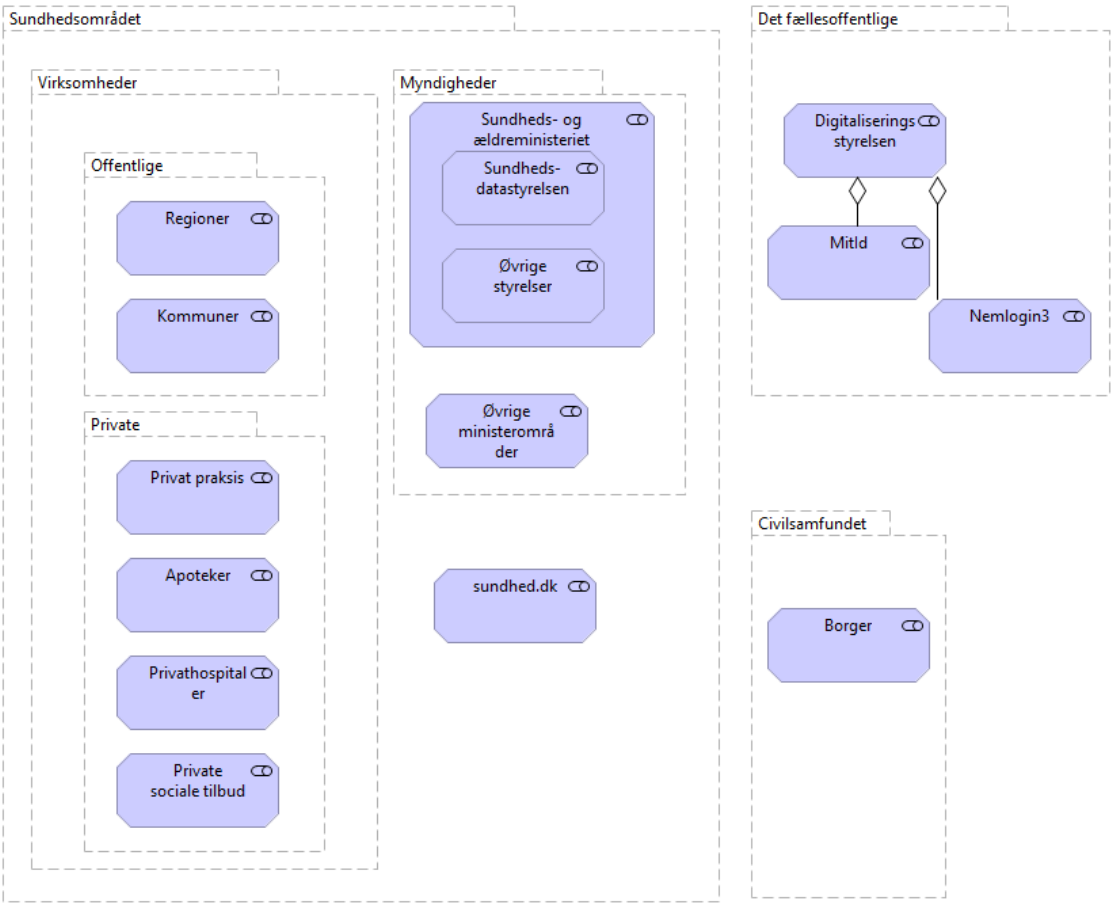
Fællesoffentligt er der også gennemført initiativer, der realiserer anbefalinger fra 2014-analysen. Der er i 2017 blevet færdiggjort en fællesoffentlig strategi [Brugerstyring-strategi] og en fællesoffentlig referencearkitektur for brugerstyring [Brugerstyring-referencearkitektur], og der blev i 2018 vedtaget en national standard for identitetssikringsniveauer [NSIS] [NSIS-vejledning], der danner grundlaget for tillid til identiteter i en føderation (trustrammeværk).

3. Styring

I dette afsnit gennemgås først målbilledets interessenter. Dernæst introduceres den overordnede føderationsmodel for sundhedsområdet efterfulgt af en gennemgang af tillidsbaserede elementer i målbilledet. Endelig introduceres de overordnede styringsrammer og –principper for interføderationen.

3.1 Interessenter og interesser

Følgende viser målbilledets centrale interessenter.



Figur 2: De centrale interessenter for den sammenhængende brugerstyring på sundhedsområdet.

I nedenstående tabel gennemgås de enkelte interessenter og deres interesser i målbilledet.

Interessent	Interesse

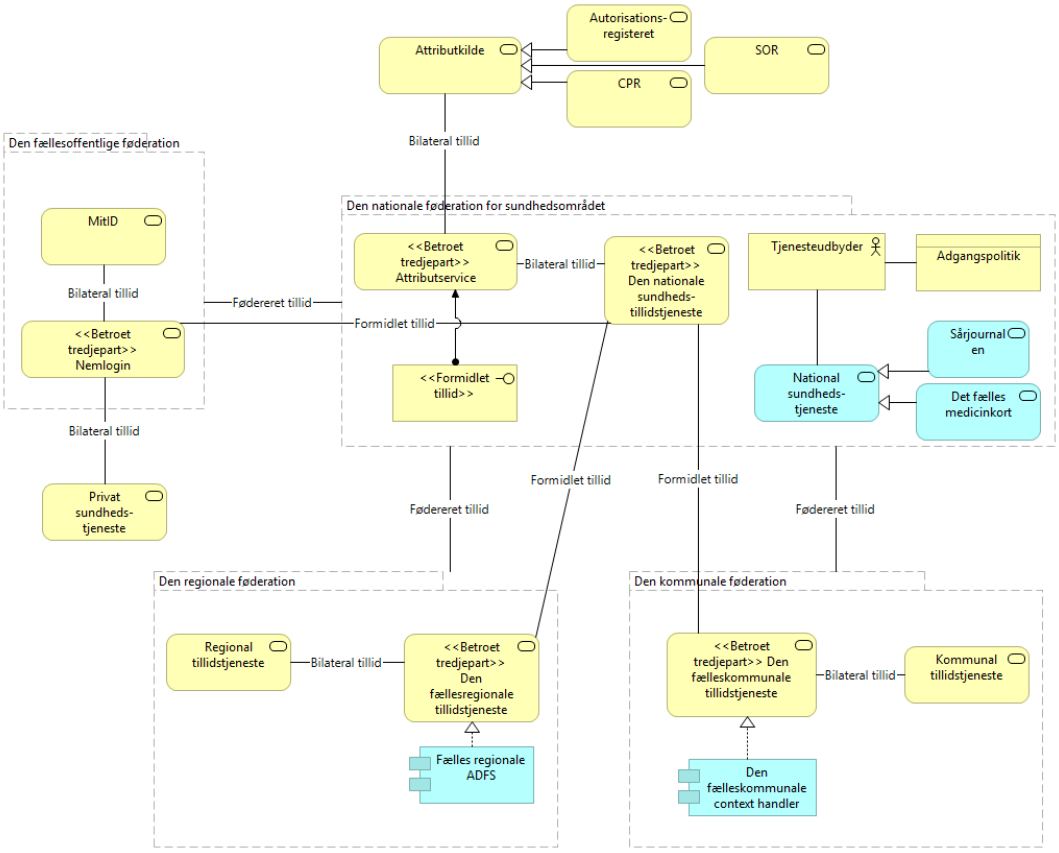
Digitaliserings-styrelsen	Forvalter den fællesoffentlige digitaliseringsindsats, og er i denne sammenhæng ansvarlig for en række overordnede krav til målbilledet samt for konkrete krav i forhold til den fællesoffentlige føderation, som realiseres med MidID og Nemlogin3
Sundheds- og ældreministeriet (SUM)	SUM har ansvaret for sundhedsloven, som regulerer adgang til sundhedsdata. Sundhedsdatastyrelsen under SUM har ansvaret for den nationale føderation for sundhedsområdet, og har desuden ansvaret for en række nationale tjenester, der giver adgang til sundhedsdata, også betegnet **nationale digitale sundhedstjenester**. Øvrige styrelser inden for SUM bidrager blandt andet med konkretisering af sundhedsloven samt visse tilsynsopgaver, der berører trustrammeværkets virkefelt. Endelig er den nationale føderation for sundhedsområdet afhængig af data fra flere søsterstyrelser data
Øvrige ministerområder	Først og fremmest foregår der sundhedsrelateret aktivitet i forsvaret og kriminalforsorgen, hvorfor der i disse organisationer ses et behov for adgang til sundhedsdata
Regioner	Regionerne har i dag egne fødererede løsninger, og har en stor interesse i at kunne anvende lokale løsninger sammen med den nationale føderation på sundhedsområdet for derigennem at opnå en mere enkel og ensartet brugerstyring. Regionerne har desuden etableret en fælles føderation, som i dag varetages af Region Nord
Kommuner	Kommunerne har i dag en fælles føderationsløsning, som forvaltes af Kombit. Derudover har kommunerne meget forskellig størrelse, og dermed også forskellige forudsætninger for at kunne gennemføre nødvendige tilpasninger
Sundhed.dk	Sundhed.dk er den centrale udbyder af nationale borgervendte digitale sundhedstjenester, og har som tjenesteudbyder en interesse i, hvordan adgangspolitikker skal implementeres
Private aktører	Private aktører omfatter blandt andet privatpraktiserende læger, apoteker, privathospitaler, bosteder med videre. Fælles for dem er, at de forventes at ville skulle gøre brug af den fællesoffentlige føderation for at kunne tilslutte sig den nationale sundhedsføderation
Borger	Borgeren har en interesse i, at sundhedsdata behandles forsvarligt og i overensstemmelse med gældende lovgivning, og har samtidig en interesse i at kunne få adgang til egne sundhedsdata

Tabel 1: Interessenter for målbilledet samt deres interesser

3.2 Interføderationen for sundhedsområdet

Målbilledet bygger på de føderationer, som parterne inden for sundhedsområdet i forvejen har etableret samt på den fællesoffentlige føderation. Denne føderation af føderationer betegnes i målbilledet som en interføderation. Der indgår en række **tillidsrelationer** i målbilledet, det vil sige en række relationer, hvor parterne stoler på, og er afhængige af overholdelse af fælles indgåede aftaler. Grundlæggende er målbilledet baseret sig på **fødereret tillid**, hvilket betyder, at tilliden til it-sikkerhedselementer parterne imellem baseres på fælles besluttede krav, aftaler og kontroller udtrykt i et trustrammeværk. De enkelte **tillidstjenester** hos de omfattede føderationer formidler information om brugere til tjenesteudbydere på vegne af tjenesteaftagere, som tjenesteudbyder er afhængig af for at kunne udføre sin lovpligtige adgangskontrol. Tillidstjenesterne agerer således **betroet tredjepart** som **formidler tillid.** På det regionale område formidler den fælleskommunale tillidstjeneste, i form af Context Handler, tillid på vegne af de enkelte kommuners tillidstjenester, og på det regionale område formidler den fællesregionale tillidstjeneste, i form af den fællesregionale ADFS, tillid på vegne af de enkelte regioners tillidstjenester. Tilsvarende formidler NemLogin3 tillid på vegne af MitID. Stamdatatjenesten i den nationale sundhedsføderation er betroet tredjepart, som stiller data til rådighed for parterne fra forskellige eksterne kilder, såsom Autorisationsregisteret, Sundhedsvæsenets organisationsregister og Det centrale personregister. Stamdatatjenesten indgår dermed i en **bilateral tillidsrelation** med de eksterne datakilder, som baserer sig på aftaler om forhold som datakvalitet og leveranceterminer.

Nedenstående figur viser interføderationen samt de overordnede tillidsrelationer i denne.



Figur 3: Interføderationen og de forskellige former for tillidsrelationer, som indgår

3.3 Tillidsbaserede elementer

3.3.1 Identiteter

Hovedparten af de nationale digitale sundhedstjenester er kendetegnet ved at være **identitets-baserede digitale tjenester,** hvormed der menes, at en brugers adgang til tjenesten forudsætter en **adgangsbillet,** som er knyttet sammen med en forudgående verifikation af brugerens **digitale identitet.** Tjenesteudbyder må derfor kunne stole på den enkelte brugers digitale identitet er korrekt håndteret.

Ved etableringen af den digitale identitet skal tjenesteudbyder kunne have tillid til, at den fysiske eller juridiske person er verificeret samt at den digitale identitet og tilhørende **identifikations-midler** er udstedt og efterfølgende forvaltet efter aftalte sikringsniveau. For borgeres vedkommende vil den digitale identitet være mitID. For virksomheder kan den digitale identitet være mitID, lokalt validerede OCES-certifikater eller egne identifikationsmidler. I sidstnævnte tilfælde vil det dog være et krav, at der indgår en national identitetskode, jf. princip 5. Hvis en part fremover ønsker at være lokal udsteder af digitale identiteter og identifikationsmidler, påtager man sig således ansvaret for registreringskapabiliteten.

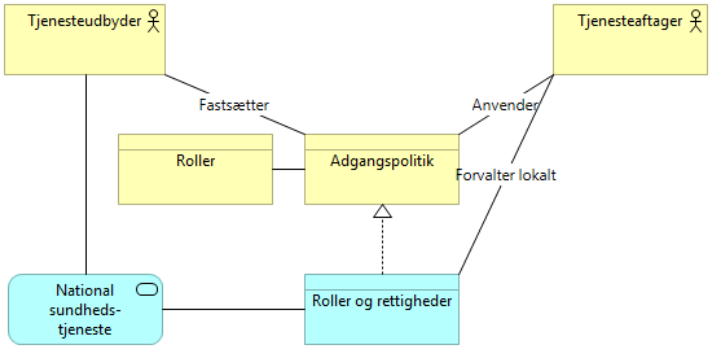
Ved autentifikation har vi tillid til, at nogen er i stand til at verificere et identifikationsmiddel på et sikringsniveau i overensstemmelse med det aftalte, hvilket indebærer at kunne verificere ægthed, holde styr på revokationer samt gyldighedsperiode. Hvis man vil være lokal identitetstjeneste, så skal man kunne dette for egne udstedte digitale identiteter.

3.3.2 Attributdata fra eksterne parter

En række eksterne registre anvendes i dag som autoritative kilder til stamdata i den nuværende nationale føderation på sundhedsområdet, herunder data, der anvendes som **attributter,** der beskriver egenskaber ved brugere, såsom brugernavn, CPR-nummer, autorisationsnummer med videre. Det er kendetegnende for de eksterne registre, at de er skabt i en anden kontekst og med et andet forretningsmæssigt formål end brugerstyring for øje. Det er typiske Sundhedsdatastyrelsen, som agerer betroet tredjepart i denne sammenhæng, og der påhviler derfor Sundhedsdatastyrelsen et ansvar for, at de nødvendige bilaterale aftaler er etableret i overensstemmelse med datas betydning i interføderationen.

3.3.3 Adgangspolitikker, roller og rettigheder

Tjenesteudbyder er ansvarlig for at fastlægge en adgangspolitik for en given digital tjeneste ud fra lovgivningsmæssige rammer og krav samt en risikovurdering for den pågældende tjeneste. Adgangspolitikken vil typisk forholde sig til, hvilke forretningsmæssige rettigheder forskellige forretningsmæssige roller skal have i forhold til tjenesten. Adgangspolitikken omsættes herefter til en række tekniske roller og rettigheder, som gør det muligt at implementere teknisk adgangskontrol for den pågældende digitale tjeneste. Nedenstående figur illustrerer dette:



Figur 4: Adgangspolitikker, roller og rettigheder

Hos tjenesteaftager vil rettigheder for den enkelte bruger være knyttet sammen med organisation. Tilknytning af organisation og rettigheder forbundet hermed, herunder ledelsesbestemte delegeringer jf. gældende lov og samt ledelsesbesluttede indskrænkninger i forhold til individuelle autorisationer afspejlet i autorisationsregisteret, administreres lokalt. Tjenesteudbyder har

her tillid til, at dette sker korrekt, og at sikkerheden i brugeradministrationsløsningerne er tilstrækkelig høj.

Målbilledet tager ikke stilling til, hvordan nationale, tjenestespecifikke og lokale roller og rettigheder skal fastlægges og forvaltes. Målbilledet lægger derfor op til, at der udarbejdes en referencearkitektur for adgangspolitikker, roller og rettigheder.

3.3.4 Kontekstoplysninger

Når brugeren tilgår nationale sundhedstjenester gennem sit lokale fagsystem, har parterne tillid til, at det lokale fagsystem afleverer korrekte oplysninger om kontekst ved anvendelse af de nationale tjenester. Hvis der er en naturlig ejer-applikation af patientkonteksten, skal det kun være muligt at ændre patientkonteksten der. Hvis der er ligeværdighed mellem applikationer, skal enhver patientkontekstændring medføre koordineret kontekstskifte mellem alle applikationer, både lokale applikationer og eksterne applikationer.

3.3.5 Sessionsstyring

Når brugeren tilgår en tjeneste gennem sin applikation, vil der ofte blive dannet en **session** mellem applikation og tjenesten. Sessionen løber frem til brugeren aktivt afslutter den eller såfremt inaktivitet hos brugeren overstiger en forud fastsat tidsgrænse. Sessionsbeviset vil ligge på klientsiden, og det er derfor nødvendigt at formulere krav til opbevaring af sessionsbeviser inden for føderationen. Klienten vil som udgangspunkt bestå af en klientfrontend, eksempelvis i form af en browser, en desktopklient eller en *app*, samt en *backend*, der kommunikerer med den digitale tjeneste. Sessionsbeviser skal opbevares på klientens *backend*, og skal fjernes, når en af følgende indtræffer: brugeren logger ud eller sessionsbeviset udløber [NIST SP 800-63 B, afsnit 7].

De sessioner, som oprettes i forbindelse med login, bør have en fornuftig levetid, vurderet ud fra et sikkerheds- og risikomæssigt perspektiv. Sessionen beror på et login-bevis, hvis attributters kvalitet kan aftage over tid. I autentifikationsøjeblikket kan en dataansvarlig være ganske sikker på validiteten af login-beviset i sessionen, mens man eksempelvis ikke med samme sikkerhed kan antage, at det er den samme person, der sidder bag skærmen efter 30 minutter. Det er den dataansvarlige myndighed for en given digital tjeneste, som fastsætter, hvor længe en bruger kan opnå adgang til tjenesten i samme session, ligesom den dataansvarlige fastlægger, hvilke tekniske og administrative krav der i øvrigt er til i forhold til den enkelte tjeneste. Kravene til nationale sundhedstjenester bør dog forsøges harmoniseret gennem føderationsaftalen.

3.3.6 Opbevaring af billetter

Sundhedsvæsenet har behov for at fastlægge mere fleksible retningslinjer for billetters levetid, end de for det fællesoffentlige gældende en time. Begrundelsen herfor er en afvejning af hensynet til sikkerhed på den ene side og brugervenlighed på den anden.

