NTNU
Det skapende universitet

Elektronisk tilgang på tvers for klinisk informasjon i spesialisthelsetjenesten - Forslag til arkitektur

- Forslag til arkitektur

Erland Mathias Strømmen

Helseinformatikk
Innlevert: august 2013
Hovedveileder: Pieter Jelle Toussaint, IDI
Medveileder: Trond Elde, DIPS

Norges teknisk-naturvitenskapelige universitet
Institutt for datateknikk og informasjonsvitenskap

Elektronisk tilgang på tvers for klinisk informasjon i spesialisthelsetjenesten

- Forslag til arkitektur

Erland Mathias Strømmen

Innhold

1 Introduksjon

Behovet for elektronisk tilgang på tvers av organisasjoner og omsorgsnivåer i helsetjenesten kommer som et resultat av samfunnsutviklingen der pasienter i voksende omfang vandrer mellom omsorgsnivåer, fritt sykehusvalg i tillegg til økt spesialisering der helsepersonell ansatt i flere virksomheter deltar i behandlingen.

Elektronisk samhandling er beskrevet i St. m. nr. 47, s. 13 som: "..*Samhandling er uttrykk for helse- og omsorgstjenestenes evne til oppgavefordeling seg imellom for å nå et felles, omforent mål, samt evnen til å gjennomføre oppgavene på en rasjonell og koordinert måte..*".

Helsetjenesten er informasjonsintensiv bestående av store mengder informasjon som har krav og god kvalitet og tilgjengelighet. Mesteparten av all helseinformasjon er sensitiv, lovverket er omfattende men i konstant endring for å møte kravene. I tillegg er det mange aktører involvert i samhandlingskjeden. Figur 2 illustrerer den eksterne samhandlingen:

Figur 1. Ekstern samhandling mellom omsorgsnivå i helsetjenesten (*A, Grimsmo, Veien frem til samarbeid og samhandling i praksis* [55]).

Det har skjedd en kraftig utvikling innen IKT i helsesektoren de siste ti årene. Digitalisering av pasientjournaler fra papir, røntgeninformasjonssystemer og andre kliniske fagsystemer er eksempler på dette. Likevel ligger helsesektoren etter i forhold til mange andre sektorer og bransjer.

En god del forskning og forslag har blitt gjort for å utarbeide modeller som kommunikasjon og utveksling av informasjon mellom enheter i helsetjenesten både i Norge og utenlands. Det finnes derimot lite forskningsmateriale rundt tilgangskontroll for å dekke norske juridiske føringer for denne typen informasjonsutveksling. Denne oppgaven skal utarbeide en modell for dette med det viktigste kliniske informasjonssystemet, nemlig elektronisk pasientjournal (EPJ) som utgangspunkt. Mer konkret:

"*Hvilke informasjonselementer må forstås for å kunne foreta autentisering og autorisasjon for tilgang etter klinisk informasjon på tvers av juridiske virksomhetsgrenser i spesialisthelsetjenesten slik at Helseinformasjonssikkerhetsforskriftens oppfylles?"*

Oppgaven avgrenser seg til kun å omhandle tilgangskontroll og ikke sporing og hendelseslogging.

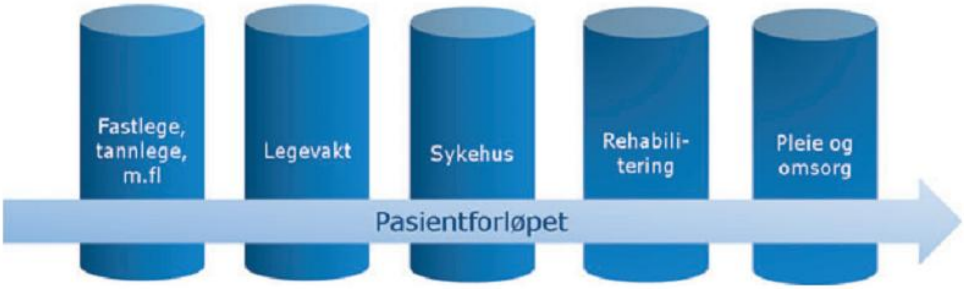
2 Bakgrunn og motivasjon

2.1 Helhetlige pasientforløp

"*De gode helhetlige pasientforløp skal i større grad enn i dag bli en felles referanse for alle aktører i helse- og omsorgstjenestene. Hva som er gode pasientforløp vil avhenge av status og utvikling av teknologi og metoder innenfor medisin og helsefag*"

