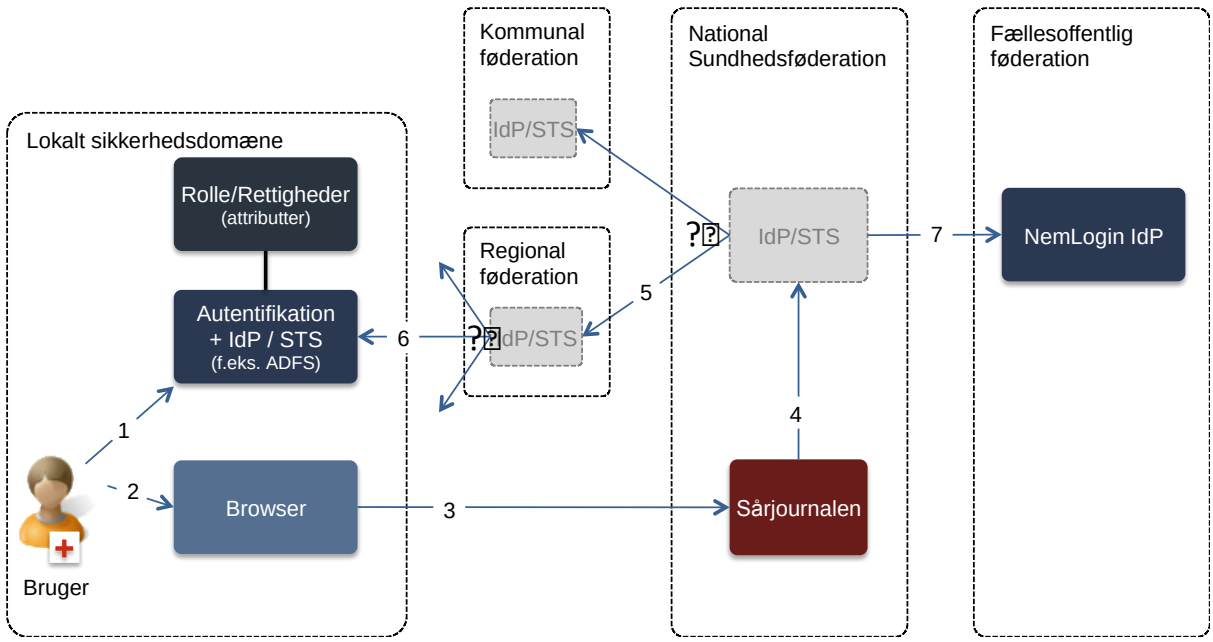
Bilag 2, Saarjournalen, sikkerhedsmodel, arkitektur

Bilag til punkt 7, Forretningsarkitektur på beskæftigelsesområdet

Føderative sikkerhedsmodeller til Sårjournalen - **Overordnet arkitektur** Version: 0.95 Udarbejdet af: Esben Andreas Dalsgaard / NSI	Statens Seruminstitut Sektor for National Sundheds-IT www.nsi.dk Artillerivej 5 2300 København S



I. Revisionshistorik

Version	Dato	Ansvarlig	Beskrivelse
0.5	2014-10-14	EAD	Modellerne uddybet og målrettet arkitekturrådsdeltagere.
0.6	2014-10-15	EAD	Midlertidig passiv model tilføjet.
0.7	2014-10-16	EAD	Uddybning af sikkerhedselementer.
0.8	2014-10-20	EAD	Forenkling af figurer og notation.
0.9	2014-10-21	EAD	Diverse omskrivninger. Notat klar til forelæggelse for regionernes og kommunernes it-arkitekturråd.
0.95	2014-11-17	EAD	Tilrettet efter behandlingen i regionernes it-arkitekturråd

II. Indholdsfortegnelse

1 Indledning

Nærværende notat beskriver de sikkerhedsmodeller der overvejes i forbindelse med Sårjournalen. Notatet har til hensigt at skabe et overblik over de arkitektoniske og strukturelle valg der kan træffes i forhold til sikker adgang til Sårjournalens helbredsinformationer, og skal danne grundlag for diskussion og beslutning af det endelige sæt af sikkerhedsløsninger, der skal anvendes i relation til Sårjournalen.

Sikkerhedsmodellerne har været diskuteret ved to møder i en arbejdsgruppe bestående at regionale arkitekter, en kommunal arkitekt, NSI og MedCom.

Målgruppen for notatet er arkitekter og beslutningstagere i Sårjournalsprojektet, samt leverandører der skal etablere de beskrevne løsninger. Endvidere er notatet tiltænkt behandling i henholdsvis regionale og kommunale it-arkitekturråd bl.a. med henblik på at vurdere løsningernes genbrugelighed i forhold til andre nationale applikationer.

1.1 Begreber / termer

Forkortelse i teksten	Beskrivelse
AD	Active Directory. En central del af Microsofts Windows platform til lagring og styring af bl.a. brugerinformationer, roller og rettigheder.
cNSP	cNSP er forkortelsen for "central NSP", dvs. den NSP-instans, der er placeret centralt i den nationale infrastruktur og som kan anvendes af de parter i sundhedssektoren, der ikke har mulighed (eller ønske om) at have egen NSP-instans (kaldet dNSP).
COTS	Commercial-Off-The-Shelf.
dNSP	dNSP er forkortelsen for "decentral NSP", og er fællesbetegnelsen for de NSP-instanser, der er placeret ude hos regionerne.
EPJ	Elektronisk Patientjournal. En portefølje af sundhedsfaglige it-systemer og -moduler, der tilsammen udgør den daglige it-værktøjskasse for bl.a. klinikere på sygehuse.
FMK	Det Fælles Medicinkort. En national it-tjeneste, der drives Statens Serum Institut (tidligere Lægemiddelstyrelsen), som gør det muligt at få informationer om alle patienters aktuelle medicinering.
IdP	”Identity Provider”. En it-tjeneste der ved hjælp af it-tekniske hjælpemidler og akkreditiver, kan kontrollere om en bruger er den, vedkommende udgiver sig for at være. En IdP opretholder ”login sessioner” på tværs af web applikationer. Dermed kan der opnås ”Single Sign On”, dvs. brugeren behøver kun logge på én gang for at få adgang til alle web applikationerne, der er med i IdP sammenslutningen. Nogle IdP’er implementeringer understøtter også ”Single Log-out”, så brugeren automatisk ”logges af” i alle tilsluttede web applikationer.
LPS	Lægepraksissystem.

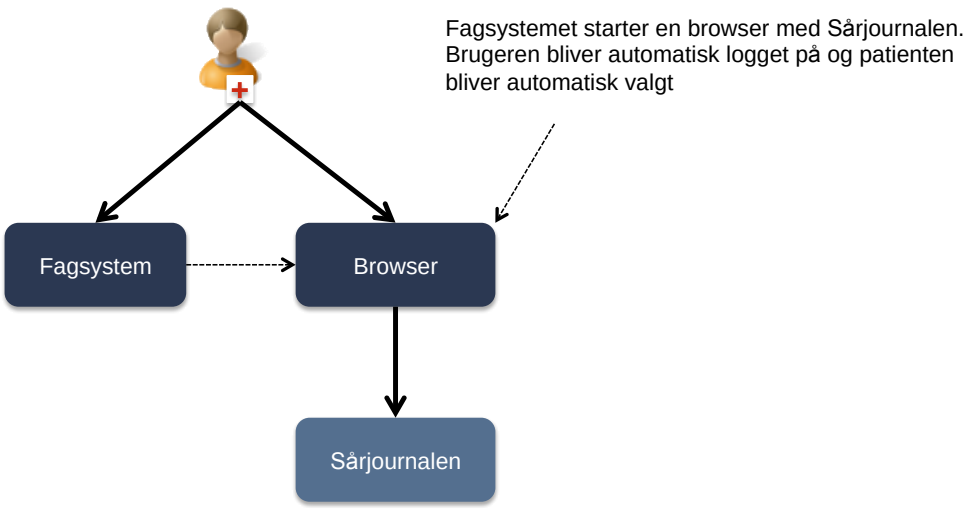
NIST	National Institute of Standards and Technology. Standardiseringsorganisation i USA.
NSI	Sektor for National Sundheds-it, Statens Serum Institut.
NSP	Den Nationale Serviceplatform på sundhedsområdet. En platform med en række it-infrastrukturelementer, der gør det nemmere, billigere og mere sikkert at udveksle sundhedsdata
OCES	Offentlige Certifikater til Elektroniske Services. Det danske fællesoffentlige system til digitale signaturer.
Security Token	En digital "klump" af data der indeholder sikkerhedsattributter der relaterer sig til en bruger, et system eller en virksomhed. I sundhedsdomænet er security tokens struktureret efter SAML2 standarden.
SOSI	ServiceOrienteret SystemIntegration. SOSI leverer integrationsmekanismer, infrastrukturkomponenter og værktøjer til webservicebaseret integration mellem anvendersystemer (f.eks. regionale EPJ-systemer eller lægepraksissystemer) og nationale services. SOSI udgør en væsentlig del af det tekniske fundament for NSP infrastrukturkomponenterne.
STS	Security Token Service. En it-tjeneste i infrastrukturen, som udsteder "security tokens". Disse "tokens" indeholder typisk informationer om brugeren som STS tjenesten har kontrolleret og som den modtagende part dermed kan stole på.
SOSI-GW	SOSI-Gateway. En security token cache i den nationale sundhedsinfrastruktur.