Der skelnes i den forbindelse mellem krav til henholdsvis **omvekslingsbilletter** og **adgangsbilletter**. En omvekslingsbillet fungerer som et bevis for en autentifikation, og skal derfor blandt andet kommunikere autentifikationens sikringsniveau. Omvekslingsbilletten dannes ved login og konstituerer brugerens session. For at få adgang til digitale tjenester skal omvekslingsbilletten veksles til en tjenestespecifik adgangsbillet. Omvekslingsbilletter kan opbevares og gøres mobile, så de kan anvendes på tværs af applikationer og platforme ud fra organisationens behov. Da der til stadighed skal kunne være tillid til alle parters håndtering af login-sessioner, vil det være nødvendigt at stille højere krav til validitet, integritetssikring, kommunikation og opbevaring af omvekslingsbilletter, ligesom disse løsninger skal undergå revision på lige fod med identitets-løsningerne.

Generelt opereres der derfor med en længere levetid inden for sundhedsområdet, som dog kan fraviges af de enkelte tjenesteudbydere. Der skal opstilles krav til opbevaring af billetter inden for føderationen på sundhedsområdet som modsvarer de risici, som følger af den længere levetid.

3.4 Trustrammeværk

Den aftalebaserede tillid er underbygget af en række aftaler og politikker. Aftaler og politikker er beskrevet i nedenstående tabel, og vil blive udarbejdet i forlængelse af målbilledet. Lokal efterlevelse bliver sikret gennem en række kontroller i form af tilsyn og ekstern revision.

Aftale/politik/retningslinje	Beskrivelse
Tilslutningsaftale for den nationale sundhedsføderation	Overordnede krav til parter, der tilslutter sig interføderationen, herunder krav til omfang og karakter af den revision, som parterne forpligter sig til ved tilslutning. Overordnet er der krav om overholdelse af NSIS og ISO 27001. Disse dækker tilsammen, blandt meget andet, krav til brugerstyring
National standard fro attributkvalitet på sundhedsområdet (NSAK)	Krav til kvalitet ved anvendelse af attributdata (analogt til NSIS sikringsniveauer), eksempelvis for caching af lokale kopier samt krav til aftaler med dataleverandører

Politik for håndtering af adgangsbilletter og sessionshåndtering	Rammer og retningslinjer for sessions- og fødereationshåndtering, der svarer til det der reguleres i NIST SP800-63B (autentifikation, reautentifikation og sessioner) og SP800-63C (føderationer). Der tages udgangspunkt i [SOSI-politik]
Politik for kontekshåndtering	Retningslinjer, som skal sikre korrekte patientrelaterede data ved anvendelse af nationale sundhedstjenester
Politik for adgangspolitikker, roller og rettigheder	Politik, der fastlægger retningslinjer for nationale, tjenestespecifikke og lokale adgangspolitikker og retningslinjer i forbindelse med adgang til nationale digitale tjenester på sundhedsområdet

3.5 Godkendelsesproces for politikker

Godkendelse af politikker og aftalekrav følger den etablerede it-governance for sundhedsområdet.

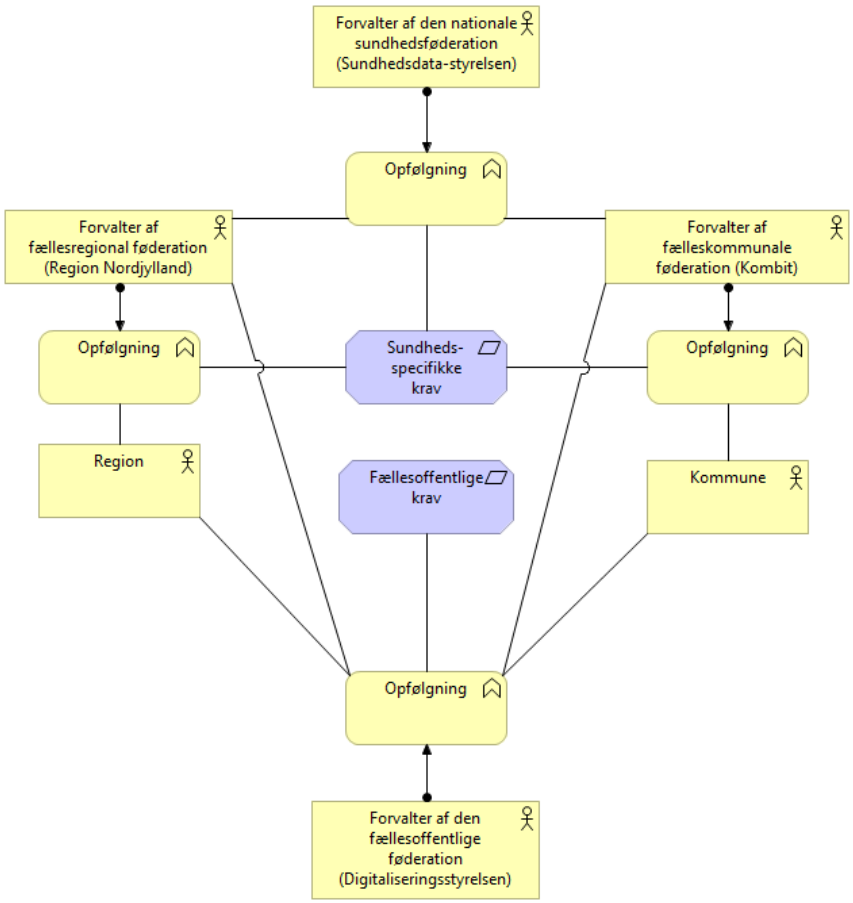
3.6 Revision og opfølgning

Overholdelse af aftaler og politikker inden for interføderationen sikres gennem revision og opfølgning.

Sundhedsdatastyrelsen er som myndighed kravstiller i forhold til interføderationen. Digitaliseringsstyrelsen er kravstiller, hvad angår de fællesoffentlige krav. En del af de krav, som gælder for interføderationen, er dækket af de fælles-offentlige krav, som Digitaliserinsgstyrelsen varetager tilsynet af. De øvrige krav, udtrykt i ovenstående politikker, er Sundhedsdatastyrelsen ansvarlig myndighed for.

Sundhedsdatastyrlsen følger op i forhold til de betroede aftaleparter Region Nordjylland og Kombit. Den regionale aftalepart og den kommunale aftalepartaftalepart har ansvaret for at følgefølge op i forhold til henholdsvis de fem regioner og de 98 kommuner. Dette drejer sig eksempelvis om at sikre, at fagapplikationer lever op til gældende politikker.

Ansvarsfordelingen for tilsyn fremgår af nedenstående figur:



Figur 5: Ansvarlige for opfølgning i interføderationen.

For at leve op til de fællesoffentlige krav såvel som de sundhedsspecifikke krav til brugerstyring, vil der være behov for øget revision, herunder krav om ekstern revision. Opfølgning vil omfatte at følge op på revisioner samt at aftale og følge op på handlingsplaner i forhold til eventuelle uhensigtsmæssigheder.

4. Strategisk

4.1 Hvad driver udviklingen?

Målbillede indgår som en del af arbejdet med at forberede indførelsen af mitID og NemLog-in3 på sundhedsområdet, og er som sådan en bunden opgave. Moderniseringen af den fællesoffentlige infrastruktur betyder markante ændringer i betingelserne for de anvendende parter.

Med overgangen til MitID og NemLog-in3 og indførelsen af ny national standard for identiteters sikringsniveauer [NSIS] ændres der på principperne for validering af identifikationsmidler. Dette betyder, at der er behov for at sikre overblik over hvor valideringen af identifikationsmidlerne sker, således at kravene til de nødvendige identitetssikringsniveauer mødes.

Blandt ændringerne er også, at MitID, i modsætning til nemID, kun vil levere autentifikation gennem brokere. Samtidig sker der et generelt løft i sikkerhedsniveaet, afspejlet i NSIS samt gennem nye standarder for certifikater. Eksempelvis gøres der op med den praksis, at certifikater opbevares hos mindre, private aktører under forhold, som ikke er sikkerhedsmæssigt tilfredsstilende.

Arbejdet med målbilledet er desuden drevet af det strategiske mål om bedre sammenhæng i sundhedsvæsnet, og den bredere adgang til nationale digitale sundhedstjenester. Udviklingen er ligeledes drevet af et ønske blandt parterne på sundhedsområdet om en større ensartning af adgangsstyring til nationale sundhedstjenester.

Opdateringen af den fællesoffentlige infrastruktur falder sammen med den teknologiske opdatering af SOAP-baserede services fra DGWS til IDWS, og det forventes, at der kan skabes synergi mellem de to tiltag.

4.2 Vision

Visionen er formuleret som følger:

Målbilledet skal

- *beskrive en sammenhængende brugerstyring, som sikrer at borgeren og den sundhedsfaglige, på baggrund af sine rettigheder, til enhver tid, på ethvert sted og ad enhver kanal kan opnå enkel og sikker adgang til nationale digitale sundhedstjenester*
- *sikre, at brugerstyring sker på en måde som opfylder lovkrav, fremmer sikkerhed, tillid, privatlivsbeskyttelse, valgmuligheder, innovation, og som øger anvendelsen af tjenester*
- *Sikre parterne lokal frihed under fælles rammer til at udforme egne løsninger*

Visionen er formuleret med afsæt i den fællesoffentlige vision om let og effektiv brugerstyring, sammenhæng af løsninger på tværs samt fremme af sikkerhed, tillid, privatlivsbeskyttelse, valgmuligheder og innovation [Brugerstyring-strategi]. Dernæst tager visionen afsæt i visionen om, at digital information er tilgængelig for aktører på sundhedsområdet ud fra rettigheder uanset tid og sted [INFSIK-REF].

4.3 Målsætninger

Visionen er nedbrudt i følgende målsætninger:

Målsætning	**Gevinst**
Sundhedspersoners og borgeres adgang til nationale digitale tjenester er uafhængig af adgangsvej	Større tiltro til digitale løsninger hos sundhedspersoner og borgere når man ser det samme
Sundhedspersoner og borgere skal bevare tillid til sikkerhed og privatlivsbeskyttelse	Tillid til sikkerhed og privatlivsbeskyttelse er kritisk for sundhedsvæsnets brug af data
Sundhedspersoner og borgere skal opleve mindst mulig gene ved brug af tillidstjenester under udførelse af deres faktiske gøremål	Sundhedspersoner anvender ikke unødig tid og koncentration, borgere oplever ikke unødig ulempe
De deltagende parter skal have frihed til at udforme lokale løsninger inden for de fælles rammer og retningslinjer	Størst mulig fleksibilitet og udnyttelse af egne investeringer
Alle relevante parter, som kan overholde føderationens regler, skal kunne tilslutte sig føderationen	Størst mulig anvendelse af nationale digitale sundhedstjenester hvor det giver værdi
Føderationen skal også kunne fungere sammen med åbne netværk	Mindre barrierer for tilslutning
Det skal sikres, at de muligheder, parterne har med eksisterende identifikationsmidler, også kan opnås, når der nye identifikationsmidler i form af MitID og NemLog-in3 er indført	Brugere oplever uændrede eller forbedrede arbejdsgange
Større ensartethed på tværs af nationale digitale sundhedstjenester	Større ensartethed i adgangspolitikker og autorisationsløsninger giver lettere administration for tjenesteudbydere og –aftagere og bidrager til øget sikkerhed

4.4 Principper

Målbilledet er formuleret under iagttagelse af en række overordnede, fastsatte principper. Det drejer det sig om de fællesoffentlige arkitekturprincipper formuleret i [Hvidbog], de generelle arkitekturprincipper for sundhedsområdet [Arkitekturprincipper] samt de mere specifikke principper for informationssikkerhed inden for sundhedsområdet [INFSIK-REF]. Nedenfor listes et antal principper, som har særlig relevans for arbejdet med målbillede. Af listen fremgår desuden reference til overliggende principper, hvor det er relevant:

Nr.	Princip	Reference
1	Skab effektive sikkerhedsløsninger	[Hvidbog AR 8.1]
2	Skab brugervenlige sikkerhedsløsninger	
3	Billetter er målrettet en modtager og indeholder kun attributter, der er nødvendige for denne	
4	Gør brugerstyring så enkel som muligt for tjenesteudbydere og anvendersystemer	
5	Den nationale infrastruktur er standardiseret og ansvaret for at integrere hertil ligger lokalt	[Arkitekturprincipper T5]
6	Benyt standarder med stor markedsdækning	[Hvidbog AR 2.2], [Arkitekturprincipper T2]
7	Overvej genbrug af eksisterende systemer før indkøb af nye systemer, overvej indkøb af standardsystemer før udvikling af nye systemer, overvej fælles indkøb før individuelt indkøb.	[Arkitekturprincipper A1]
8	Logning i de forskellige løsninger skal kunne bindes sammen, så et specifikt kald kan følges mellem parterne (fuldt transaktionsspor)	

Principperne gennemgås enkeltvis nedenfor:

Princip 1	Skab effektive sikkerhedsløsninger
Rationale	Driftseffektivitet (tilstrækkelig performance) er en forudsætning for at løsninger anvendes. En brugervenlig, privatlivsbeskyttende og sikker løsning, der giver en god understøttelse af arbejdsgange, vil ikke blive anvendt, hvis den er for langsom.
Implikationer	Benyt infrastrukturen til at optimere performance. Foretag caching af attributter og billetter. Undgå indsnævring af adgangsbilletters virkefelt (scope/audience restriction), hvis det reelt ikke har den store betydning i forhold til sikkerhed og privatlivsbeskyttelse. Overvej, om der skal stilles samme krav (dataminimering, gyldighedsperiode, kryptering

	etc.) til billetter, der kommunikeres mellem betroede infrastrukturkomponenter ad beskyttede forbindelser, som der skal stilles til billetter, der kommunikeres til tjenesteudbydere og tjenesteanvendere i mere åbne miljøer. Overvej, om der skal være differentierede krav til performance og til privatlivsbeskyttelse for forskellige typer af brugere (system, medarbejder, borger).

Princip 2	Skab brugervenlige sikkerhedsløsninger
Rationale	Brugere vil omgå sikkerhedsløsninger, som ikke er brugervenlige. Hvis det bliver for besværligt at løse sine opgaver, omgås sikringsforanstaltningerne (hvis mange forskellige personlige adgangskoder eksempelvis skal huskes, vil man enten skrive dem ned, eller benytte samme adgangskode flere steder). Denne omgåelse vil svække sikkerheden.
Implikationer	Benyt så vidt muligt de samme autentifikationsmekanismer og identifikationsmidler til den samme brugergruppe. Udstyr sundhedspersoner med identifikationsmidler, der kan integreres tæt med lokale løsninger og lokale arbejdsgange. Udnyt teknologiens muligheder til at reducere behovet for udførelse af manuelle procedurer (udnyttelse af Near Field Communication etc.). Minimer antallet af gange en bruger skal afgive en kode (understøt eksempelvis Single Sign-on på tværs af parter).

Princip 3	Billetter er målrettet en modtager og indeholder kun attributter, der er nødvendige for denne.
Rationale	Målbilledet følger et dataminimeringsprincip ud fra gængs *privacy by design*.
Implikationer	Autentifikationstjenester udsteder billetter, der snævert udtaler sig om identitet. Adgangsbilletudstedere udleverer kun de brugerattributter, der er strengt nødvendige til adgangsstyring og logning hos de respektive tjenesteudbydere. Hvis en betroet infrastrukturkomponent / tillidstjeneste har til formål at udstede tjenestespecifikke adgangsbilletter, kan infrastrukturkomponenten selv modtage en mere beriget adgangsbillet med henblik på tidsbegrænset caching af oplysninger på brugeren.

Princip 4	Gør brugerstyring så enkel som muligt
Rationale	Interføderationen bør være så enkel og overskuelig som mulig for dermed at lette opfølgning på aftaler. Tjenesteudbydere og –anvendere bør kunne have fokus på deres egentlige opgave uden at skulle anvende for mange ressourcer på brugerstyring

Implikationer	Interføderationen indgås med så få aftalepunkter som muligt. For eksempel tilgås interføderationen fra kommunalt hold via Kombits context handler og fra regionalt hold via den fællesregionale ADFS-løsning. Attributter fastlægges så vidt muligt af infrastrukturen/tillidstjenesterne (tjenesteanvendere og -udbydere kan spare opslag og integrationer til attributkilderne).

Princip 5	Den nationale infrastruktur er standardiseret og ansvaret for at integrere hertil ligger lokalt
Rationale	Princippet er med til at håndhæve en klar ansvarsfordeling mellem den decentrale- og den nationale infrastruktur, hvor ansvaret for mapning fra lokale formater og lokal semantik bevares ved den part, der har det dybe kendskab til lokale modeller og deres implementering. Da den fælles infrastruktur ikke bygger på viden om specifikke lokale løsninger, modeller eller protokoller, vil lokale ændringer af infrastruktur kunne gennemføres uden væsentlige ændringer i det fælles (og uden væsentlig involvering af den eller de parter, der har ansvar for at drive fælles infrastruktur). Dermed undgås centrale flaskehalse (teknisk og organisatorisk).
Implikationer	Lokale sikkerhedskomponenter skal kunne veksle til billetter, som kan forstås af nationale komponenter. En national sikkerhedskomponent har ikke ansvaret for at kunne forstå forskellige lokale billetformater, -klassifikationer og -indhold. Specifikt skal personer og organisationer kunne identificeres med koder fra nationale registre (CPR, CVR, SOR etc.). Hvis brugere identificeres med en kode (UUID) fra Erhvervsstyrelsens erhvervsidentitetsadministration (EIA) skal der være registreret et CPR-nummer på den pågældende identitet i denne administrationsløsning. Dette gør det muligt at foretage opslag af brugeren i andre registre (herunder Autorisationsregistret).

Princip 6	Benyt standarder med stor markedsdækning
Rationale	Ved at bruge markedsløsninger står man ikke alene med udvikling, support og vedligehold af løsningerne. For sygehusvæsenet, der arbejder meget internationalt, og som derfor ofte kan understøttes af internationale løsninger, er det væsentligt at lægge sig op ad de internationale standarder, som markedet understøtter. Anvendelsen af standarder muliggør udskiftning af løsninger eller delløsninger.
Implikationer	Lad markedsunderstøttelse indgå i kriterierne for valg af standarder.

	Undlad så vidt muligt at stille krav som ikke kan dækkes af standardiserede løsninger og af markedsprodukter.