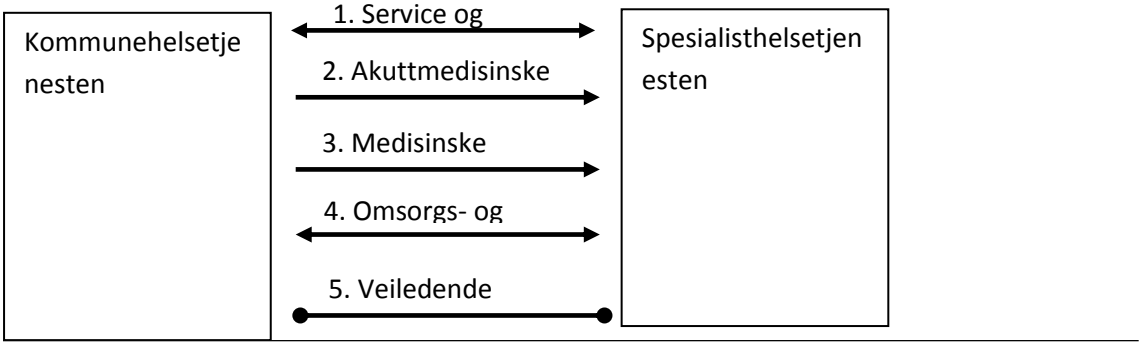
(St. m. nr. 47, s. 15).

Et av de grunnleggende kravene i de ulike nasjonale føringene er å kunne støtte et helhetlig pasientforløp både internt og på tvers av omsorgsnivå og IKT-systemer.



Figur 2 Logisk illustrasjon av helhetlig pasientforløp *(Tjenesteorientert arkitektur i spesialisthelsetjenesten[32])*

Som et verktøy for å beskrive samhandlingskjedene i helsetjenesten kan pasientforløpet benyttes som en grunnleggende verdikjede[31]:



Figur 3 Medisinske samhandlingskjeder mellom kommune og spesialisthelsetjenesten, (Elektronisk *samhandling i helse- og omsorgssektoren, Hygen, Heimly, Landsem(2009)).*

1. **Service og- støttetjenestene** beskriver kommunikasjonen mellom kommunehelsetjenesten og spesialisthelsetjenesten knyttet til service og støttefunksjoner. Eksempler kan være laboratorieprøver og syketransport der spesialisthelsetjenesten er tjenesteleverandør, men der behandlingsansvaret er tydelig forankret i kommunehelsetjenesten.

2. **Den akuttmedisinske kjeden** omfatter legevakten i kommunene, ambulansene og akuttmottak i sykehusene. AMK og de lokale legevaktsentralene utgjør kommunikasjonsberedskapen.

3. **Den medisinske samhandlingskjeden** gjelder kommunikasjon mellom leger i kommunehelsetjenesten og spesialisthelsetjenesten. Dette gjelder henvisning til videre undersøkelse og behandling i spesialisthelsetjenesten og epikrise (tilbakemelding om undersøkelse og behandling etter opphold i spesialisthelsetjenesten).

4. **Den omsorgsmessige samhandlingskjeden** er knyttet til samspillet mellom sykehus og kommuner ved utskrivning av pasienter som har behov for rehabilitering og omsorgstjenester. For disse pasientene er tilgang til og tilpassede pleie- og omsorgstjenester i kommunen en forutsetning for at pasienten kan avslutte oppholdet i sykehuset.