2 Forventede anvendelsesscenarier

Nærværende afsnit redegør for de forventede brugsscenarier i Sårjournalen. Det er vigtigt at sikkerhedsinfrastrukturen og sikkerhedsmodellerne forholder sig til disse, så det sikres at brugernes brug af løsningen bliver så smidig som mulig.

2.1 Sundhedsperson anvender Sårjournalen gennem fagsystem

En sundhedsperson, der arbejder i sit fagsystem, får brug for at se oplysninger i Sårjournalen og aktiverer Sårjournalen ved at trykke på en knap i fagsystemet. Herefter åbner Sårjournalen i et browser vindue (enten selvstændig browser eller indlejret i fagsystemet), hvor sårjournalen viser data på den patient man arbejdede med i fagsystemer.
Løsningen skal sikre at sundhedspersonen ikke skal logge sig på igen eller fremsøge den pågældende patient i forbindelse med åbning af sårjournalen.
Af patientsikkerhedsmæssige årsager er det vigtigt, at løsninger der benytter sig af denne type systemintegration bedst mulig sikrer, at der ikke opstår situationer, hvor patienten i fagsystemet er en anden end den vist i browservinduet. Denne risiko kan reduceres ved at sikre, at man ikke i Sårjournalen kan navigere til andre patienter end den, der blev "aktiveret" fra fagsystemet. Tilsvarende skal fagsystemet så vidt muligt forsøge at sikre at lukke browservinduer med patienter, der ikke længere er i fokus i fagsystemet. Ofte kan dette bedst sikres gennem indlejrede browservinduer og/eller ved anvendelse af visuelle virkemidler[1], der gør brugerne opmærksomme på denne risiko.



2.2 Link tilgår sundhedspersonen gennem korrespondancemeddelelse

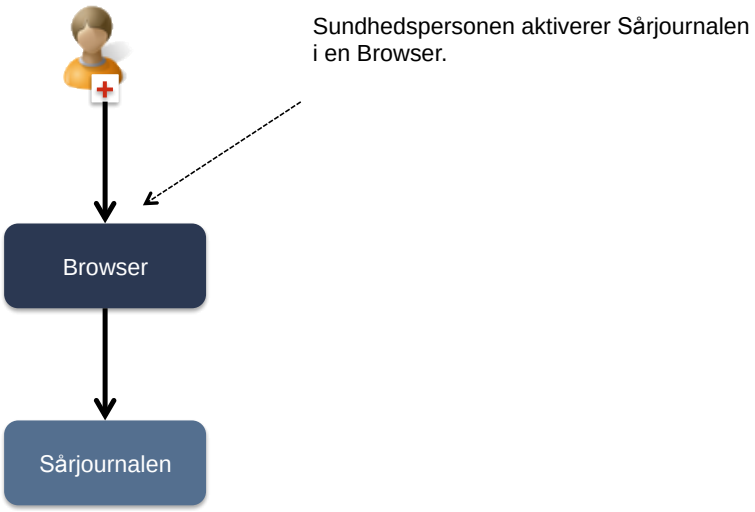
En sundhedsperson modtager et link i en korrespondancemeddelelse, der henviser til en person/registrering i Sårjournalen. Sundhedspersonen klik-

[1] Region Sjælland har erfaringer med denne type løsninger.

ker på linket, og kan gå ind og se den pågældende person/registrering uden at skulle logge på igen (hvis dette er sket tidligere).

2.3 Anvendelse af Sårjournalen i en browser

En sundhedsperson aktiverer selv en web browser og går ind i sårjournalen for at arbejde (opstart af browser uden fagsystem). Hvis brugeren allerede har været i kontakt med Sårjournalen (eller anden tjeneste, der i fremtiden er i samme 'føderation'), vil vedkommende ikke blive bedt om at logge ind igen. Vedkommende kan nu navigere rundt blandt de patienter som vedkommende har en behandlingsmæssig relation til.

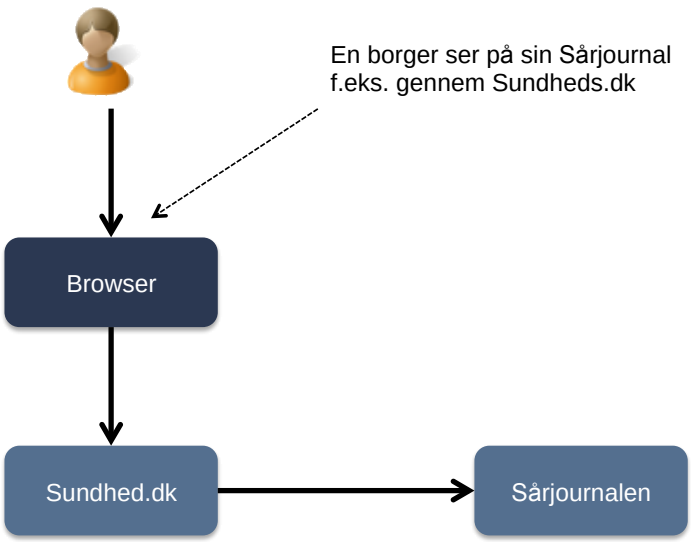


1. Anvendelse af Sårjournalen "på farten"

En sårsygeplejerske tager billeder af sår i hjemmet og uploader disse til sårjournalen sammen med en beskrivelse / andre registreringer. (Se også anvendelsesscenariet med mobile devices nedenfor).

2.4 Borgerens egen adgang

En borger ønsker selv indsigt i Sårjournalen og tager adgang til journalen f.eks. gennem Sundhed.dk. Der kan i fremtiden tænkes andre adgange til Sårjournalen, f.eks. adgang gennem særlig 'app' eller lignende.

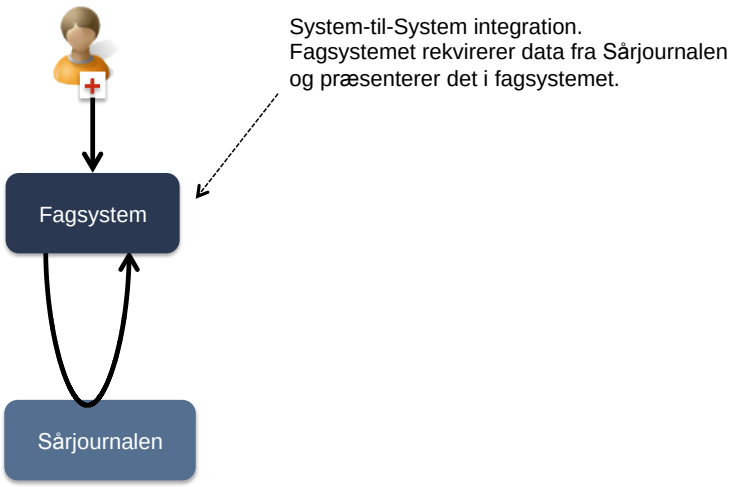


2.5 Sundhedspersoners adgang til Sårjournalen gennem mobile devices

Der er et stigende behov for at kunne anvende mobile devices (f.eks. iPad) i de sundhedsfagliges arbejdsdag. Dette kan enten være gennem et device leveret af arbejdsstedet eller ved anvendelse af eget device (”Bring your own deveice”, BYOD). Her skal det være muligt at logge på og navigere til patienten i Sårjournalen.