Princip 7	Overvej genbrug af eksisterende systemer før indkøb af nye systemer, overvej indkøb af standardsystemer før udvikling af nye systemer, overvej fælles indkøb før individuelt indkøb.
Rationale	Princippet understøtter direkte målsætningerne om effektivitet ved at trække på såvel erfaringer som løsninger, der allerede har bevist deres værdi eller, såfremt sådanne ikke findes, at slå sig sammen om at indkøbe løsninger. Med princippet forpligter parterne sig til at orientere sig om andre parters erfaringer og løsninger mhp. muligt genbrug.
Implikationer	Anvend fællesoffentlige identifikationsmidler med mindre væsentlige grunde taler for andre identifikationsmidler. Gå sammen med andre parter om valg af identifikationsmidler med mindre man kan begrunde væsentlige forskelle i behov. Benyt fælles sikkerhedskomponenter med mindre behovet for driftsstabilitet og driftseffektivitet tilsiger mere lokale løsninger.

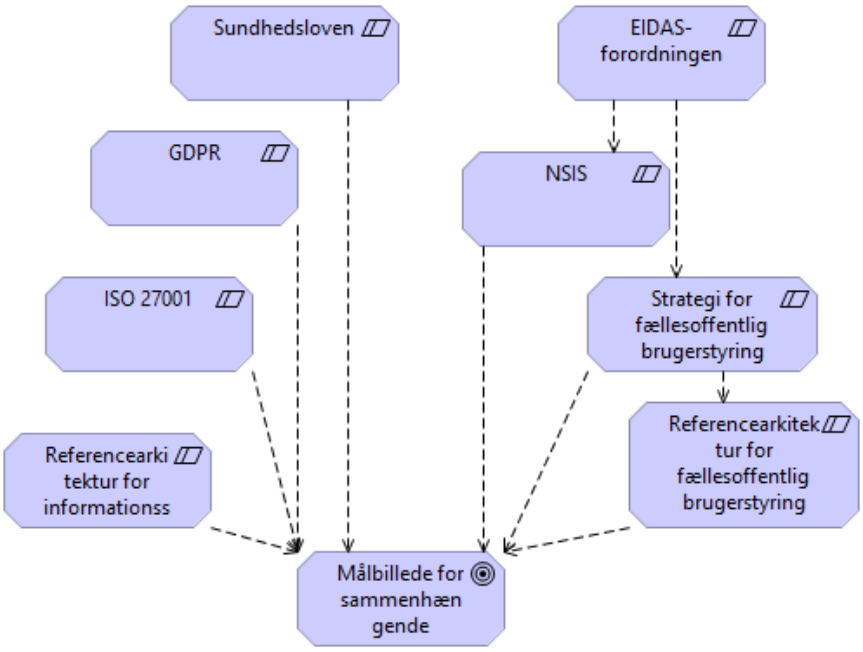
Princip 8	Logning i de forskellige løsninger skal kunne bindes sammen, så et specifikt kald kan følges mellem parterne (fuldt transaktionsspor)
Rationale	Det skal være muligt at følge en given sessions forskellige trin, herunder at identificere kilden for autentifikation, ved at gennemgå de relevante logs.
Implikationer	Der skal implementeres en teknologi, der gør det muligt at logge en sessions forløb på tværs af de løsninger den gennemløber, og efterfølgende genskabe dette forløb.

5. Jura

Målbilledet for sammenhængende brugerstyring skal sikre brugeres adgang til sundhedsdata via nationale digitale tjenester på sundhedsområdet, og er som sådan underlagt Sundhedsloven og Lov om autorisation af sundhedspersoner og om sundhedsfaglig virksomhed samt de bekendtgørelser, som uddyber disse. I forlængelse heraf tager målbilledet desuden afsæt i referencearkitekturen for informationssikkerhed for sundhedsområdet [INFSIK-REF]. Denne arkitektur har som primært fokus at fastlægge løsningskoncepter, som operationaliserer sundhedslovens bestemmelser om indhentning og videregivelse af information. Referencearkitekturen er primo 2020 under revision.

Dernæst er målbilledet underlagt fællesoffentlige rammer for digitalisering, herunder specifikke love, regler og retningslinjer for brugerstyring. De overordnede mål for brugerstyring inden for det offentlige er udtrykt i den fællesoffentlige strategi for brugerstyring [Brugerstyring-strategi]. Strategien har følgeskab af den fællesoffentlige referencearkitektur for brugerstyring [Brugerstyring-referencearkitektur], og til sammen skal de to bidrage til en større sammenhæng af brugerstyringsløsninger inden for forskellige områder og sektorer. De overliggende lovgivningsmæssige rammer er givet i [EIDAS], som blandt andet opstiller regler for tillidstjenester og digitale identiteter. EIDAS-forordningen kommer blandt andet til udtryk den nationale standard for identiteters sikringsniveau [NSIS]. NSIS er derfor en central del af rammerne for målbilledet.

Endelig er GDPR og ISO 27001 rammesættende for målbilledet. Figuren nedenfor viser de rammesættende elementer.



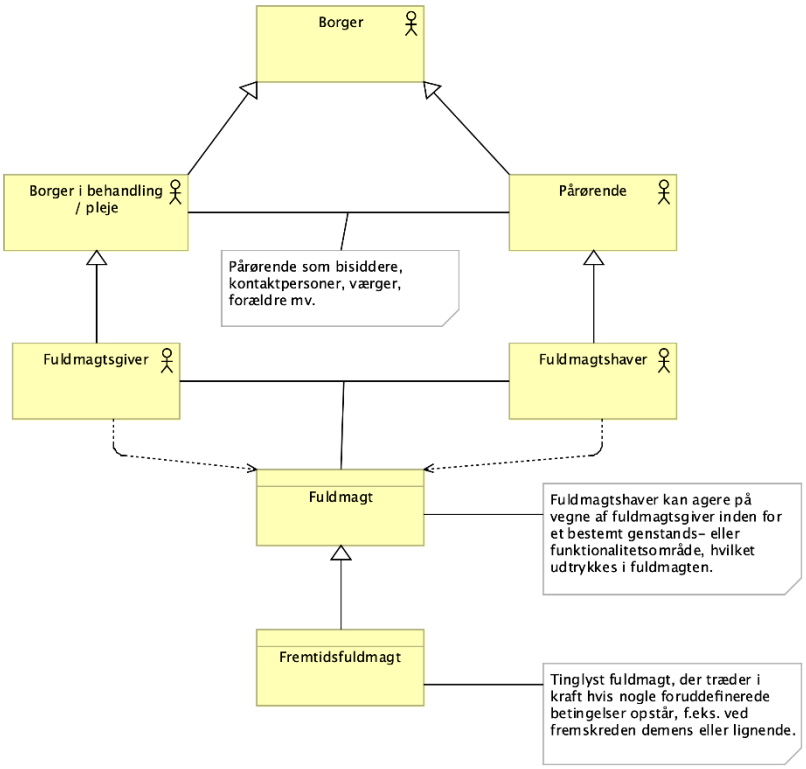
Figur 6: Rammerne for sammenhængende brugerstyring

6. Forretningsmæssigt

6.1 Modellering af forretningsobjekter

I dette afsnit gennemgås de overordnede forretningsobjekter, der er involveret i målbilledet for tillidstjenester samt de grundlæggende relationer, der eksisterer mellem forretningsobjekterne.

6.1.1 Borgere og pårørende

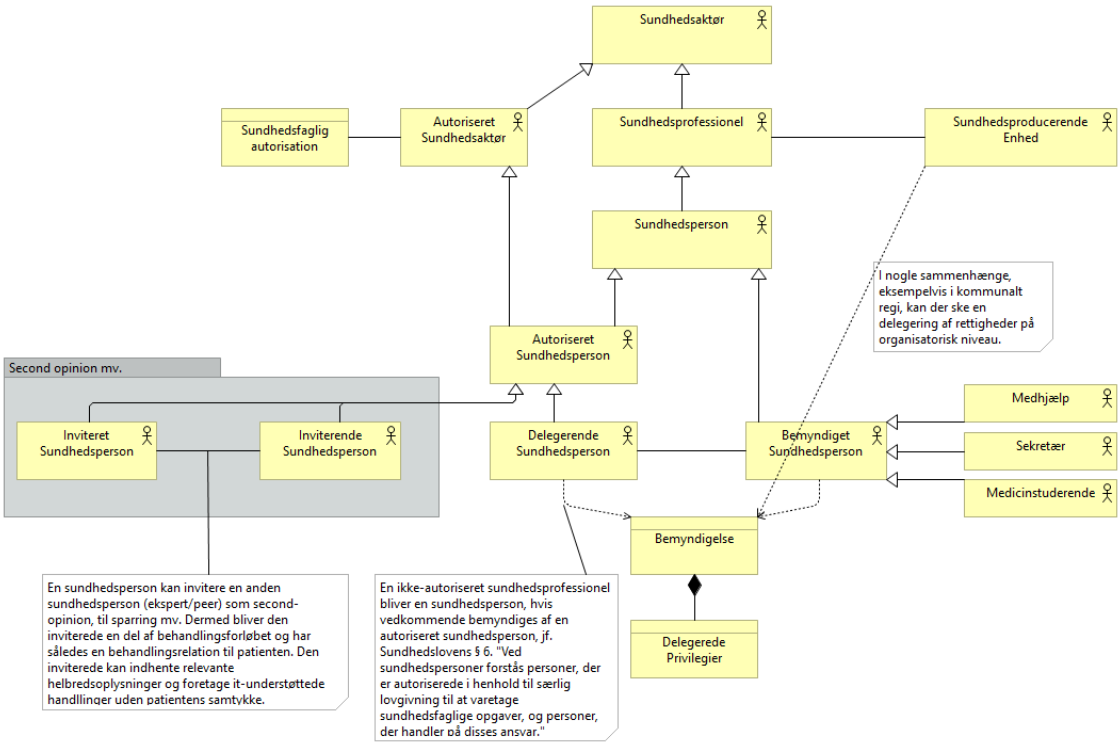


Figur 7: Borgere og relationer mellem borgere.

Ovenfor illustreres forretningsobjektet *Borger*. De borgere, som har kontakt med sundhedsvæsenet er illustreret som *Borger i behandling / pleje*. Disse har ofte *Pårørende* eller nærtstående, som er involvereret i forløbet som kontaktpersoner, bisiddere eller værger/forældre, og som i nogle tilfælde skal kunne agere på vegne af borgeren i behandling / pleje. Forældre og værger har implicit visse muligheder for at kunne agere på vegne borgeren i behandling / pleje, mens andre skal have en eksplicit *Fuldmagt* af borgeren for at kunne agere på dennes vegne. En særlig form for fuldmagt er *Fremtidsfuldmagter*[2]. Disse er planlagte og tinglyste fuldmagter, der træder i kraft, hvis eller når særlige betingelser opstår, for eksempel ved fremskreden demens eller lignende.

[2] http://www.tinglysningsretten.dk/hvad/Pages/Fremtidsfuldmagter.aspx

6.1.2 Sundhedspersoner og bemyndigede



Figur 8: Aktører og forretningsobjekter relateret til sundhedspersoner.

En **Sundhedsaktør** er en aktør (typisk person), der er involveret i en sundhedsrelateret aktivitet. Begrebet er et samlende begreb for alle, der er involveret i en sundhedsaktivitet dvs. patienter, læger, sygeplejersker, plejepersonale osv.

Nogle af disse, for eksempel læger, er **autoriserede sundhedsaktører**, der har modtaget en dansk sundhedsfaglig autorisation af Styrelsen for Patientsikkerhed. Autorisationen viser, at vedkommende har gennemgået en relevant uddannelse og derigennem har opnået kompetence til at bestride særlige roller i sundhedsvæsenet. Styrelsen kan også fratage autorisationen eller dele af den igen.

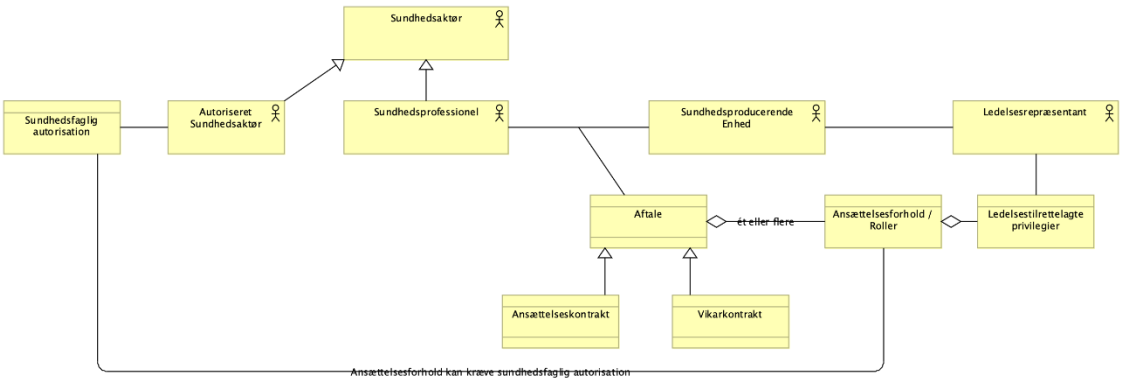
En sundhedsaktør der er tilknyttet en **sundhedsproducerende enhed** og beskæftiger sig med sundhedsrelaterede aktiviteter kaldes en **Sundhedsprofessionel**. Hvis den ansatte samtidig har en sundhedsfaglig autorisation der benyttes i ansættelsesforholdet, betegnes denne som en **Autoriseret Sundhedsperson**. Sundhedspersoner er defineret i Sundhedslovens §6 som personer med særlig sundhedsfaglig autorisation og personer, der handler på disses ansvar, hvilket bringer os til bemyndigelsesbegrebet. Sundhedspersoner autoriseres efter autorisationsloven. Nogle typer af autorisation giver adgang til **privilegier** i form af **forbeholdt sundhedsfaglig virksomhed**. En autoriseret sundhedsperson kan, inden for lovgivningen samt de rammer, der er

udstukket af ledelsen på den pågældende arbejdsplads, delegere privilegier til en bemyndiget, der derved i lovens forstand bliver en sundhedsperson. Den bemyndigede kan under instruks og supervision handle på den delegerendes ansvar. Bemyndigelsen definerer hvilke privilegier, den bemyndigede opnår, under hvilke forhold og i hvilken periode de kan anvendes osv. Eksempler på bemyndigede er sekretærer, medicinstuderende og anden medhjælp. Bemyndigelse kan nogle situationer også finde sted på organisatorisk niveau. I disse situationer påhviler det ledelsen at sikre, at personalet har de tilstrækkelige kvalifikationer og instrukser. I kommunalt regi har kommunalbestyrelsen det endelige ansvar herfor. Endelig kan den bemyndigede også i nogle situationer videredelegere tildelte privilegier.

En sundhedsaktør med sundhedsfaglig autorisation som agerer uden for et ansættelsesforhold, er ligeledes at betragte som en sundhedsperson, og oppebærer visse privilegier i kraft af sin autorisation. For eksempel må læger ordinere medicin til familie og bekendte i privat sammenhæng.

Endelig inkluderer modellen også behovet for at sundhedspersoner kan invitere andre sundhedspersoner med ind i et behandlings- eller plejeforløb ved ønsket om second opinion eller ved ønske om sparring fra en kollega eller ekspert. Den inviterende sundhedsperson vurderer behovet for dette, og efter eksperten er inviteret er denne nu en del af det aktuelle behandlingsforløb. Dermed har eksperten retmæssig adkomst til helbredsoplysninger på lige fod med de øvrige involverede sundhedspersoner uden at skulle anmode om samtykke fra borgeren i behandling/pleje.

6.1.3 Sundhedsfaglig ansættelse og ledelse



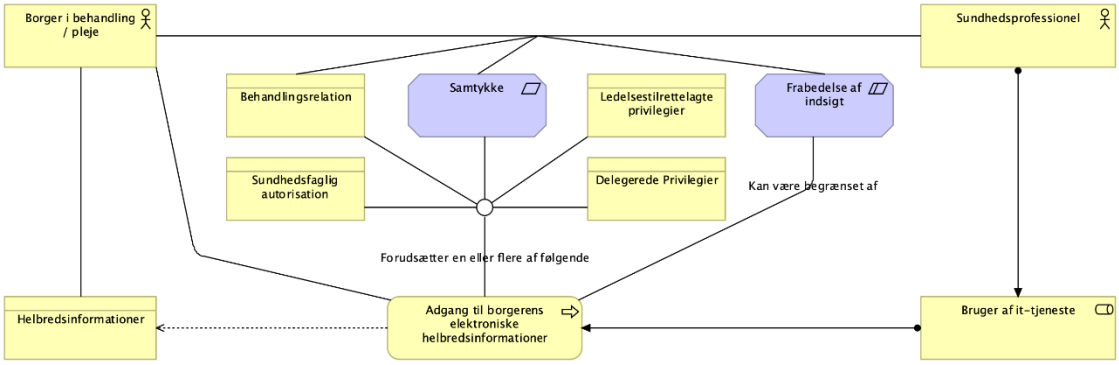
Figur 9: Ansættelsesforhold og ledelsestilrettelagte privilegier.

Som tidligere nævnt er en sundhedsprofessionel tilknyttet en sundhedsproducerende enhed. Tilknytningen kan være en fast ansættelse eller kan være en løst tilknytning for eksempel som vikar eller konsulent. Under alle omstændigheder reguleres ansættelsesforholdet af en aftale, der specificerer hvilken rolle eller hvilke roller den sundhedsprofessionelle skal spille i ansættelsen. I it-mæssig sammenhæng definerer rollen eller ansættelsesforholdet typisk også hvilke privilegier/rettigheder man skal have som medarbejder i virksomheden. Hos især større virksomheder og myndigheder kan dette være nogle relativt komplicerede rettighedstildelinger, hvor

der for eksempel kan være forskel på, hvad man må afhængig af, hvor man geografisk befinder sig, om der gås tilsyn eller lignende.

For autoriserede sundhedspersoner kan de ledelsestilrettelagte privilegier ikke overstige de privilegier, sundhedspersonen har fået af autorisationen af Styrelsen for Patientsikkerhed eller som kan delegeres jævnfør autorisationsloven. Ledelsen har omvendt ret til at fratage privilegier som led i den arbejdsmæssige tilrettelæggelse. Der kan således være privilegier, som den autoriserede sundhedsperson er berettiget til i kraft af sin autorisation, men som vedkommende ikke må/kan anvende i arbejdsmæssig sammenhæng, fordi ledelsen ikke ønsker det på den pågældende arbejdsplads eller i det pågældende ansættelsesforhold.

6.1.4 Adgang til borgerens helbredsoplysninger



Figur 10: Sundhedsprofessionelles adgang til elektroniske helbredsoplysninger.