5. **Den veiledende samhandlingen** gjelder oppfølging av alvorlig syke pasienter som er overført til kommunehelsetjenesten. Det er pasienter som samtidig har behov for jevnlig oppfølging av spesialisthelsetjenesten eller som ønsker å være hjemme i en sluttfase av livet.

2.2 IKT i helsesektoren – kartlegging av dagens situasjon

Som en indikator i forhold til innføring og bruk av IKT i helsesektoren utførte HIMMS i 2011 en undersøkelse der 293 europeiske sykehus deltok som målte modenheten i bruk av IKT[29]. Skalaen som går fra 0 som dårligste til 7 som beste score viste at de fleste av helseforetakene i Helse-Sør-Øst ligger på nivå 2. Kun 80 sykehus internasjonalt har en score på 7. Nasjonale og regionale føringer for å øke innføring og bruk av IKT i helsesektoren ble nevnt innledningsvis og felles for alle er at de peker bl.a. på samhandling mellom systemer både innenfor og mellom omsorgsnivå som et viktig innsatspunkt.

Samspill 2.0 sitt innsatsområde 1 “Nasjonalt meldingsløft” har bidratt til en styrket samhandling basert på meldinger. En rapport fra 2009 viser graden av forutsetninger for IT-støttet samhandling mellom de ulike samhandlingskjedene[31]. Figur 4 viser graden av samhandling mellom de ulike samhandlingskjedene. Merk at her er det listet opp tre ekstra samhandlingskjeder utover de fem som nevnes senere i dette kapittelet.

Sam-handlings-kjede/ Aktør	Medisinsk sam-handling	Omsorgs-kjede	Vei-ledende (shared care)	Akutt-medisin	Service og støtte (eks. lab)	Fore-byggende	Trygde-medisinsk sam-handling	Punkt-kontakt Pasien/ lege eller tannlege
Pasient	1	1	1	1		1	1-2	1-2
Kommunal omsorgstj.	3	3	1-2					
Fastlege	2-3	3	1-2	1-2	3	1-2	3	1-2
Legevakt				1-2				
Helse-stasjon	1-2					1-2		
Sykehus	2	2	1-2	1-2	3	1-2	2	
Avtale-spesialis-ter	2-3		1-2	1-2	2	1-2	3	
Apotek/ Bandasjist	1	1			1		2	
Tannhelse								1
NAV							3	
Hab/ rehab	1-2	1-2	1					
Lab/ Røntgen	3				3			
Ambulanse (bil/båt/luft)				1				
Arbeids-giver							1	

Figur 4: Grad av samhandling mellom de enkelte samhandlingskjedene.

	Lite aktuell
1	Det mangler standarder for viktig kommunikasjon. Få samhandlingsløsninger er implementert.
2	De mest sentrale standarder finnes. Få samhandlingsløsninger er implementert.
3	De mest sentrale standarder finnes og flere samhandlingsløsninger basert på standardene er implementert.
4	Sertifiserte og standardisert kommunikasjon er implementert i de mest aktuelle fagsystemer

Figur 5: Vektingstabell.

2.3 Nasjonale satsingsområder

En rekke Nasjonale satsingsområder har som formål å øke og forbedre helsetjenesten, herunder også elektronisk samhandling:

- Samspill 2.0[1] med sitt innsatsområde 5: *"Tilgang til pasient-informasjon – kjernejournal, tilgang på tvers av virksomheter m.m.*"

- Samhandlingsreformen[2] trådte i kraft 1. januar 2012 og har som mål å få et bedre og mer helhetlig helsetilbud i tillegg til å håndtere fremtidens helseutfordringer ved å forebygge sykdom og gi pasientene bedre tilbud der de bor. Samfunnsøkonomisk skal dette gi store gevinster også ved å redusere antall liggedøgn på sykehus.

- Etablering av nasjonal kjernejournal[3] som har som mål å gjøre viktige helseopplysninger tilgjengelig for behandlende personell.