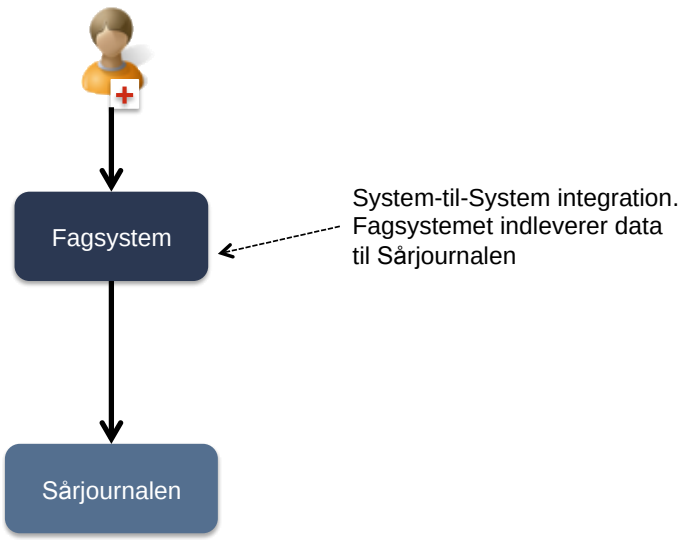
2.6 System-til-System rekvirering af Sårjournaldata

En bruger aktiverer en funktion i et fagsystem, der er integreret med Sårjournalen gennem tekniske system-til-system snitflader. Under antagelse af, at brugeren tidligere har foretaget stærk autentifikation (f.eks. ift. FMK) rekvireres data fra Sårjournalen nu på brugerens vegne uden brugeren skal logge ind eller angive patient.



2.7 System-til-System registrering i Sårjournalen

En bruger aktiverer en funktion i et fagsystem, der er integreret med Sårjournalen gennem tekniske system-til-system snitflader. Under antagelse af, at brugeren tidligere har foretaget stærk autentifikation (f.eks. ift. FMK) indleveres data til Sårjournalen nu på brugerens vegne uden at brugeren skal logge ind igen og uden at skulle genindtaste data.



Scenarium 7 og 8 er medtaget som en fremtidig mulighed for at integrere fagsystemerne tættere med Sårjournalen. Det er ikke målet for det nuværende projekt at etablere disse integrationer, og scenarierne vil ikke blive behandlet yderligere i dette notat. Det skal dog nævnes, at der allerede eksisterer en sikkerhedsmodel, som understøtter disse scenarier (samme sikkerhedsmodel, som FMK anvender).

3 Principper

Sikkerhedsmodellerne i nærværende notat baserer sig på en række principper. Principperne skaber grundlaget for sikkerhedsmodellerne og sikrer at modellerne holder sig inden for nogle fornuftige af veldefinerede rammer. Samtidig sikrer principperne at modellerne retter sig mod nogle centrale gevinster, og at nogle typiske risici imødegås. Nedenstående afsnit beskriver de principper som sikkerhedsmodellerne baseres på.

3.1 Udnyt så vidt muligt eksisterende løsninger

Det er generelt et sundt princip at genanvende eksisterende og velafprøvede løsninger og standarder. Der skal naturligvis være plads til fornyelse og modernisering, men det skal ske kontrolleret og efter grundige analyser og overvejelser. I sårjournalprojektet, hvor sikkerhedsløsninger kun udgør en del af projektet, er det endvidere vigtigt, at disse aktiviteter ikke kommer til at ”suge kræfterne ud” af alle de andre aktiviteter, der skal gennemføres i regi af projektet.

Gevinster: Ved at genanvende eksisterende løsninger minimeres omkostningerne ift. sikkerhedsløsningerne. Ved at holde sig inden for velkendte ’kompetenceområder’ skabes der endvidere generelt bedre adgang til ressourcer hos leverandører, kunder og eksperter, hvilket minimerer tids- og ressourcemæssige risici i projekterne. Endelig undgår man en række ”børnesygdomme” som erfaringsmæssigt følger med nyudviklingsprojekter.

3.2 Brugeradministration foretages i egne systemer

Parterne omkring Sårjournalen ønsker som udgangspunkt at kunne administrere brugernes adgang til og privilegier i Sårjournalen gennem egne brugerstyringssystemer. Dette kan opnås gennem etablering af føderativ adgang. Der er allerede etableret en føderativ løsning i forbindelse med PPJ løsningen, og sammenholdt med princip 1 kalder det på at genanvende denne. Tilsvarende er KOMBIT ved at opbygge en føderativ løsning for kommunerne, som skal kunne indgå i sikkerhedsmodellerne.

Gevinster: Dette princip sikrer at meromkostningerne i den daglige administration af Sårjournalen minimeres. I en fødereret løsning vil oprettelse, ændring og nedlæggelse/suspendering af brugerkonti i egne brugerrettighedssystemer automatisk give, ændre eller fjerne adgang til Sårjournalen.

3.3 Samme autentifikationssikkerhed som ved Fælles Medicinkort

Da Sårjournalen kan indeholde følsomme helbredsinformationer er det nødvendigt at være sikker på brugerens identitet og autenticitet ved adgang til journalen. Der ønskes derfor samme autentifikationssikkerhed som Fælles Medicinkort, dvs. stærk autentifikation af brugeren, enekontrol over ak-

kreditiver (certifikat og kodeord) mm.. For nuværende[2] er det kun den såkaldte SOSI-STS og NemID der har den fornødne egenskaber i identifikations- og udstedelsesprocedurerne og i de tekniske akkreditiver til at kunne sikre stærk autentifikation.

Gevinster: Det er vigtigt at bevare samfundets/borgernes tillid til fælles systemer. Mister vi denne tillid kan det skabe et meget vanskelligt klima, hvor nogle af de centrale gevinster ved sikker deling af data på tværs af sundhedsdomænet bliver vanskellige at etablere. Den foreslåede løsning forbedrer sikkerheden i sårjournalen på nogle kritiske punkter, bl.a. i forhold til links i korrespondancebeskeder og i forhold til adgangen via Internet.

3.4 Skab bedre sammenhæng mellem systemer

Gennem en fokuseret indsats er udfordringerne omkring sundhedspersoners mange logins og genindtastninger nu på vej til at blive reduceret. Dette projekt medvirker til denne tendens ved at sikre gode integrationsmuligheder, hvor det f.eks. bliver muligt at logge ind på Sårjournalen gennem eget fagsystem. Hvis der allerede er foretaget stærk autentifikation tidligere (f.eks. fordi at brugeren har haft adgang til FMK), bør denne autentifikation kunne genanvendes og give adgang til Sårjournalen.

3.5 Tænk fremad så kommende løsninger får gavn af indsatsen

Princip 1 sikrer at vi optimerer tidligere projekters investeringer. På samme måde bør man forsøge at sikre at eventuelle nyskabelser i dette projekt peger i en retning, som formodes at komme fremtidige initiativer til gode.

3.6 Løsningen må ikke være unødigt svær at administrere

Sikkerhedsløsningen for Sårjournalen må ikke være unødig svær at administrere. F.eks. er der en vis dynamik i sundhedsvæsenets organisering og det må forventes at de forskellige dele af væsenet vil blive klar til føderering i lidt forskellige tempi. En løsning, hvor alle kommuners og regioners IdP/STS-certifikater skal håndteres (også ift. fornyelse etc.) vil derfor ikke være ønskelig.