Gennem de ledelsestilrettelagte privilegier kan en sundhedsprofessionel have adgang til digitale tjenester, der indeholder elektroniske helbredsoplysninger om borgere i behandling/pleje. Er den sundhedsprofessionelle en autoriseret eller bemyndiget sundhedsperson, reguleres adgangen af sundhedsloven (primært §42a), hvor sundhedspersonen under visse betingelser har adkomst til helbredsoplysningerne uden et eksplicit samtykke fra borgeren, såfremt sundhedspersonen har patienten i aktuel behandling og der er tale om relevante informationer. Optræder den sundhedsprofessionelle ikke som sundhedsperson eller er betingelserne for adgang uden samtykke ikke opfyldt for sundhedspersonen, vil adkomst kræve eksplicit samtykke fra borgeren.

6.2 Brugsscenarier / user stories

6.2.1 User stories for autoriserede sundhedspersoner, deres medhjælp, og løst ansatte

6.2.1.1 Enkel adgang på tværs

"Som sundhedsperson ønsker jeg – som udgangspunkt gennem et specialiseret fagsystem *– at kunne anvende alle nødvendige digitale tjenester, som jeg er* berettiget til *at få adgang til, så jeg får den bedst mulige procesunderstøttelse og det bedst mulige datagrundlag for mine beslutninger, handlinger og dokumentation."*

Denne user story dækker alle sundhedspersoners adgang til digitale tjenester, for eksempel adgang til Fælles Medicinkort gennem EPJ (sygehuse), LPS (praksislæger), EOJ (kommuner) osv. *Nødvendige digitale tjenester* kan være virksomhedsinterne tjenester såvel som tjenester hos eksterne virksomheder eller myndigheder og *berettiget til* refererer til sundhedslovens som øvrig lovgivnings regulering af adgang til at indhente, videresende og ændre elektroniske helbredsoplysninger og foretage elektroniske handlinger/funktioner samt til ledelsens ret og pligt til at tilrettelægge arbejdsfunktioner hos virksomheden/myndigheden og dermed at tildele eller fratage visse privilegier i forhold til de elektroniske systemer.

Det er vigtigt at understrege, at de underliggende processer og anvendelse af infrastruktur kan være meget forskellige afhængig af, hvilken part brugeren repræsenterer. Processerne kan også være forskellige som følge af systemtype (fagsystem, web applikation, mobil app osv.) og enhedstype (PC, kiosk PC, tavle-løsninger, mobile enheder, adgang via specialiseret udstyr såsom scannere osv). Så denne user story dækker med andre ord over mange forskellige flows.

6.2.1.2 Samme privilegier til samme tjeneste uanset adgangsvej

"Som sundhedsperson ønsker jeg samme muligheder og/eller begrænsninger i forhold til en given digital tjeneste uanset om jeg vælger den ene eller den anden ***adgangsvej*** *til tjenesten. Det understøtter min fokus på mit sundhedsarbejde og underbygger min tillid til sikkerhedshåndteringen."*

Med adgangsvej menes for eksempel gennem eget fagsystem med integration til ekstern tjeneste eller adgang gennem en browser-baseret snitflade til samme tjeneste via Internettet.

6.2.1.3 Afkræv kun de nødvendige handlinger og valg af sundhedspersoner

*"Som sundhedsperson ønsker jeg kun at **autentificere** mig, bevise min tilstedeværelse eller i øvrigt foretage sikkerhedsmæssige handlinger og valg, når det er nødvendigt ud fra et sikkerhedsmæssigt perspektiv, reguleret af lovgivning, retspraksis eller konkrete aftaler mellem parterne på sundhedsområdet. Dermed kan jeg bruge min tid optimalt i forhold til min arbejdsfunktion"*

Med **autentifikation** menes her at bevise, at jeg er i kontrol over den påståede digitale identitet ved at bevise besiddelse af fysiske autentifikationsfaktorer og viden i typiske login-handlinger. Der bør i størst mulig udstrækning være **single-sign-on** til de digitale tjenester (lokale som eksterne), som sundhedspersonen anvender. Med sikkerhedsmæssige handlinger og valg menes for eksempel valg mellem arbejdsfunktioner, valg mellem sundhedsfaglig autorisation (hvis personen besidder flere) etc. Hvis sundhedspersonen aktuelle arbejdsfunktion allerede kendes i det lokale fagsystem, skal eksterne tjenester ikke også bede sundhedspersonen om at vælge dette ud fra en liste. Det samme gælder sundhedsfaglig autorisation og øvrige sikkerhedsmæssigt kontekstsættende valg.

6.2.1.4 Fastholdelse af Patientkontekst mellem applikationer

"Som sundhedsperson ønsker jeg, at den kontekst, jeg befinder mig i én applikation, automatisk kendes i de andre applikationer, jeg skulle åbne eller blive stillet videre til. Dermed øges patientsikkerheden, risikoen for fejl og ressourcespild ved dobbeltindtastning minimeres.

Hvis der er en naturlig ejer-applikation af patientkonteksten, skal det kun være muligt at ændre patientkonteksten der. Hvis der er ligeværdighed mellem applikationer, skal enhver patientkontekstændring medføre koordineret kontekstskifte mellem alle applikationer, både lokale applikationer og eksterne applikationer. Denne user story er medtaget for at sikre, at patientkontekst og det at signalere hvorvidt den må ændres eller ej, kommer med i målbilledet/målarkitekturen.

6.2.1.5 Delegering af privilegier under ansvar

"Som sundhedsperson ønsker jeg, inden for lovgivningens rammer og inden for de rammer, der er udstukket af virksomhedens/myndighedens ledelse, at kunne bemyndige en medhjælp / studerende / yngre kollega med dele af mine privilegier. Dermed skal de, i mit navn, under min supervision og under mit ansvar, kunne foretage handlinger, rekvirere og videresende helbredsoplysninger, i det omfang jeg selv er berettiget til det, og i det omfang der ikke er andre foranstaltninger, der skal forhindre den delegerede i at kunne dette. Dermed opnår jeg optimeret ressourceudnyttelse og at opnå et tilstrækkelig operationelt arbejds- og læringsmiljø"

Med "… og i det omfang der ikke er andre foranstaltninger, der skal forhindre den delegerede i at kunne dette." menes for eksempel at borgeren kan have frabedt sig indsigt fra den delegerede. I så fald må den delegerede ikke få adgang til data, selv om vedkommende arbejder i en andens navn. Denne use case dækker også over videredelegering, i hvilket tilfælde det fortsat er den oprindelige delegator, som er ansvarlig.

6.2.1.6 Den delegeredes valg af delegerede privilegier

"Som delegeret sundhedsperson ønsker jeg i en given situation at kunne vælge, hvilke delegerede privilegier, jeg ønsker at optræde med, så jeg kun optræder som særligt privilegeret, når jeg rent faktisk gør brug af det og så min privilegiestatus ikke spredes unødigt."

6.2.1.7 Løst ansattes adgang til tjenester

"Som løst ansat *i en virksomhed skal jeg kunne få en elektronisk identitet og kunne få adgang til nationale sundhedstjenester gennem de privilegier, jeg har fået af ledelsen i den hyrende virksomhed/myndighed."*

Med løst ansatte menes for eksempel vikarer, konsulenter, studerende mv. der typisk ikke er oprettet i lønsystemer (som fastansatte). Det centrale er dog, at de stadig skal kunne opnå en elektronisk identitet i virksomheden/myndigheden og dermed få privilegier til at agere på en hyrende virksomheds/myndigheds vegne i forhold til den arbejdsfunktion den løst ansatte bestrider. Dette gælder også adgang til fødererede digitale tjenester i relevant omfang.

6.2.1.8 Sundhedspersoners adgang med samtykke

"Som borger vil jeg kunne give mit samtykke til, at en sundhedsperson uden for et behandlingsforløb kan foretage handlinger eller se helbredsrelaterede data knyttet til mig. Det er med til at give mig tryghed og handlemuligheder uden for normale behandlingsforløb."

Hvis en borger kender en sundhedsperson privat eller tager kontakt til en sundhedsperson uden for et behandlingsforløb, skal det være muligt for sundhedspersonen at foretage handlinger inden for den sundhedsfaglige autorisation og kompetence sundhedspersonen har. For eksempel at en ven eller et familiemedlem, der er læge, kan udskrive recepter til borgeren.

6.2.1.9 Sundhedspersoners ønske om *second opinion* eller sparring.

"Som autoriseret sundhedsperson ønsker jeg at kunne involvere en anden behandlingsperson (ekspert) i behandlingsforløbet med henblik på kvalitetssikring og for at sikre den bedste behandling og pleje for borgeren. Den involverede sundhedsperson bliver derved direkte involveret i behandlingsforløbet, og har således en behandlingsrelation til patienten."

Denne user story minder lidt om delegering, men i modsætning til delegering, hvor der handles på den delegerendes ansvar, inviterer en sundhedsperson, der er direkte involveret i et behandlingsforløb, en ekspert eller fagfælle, der ikke er direkte involveret i forløbet, til at handle eller se på helbredsoplysninger. Dette skal – under ansvar og kompetence fra den inviterende - kunne lade sig gøre uden at afkræve samtykke fra borgeren/patienten.

6.2.2 User Stories for brugeradministratorer

*Som brugeradministrator i en organisation med eget **brugeradministrationssystem** ønsker jeg at kunne tildele roller/privilegier gennem organisationens eget administrationssystem, så der ikke skal administreres flere steder på tværs af de fødererede parter.*

Brugeradministrationssystem dækker over et system til administration af elektroniske identiteter samt tilknytning af roller og rettigheder (Identity Management System, IdM). Der vil typisk være tale om en større organisation. Med **brugeradministrator** menes administrativt personale i organisationen, der administrerer elektroniske identiteter og deres adgange til interne og eksterne systemer. Med flere steder menes i flere brugeradministrationsgrænseflader ejet af forskellige organisationer.

6.2.3 User Stories for borgere

6.2.3.1 Borgerrettede løsninger skal benytte kendte fællesoffentlige login-mekanismer

Som Borger vil jeg kunne få adgang til borgervendte digitale tjenester med de almindeligt kendte fællesoffentlige login-mekanismer, for eksempel NemID/NemLogin eller dennes afløsere, så jeg ikke skal til at lære at bruge flere forskellige løsninger.

6.2.3.2 Borgeren skal kunne give fuldmagt til en pårørende

Som Borger ønsker jeg at kunne give en pårørende fuldmagt til at kunne agere digitalt på mine vegne. Fuldmagten skal kunne rettes mod en bestemt kontekst, behandlingsforløb eller lignende, og må ikke kræve kendskab til den systemmæssige indretning af sundhedsvæsenet. Det vil give mig tryghed og øge de digitale muligheder for mig, selv om jeg ikke selv er i stand til at agere digitalt.

Med *Fuldmagten skal kunne rettes mod en bestemt kontekst, behandlingsforløb eller lignende* menes at det som fuldmagtsgiver skal være muligt at give en pårørende tilstrækkelige men begrænsede handlemuligheder, når vedkommende skal repræsentere mig. Det skal være muligt at balancere indsigts- og handlemuligheder for eksempel i forhold til forløb, tid eller geografi, så den pårørende på den ene side modtager tilstrækkelige handlemuligheder, men på den anden side ikke får uindskrænket magt og indsigt.

Med *må ikke kræve kendskab til den systemmæssige indretning af sundhedsvæsenet* menes, at der ikke skal gives fuldmagt til en løsning eller et dataobjekt, der tydeligt hører til en bestemt løsning. Fuldmagter skal udtrykkes mere generelt, så der ikke skal indsamles fuldmagt til mange forskellige løsninger før en pårørende kan repræsentere en borger.

6.2.3.3 En pårørende skal kunne repræsentere en borger

Som Pårørende skal jeg med fuldmagt kunne anvende digitale tjenester på vegne af en nærtstående. Fuldmagtens udstrækning skal være nem at forstå og må ikke kræve kendskab til systemlandskab og særlige løsninger/applikationer i sundhedsvæsenet.

Som under 6.2.3.2.

6.2.3.4 Forældre og børn

Som Forælder med forældremyndighed skal jeg have adgang til mit barns helbredsoplysninger i det omfang loven giver mig ret til dette, så jeg bedst muligt kan repræsenter mit barn i et behandlingsforløb.

6.2.4 User Stories vedrørende administration og kontrol i føderationer

6.2.4.1 Dataansvarliges muligheder for kontrol og stikprøvekontrol

Som repræsentant for en dataansvarlig organisation/myndighed, skal det på en enkel og sikker vis være muligt at følge op på føderativ adgang til de digitale tjenester, organisationen/myndigheden er ansvarlig for, så der dels ikke spildes unødigt mange kræfter på kontrollen og dels ikke kan skabes tvivl om omfanget eller kvaliteten af vores kontrol.

Opfølgning kan for eksempel være stikprøvebaseret kontrol af sundhedsfaglig autorisation, aktuel behandlingsrelation, kontrol af spærringer/samtykker eller lignende. Det skal være nemt for de dataansvarlige at kontrollere disse oplysninger. Hvis det bliver for svært vil det enten ikke blive gjort i tilstrækkeligt omfang eller pålægge den pågældende organisation en unødig stor byrde.

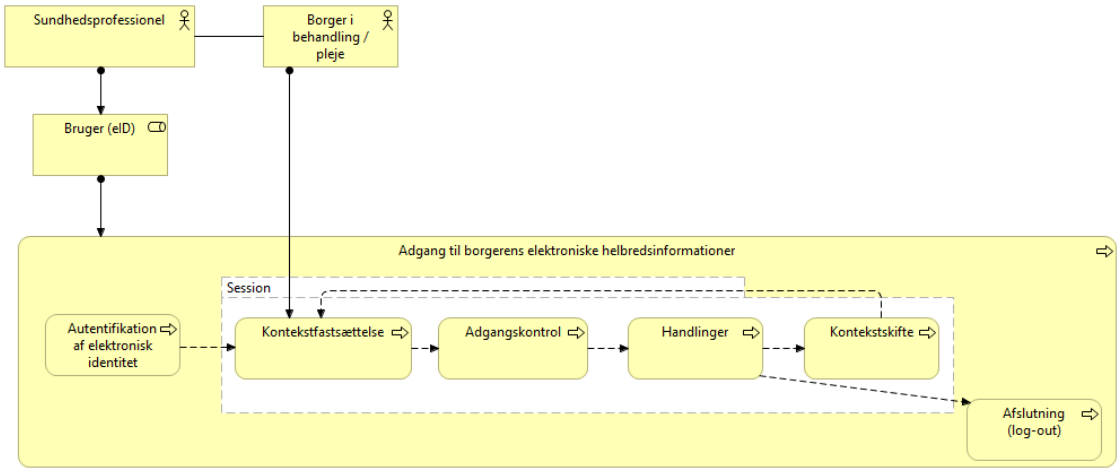
6.2.4.2 Dataansvarliges muligheder for kontrol og stikprøvekontrol

Som repræsentant for en dataansvarlig organisation/myndighed, skal det på en enkel vis være muligt at inspicere resultatet af andre føderationsdeltageres seneste revision / audit, så jeg kan sikre mig, at alle i føderationen følger de spilleregler vi er blevet enige om.

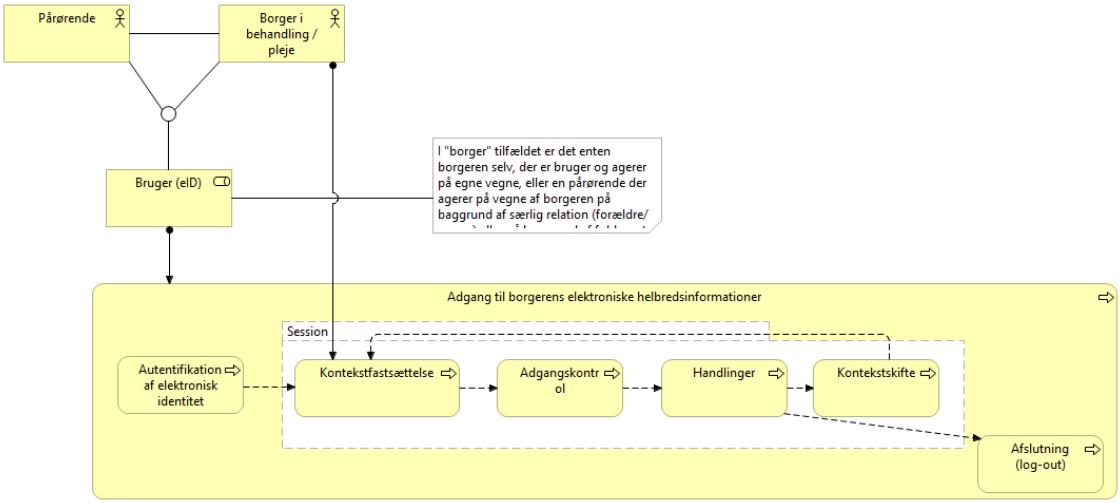
6.3 Forretningsprocesser

I nedenstående afsnit gennemgås de overordnede forretningsprocesser for adgangsstyring til nationale digitale sundhedstjenester for henholdsvis sundhedsprofessionelle og borgere. De administrative processer, der går forud for adgangsprocesserne, berøres ikke, dvs. der forudsættes, at brugeren har de fornødne elektroniske identiteter, privilegier og relationer til borgeren i behandling/pleje osv. for potentielt at kunne få adgang.

Som det ses af de næste to illustrationer, er det de samme processer, der gennemføres hvad enten der er tale om borgeres eller sundhedsprofessionelle adgang til digitale tjenester. Det er dog vigtigt at bemærke, at processernes indhold er forskelligt afhængigt af, om de gennemføres i den ene eller anden kontekst.



Figur 11: Overordnede forretningsprocesser ved adgangsstyring af sundhedsprofessionelle.



Figur 12: Borgere og pårørendes adgang til nationale digitale sundhedstjenester.

6.3.1 Autentifikation

Autentifikation har til formål at genkende og verificere borgeren, den pårørende eller den sundhedsprofessionelle på baggrund af tilhørende elektroniske identifikationsmidler med den troværdighed, som kan forventes på det pågældende NSIS sikringsniveau. I praksis er det typisk en log-in handling til it-platform, fagsystem, webapplikation eller app. Sidstnævnte kan være implicit via ejerskab til device, hvor brugeren typisk[3] har autentificeret sig ved installation eller opstart af app'en, men kan også være indbygget i appen i et samspil med de sikkerhedsmekanismer, der er på devicet (fingeraftryk, ansigtsgenkendelse osv.).