- St. meld. 9 (2012-2013) "Én innbygger – én journal"[4], har som mål å gjøre klinisk informasjon tilgjengelig uavhengig av sted og omsorgsnivå. Dette vil sette nye krav til dagens EPJ-plattform med tanke på interoperabilitet, identitets og- tilgangsstyring og endring av ytterligere lovverk.

- Helseinformasjonssikkerhetsforskriften[5] kom i 2011 (ikke trådt i kraft) som et behov for å fjerne regelverksmessige hindre for effektiv og trygg kommunikasjon av helseopplysninger i helsetjenesten, samtidig som pasientens rett til konfidensialitet og vern om personlige integritet ivaretas. Med denne forskriften vil det være mulig å utføre tilgang på tvers av virksomheter i helsetjenesten. Forskriften kom på bakgrunn av Odelstingsproposisjon 51, "Om lov og endringer i helseregisterloven og helsepersonelloven" (2008). Bakgrunnen for denne var å tilrettelegge juridiske elementer for å kunne realisere elektronisk tilgang og etablering av behandlingsrettede helseregistre på tvers av virksomhetsgrenser. Dette innebar endringer i helseregisterloven og helsepersonelloven. Endringene medførte nye eller endrede bestemmelser i helseregisterloven §§ 6a, 6b og 13, med tilhørende forskriftshjemler.

Helseinformasjonssikkerhetsforskriftens gjelder for alle typer behandlingsrettede helseregistre, ikke bare registre som inneholder opplysninger som inngår i de elektroniske pasientjournalene (ofte kalt EPJ) eller pasientadministrative systemene (PAS) i primær- og spesialisthelsetjenesten. For å gi et bilde av interessenter som har behov for tilgang på tvers viser tabellen under tall fra Nasjonalt senter for samhandling og telemedisin (NST) [6]som viser antall forespørsler om tilgang til pasientjournaler fordelt på organisasjon:

Organisasjon	Estimat årlige forespørsler om tilgang nasjonalt
Norsk Pasientskadeerstatning	32 000
Forsikringsselskap	22 000
Spesialisthelsetjenesten	20 000
Pasienten	9000
Primærhelsetjenesten	8000
Pasientens advokat	5000
Helsetilsynet	4000
NAV	4000
Privat helsetjeneste	4000
Pasientombud	2000
Pårørende	1000
Statens pensjonskasse	1000
Utenlandsk helsetjeneste	500
Rettsvesen	500
Barnevernet	500
Politiet	500
Asylmottak	200
Arbeidsmiljøinstituttet	200
Totalt	**100 000**

Figur 6: Interessenter for tilgang til pasientjournal.

Med et stort antall interessenter som allerede i dag genererer 100 000 forespørsler om innsyn i pasientjournal vil det med dagens trend i distribuert behandlingskjede bety at antallet vil øke for hvert år. Dette betyr at det er et behov for en enhetlig tilnærming til teknisk arkitektur på IT-siden for å kunne støtte oppunder de nye kravene for elektronisk tilgang på tvers.

Helseinformasjonssikkerhetsforskriften sier eksplisitt i § 10 *"Retten til tilgang til helseopplysninger skal følge av en konkret beslutning om å yte helsehjelp til pasienten og være tilpasset pasientens behov for helsehjelp. Beslutningen skal dokumenteres."* Dette bringer inn elementet "beslutningsstyrt tilgang" inn informasjonssikkerhetskonteksten utover vanlig autentisering og autorisering som skal ligge til grunn for enhver tilgang til pasientinformasjon som benyttes i dag ved intern tilgang.