3.7 Følg referencearkitekturer og øvrige analyser

Sikkerhedsløsningen for Sårjournalen skal følge den vedtagne referencearkitektur for informationssikkerhed [REFARK_SIK] og følge de analyseresultater og anbefalinger der fremkom som resultat af initiativ 3.4 i digitaliseringsstrategien for sundhedsvæsenet 2013-2017 vedrørende sikkerhedsstandarder og –løsninger [ANALYSE_SIKKERHED]. Samlet peger disse på yderligere føderering af systemer i sundhedsdomænet og på tværs af domæner.

[2] Anvendelse af lokale akkreditiver (f.eks. login gennem AD med token eller smartcard) kan etableres senere, men vil kræve at der er oprettet et såkaldt trust rammeværk mellem parterne. Trust rammeværket skal sikrer samme sikkerhed i indrullerings- og anvendelsesprocedurer som NemID.

4 Sikkerhedsmodeller

Nærværende kapitel giver et overblik over de sikkerhedsmodeller, der er i spil i forhold til Sårjournalen. Der er *ikke* tale om gensidigt udelukkende modeller, men nærmere om et katalog af mulige sikkerhedsmodeller, som kan bringes i anvendes i forskellige sammenhænge. Modellerne illustreres i deres anvendelse fra en regional, kommunal og privat sammenhæng (LPS hhv. borger).

4.1 Arkitektoniske præmisser, valg og fravalg

Modellerne i dette kapitel forsøger i videst mulig omfang at imødekomme de ovennævnte principper, men derudover er der en række andre arkitektoniske præmisser og valg, der er vigtige at kende inden modellerne gennemgås:

Den nationale infrastruktur binder op til fællesregional- og fælles kommunal infrastruktur
Infrastrukturen udnytter således at regioner og kommuner selv har skabt (eller er ved at skabe) en sammenhængende sikkerhedsinfrastruktur mellem de enkelte regioner eller kommuner. Den nationale infrastruktur har tillid til disse.

Dermed skabes ikke stærke bindinger mellem den nationale infrastruktur og de enkelte regioner og kommuner) og den administrative opgave med vedligeholde tillidsrelationer (herunder håndtering af certifikater) og omveksle sikkerhedsbilletter (security tokens) mellem individuelle formater minimeres.

Denne beslutning har administrative fordele men kan have robustheds-mæssige ulemper, idet robustheden af den nationale infrastruktur for brugere i en region eller kommune ikke kun afhænger af den lokale og den nationale infrastruktur, men også af den fællesregionale hhv. fælleskommunale infrastruktur.

OIOSAML (OIO imellem føderationer)
I forbindelse med initiativ 3.4 vedr. analyse af sikkerhedsstandarder og –løsninger blev det anbefalet at al kommunikation mellem føderationer bør ske på baggrund af fællesoffentlige standarder (OIO-*). Derfor vil tokenformater mv. holde sig til disse standarder i nedennævnte modeller.

Ikke flere udvidelser af SOSI-STS
NSI er blevet frarådet at fortage udvidelser af den nuværende SOSI-STS for at imødekomme login til nationale browserbaserede tjenester. Der findes flere COTS produkter, der kan anvendes til dette.

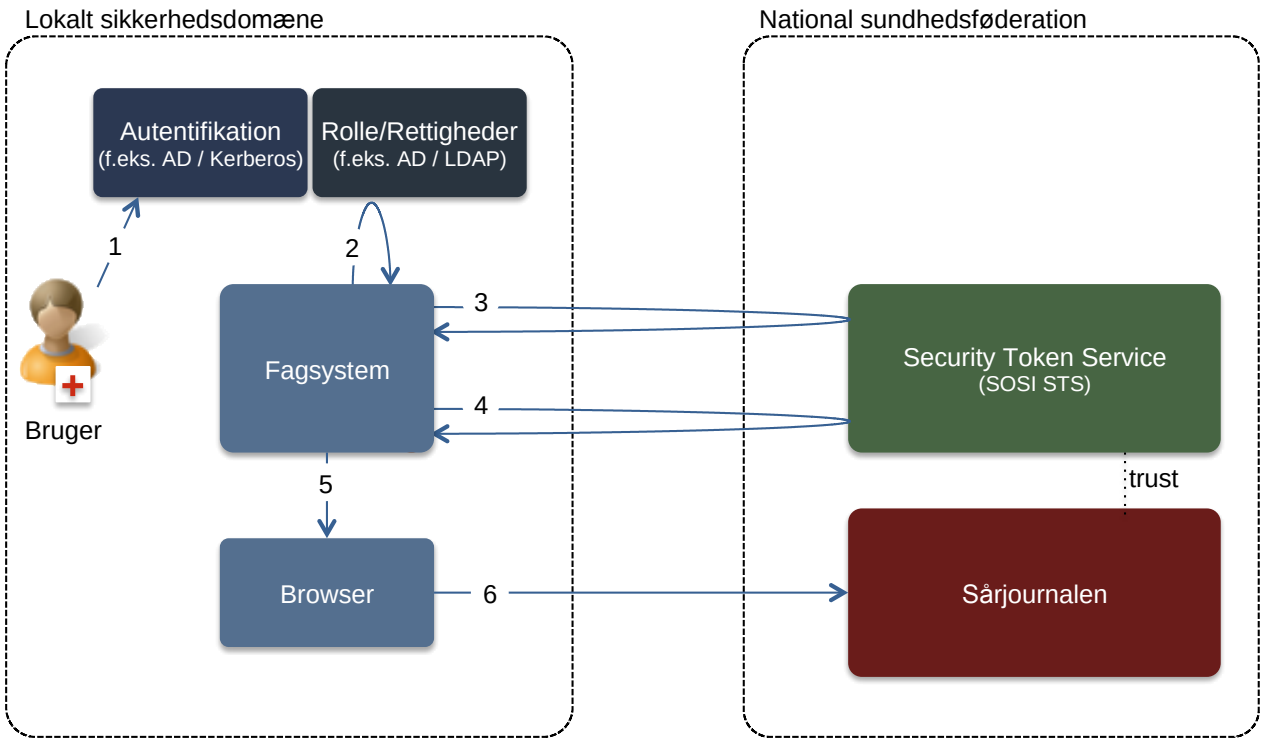
Midlertidig accept af lille risiko for kompromittering af føderationscertifikater
I den nuværende sikkerhedsinfrastruktur i sundhedsvæsenet er føderationsnøglerne (dem der anvendes til underskrift af tokens fra SOSI-STS) ganske godt beskyttet gennem hardwarebeskyttede sikkerhedsmoduler (Hardware Security Modules, HSM), videoovervågning og fastlagte administrationsprocedurer. Øvrige parter vil sandsynligvis ikke opnå samme sik-

kerhed fra begyndelsen. Denne risiko vælger NSI at acceptere i første omgang.

Flere SAML assertions ikke understøttet af standardprodukter.
I nogle af modellerne ville det være optimalt at parterne kunne udstede forskellige SAML assertions med deres egen signatur for de dele af sikkerhedsinformationerne som parten er autoritet for. På trods af at dette er understøttet af SAML standarden, understøttes det typisk ikke af COTS produkter, hvorfor modellerne ikke opererer med flere assertions.