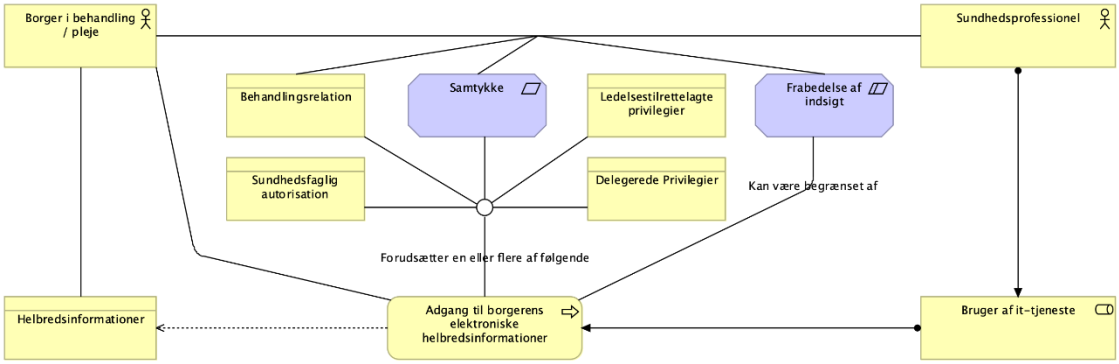
[3] Disse sessioner kan i nogle tilfælde være meget langvarige. Et eksempel er anvendelse af NemID ved konfigurering/opstart af Medicinkort-appen.

6.3.2 Kontekstfastsættelse og sessioner

Ved autentifikation bliver der dannet en session, inden for hvilken brugeren kan foretage sig handlinger uden igen at skulle autentificere sig. Der kan i nogle tilfælde være behov for, at brugeren foretager sig nogle valg for at fastsætte, hvilken kontekst man agerer i. Som borger kan man enten agere på egne vegne eller på vegne af den, man er pårørende til. Borgeren kan endvidere være pårørende til en række personer og/eller kan have fået fuldmagt fra flere. Derfor skal der træffes et valg, før systemerne kan vide, hvilke informationer der skal vises og dermed hvilke adgangsbestemmelser, der skal kontrolleres.
Som sundhedsprofessionel kan det være et valg af arbejdsfunktion, hvis man kan optræde i forskellige roller/jobfunktioner hos den pågældende arbejdsgiver, valg af sundhedsfaglig autorisation, som man agter at benytte sig af i adgangen, hvis den ikke entydigt er knyttet til arbejdsfunktionen, valg af afdeling etc. Valg af patient kan også være en del af konteksten, hvilket dog typisk ændrer sig noget oftere end de øvrige kontekstelementer. Konteksten kan skiftes inden for samme session.

6.3.3 Adgangskontrol

Når brugeren ønsker adgang til bestemte digitale tjenester, skal den dataansvarlige på fornøden betryggende vis sikre sig, at der er retmæssig adgang til disse handlinger/informationer. Adgangskontrollen vil være forskellig afhængig af, om brugeren er borgeren selv, en pårørende eller en sundhedsperson i privat eller professionel regi. Borgeren har som udgangspunkt altid adgang til egne data og digitale handlemuligheder[4]. Pårørende kan have implicit adgang som følge af forældre- eller værgerelationer til borgeren (forældre typisk kun op til barnet er fyldt 15) eller som følge af fuldmagt. Sundhedspersoners adgang reguleres af sundhedslovens bestemmelser. Her vil en sundhedsperson som udgangspunkt kunne indhente helbredsinformationer uden samtykke fra patienten, såfremt patienten er i aktuel behandling, de rekvirerede data er relevante i konteksten og at borgeren ikke eksplicit har frabedt sig adgang til informationerne eller har frabedt sig adgang fra den pågældende sundhedsperson.



Figur 13: Adgangskontrol for sundhedspersoner / sundhedsprofessionelle kan være ganske kompleks.

[4] Kan dog eventuelt være begrænset af alder og eventuel umyndiggørelse i forhold til visse handlinger / områder.

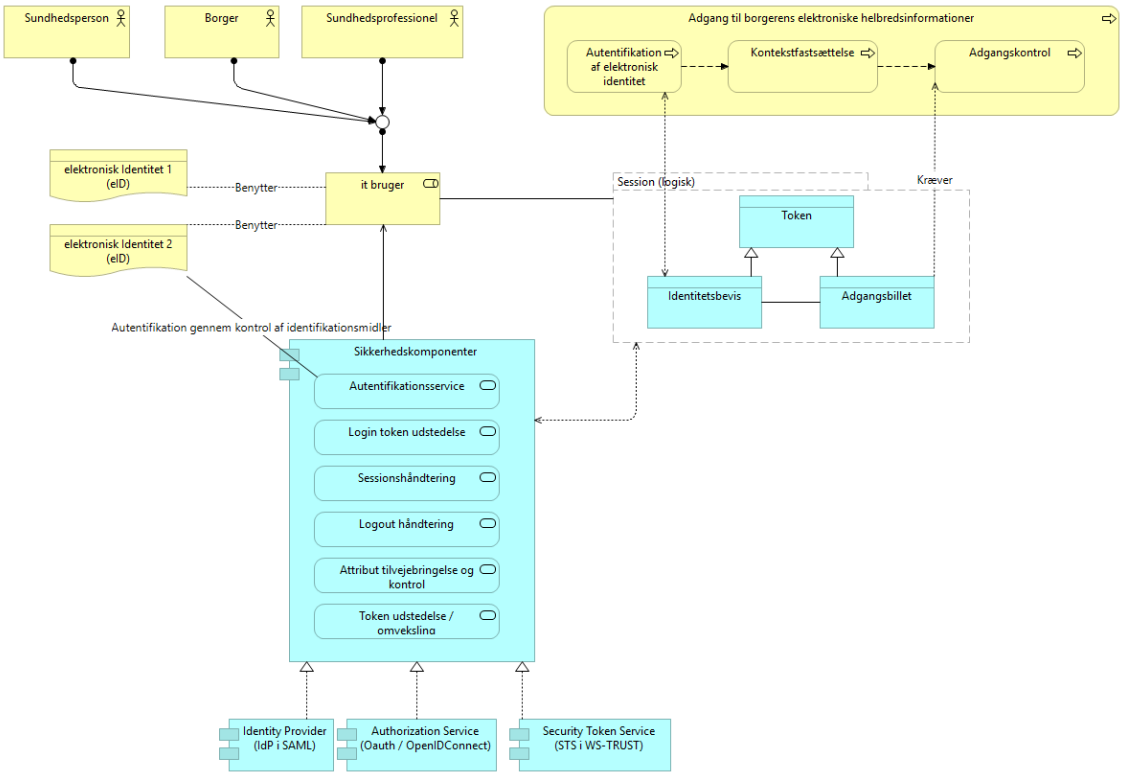
6.3.4 Kontekstskifte

Sundhedspersoner skifter ofte kontekst i løbet af en arbejdsdag ved at tilse forskellige patienter og i nogle tilfælde ved at bestride forskellige arbejdsfunktioner. Dele af konteksten ændrer sig derfor i løbet af arbejdsdagen. Det skal være muligt at skifte dele af konteksten inden for den samme login-session, det vil sige uden at brugeren igen skal autentificere sig eller i øvrigt fastlægge kontekst, som ikke har ændret sig.

6.3.5 Sikker afslutning af session (log-out)

Brugeren skal også have mulighed for at afslutte sin session på sikker vis. Dette foregår typisk gennem ***logout***, hvor sessionen afsluttes, så en anden bruger, der tilgår it-platformen eller systemet ikke kan overtage sessionen. I mange tilfælde afsluttes sessioner også automatisk, hvis den ikke har været aktiv i en periode (timeout).

7. Applikationer og teknik

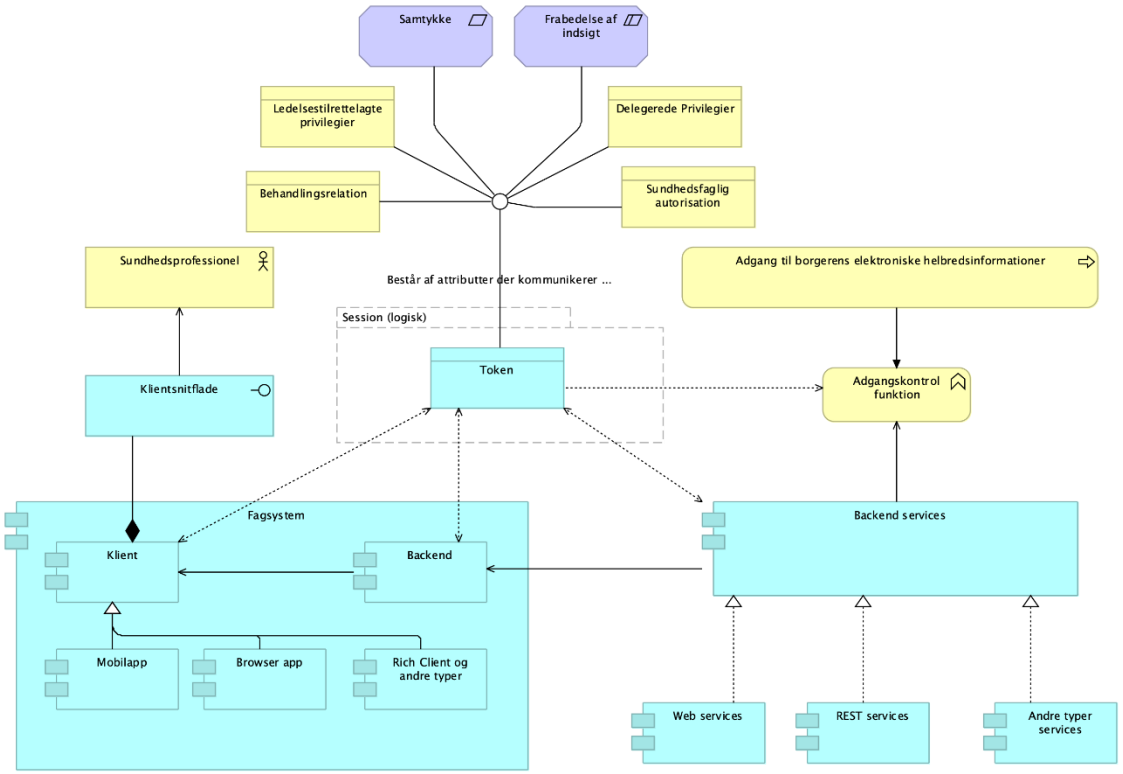


Figur 14: Logiske komponenter involveret i forretningsprocesserne vedrørende adgangsstyring til nationale digitale sundhedstjenester. Adgangsstyring baseres på såkaldte *tokens* (centralt i figuren), der bærer informationer fra brugerens session.

Ovenstående figur viser hvilke logiske applikationskomponenter, der er involveret i adgangsstyring til nationale digitale sundhedstjenester, hvad enten brugeren er borger, ansat sundhedsprofessionel eller en sundhedsperson, der agerer i privat sammenhæng. Centralt i figuren er de såkaldte ***tokens***. *Tokens* er dataobjekter, der har til formål at bevise en brugers identitet, et såkaldt **identitetsbevis**, eller anvendes ved adgang til digitale tjenester, en såkaldt **adgangsbillet.** På det logiske plan tilvejebringes disse *tokens* gennem forskellige sikkerhedsservices i nogle sikkerhedskomponenter. Nederst i figuren illustreres nogle af realiseringerne af disse tjenester i forskellige standarder (*SAML, WS-TRUST, OAuth/OpenID-Connect*).

Gennem livscyklussen kommunikeres der forskellige *tokens*, der afspejler brugerens kontekst/session over for den enkelte digitale tjeneste. *Tokens* tilpasses løbende i en balance mellem *privacy-by-design*-principper om dataminimering og minimering af dataspredning på den ene side og praktiske hensyn i forhold til den dataansvarliges muligheder for opfølgning og kontrol på den anden. De konkrete *tokens* afspejler derfor dels de valg en bruger har truffet (hvilken **elektronisk identitet** skal anvendes, hvilken autorisation, hvilken arbejdsfunktion, hvilken organisatorisk enhed arbejdes der for, eventuelle bemyndigede privilegier etc.) men filtreret mod det behov den enkelte tjeneste har for informationer i forhold til at kunne give adgang og foretage fornuftig logning.

Tokens anvendes lidt forskelligt afhængig af systemtype. Browserbaserede applikationer anvender typisk *SAML 2*-standarden, hvor webapplikationens *backend* er kontekstbærende, mens *rich client*-systemer anvender *tokens* på en lidt anden måde. Dette behandles nærmere nedenfor.



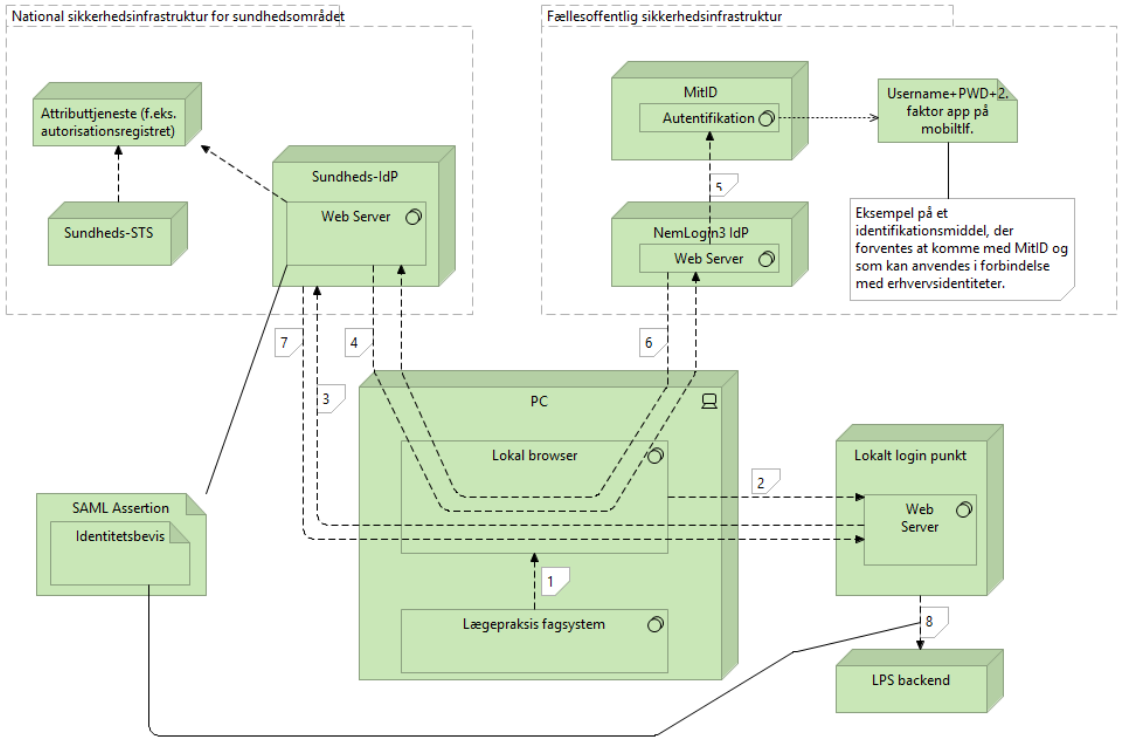
Figur 15: Illustration af *token*-anvendelse i forbindelse med fagsystemers kald af nationale digitale sundhedstjenester (adgangskontrol funktion).

Ovenstående figur viser en logisk arkitektur for adgangskontrol systemer som understøtter sundhedspersoner i deres håndtering af borgeres helbredoplysninger. Arkitekturen er generel og dækker over *rich client*-fagapplikationer, webapplikationer og *apps* afviklet på mobile platforme. I de fleste tilfælde har disse systemer en *backend*, der rekvirerer eller producerer data, foretager beregninger etc., men der kan være stor forskel på, hvor tung klienten er i forhold til forretningslogik.

7.1 Flows/sekvensdiagrammer for autentifikationsprocesser

I dette afsnit gennemgås flows, der er involveret i autentifikationshandlinger.

7.1.1 En sundhedsprofessionel i organisation uden egen IdP autentificerer sig i forhold til den nationale infrastruktur for sundhedsområdet (Rich-Client + SAML)



Figur 16: Flow for autentifikation i den nationale/fællesoffentlige infrastruktur fra et *rich client* fagsystem i en organisation, der ikke har egen IdP.

I dette afsnit gennemgås flowet for adgang fra et *rich client*-fagsystem, i illustrationen eksemplificeret gennem et lægepraksissystem, til en national digital sundhedstjeneste (her FMK). I dette flow har lægepraksissen valgt at anvende elektroniske identifikationsmidler fra MitID. I eksemplet bringes disse først i anvendelse på det tidspunkt brugeren første gang ønsker adgang til FMK, men i praksis er der flere løsningsmuligheder, for eksempel at autentifikationen foregår i forbindelse med login til applikationen eller i en anden applikation for eksempel ved opstart af arbejdsdagen (og når sessionen udløber). Der er flere realiseringer af dette flow. I dette afsnit gennemgås et forslag til løsning baseret på *SAML 2*, *WS-TRUST* og *IDWS*-profilerne.

1. Brugeren er logget på it-platformen og fagsystemet (fagsystemapplikationen) og aktiverer en funktion i fagsystem-klienten, der kræver anvendelse af digital tjeneste hos FMK (for eksempel opdater medicinkort). Det antages, at brugeren ikke allerede har en session med gyldige *tokens* til at kunne få adgang til FMK. Fagsystem-klienten åbner en

browser-applikation (enten systembrowser eller en browser-komponent, der kan indlejres).
2. Browseren sættes til at kontakte en lokal webserver som øjeblikkeligt omdirigerer browseren ...
3. ... til den **nationale IdP for sundhedsområdet** med en anmodning om at autentificere brugeren.
4. Den nationale sundhedsIdP konstaterer, at brugeren ikke har en gyldig login-session og at brugeren kommer fra en organisation, der anvender MitID identifikationsmidler. Browseren omdirigeres derfor til den fællesoffentlige IdP (Nemlogin IdP'en).