Beslutningsstyrt tilgang er beskrevet i KITH EPJ-standarden del 2[8]: *"… sikre at helsepersonell med legitimt behov får tilgang til nødvendige helseopplysninger, samtidig som de blir nektet tilgang til andre helseopplysninger…".*

§ 11 åpner for "*Avtale om lesetilgang på tvers av virksomheter"*. Databehandlingsansvarlige ved virksomheten kan inngå avtale med annen virksomhet om lesetilgang til strukturerte helseopplysninger i behandlingsrettet register som virksomheten er ansvarlig for dersom[5]:

a) formålet med tilgangen er å yte helsehjelp til pasient

b) begge virksomheter har tekniske løsninger som kan avgrense tilgangen til å omfatte strukturerte helseopplysninger knyttet til en navngitt pasient

c) gjennomføringen ikke svekker informasjonssikkerheten ved behandling av helseopplysninger ved noen av virksomhetene

d) begge parter i avtalen kjenner den andre partens sikkerhetsmål og sikkerhetsstrategi.

Avtalen skal angi

a) typer helsehjelp avtalen gjelder

b) de tekniske løsningene som skal benyttes ved tilgangen

c) eventuelt andre vilkår for tilgangen.

Beslutningen om helsehjelp må også foreligge i tilgang på tvers. Dette setter enda et nytt krav til både informasjonsarkitekturen i form av hvilke type informasjon som må utveksles i autorisasjonsøyemed i tillegg til den tekniske arkitekturen.

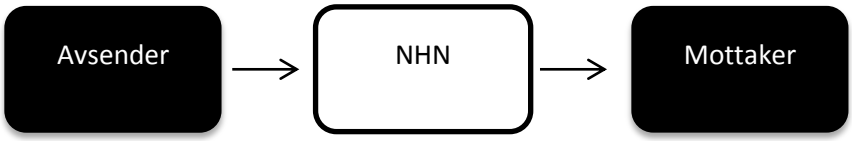
2.4 Teknologiske føringer

2.4.1 Dagens situasjon - meldinger/asynkron kommunikasjon

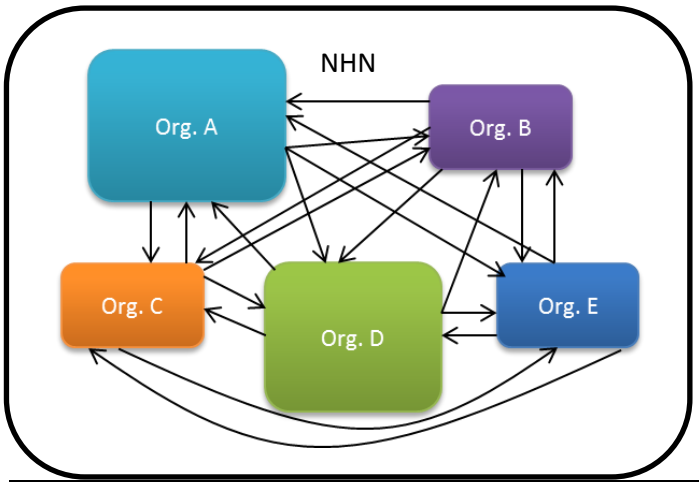
Generelt finnes det to typer av elektronisk kommunikasjon:

- Asynkron kommunikasjon – krever *ikke* at kommunikasjonspartnerne er tilgjengelig til samme tid. Eksempler på dette er epost og køsystemer.
- Synkron kommunikasjon – krever at kommunikasjonspartnerne er tilgjengelig til samme tid. Eksempler på dette er TCP og HTTP.

Utvekslingen av informasjon i helsevesenet baserer seg på meldinger i en asynkron modell. Det viktigste ved denne modellen er at informasjonen sendes til mottaker via en SMTP-postkasse i Norsk Helsenett som vist i figur 7. Et eksempel kan være henvisning fra fastlege til spesialist på sykehus og epikrise som sendes som svar etter at pasienten er behandlet. Dette har stor betydning for juridiske aspekter ved at tilgangskontroll for informasjon ikke er nødvendig fordi informasjon *sendes* til mottaker (Helseregisterloven § - 13 tilgang eller utlevering av helseopplysninger). Meldingsbasert utveksling av informasjon i helsevesenet er en gammel modell som over tid har blitt komplekst med tette koblinger. Den gir heller ingen mulighet for synkrone spørringer mot kliniske data, eksempelvis EPJ. Figur 8 viser kompleksiteten ved elektronisk meldingsutveksling.