4.2 Aktiv SAML login model – Sikker Browseropstart

I forbindelse med blandt andet e-Journal og Sundhedsjournalen blev der etableret en mulighed for at genanvende et tidligere afgivet "log-in" til at skabe Single Sign-On mellem fagsystemer og browserløsninger. I regionerne kendes denne løsning også som "knapløsningen" eller "sikker browseropstart".
I denne sikkerhedsmodel oplever brugeren, at når der trykkes på en knap i et fagsystem (typisk et EPJ system) startes der en browser (eller en indlejret browserkomponent), hvor brugeren automatisk er logget ind. I protokollen overføres også de nødvendige kontekstinformationer (f.eks. patient) og evt. rolle/rettighedsinformationer fra den lokale kontekst.
Scenariet er kendt som et "aktivt" scenarie fra SAML profilerne, idet klienten (*user agent*) aktivt autentificerer sig *inden* serviceudbyderen kontaktes, i modsætning til det passive scenarie, hvor en browser blot kontakter en serviceudbyder, og hvor serviceudbyderen så må sikre at brugeren bliver passende autentificeret (typisk gennem redirigering til en IdP/STS).
Flowet i den eksisterende løsning er illustreret i nedenstående Figur 1 og er ens uanset hvilken sammenhæng der er tale om (regional f.eks. EPJ, kommunal f.eks. EOJ, privat f.eks. LPS). Modellen gælder dog kun professionelle brugere og kræver at man kan få adgang til den nationale STS, hvilket alene kan ske via sundhedsdatanettet.



Figur 1 - Sikker Browseropstart. Løsningen eksisterer i dag som en del af den nationale service platform.

Skridt:

1. Brugeren autentificeres i det lokale sikkerhedsdomæne (f.eks. Kerberos / LDAP / AD). Dette kan ske ved login på brugerens digitale arbejdsplads eller ved login til fagapplikationen.
2. Brugeren kontrolleres for de nødvendige privilegier ift. at kunne aktivere "knappen". Evt. rollenavne eller lignende ift. sårjournalen rekvireres fra den lokale brugerstyringsløsning.
3. Hvis ikke brugeren allerede har et SOSI id-kort (token udstedt af SOSI STS'en, som f.eks. anvendes i FMK), skal dette udstedes inden sikker browseropstartsprocessen kan fortsætte. Dette vil pt. kræve at brugeren autentificeres med sin medarbejder NemID, dvs. stærk autentifikation på NIST niveau 3. STS'en kontrollerer det fremsendte autentifikationsbevis og udsteder et SOSI id-kort signeret af STS'en.
4. Fagsystemet rekvirerer et SAML token, som skal anvendes til autentifikation hos Sårjournalen. SOSI id-kortet medsendes i dette request. SOSI STS'en returnerer et token, der overholder OIOSAML standarden) hvori SOSI id-kortet *kan* indlejres (afhængig af aftale ift. den konkrete service, her Sårjournalen). Det udstedte SAML token bliver krypteret under Sårjournalens offentlige nøgle, så tokenet (og det evt. indlejrede SOSI id-kort) kun er læsbart af Sårjournalen.
5. Det rekvirerede token indlejres i et stykke HTML (med et såkaldt post-redirect kald) og en browser åbnes til at vise dette HTML.
6. Browseren redirigeres til Sårjournalen som modtager det indlejrede token. Sårjournalen ser dette som en del af en **standard SAML protokol** (såkaldt *unsolicited IdP response*), og kan nu etablere en session med brugeren.

Sårjournalen har nu "logget" brugeren ind, på baggrund af det kryptografisk sikrede informationer om brugeren (navn, CPR, evt. sundhedsfaglig autorisation) og et 'bevis' på at vedkommende er stærkt autentificeret. Øvrige kontekstinformationer skal fagsystemet supplere med, herunder patientidentifikation og andre informationer, der skal anvendes til adgangskontrol, kontrol af behandlingsrelation, samtykkekontrol etc. Disse vil i den nuværende/kørende løsning ikke være en del af det fremsendte token, men blive suppleret som kontekstinformation ved siden af tokenet.

Dette scenarie imødekommer brugsscenarie 1. Brugsscenarie 4 og 6 (mobile devices) kan også imødekommes, men det kræver at løsningen knyttes op som klient til fagsystemet.

Gevinster:

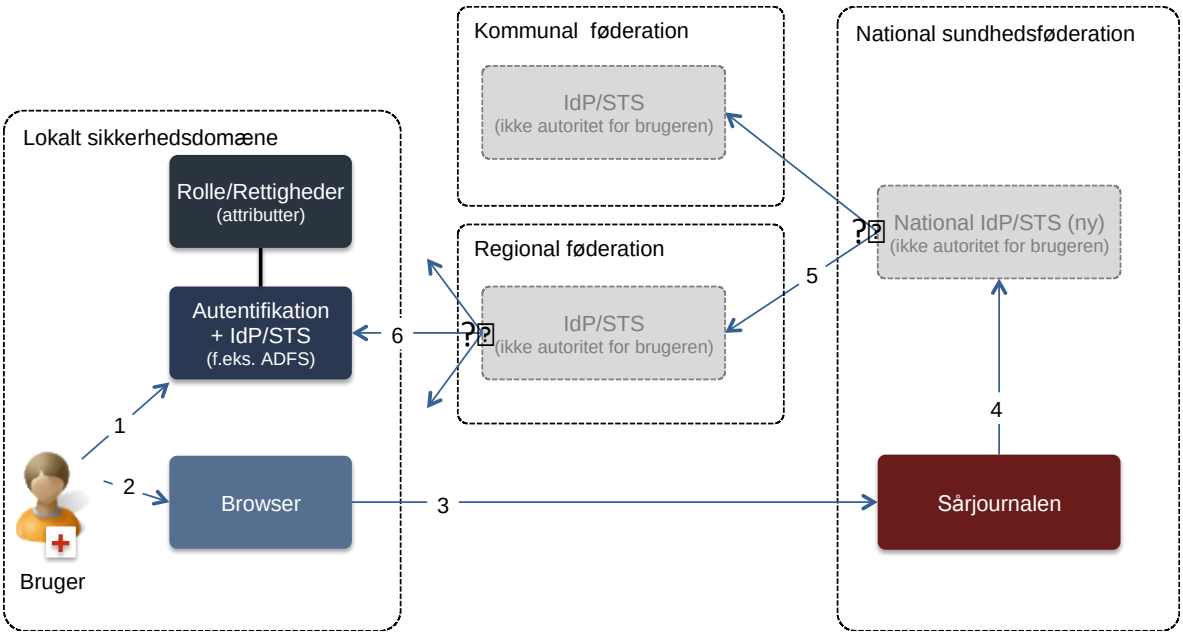
- Høj grad af genanvendelse
- Afprøvet og kørende løsning
- Relativ simpel protokol
- Baseret på internationalt anerkendte standarder
- Er i nogen grad understøttet af standardrammeværk og –løsninger
- Ingen afhængighed til eksterne (fællesoffentlige) identitetsløsninger og dermed robust ift. temporære udfald af disse.
- Robust løsning ift. regionerne idet SOSI-STS er distribueret til hver region (dNSP). Kommuner og LPS skal anvende den centrale cNSP STS.

Ulemper/Risici:

- Kontekstinformation skal suppleres af fagsystemet og er pt. ikke standardiseret.
- Selve opstartsfunktionaliteten (opstart af browseren vha. post-redirect) kan være kompleks i visse sammenhænge.
- Det kan være komplekst at lave en fagsystem-til-browser løsning, der i fornødent omfang sikrer mod visning af flere patienters data på samme tid.
- Løsningen kræver adgang til sundhedsdatanettet.

4.3 Passiv fødereret model

Denne model beskriver et klassisk SAML2 føderationsscenarium, hvor brugerens browser redirigeres til en "login kontekst", hvor brugeren har mulighed for at autentificere sig, og hvor der autoritativt kan siges noget om brugerens attributter (roller). Da Sårjournalen ikke umiddelbart kan se, hvilken organisatorisk sammenhæng (f.eks. regional / kommunal) brugeren kommer fra, vil det være nødvendigt enten at spørge brugeren (vise en HTML side med nogle valg) eller via tekniske informationer (IP range eller lignende) forsøge at gætte hvilken login-kontekst brugeren kommer fra. Hovedflowet i den påtænkte løsning er gennemgået i Figur 2.



Figur 2 - Hovedflow i et standard passivt SAML SSO login med flere føderationer og IdP/STS'er.