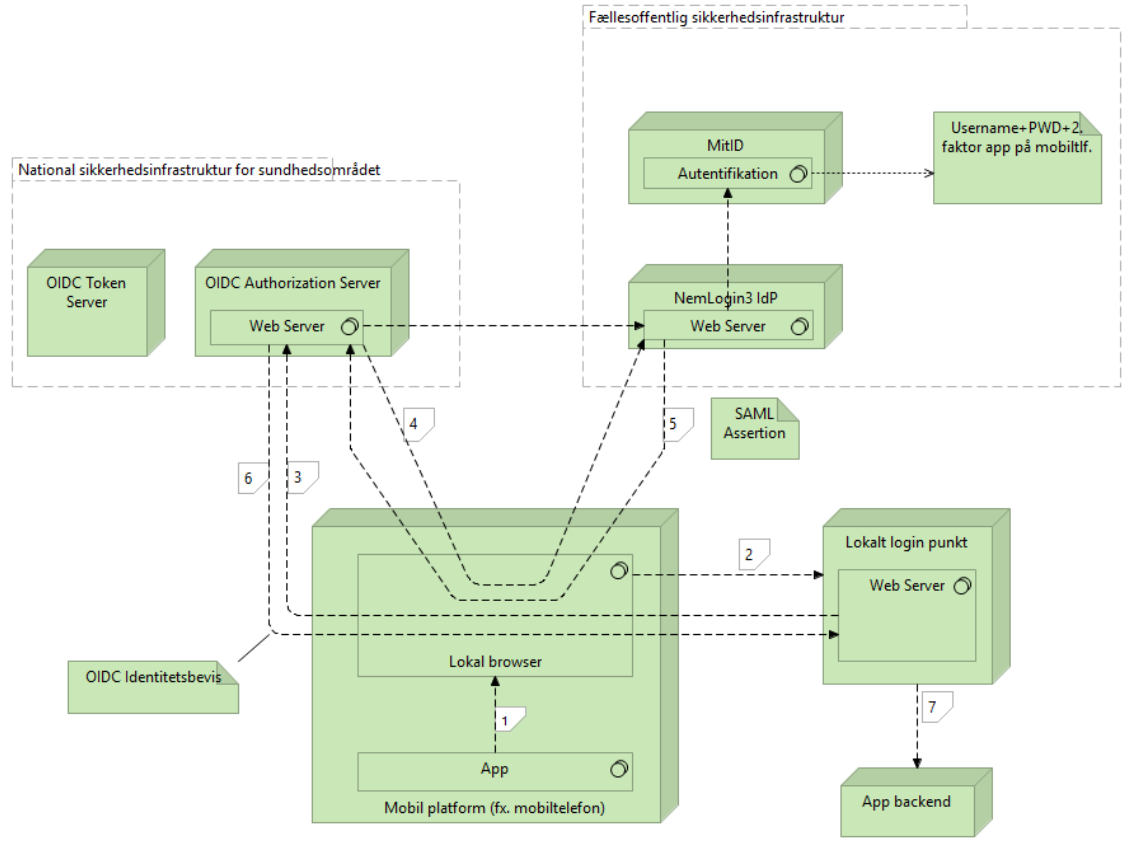
5. NemLogin IdP'en modtager anmodningen og konstaterer at der heller ikke her findes en gyldig session med brugeren/browseren. Brugeren skal derfor gennemføre autentifikationsprocessen hos NemLogin. NemLogin konstaterer at brugeren skal autentificeres med MitID identifikationsmidler og anvender MitID autentifikation-software til autentifikationen. MitID autentificerer brugeren (her eksemplificeret gennem anvendelse af brugernavn-password og aktivering af mobil-app som 2. faktor). Efter succesfuld autentifikation udsteder NemLogin IdP'en nu et OIOSAML *token* med indlejret identitetsbevis.
6. Browseren omdirigeres tilbage til den nationale web server tilknyttet sundhedsIdP'en.
7. Den nationale IdP for sundhedsområdet udsteder SAML *token* og indlejret identitetsbevis. IdP'en kan eventuelt berige med attributter eller verifikation af attributter fra autoritative kilder. Browseren omdirigere tilbage til den lokale webserver.
8. Den lokale web server uddrager[5] identitetsbeviset og sender det / deler det med fagsystemet.

Brugeren er nu logget ind i forhold til den nationale infrastruktur for sundhedsområdet og har de fornødne elementer til i sidste ende at kunne kalde en national digital sundhedstjeneste (for eksempel FMK).

7.1.2 En sundhedsprofessionel autentificerer fra mobil platform (App + OpenIDConnect)

I dette afsnit illustreres den samme løsning som ovenfor, men hvor den grundlæggende standard er *OpenID Connect* i stedet for *SAML 2*.

[5] SAML assertion (og det indlejrede Identitetsbevis) vil være krypteret under det kaldende systems public key. For at få adgang til Identitetsbevis skal der derfor dekrypteres.



Figur 17: Login til den nationale infrastruktur for sundhedsområdet baseret på OpenID Connect.

1. Som i *SAML*-eksemplet er der behov for at aktivere en browser/browserkomponent. Brugeren skal i sidste ende (om et øjeblik) anvende denne til autentifikation vha. sine MitID identifikationsmidler.
2. Browseren dirigeres til en lokal web server.
3. Web serveren omdirigerer browseren til en national *OpenID Connect Authorization server* for sundhedsområdet ved hjælp af det såkaldte *code flow* i *OpenID Connect*.
4. Da brugeren endnu ikke er autentificeret, omdirigerer *Authorization Server* brugerens browser til NemLogin, hvor brugeren præsenteres for en autentifikations-brugergrænseflade, der passer til det identifikationsmiddel, som brugeren anvender. Brugeren autentificerer sig og der udstedes et *SAML token*
5. *SAML token* returneres til *Authorization Server*, hvor der på baggrund af dette token udstedes et *OIDC* identitetsbevis.
6. *OIDC Authorization server* returnerer med det udstedte *OIDC* identitetsbevis.
7. De nødvendige elementer overføres til / deles med *app backend*, der nu er logget ind i den nationale infrastruktur for sundhedsområdet og senere kan veksle *OIDC* identitetsbevis til en adgangsbillet.

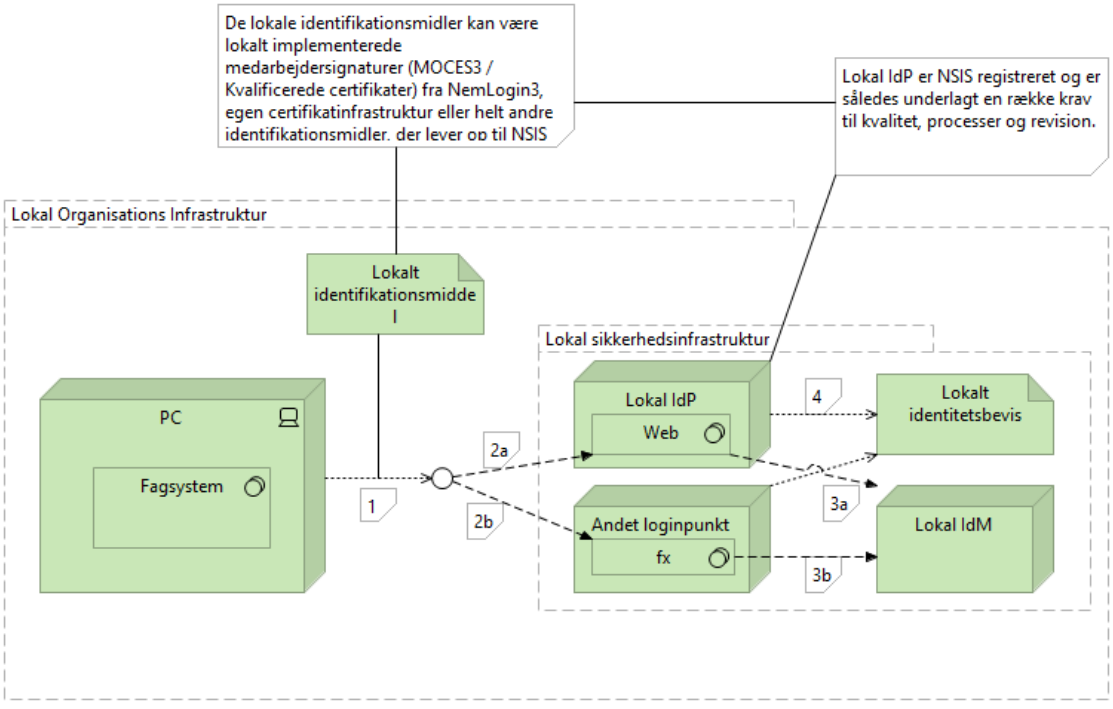
Bemærk, at flowet i det store hele er lig *SAML*-flowet, men der opereres med andre *token*-typer og formater.

7.1.3 En sundhedsprofessionel i en organisation med egen IdP/IdM autentificerer sig i forhold til den nationale infrastruktur for sundhedsområdet (Rich-Client + SAML)

I dette flow har organisationen egen IdP som kan autentificere brugeren enten gennem kontrol af besiddelse af den fællesoffentlige, digitale medarbejdersignatur eller ved kontrol af egne identifikationsmidler.

Bemærk:

- Den lokale autentifikation gennemgås ikke her, da den beror på typen af implementeret identifikationsmiddel og lokal infrastruktur. Det kan for eksempel være baseret på anvendelse af NemLogin3s medarbejdersignaturer (MOCES3 eller kvalificerede certifikater), egen certifikatinfrastruktur eller egne identifikationsmidler, hvor både processer og identifikationsmidler lever op til det fornødne sikringsniveau.
- Tilsvarende kan organisationen være forbundet med en sektorspecifik IdP (for eksempel en fællesregional eller fælleskommunal IdP) som kan være placeret mellem den konkrete organisation og den nationale infrastruktur for sundhedsområdet. Dette er ikke illustreret her. Der henvises til [Interføderation] for nærmere detaljer og overvejelser om dette.



Figur 18: Autentifikationsflow når organisationen har egen IdP / IdM.

1. Brugeren logger på enten på platformen (PC, Citrix) eller et lokalt fagsystemet

2. Organisationen har frihed til lokalt at benytte de standarder eller protokoller som bedst passer til organisationen. Her er to muligheder illustreret, SAML og Kerberos. I begge tilfælde skal brugeren anvende sine lokale identifikationsmidler til login.
3. IdP eller Kerberosserveren anvender IdM til at verificere bruger-identitet (brugeren er en valid og kendt bruger).
4. Efter succesfuld autentifikation udstedes et lokalt identitetsbevis med ganske få attributter, som senere skal veksles til en adgangsbillet for at kunne få adgang til en nationale digital sundhedstjeneste.

Bemærk: autentifikationsflowet er helt uafhængig af eksterne[6] systemer og således robust over for udfald i centrale infrastrukturkomponenter.

7.2 Flows/sekvensdiagrammer for autentifikation og adgangsstyring til browserbaserede systemer

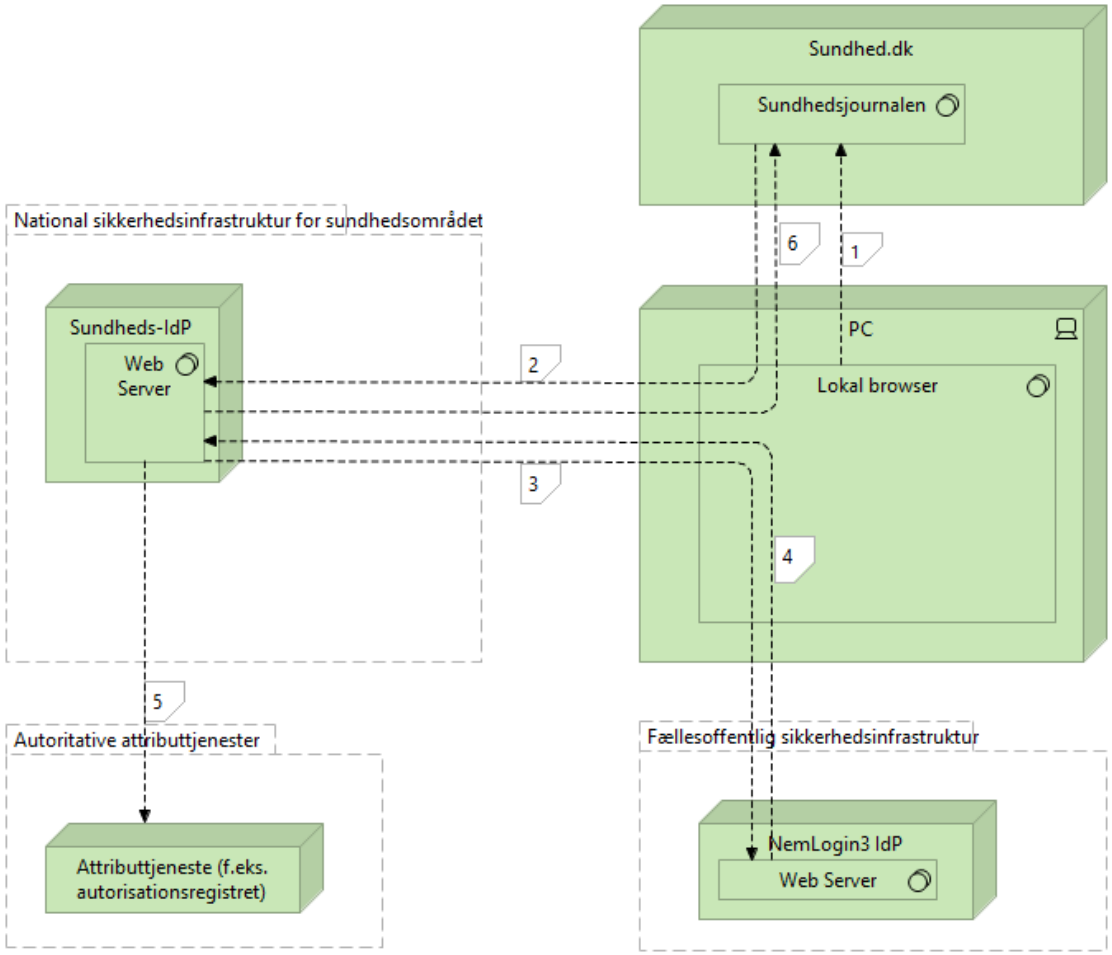
Når der er tale om et browserbaseret system, er de tekniske flows generelt en lille smule anderledes. I skrivende stund er SAML den mest udbredte standard til *Web Single Sign-On* og derfor er det også disse flows der gennemgås nedenfor.

En særlig udgave af adgang til browserbaserede systemer er den såkaldte Sikker Browseropstart, hvor et fagsystem på baggrund af et allerede etableret login (og kontekstfastsættelse) aktiverer en browserbaseret applikation, og hvor både login og kontekst overføres til applikationen uden at brugeren igen bedes om at logge på eller vælge kontekst.

7.2.1 En sundhedsprofessionel i organisation uden egen IdP åbner ny browser og tilgår nationale sundhedstjenester (SAML)

Dette flow svarer helt til det flow som NemLogin både nu og i fremtiden har som hovedflow. På sundhedsområdet vil det dog være nødvendigt at komme forbi den nationale Idp for sundhedsområdet for at få adgang til nationale, browserbaserede sundhedstjenester.

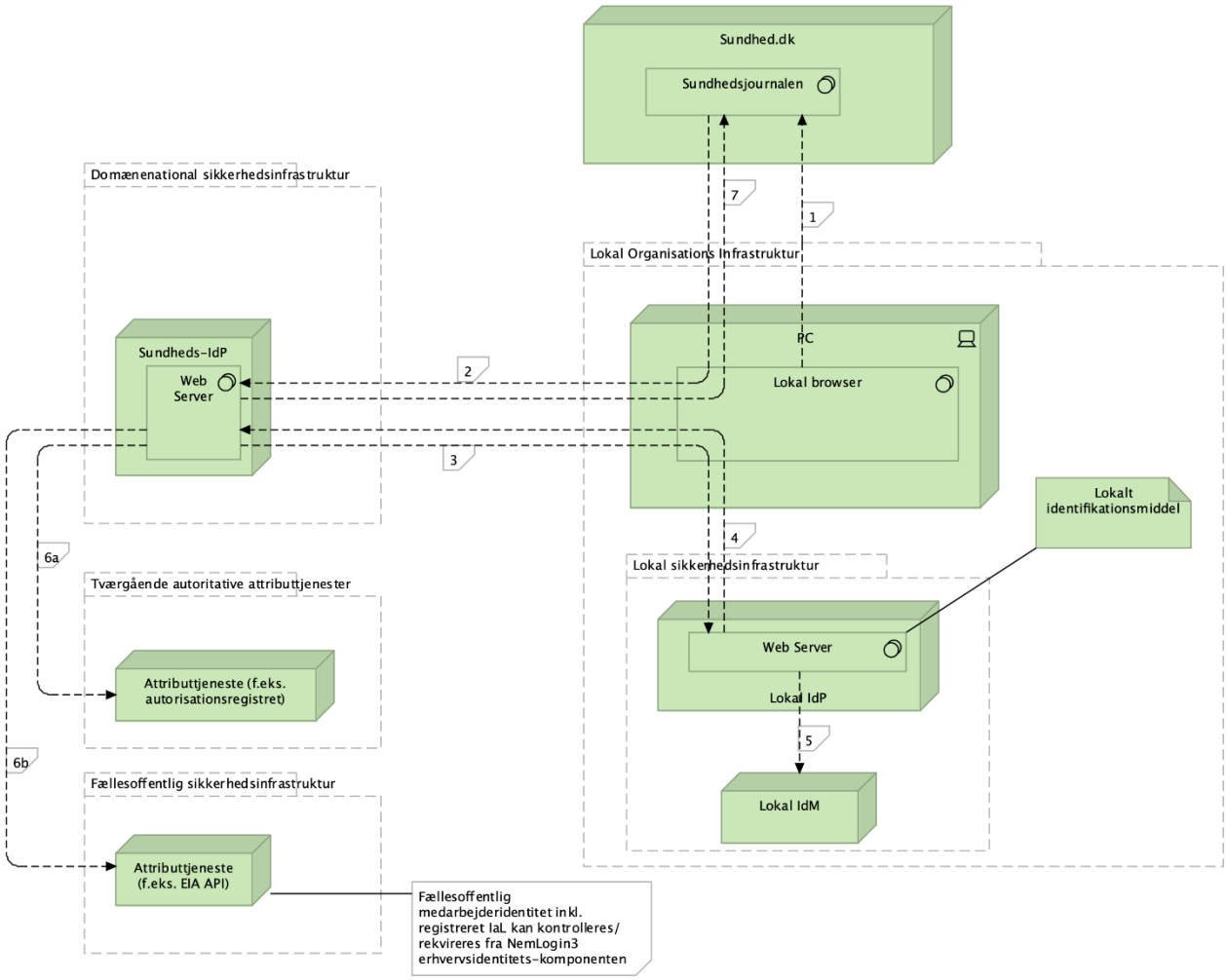
[6] Hvis login-løsningen baseres på fællesoffentlige certifikater, kan det være nødvendigt at kontrollere spærrelister for certifikaterne. Disse ligger online hos NemLogin3, men kan cashes. Såfremt organisationen ikke har online-adgang til de aktuelle lister, vil man i den periode operere med en forhøjet risiko, hvilket organisationen kan have særskilte beredskabsprocesser for.



Figur 19: Brugeren fra en organisation uden egen IdP logges ind i en browserbaseret, national sundhedstjeneste. Brugeren har MitID identifikationsmidler.