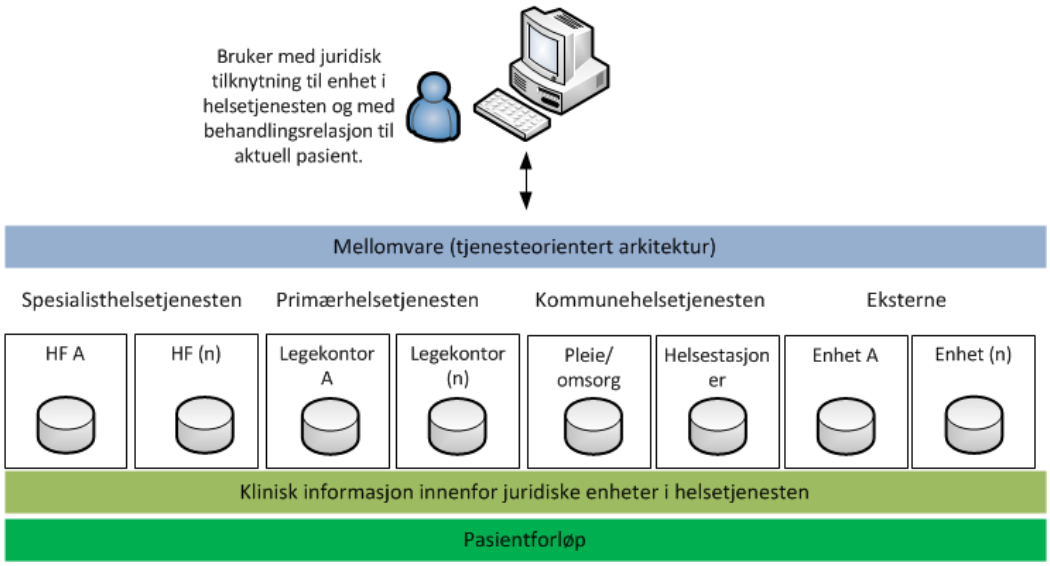
Figur 7. Tradisjonell asynkron meldingsutveksling via Norsk helsenett. Avsender sender melding til mottaker via email protokoll (SMTP). Meldingen hentes av mottaker via email klient (POP3).



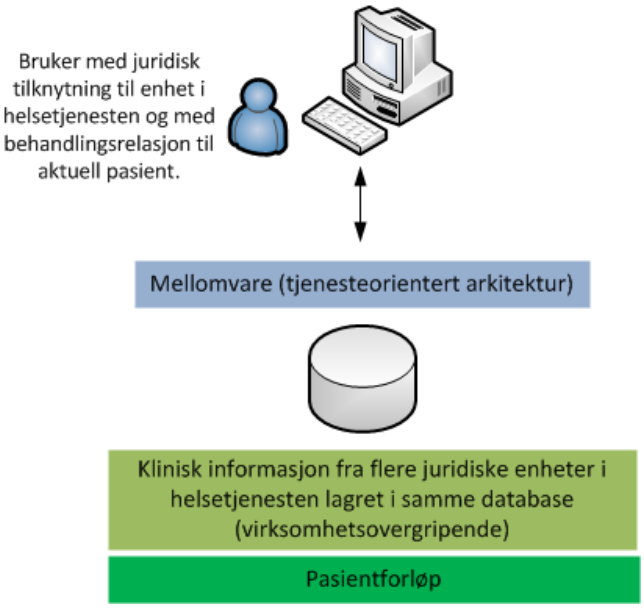
Figur 8. Meldingsutveksling – prinsippet om mange til mange.