Skridt:

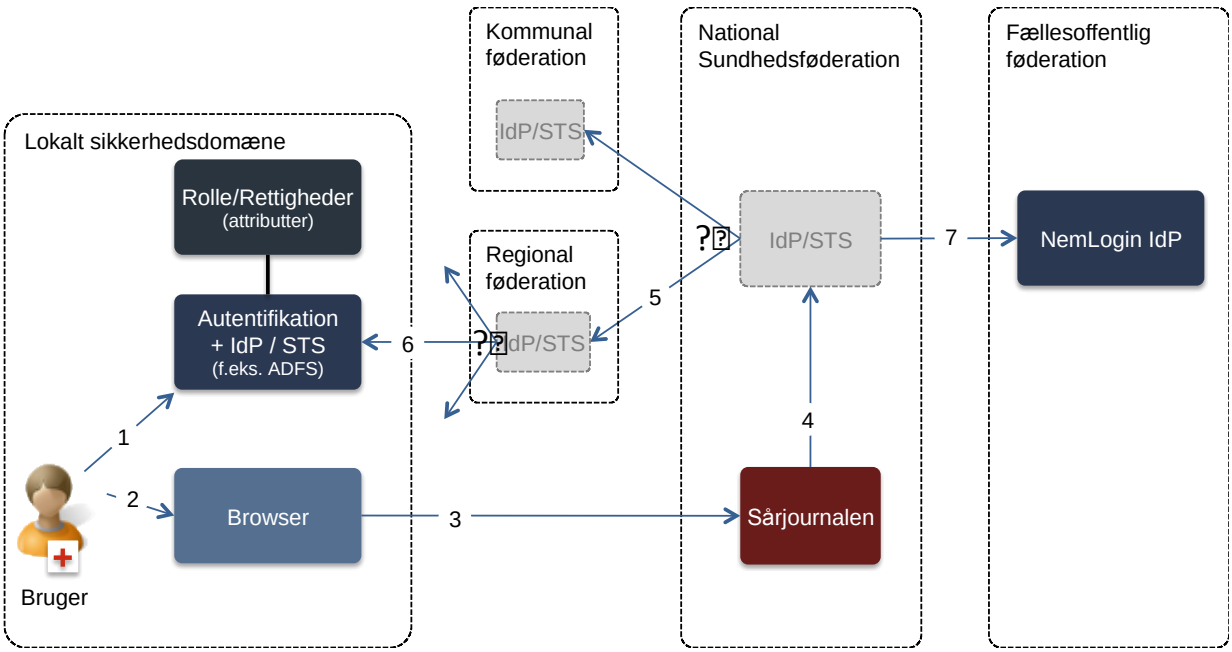
1. Brugeren autentificeres i det lokale sikkerhedsdomæne (f.eks. Kerberos / LDAP / AD). Dette kan som tidligere nævnt f.eks. ske ved login på brugerens digitale arbejdsplads eller ved login til fagapplikationen.
2. Brugeren starter en browser.
3. Brugeren indtaster sårjournalens URL i adressefeltet eller ledes dertil fra intranet eller lignende.
4. Sårjournalen redirigerer browseren til den nationale IdP/STS
5. IdP/STS'en søger at fastslå hvilken sikkerhedskontekst brugeren kommer fra (f.eks. regional eller kommunal) enten ud fra tekniske informationer (evt. URL parameter, IP adresser) eller ved at spørge brugeren. Den nationale IdP/STS redirigerer browseren til en IdP/STS for det pågældende sikkerhedsdomæne.

6. Den (i eksemplet) regionale IdP/STS vil igen forsøge at afgøre hvilket lokal sikkerhedsdomæne brugeren kommer fra og redirigere browseren til den lokale IdP/STS, der kontrollerer at brugeren er logget ind i den lokale kontekst, kontrollerer/indsamler rolleinformationer, og udsteder et SAML token med bevis for autenticitet og rollerinformationer. Browseren redirigeres tilbage til sårjournalen med det udstedte token.

I skridt 5 og 6 skifter IdP/STS'en 'rolle' og bliver klient til den næste IdP/STS i rækken. Denne funktionalitet er ikke beskrevet som en del af SAML web SSO protokollen, men er noget flere produkter understøtter. Som klient overholder IdP/STS'en dog stadig SAML standarden/protokollen.

I sin reneste form kræver ovenstående model, at hver part har etableret mulighed for stærk autentifikation og at der mellem parterne er skabt et 'trust framework' med aftaler, audit og hvad dertil hører.

I den nuværende infrastruktur er det ikke muligt at opnå stærk autentifikation hos parterne baseret på et fælles 'trust framework'. Indtil dette opnås, kan man indsætte et ekstra trin (7), hvor brugeren autentificeres hos NemLogin IdP/STS'en (hvis vedkommende ikke allerede tidligere er autentificeret) og dermed anvende OCES politikkerne og løsningerne ift. sikring af de fornødne processer etc.



Figur 3 - Samme forløb for ovenfor, men med et ekstra trin indsat til stærk autentificering af brugeren hos NemLogin IdP'en.

7. Sårjournalen redirigerer browseren til NemLgin, hvor brugeren autentificeres vha. NemID for medarbejder.

Hver IdP/STS skaber et token, der krypteres under den offentlige nøgle for den forrige IdP/STS i kæden. Når tokenet på returvejen modtages af den forrige IdP/STS dekrypteres og rekrypteres ift. den forrige IdP/STS etc. Til sidst modtages tokenet af den nationale IdP/STS, dekrypteres og kombineres med NemLogin tokenet og der udstedes et nyt token, der krypteres under sårjournalens offentlige nøgle, så det sikres at kun sårjournalen kan læse/anvende tokenet.

Det karakteristiske ved modellen er at den ”fødererer” delområderne i sundhedssektoren (nationale tjenester hhv. regionale tjenester og kommunale tjenester), og den genanvender de enkelte parters nuværende eller snart kommende føderationsløsninger. Modellen har en særlig styrke i at al sessions-kontrol (kontrol af at brugeren stadig er logget på i den pågældende parts it-infrastruktur) sker i egen infrastruktur.

Dette scenarie imødekommer brugsscenarie 2,3 og 5. Brugsscenarie 4 og 6 (mobile devices) kan også imødekommes, men det kræver at løsningen enten kommunikerer med lokal infrastruktur (herunder lokal signaturserver) eller at brugerne udstyres med centralt opbevaret NemID med nøgleviser.

Gevinster:

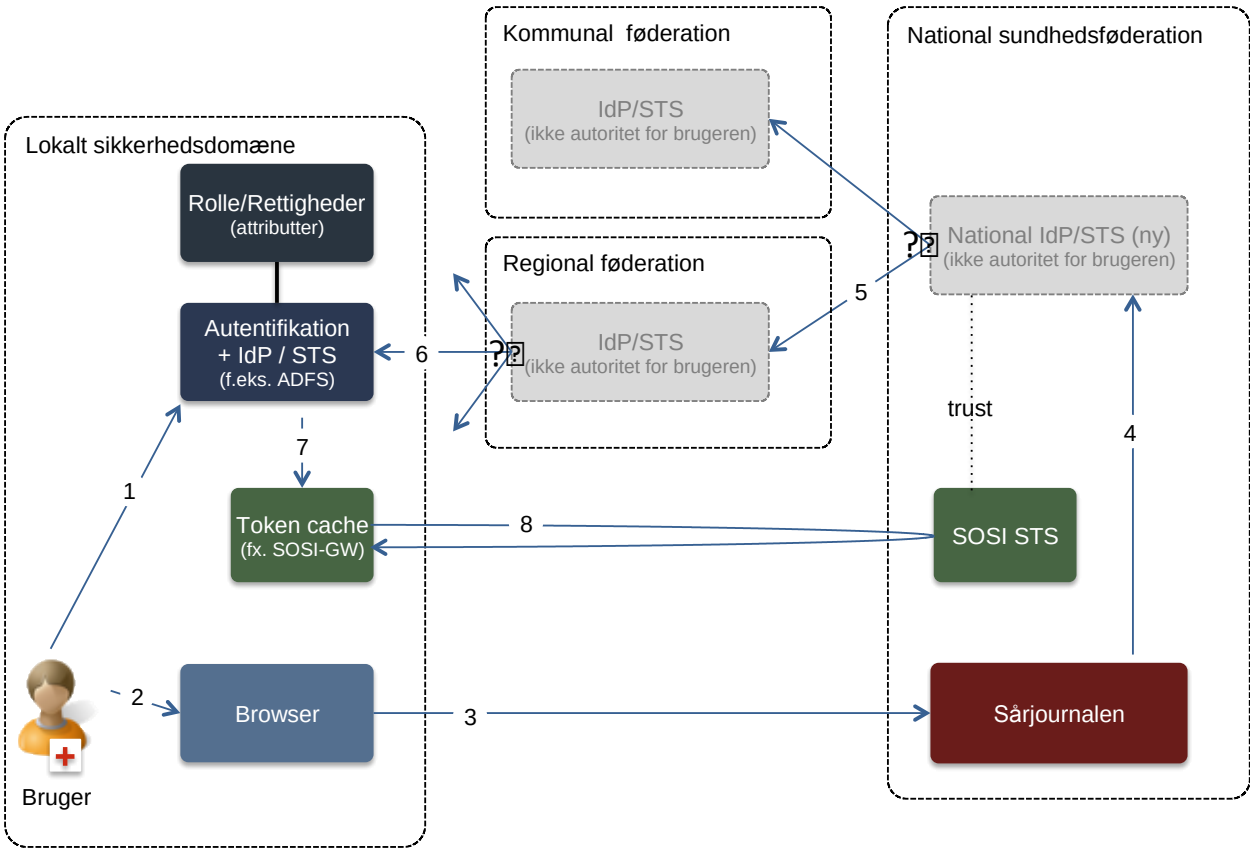
- Modellen genanvender en stor del af den eksisterende sikkerheds-infrastruktur
- Store dele af løsningen er velafprøvet
- Der skal kun ske få tilretninger i PPJ for at kunne håndtere Sårjournalens rolle/rettighedsmodel. Der forventes heller ikke store ændringer i forhold til KOMBITs løsning.
- Baseret på internationalt anerkendte standarder
- ”Klassisk” føderationsløsning mellem større parter på sundhedsområdet.
- Er i høj grad understøttet af standardrammeværk og –løsninger

Ulemper/Risici:

- Der skabes en afhængighed mellem sundhedsområdets sikkerhedsløsninger og den fællesoffentlige sikkerhedsløsning.
- Det skal sikres, at der ikke er problemer i forhold til aftaler og politikker, der er gældende for NemLogin.

4.4 Passiv model med SOSI STS til stærk autentifikation

Der er arbejdet med et alternativ til ovenstående passive model, der ikke benytter NemLogin, men i stedet den på sundhedsområdet etablerede autentifikationsmekanisme (SOSI-STS). Denne kræver langt større tilpasning af den lokale infrastruktur og den vil ikke dække borgerens adgang til sårjournalen (scenarium 5), men gennemgås for fuldstændighedens skyld nedenfor i Figur 4.



Figur 4 - Passivt login scenarie med anvendelse af SOSI-STS i stedet for NemLogin til stærk autentificering.

Skridt:

Skridt 1-6 er de samme som i ovenstående passive model.

7. Den lokale IdP/STS kontrollerer om brugeren allerede har et gyldigt SOSI-ID-kort. I regional sammenhæng kan dette kontrolleres i SOSI-GW komponenten. Har brugeren ikke det, skal brugerens browser redirigeres til en side, hvor der afgives digital signatur og der udstedes et SOSI id-kort (ny funktionalitet eller genanvendelse af eksisterende funktionalitet). Det vil kræve ny funktionalitet i de lokale IdP/STS instanser at foretage denne kontrol/nyudstedelse.
8. Den lokale IdP/STS "veksler" nu SOSI id-kortet til et OIO-SAML token, der krypteres under den nationale IdP/STS's offentlige nøgle. Dette er eksisterende funktionalitet i SOSI-STS'en.

Gevinster:

- Modellen genanvender en stor del af den eksisterende sikkerheds-infrastruktur
- Flere dele af løsningen er velafprøvet
- Uafhængighed af fællesoffentlige login tjenester

Ulemper/Risici:

- Alle lokale parter skal udvikle funktionalitet til kontrol/udstedelse af SOSI id-kort fra egen IdP/STS

Det vil være teknisk muligt at gennemføre begge passive modeller og dermed give kommuner og regioner valgfrihed i forhold til, hvordan føderationsadgang etableres. Det skal dog bemærkes at der er væsentlige udvik-

lingsaktiviteter forbundet med denne model, og der skal derfor være gode argumenter for at gå i denne retning, for at det giver mening at implementere den.

4.5 Emner der bør analyseres nærmere

Samtidig adgang til sundhedsdatanet og internet. Da en række aktører forventes at skulle have adgang til Sårjournalen, herunder private virksomheders løsninger til sundhedspersoner og borgere, skal sikkerhedsmodellen sandsynligvis kunne håndtere samtidig adgang til/fra sundhedsdatanettet og internettet. Dette er særligt en emne i forbindelse med det fødererede scenarie med anvendelse af NemLogin. Her skal kommunikationen til eksempelvis den fællesregionale IdP ske via sundhedsdatanettet mens dette ikke vil være tilfældet, når browseren redirigeres til NemLogin. Det skal analyseres nærmere om dette 'netværksskifte' kan give problemer.

Tokenformat og -indhold.
I det aktive scenarium ("sikker browseropstart") er det muligt at fremsende en relativ præcis kontekst sammen med autentifikationsbeviset (valgt patient mm.) netop fordi browsersessionen initieres fra et fagsystem. Dette er ikke muligt i det passive scenarium, hvor konteksten som hovedregel først skabes efter autentifikation.
Security tokens for begge scenarier skal beskrives og det skal tilstræbes at holde dem så ens som mulige (om muligt gerne samme format). Hvis det i det passive scenarium bliver nødvendigt at lægge flere informationer i security tokenet (eksempelvis information om samtlige sundhedsfaglige autorisationer), er der så adgang til attributservices med denne information?

Håndtering af links i det aktive login scenarium ("sikker browseropstart")
I det aktive scenarium overføres oplysninger om bruger og patientkontekst med et såkaldt http post-redirect kald. Oplysninger om patientkontekst (patient- eller kontaktID) fremgår altså ikke af browserens URL ved opstart. Det skal undersøges, om dette er et problem i forhold til understøttelse af anvendelsesscenarium 2.2 (link i korrespondancebesked).