1. Brugeren åbner en browser og indtaster URL'en på en browserbaseret, national sundhedstjeneste (for eksempel sundhedsjournalen i Sundhed.dk).
2. Sundhed.dk kan ikke se, at der er en aktiv session med brugerens browser, og omstilles den til den nationale Sundheds-IdP.
3. Her er der heller ingen aktiv session, og browseren omstilles til NemLogin3 IdP'en.
4. Heller ikke her er der en aktiv login-session, så brugeren anmodes om at autentificere sig med sine MitID-identifikationsmidler. Derefter omstilles browseren tilbage til Sundheds-IdP'en
5. Sundheds-IdP'en udsteder de nødvendige login-*tokens* og kan i den sammenhæng eventuelt berige dem med nationale attributter, for eksempel listen over autorisationer, som brugeren kan optræde med.
6. Browseren omstilles til Sundhedsjournalen, der nu kan logge brugeren ind.

7.2.2 En sundhedsprofessionel i organisation med egen IdP åbner ny browser og tilgår en national digital sundhedstjeneste (SAML)



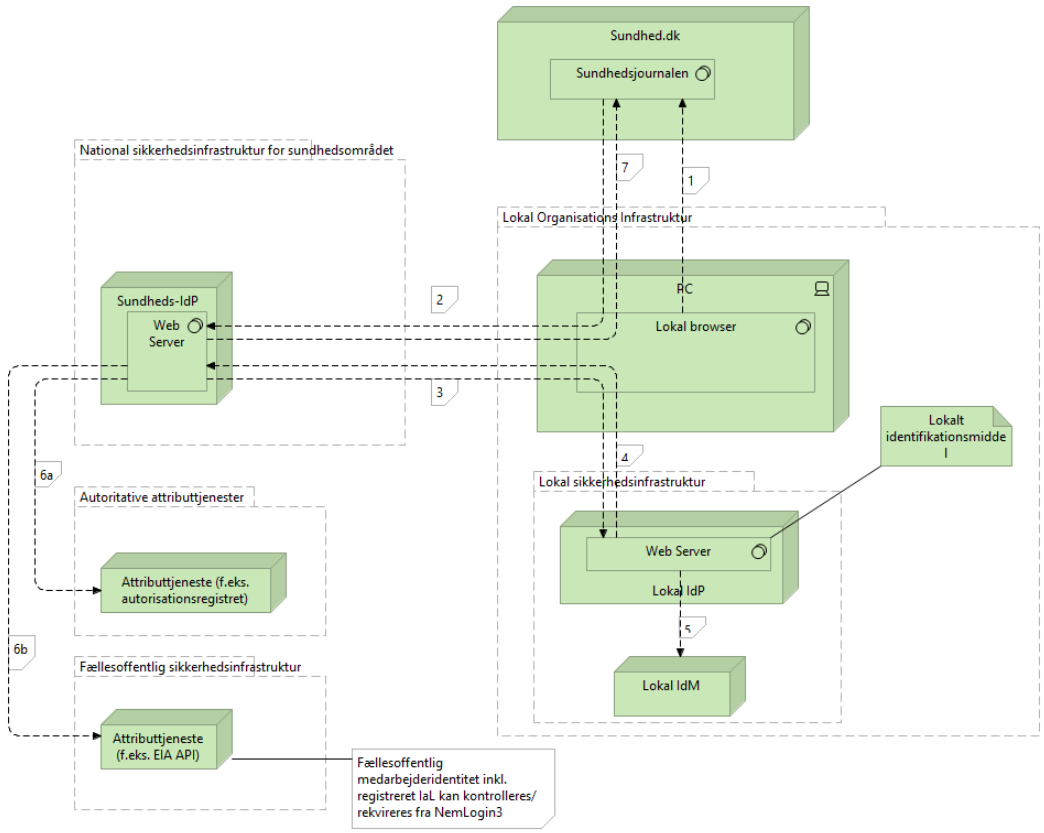
Figur 20: Bruger fra organisation med egen IdP tilgår en browserbaseret, national sundhedstjeneste. Bemærk at der i dette flow kommer autoritative rolleoplysninger med i flowet (IdM).

1. Brugeren åbner en browser og indtaster URL'en på en browserbaseret, national sundhedstjeneste (for eksempel sundhedsjournalen i Sundhed.dk).
2. Sundhed.dk kan ikke se, at der er en aktiv session med brugerens browser, og omstilles den til den nationale SundhedsIdP.
3. Her er der heller ingen aktiv session, og browseren omstilles denne gang til den fællesregionale ADFS eller den fælleskommunale Contexthandler
4. Lokalt kan der være en aktuel login-session (baseret på login til den lokale infrastruktur), i så fald bliver brugeren ikke bedt om at autentificere sig igen. Såfremt der ikke er en aktiv session, skal den lokale IdP præsentere en brugergrænseflade, der beder brugeren anvende sine identifikationsmidler. Disse kan være certifikatbaserede (enten MOCES eller fællesoffentlige kvalificerede certifikater, egne certifikater eller helt andre lokale identifikationsmidler).

5. Den lokale IdP kan også autoritativt sætte rolleoplysninger på i det udstedte *token*. Disse oplysninger kommer fra den lokale IdM (eller en tilknyttet attributtjeneste). Browseren omstilles tilbage til den nationale sundhedsIdP.
6. SundhedsIdP'en udsteder de nødvendige login-*tokens*, og kan i den sammenhæng eventuelt berige dem med nationale og fællesoffentlige attributter.
7. Browseren omstilles til Sundhedsjournalen, der nu kan logge brugeren ind og anvende de lokalt administrerede rolleinformationer til at give adgang til de relevante funktioner i webapplikationen.

En særlig udgave af dette flow er i relation til kommunerne og regioner. I kommunalt regi er der etableret den såkaldte Context-handler, der er en fælleskommunalt *entrypoint* som kan stille om til lokale IdP'er. I kommunal sammenhæng vil denne være for enden af skridt 3 ovenfor, og vil stille videre til den relevante IdP i den kommunale føderation.
Tilsvarende er der etableret et fællesregional *entrypoint* i forbindelse med PPJ i form af den fællesretionale ADFS, som siden også er anvendt i Sårjournalssammenhæng. Også her vil denne blive skubbet ind som den fællesregionale IdP i skridt 3.

7.2.3 En sundhedsprofessionel aktiverer en browserbaseret tjeneste fra fagsystem (Sikker browseropstart baseret på SAML)



Figur 21: Flow for adgang til et browserbaseret system for eksempel Sundhedsjournalen ved hjælp af Sikker Browseropstart.

I dette flow tager den privatpraktiserende læge adgang til en browserbaseret tjeneste fra sit fagsystem. Dette kan gøres ved hjælp af metoden Sikker Browseropstart, som også videreføres i målarkitekturen. Det forudsættes at brugeren allerede er logget ind gennem flowet beskrevet i afsnit 7.1.1 "En sundhedsprofessionel i organisation uden egen IdP autentificerer sig i forhold til den nationale infrastruktur for sundhedsområdet (Rich-Client + SAML)".

1. Brugeren aktiverer en funktion i fagsystemet, der kræver adgang til en en browserbaseret tjeneste.
2. Fagsystem Backend rekvirerer et Sikker Browseropstarts-*token* hos den nationale Sundheds-STS og sender brugerens identitetsbevis samt andre kontekstdannende *claim*-værdier med i kaldet.
3. STS'en danner et Sikker Browser-opstarts*token* (SAML assertion) og returnerer det til LPS backend, hvor den gemmes og identificeres med et unikt id (*nonce*).
4. Fagsystemsklienten modtager id'et ...
5. ... og kan nu starte en browser, der peger på en lokal webserver (med id'en som URL parameter).
6. Browseren kontakter den lokale webbrowser ...
7. ... som øjeblikkeligt sender brugerens browser videre til Sundhedsjournalen. I kaldet indlejres Sikker Browseropstarts*tokenet*.
8. Sundhedsjournalen kan nu logge brugeren ind, da *tokenet* viser at brugeren er passende autentificeret. Desuden kan Sundhedsjournalen konfigurere hvilke funktioner, der skal være tilgængelig for brugeren ud fra de attributter der blev modtaget i *tokenet*, herunder eventuelle rolle/rettigheds-attributter.

Bemærkninger:

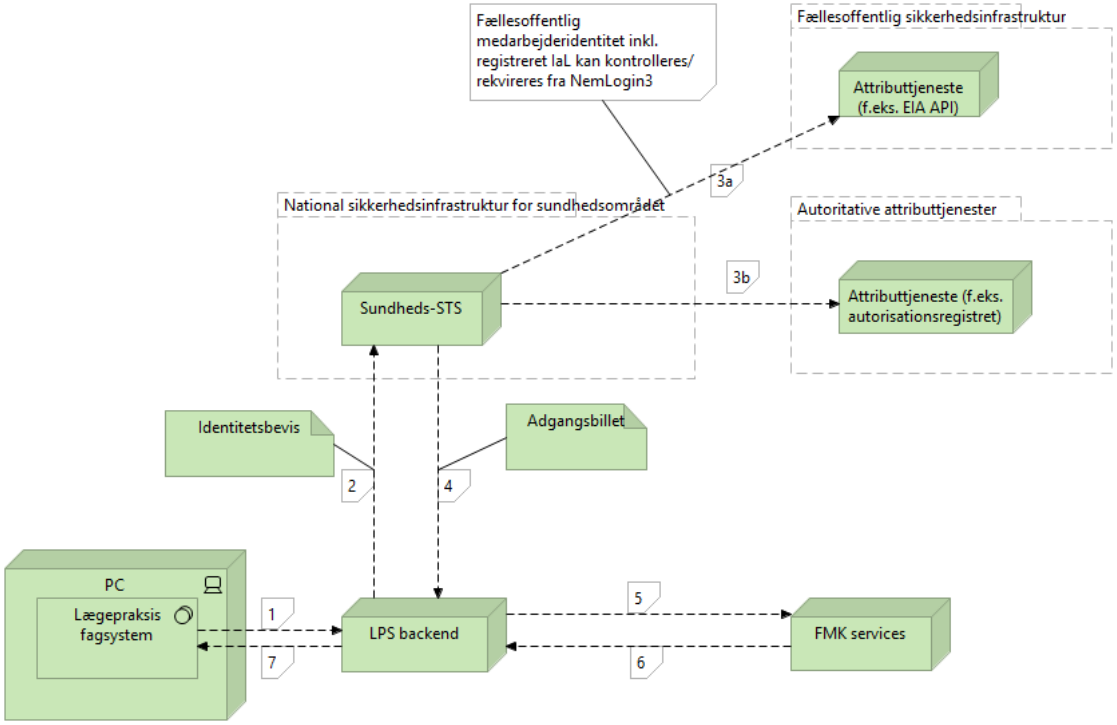
- I Sikker Browseropstartsscenariet medsendes attributter som kan styre adgangen til brugergrænsefladen. Dette vil typisk være gennem nogle rolle/rettighedssæt, der er defineret af den pågældende web-baserede tjeneste, og som fagsystemet har knyttet (mappet) til de lokale roller/rettigheder. Desuden kan der medsendes mere flygtige kontekstinformationer for eksempel patient-id etc.
- Denne case er den samme om man har egen IdP eller ej.

7.3 Flows for kontekstfastsættelse og anvendelse af nationale digitale sundhedstjenester

I dette afsnit gennemgås flows for kontekstfastsættelse og anvendelse af nationale digitale sundhedstjenester. Kontekstfastsættelsen skal ses i relation til den efterfølgende anvendelse af en national digital sundhedstjeneste, og sker i praksis ved at veksle et identitetsbevis til en tjenestespecifik adgangsbillet, hvori der indgår attributter om brugeren og brugerens kontekst, som kan anvendes til adgang og logning hos den nationale sundhedstjeneste.

7.3.1 Et fagsystem tager adgang til en national digital sundhedstjeneste (Rich-Client + IDWS)

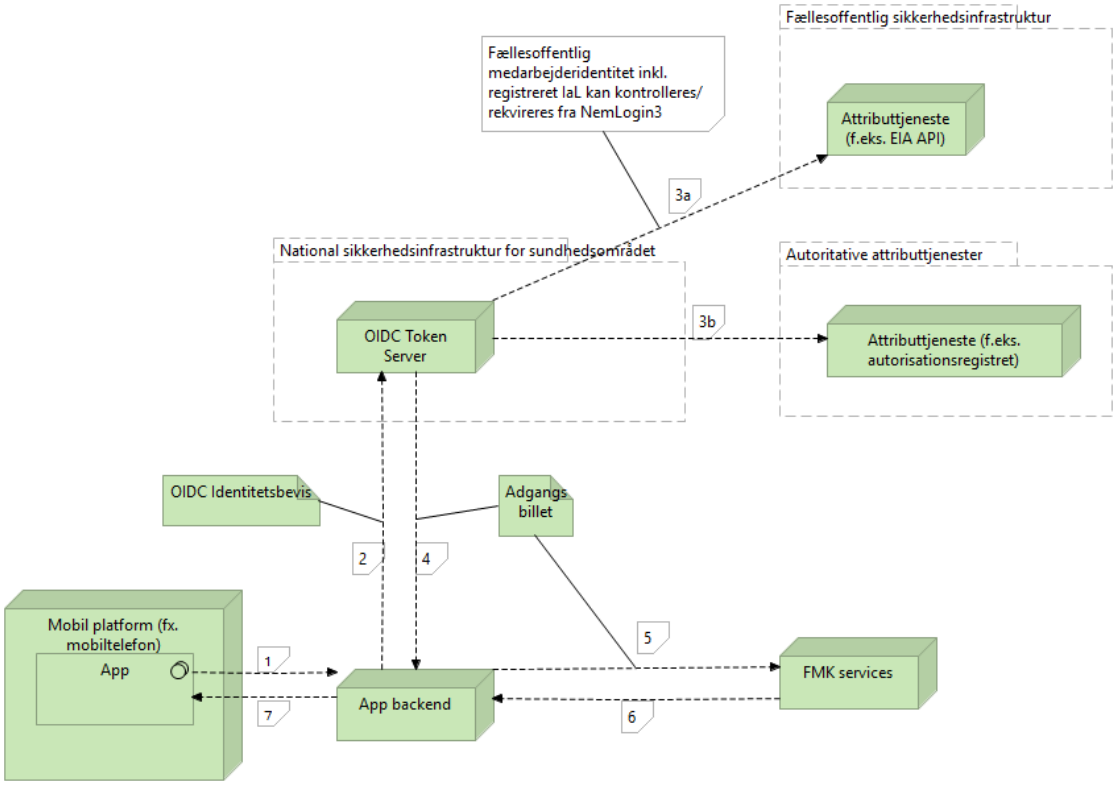
For at kunne kalde FMK via web-services, skal der udstedes en adgangsgivende billet. Fagsystemet skaffer et sådant ved at veksle brugerens identitetsbevis til en tilpasset adgangsbillet. Dette gennemgås i nedenstående flow.



Figur 22: LPS kald af FMK efter autentifikation. Identitetsbeviset veksles til en adgangsbillet.

1. Brugeren aktiverer en funktion i fagsystemet, der kræver adgang til FMK. Fagsystemklienten kontakter fagsystem-backend (LPS backend).
2. LPS-backend kalder den nationale sundheds-STS med en række *claims* og det tidligere rekvirerede identitetsbevis.
3. Den nationale sundheds-STS verificerer kaldet og identitetsbeviset. Hvis nogle af de fremsendte *claims* kræver validering hos autoritative tjenester eller hvis der i føderationsaftalen er aftalt, at STS'en skal berige adgangsbilletten med relevante attributer, sker dette nu.
4. STS'en producerer et adgangsbilletten med et for FMK relevant indhold (dataminimering/privacy-by-design) og returnerer dette til LPS backend.
5. LPS *backend* danner nu et kald til FMK og indlejrer adgangsbilletten.
6. FMK kontrollerer adgangsbilletten og giver adgang såfremt attributterne i adgangsbilletten berettiger dette. FMK returnerer data til LPS *backend*.
7. LPS *backend* returnerer data til brugergrænsefladen og disse præsenteres for den sundhedsprofessionelle.

7.3.2 En sundhedsprofessionel anvender FMK gennem en mobil app (App + OpenID Connect)

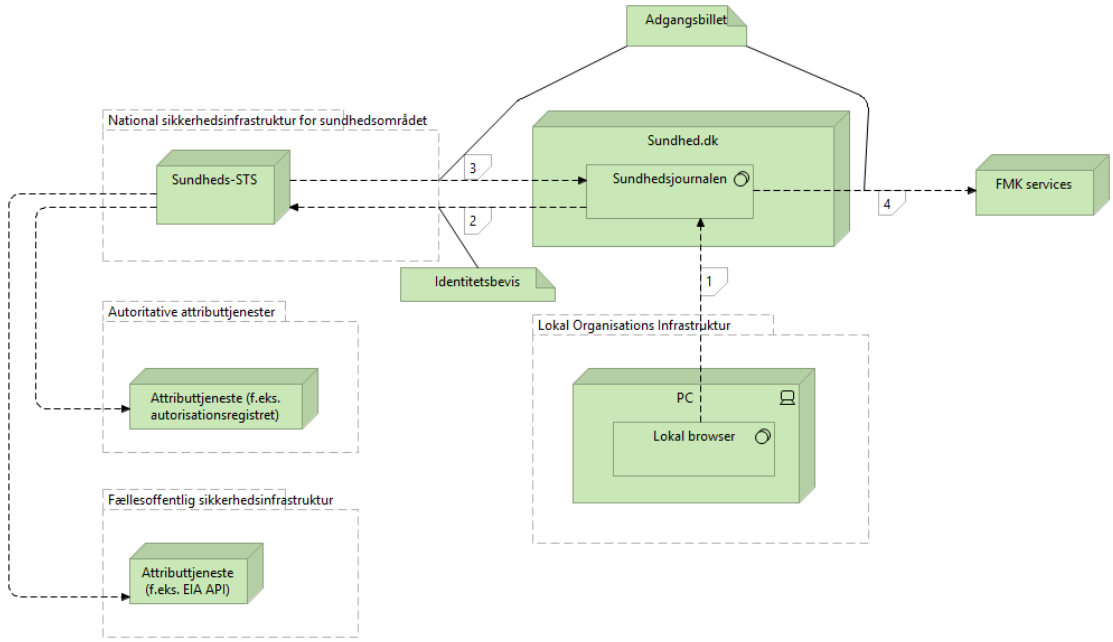


Figur 23: Kald af en national digital sundhedstjeneste med OpenID Connect (REST service).

Flowet er identisk med kald af nationale *webservices* baseret på SAML / IDWS, men komponenterne hedder noget andet, og *token*-formatet er anderledes. Flowet gennemgås ikke i detaljer.