2.4.2 Paradigmeskifte – synkron kommunikasjon - fra «send til hent»

Som nevnt i avsnittet over baserer storparten av elektronisk informasjonsutveksling i dag seg på sending og mottak av meldinger (Meldingsløftet). Kravene til tilgang til klinisk informasjon har vokst i takt med samfunnsendringene. Det er ikke lenger nok å ha et avgrenset sett med pasientdata i hver enhet pasienter mottar behandling i. Pasientforløpet og verdikjeden rundt den prosessen må sees på i en helhetlig sammenheng. Felles for disse nye kravene er at det *etterspørres* informasjon i stedet for å *sende* informasjon. Dette betyr en sentralisering av tilgangen til informasjonen nettopp for å kunne innhente et helhetlig pasientforløp på tvers av regioner og omsorgsnivå. Med sentralisering av tilgangen til informasjon menes det ikke nødvendigvis at det etableres en sentral database. Datakildene kan gjerne være lagret i en distribuert modell mens selve brukeropplevelsen oppfattes som om informasjonen etterspørres fra et sentralt punkt. Se figur 9 og 10 for sentral versus distribuert modell:



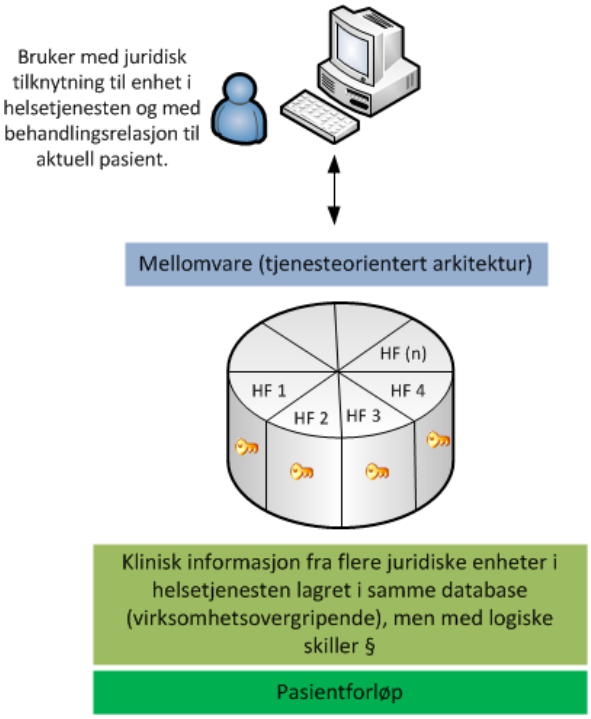
Figur 9: Distribuert modell der informasjonen er lagret i de enkelte juridiske enhetene slik de gjør i dag.



Figur 10: Sentralisert modell der informasjonen er lagret i samme database.

Kjernejournal og Meld. St. 9 "Én innbygger – én journal" vil basere seg på en av modellene beskrevet i figur 9 eller 10.

Slik lovverket i skrivende stund er utformet vil det være nødvendig med skillemekanismer i databasen ved en sentralisert modell som skiller datalagringen med logiske skillemekanismer basert på juridisk enhet. Figur 11 viser dette:



Figur 11: Sentralisert modell der informasjonen er lagret i samme database med logiske skiller basert på enhet.

Behovet for elektronisk tilgang på tvers av organisasjoner og omsorgsnivåer i helsetjenesten kommer som et resultat av samfunnsutviklingen der pasienter i voksende omfang vandrer mellom omsorgsnivåer, fritt sykehusvalg i tillegg til økt spesialisering der helsepersonell ansatt i flere virksomheter deltar i behandlingen. En god del forskning og forslag har blitt gjort for å utarbeide modeller som kommunikasjon og utveksling av informasjon mellom enheter i helsetjenesten både i Norge og utenlands. Det finnes derimot lite forskningsmateriale rundt tilgangskontroll for å dekke norske juridiske føringer for denne typen informasjonsutveksling. Denne oppgaven skal utarbeide en modell for dette med det viktigste kliniske informasjonssystemet, nemlig elektronisk pasientjournal (EPJ) som utgangspunkt.