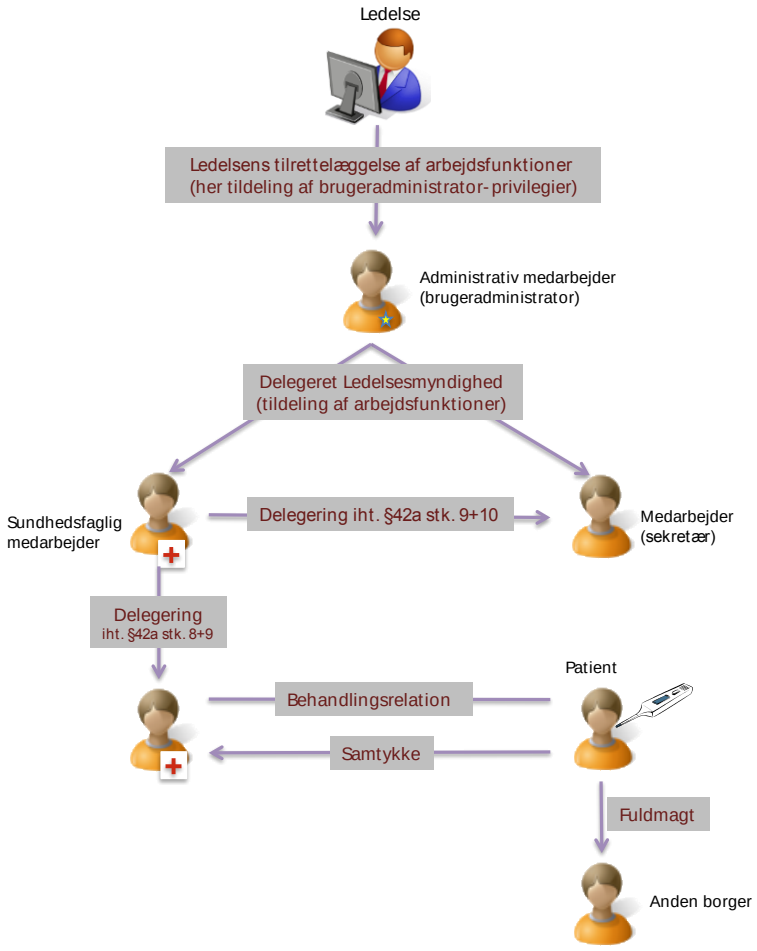
Kan modeller optimeres ved brug af SAML IdP Discovery Service Protocol?
I hvilket omfang er SAML IdP Discovery Service Protocol understøttet af markedsprodukter og kan denne protokol anvendes i de beskrevne modeller til at reducere antallet af re-directs, krypteringer og dekrypteringer samt signeringer af securitytokens? Hvilke konsekvenser vil en sådan anvendelse have ift. drift og vedligehold?

5 Andre sikkerhedsovervejelser

Ovenstående redegør for autentifikation og for dele af informationsgrundlaget for autorisation af brugere til Sårjournalen. Som national service skal Sårjournalen naturligvis overholde øvrige dele af lovgivning, bekendtgørelser og vejledninger, herunder

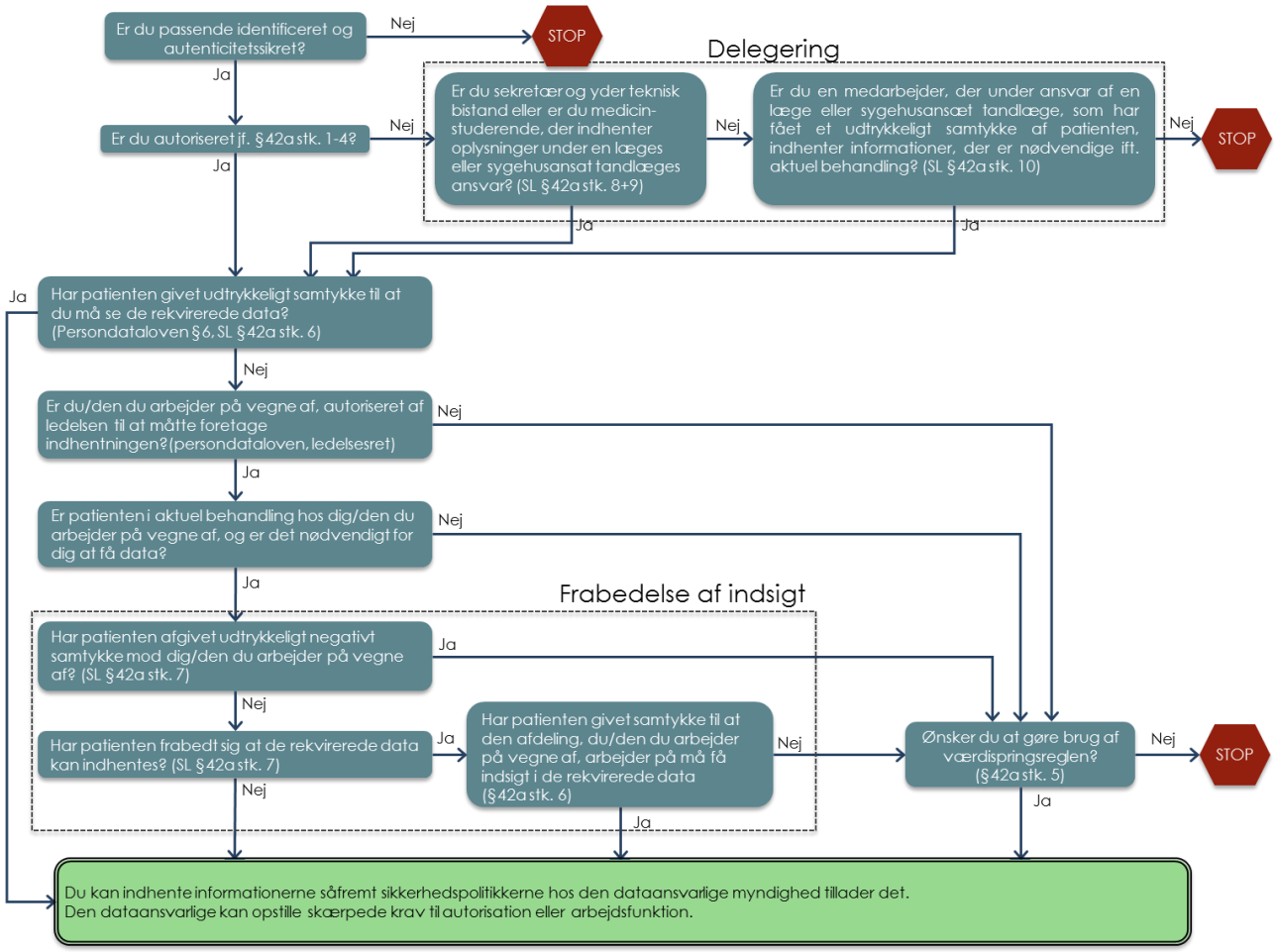
- Kontrol/Opfølgning af aktiv behandlingsrelation mellem patient og bruger
- Kontrol af evt. samtykkeforhold / frabedelse af indsigt
- Fuldmagtsrelationer mellem borgere
- Delegeringsrelationer mellem sundhedspersoner
- Håndtering af værdispring
- Orientering af borgeren gennem MinLog

Disse sikkerhedsaspekter er beskrevet nærmere i Referencearkitektur for Informationssikkerhed [REFARK-SIK], men skal kort skitseres her. De forskellige relationer og sikkerhedsbegreber er illustreret nedenfor i Figur 5.



Figur 5 - Øvrige sikkerhedsaspekter og sikkerhedsrelaterede relationer mellem personer.

I nedenstående Figur 6 ses en 'beslutningsgraf' for Sundhedslovens §42a, som kan anvendes ift. designet af den tekniske sikring af digitale tjenester i sundhedsvæsenet.



Figur 6 - 'Beslutningsgraf' for Sundhedslovens §42a vedrørende sundhedspersoners indhentning af helbredsinformation.

Sårjournalen håndterer i dag flere af disse aspekter på sin egen måde (f.eks. sikres behandlingsrelation gennem oprettelse af grupper af patienter) og på et eget niveau.

Det kan på længere sigt overvejes, om Sårjournalen med fordel kunne tilrettes nationale og fællesoffentlige tjenester, der kan foretage forskellige kontroller i forbindelse med adgang til Sårjournalen.

6 Referencer

[ANALYSE-SIKKERHED]	”Fællesoffentlige brugerstyringsløsninger - en analyse af sikkerhedsstandarder og –løsninger”, v.0.9, NSI, 30. september 2014. Denne analyse vil snart være at finde i version 1.0 (ny forside) på SSI’s hjemmeside. Indtil da kan version 0.9 udleveres ved henvendelse til NSI.
[REFARK-SIK]	Referencearkitektur for informationssikkerhed, NSI, 2013, http://www.ssi.dk/~/media/Indhold/DK%20-%20dansk/Sundhedsdata%20og%20it/NationalSundheds-It/Standardisering/Referencearkitektur%20for%20informationssikkerhed%20v%20%201%200%20nyt%20layout.ashx