7.3.3 Et browserbaseret system anvender bagvedliggende identitets-baseret tjeneste (IDWS hhv. OIDC)

I dette flow er fagsystemnet / klientsystemet et browserbaseret system, der får behov for at kalde en identitets-baseret tjeneste for at kunne præsentere de rette data eller gennemføre de nødvendige handlinger. Et eksempel er Sundhedsjournalens anvendelse af FMK tjenester til visning for borgere.



Figur 24: Browserbaseret system kalder identitetsbaseret tjeneste på vegne af brugeren.

1. Brugeren aktiverer en funktion i web-applikationen, der kræver adgang til en national digital sundhedstjeneste (her FMK).
2. I sessionen med browseren ligger der et identitetsbevis. Dette skal veksles til et FMK specifikt adgangsbillet hos Sundheds-STS'en.
3. Sundheds-STS'en udsteder et passende adgangsbillet til Sundhedsjournalen. Her indlejres de nødvendige/relevante attributter, der kan anvendes til adgangskontrol og logning hos FMK.
4. Sundhedsjournalen medsender nu adgangsbilletten til FMK, der kontrollerer billetten, gennemfører handlingen og returnerer med et passende svar til Sundhedsjournalen. Sundhedsjournalen viser de nødvendige elementer for brugeren.

7.4 Identifikation af attributindhold og –tjenester

Grundlaget for adgangspolitikker er tilknytning af attributter til elektroniske identifikationsmidler. Tjenesteudbydere er ansvarlige for at fastlægge og gennemføre adgangspolitikker for den pågældende tjeneste. Ved anvendelse af nationale digitale sundhedstjenester har tjenesteudbyder derfor tillid til, at tjenesteanvender tilknytter de rette attributter, eksempelvis at de rette organisationsoplysninger er tilknyttet, og at eventuelle kopier af stamdata hos tjenesteanvender stemmer overens med de autoritative kilder for samme. Såvel tjenesteanvender som tjenesteudbyder har tillid til at autoritative kilder er opdaterede og korrekte.

Nedenstående tabel giver et overblik over de væsentligste attributter og deres autoritative kilder:

Attribut	Autoritativ kilde / ansvarlig organisation	Bemærkninger
Personidentitet	MitID / DIGST	Den nationale personidentitet danner grundlaget for sporbarhed, som beskrevet i princip 8
CPR	CPR-kontoret	
Fuldmagt	DIGST	
Samtykke	Sundhedsdatastyrelsen	
Bemyndigelse	Sundhedsdatastyrelsen	
Autorisationsoplysninger	Autorisationsregisteret / Styrelsen for patientsikkerhed	Autorisationsoplysninger danner grundlaget for rettigheder til adgang til data jævnfør sundhedsloven.
Tilknytning til organisation, roller og rettigheder	Lokal brugerstyring / lokal organisation for regioner og kommuner. FBRS eller SEB for øvrige parter	Tilknytning til organisation, roller og rettigheder i organisationen, herunder Medhjælp og Arbejder på vegne af (§42)
Kontekst	Lokalt fagssystem /lokal organisation	Omfatter blandt andet patientid, formål, afdeling, ansættelsesforhold, på vegne af.
Organisation	Sundhedsvæsnets Organisationsregister / Sundhedsdatastyrelsen	SOR erstatter øvrige organisationsklassifikationer og registre, som har været anvendt til organisationsidentifikation. SOR danner grundlag for validering af organisationskoder

Det er nødvendigt at kunne vurdere kvaliteten af attributters værdi, når disse anvendes i brugerstyringsmæssig sammenhæng. Målbilledet lægger derfor op til at indføre en klassifikation af sikringsniveauer for tilknyttede attributter som har til formål at muliggøre graduerede krav til attributter. Klassifikationen er analog til klassifikationen i NSIS, og skal eksempelvis kunne angive forskellige krav til opdatering og korrekthed af lokale kopier af stamdata samt krav til lokale brugerstyringsløsninger og fagsystemer ved fastlæggelse af organisatoriske data og kontekstdata.

7.5 Identifikation af *token*profiler

Der fastlægges standarder og profiler for *tokens* inden for den nationale føderation på sundhedsområdet. Lokale *token*formater skal derfor omveksles til nationale formater ved kald af tjenester i føderationen. Standarder og profiler identificeres og udarbejdes i forlængelse af målbilledet.

Henvisninger

[Analyse2014] Fællesoffentlige brugerstyringsløsninger - en analyse af sikkerhedsstandarder og –løsninger, National Sundheds-it (NSI), 2014.

[Arkitekturprincipper] Arkitekturprincipper for Sundhedsområdet - en ramme for udformning af fremtidens nationale it-arkitektur for sundhedsvæsenet, Sundhedsdatastyrelsen, 2017, https://sundhedsdatastyrelsen.dk/-/media/sds/filer/rammer-og-retningslinjer/referenceaktitektur-og-it-standarder/arkitekturprincipper_version-2,-d-,0.pdf?la=da

[Brugerstyring-strategi] Fællesoffentlig strategi for brugerstyring, Digitaliseringsstyrelsen, april 2017, https://arkitektur.digst.dk/sites/default/files/123_strategi_for_brugerstyring_pdfa.pdf

[Brugerstyring-referencearkitektur] Fællesoffentlig referencearkitektur for brugerstyring, Digitaliseringsstyrelsen, april 2017, https://arkitektur.digst.dk/sites/default/files/123_referencearkitektur_for_brugerstyring_pdfa.pdf

[Certifikater-afklaring] Certifikater i den fællesoffentlige infrastruktur, notat af 15. marts 2019 (Digitaliseringsstyrelsen).

[Hvidbog]

[IDWS-anvendelsesscenarier] Anvendelsesscenarier - identitetsbaserede serviceintegrationer på sundhedsområdet, v 1.0, Sundhedsdatastyrelsen

[IDWS-målbilleder] Målbilleder - identitetsbaserede serviceintegrationer på sundhedsområdet, v 1.0, Sundhedsdatastyrelsen

[IDWS-målarkitektur] Målarkitektur - identitetsbaserede serviceintegrationer på sundhedsområdet, v 0.8, Sundhedsdatastyrelsen

[IDWS-datamodel] Konceptuel datamodel - identitetsbaserede serviceintegrationer på sundhedsområdet, v 0.41, Sundhedsdatastyrelsen

[INFSIK-REF] Referencearkitektur for informationssikkerhed, v. 1.0, National Sundheds-it (NSI), september 2013. https://sundhedsdatastyrelsen.dk/-/media/sds/filer/rammer-og-retningslinjer/referenceaktitektur-og-it-standarder/referencearkitektur/referencearkitektur-informationssikkerhed.pdf?la=da

[Interføderation] Målbillede for interføderation i sundhedsvæsnet, v 0.4, Sundhedsdatastyrelsen

[Nationale begrebsdatabase] Sundhedsvæsenets begrebsdatabase. https://sundhedsdatastyrelsen.dk/nbs

[NSIS] National Standard for Identiteters Sikringsniveauer (NSIS), Version 2.0.01, Digitaliseringsstyrelsen, 5. oktober 2018, https://digst.dk/media/20287/national-standard-for-identiteters-sikringsniveauer-nsis-version-201.pdf

[NSIS-vejledning] Vejledning til National Standard for Identiteters Sikringsniveauer (NSIS), Digitaliseringsstyrelsen, 2. november 2018, https://digst.dk/media/18660/vejledning-til-national-standard-for-identiteters-sikringsniveauer-nsis-version-20.pdf

[OIOBPP] OIO Basic Privilege Profile, version 1.1, Digitaliseringsstyrelsen, januar 2019, https://digst.dk/media/19020/oiosaml-basic-privilege-profile-1_1.pdf

[OIOSAML] OIOSAML Web SSO Profile 3.0 'Release Candidate', Digitaliseringsstyrelsen, 22. januar 2019, https://digst.dk/media/19019/oiosaml-web-sso-profile-30-release-candidate.pdf

[SEB-integration] Kom godt i gang med SEB IdP og service-integrationer (UDKAST), Sundhedsdatastyrelsen, 2018.

[SOSI politik] Sikkerhedsaspekter-Opbevaring-af-SOSI-IDkort, version 1.0 2/2 2014, National Sundheds-IT

[Sårjournal-sikkerhed] Føderative sikkerhedsmodeller til Sårjournalen - Overordnet arkitektur, v.0.95, National Sundheds-it (NSI), 17. november 2014.

[Sårjournal-løsning] Sårjournalen - løsningsbeskrivelse til ændring af sikkerhedsarkitekturen, v 1.0, Lakeside, 4. juni 2015, http://medcom.dk/media/7318/loesningsbeskrivelse_saarjournal_sikkerhedsarkitektur-v10-3.pdf

Appendiks A: Termer

Term	Definition	Forklaring
Adgangsbillet	Et elektronisk objekt, der dokumenterer en anmodning fra en bruger	For at opfylde adgangspolitikken for en tjeneste, skal der indhentes et eller flere adgangsbilletter hos udstedere, som tjenesten har tillid til.
Adgangsvej	Samlede teknisk løsning som brugeren anvender for at tilgå en given digital tjeneste	Eksempel adgang gennem eget fagsystem med integration til ekstern tjeneste eller adgang gennem en browserbaseret snitflade til samme tjeneste via Internettet
Attribut	Karakteristika eller egenskaber ved en Entitet eller Identitet. Dette kan fx være et navn, brugernavn, et pseudonym, et CPR-nummer, en UUID, bopæl, rolle etc.	
Autentifikation	En proces som genkender og verificerer en Identitet (tilknyttet en Entitet) gennem anvendelse af et Elektronisk Identifikationsmiddel, der er koblet til Identiteten. Ved multi-faktor autentifikation forstås en autentifika-tionsproces, hvor det anvendte Elektroniske Identifika-tionsmiddel tilvejebringer flere Autentifikationsfaktorer fra forskellige kategorier	
Autoriseret sundhedsaktør	Sundhedsaktør, som er autoriseret efter lov om autorisation af sundhedspersoner og om sundhedsfaglig virksomhed	Efter lov om autorisation af sundhedspersoner og om sundhedsfaglig virksomhed er der i Danmark indført autorisationsordninger for en række sundhedspersoner. Der er indført autorisationsordninger for følgende grupper: Læger

		Tandlæger Kiropraktorer Sygeplejersker Jordemødre Ergoterapeuter Fysioterapeuter Bioanalytikere Kliniske diætister Radiografer Bandagister Kliniske tandteknikere Tandplejere Optikere og kontaktlinseoptikere Optometrister Fodterapeuter Social- og sundhedsassistenter
Betroet tredjepart	En uafhængig tredjepart, der inden for rammerne af et tillidsrammeværk formidler funktionalitet og/eller digitalt indhold overfor en tjenesteaftager på vegne af en tjenesteudbyder	Tjenesteudbyder og tjenesteaftager laver hver en aftale med en uafhængig betroet tredjepart. Antallet af aftaler og tekniske integrationer er begrænset af summen af aktører. Modellen er velegnet i sammenhænge, hvor parterne har en organisatorisk eller sektormæssig egenskab til fælles, eksempelvis sundhedsområdet
Bilateral tilllidsrelation	Relation direkte mellem to parter, typisk mellem en tjenesteudbyder og en tjenesteanvender, som er reguleret i en bilateral aftale de to parter imellem.	Bilateral tillid har primært sin berettigelse i sammenhænge med et begrænset antal parter, da antallet af aftaler vokser med produktet af antallet af serviceudbydere og serviceaftagere
Brugeradministrationssystem	System til administration af elektroniske identiteter samt tilknytning af roller og rettigheder	
Brugeradministrator	Administrativt personale i organisationen, der administrerer elektroniske identiteter og deres adgange til interne og eksterne systemer.	

Brugerstyring	Adgangskontrol og administration af brugere og adgangsrettigheder	Brugerstyring omfatter det, der på engelsk betegnes Credential and Identity Management (CIM), Identity Rights Management (IRM), Access Control (AC) og Identity and Access Management (IAM/IdAM). Dækker således opgaver i forbindelse med indrullering, autentificering, autorisation, osv.
Context handler	Fælleskommunale tillidstjeneste	Fælles tillidstjeneste for kommunerne, som forvaltes af KOMBIT
Den nationale føderation for sundhedsområdet	*Føderation*, som er forvaltet af Sundhedsdatastyrelsen	
Digital sundhedstjeneste	Digital tjeneste, som giver adgang til sundhedsmæssigt indhold	Den præhospitale patientjournal og sundhed.dk er begge eksempler på digitale sundhedstjenester
Elektronisk identitet	Elektronisk (digital) identitet anvendes om den digitale repræsentation af en entitet (fx person eller virksomhed). Dette svarer til eID.	
Elektronisk identifikationsmiddel	Et middel, som en entitet får udstedt til brug for on-line autentifikation (NSIS).	Midlet kan både være fysisk og virtuelt, og skal være under entitetens kontrol
Forbeholdt sundhedsfaglig virksomhed	Sundhedsaktiviteter, som er forbeholdt særlige autorisationer jævnfør autorisationsloven	
Formidlet tillid	Se betroet tredjepart	
Fællesregionale ADFS	Active Directory Federation Services (ADFS) er en komponent der installeres på en Windows Server der via Single Sign-on simplificerer adgangs-processer og gør det derved hurtigere at få adgang til valgte systemer og applikationer (https://rn.dk/sundhed/til-sundhedsfaglige-og-samarbejdspartnere/national-og-tvaerregional-it/adfs).	Region Nordjylland bruger ADFS til at give dets ansatte adgang til flere af regionens systemer. Region Nordjylland bruger også ADFS til at give adgang på dets tværregionale systemer, som for eksempel PPJ. ADFS gør det her muligt for alle fem regioners brugere at logge på det samme system (ibid.)

Fødereret tillid	Konstruktion, inden for hvilken tillid til it-sikkerhedselementer formidles mellem organisationer	Føderationstilgangen gør det muligt for organisationer at udstille og anvende services uden at skulle indgå i bilaterale aftaler med samtlige organisationer i føderationen. I stedet indgår hver organisation en føderationsaftale, hvor et sæt af krav og regler skal overholdes. Fødereret tillid har sin primære berettigelse, hvor grupper af aftagere og udbydere på tværs af domæner og sektorer indgår i en sammenhæng.
Identitetsbaseret digital tjeneste	Tjeneste, hvor adgang forudsætter adgangsbillet, som er knyttet sammen med en forudgående vellykket autentifikation af en digital identitet	Det betyder for eksempel, at et system (eller en hacker) kan ikke kalde sådanne tjeneste uden også at have hacket autentifikationssystemet, for uden et identitetsbevis kan der ikke veksles til en adgangsbillet
Identitetsbevis	Et elektronisk objekt, der dokumenterer en brugers identitet	Identitetsbeviset kan anvendes overfor en billettjeneste til at få udstedt adgangsbilletter til tjenester
Identity Provider (IdP)	Se identitetsudbyder	
Interføderation	Føderation af føderationer	Betegnelse for, at flere parter med hver deres føderation indgår i en ny føderation, i hvilken parterne enes om fælles aftaler og regler, men hvor parterne samtidig bevarer kontrollen over egen føderation, så længe dette ikke bryder med de fælles aftaler.
Identitetsudbyder	En organisation eller et system, der verificerer en brugers eller et systems identitet på baggrund af brugerens (eller systemets) besiddelse og kontrol over akkreditiver udstedt af en CSP som IdP'en har tillid til. Dertil udsteder organisationen akkreditiver til entiteter og indestår for deres identitet over for enheder, der forespørger. Det kan både	

	dække over identitetsgarant og log-in-tjeneste.	
Login	Proces, hvor en person præsenterer sine digitale identifikationsmidler for at bevise sin identitet	
Logout	Proces, hvor brugeren tilkendegiver afslutning af anvendelsen af sin identitet	
National digital sundhedstjeneste	digital sundhedstjeneste udstillet i Den nationale føderation for sundhedsområdet	Sårjournalen, sundhed.dk og det fælles medicinkort er eksempler på nationale sundhedstjenester
Nationale IdP for sundhedsområdet (Den nationale sundhedsIdP	IdP i den nationale føderation for sundhedsområdet.	
Privilegie	Se forbeholdt sundhedsfaglig virksomhed	
Session	Tidsmæssig og systemorienteret ramme, inden for hvilken en entitets digitale identitet er autentificeret og kan tilgå et system eller sæt af systemer	En session oprettes typisk i forbindelse med autentifikationshandlingen, for eksempel ved login til et fagsystem under betingelse af, at brugerens identitet kan autentificeres af det tilhørende autentifikationsmodul. Sessionen afsluttes enten ved at brugeren aktivt afslutter den eller ved at en forudgående fastsat tidsfrist for inaktivitet overskrides.
Single-sign-on	Proces, som giver adgang til flere tjenester gennem en autentifikationshandling	
Sundhedsaktør	Aktør, som er involveret i sundhedsrelaterede aktiviteter	Begrebet er et samlende begreb for alle, der er involveret i en sundhedsaktivitet dvs. patienter, læger, sygeplejersker, plejepersonale osv.
Sundhedsproducerende enhed	enhed der danner ramme for sundhedsprofessionelles sundhedsaktiviteter	
Tillidsrammeværk	Se trust framework	
Tillidsrelation	Relation, hvor en eller flere parter stoler på og er afhængig af, at en eller flere øvrige parter overholder	Tillidsrelation omfatter følgende typer af relationer, som målbilledet baserer sig på: fødereret tillid, formidlet tillid,

	forud indgåede aftaler for relationen	bilateral tillidsrelation samt formidlet tillid og betroet tredjepart
Tillidstjeneste	Tjeneste, som formidler information om brugere i form af elektronisk id og attributer	
Token	Samlebegreb for identitetsbeviser og adgangsbilletter	
Trust framework	Et trust framework rummer et sæt af retningslinjer og procedurer m.v., som parterne, der anvender trust frameworket kan acceptere at overholde, så der etableres gensidig tillid.	For at alle parter i en føderation har tillid til hinanden er det en fordel at eksplicitere, harmonisere og standardisere forskellige aspekter af sikkerhed, herunder politikker, sikkerhedsmæssige tiltag og fælles sprog. Det sker ved udarbejdelse af et såkaldt trust framework Trust frameworket fastsætter egenskaber som kvaliteten af udstedelsesprocessen af digitale identiteter, sikkerheden omkring opbevaring og transmission af identiteter, samt krav til selve autentifikationsfasen hos den enkelte IdP. For at trust frameworket har en værdi er det essentielt med bedømmelse og kontrol af de enkelte parters overholdelse af fremsatte retningslinjer og specifikationer. Dette kræver en organisation omkring trust frameworket.