2.4.3 Forskningsspørsmål (FS):

Oppgaven skal besvare følgende forskningsspørsmål:

1: Hvilke informasjonselementer må forstås for å kunne foreta autentisering og autorisasjon for tilgang etter klinisk informasjon på tvers av juridiske virksomhetsgrenser i spesialisthelsetjenesten slik at Helseinformasjonssikkerhetsforskriftens § 11c oppfylles?

3 Teori

Elektronisk samhandling i helsesektoren har stor fokus både fra myndighetenes side, men også sett fra et teknologisk og arkitekturståsted for tjenesteleverandørene til de ulike helseregionene. Innledningsvis vil teorikapittelet beskrive grunnleggende teori for arkitektur og teknologi som skal legge grunnlaget for leserens forståelse for løsningsforslaget. Videre vil det diskuteres et utvalg av artikler som adresserer lignende problemstillinger i andre land. Dette kapittelet er strukturert på følgende måte:

I kapittel 3.1 gis en oversikt over tilgangskontroll i informasjonssystemer for å gi leseren et begrepsapparat for forståelsen av dette samt for forståelsen av de neste kapitlene.

I kapittel 3.2 gis en oversikt over tilgangskontroll i kliniske informasjonssystemer der informasjonssikkerhet er særs viktig. Det vil i dette kapittelet gi leseren en oversikt over hvilke andre føringer utover vanlig tilgangskontroll som er gjeldene for denne typen av informasjonssystemer.

Kapittel 3.3 beskriver tjenesteorientert arkitektur for å gi leseren en oversikt over hvilken plattform spesialisthelsetjenesten benytter for elektronisk samhandling og for å etablere begrepsapparat for forståelsen av løsningsdesignet som presenteres i kapittel 6.

3.1 Generelt om tilgangskontroll i informasjonssystemer

Informasjonssikkerhet adresserer nødvendigheten med å beskytte data og ressurser fra uautorisert innsyn, manipulering og bruk. Det er derfor viktig å gi leseren en innføring i dette. Informasjonssikkerhet inndeles tradisjonelt i følgende kategorier:

- **Autentisering**: Omhandler prosessen for å verifisere identiteten til en person eller et subjekt. Fokus her er **hvem** er du og er du den du utgir deg for å være.
- **Autorisasjon:** Omhandler prosessen rundt hvilke tillatelser en person eller subjektet har. Fokus her er **hva** har du lov til å utføre på gitte ressurser og data.
- **Konfidensialitet:** Omhandler prosessen rundt det å sikre at data kun er tilgjengelig for autoriserte personer eller subjekter.
- **Integritet:** Omhandler prosessen rundt det å sikre at data ikke manipuleres. Et eksempel kan være at et informasjonsobjekt som sendes elektronisk fra A er nøyaktig det samme som mottas hos B.
- **Hendelseslogging:** Omhandler prosessen rundt det å logge hendelser for å kunne sikre sporbarhet.

Tilgangskontroll i informasjonssystemer har alltid vært en utfordring og har røtter tilbake til forskningsinitiativ i amerikanske forsvaret (Department of Defence)[19]. Det er i all hovedsak to tradisjonelle modeller for tilgangskontroll til informasjonssystemer og en nyere mer dynamisk modell som tas i bru i større og større omfang:

- Access Control Lists (ACL)[20]
- Role Based Access Control (RBAC)l[20]
- Attribute Based Access Control (ABAC)[24]

3.1.1 ACL:

Ved bruk av ACL blir hvert brukernavn mappet til separate sett med tillatelser som gir tilgang til spesifikke ressurser. Tillatelsene omhandler å lese, skrive, oppdater og utfør/eksekver-operasjoner. Det benyttes ofte såkalte tilgangsmatriser og lister til dette formålet.

3.1.2 RBAC:

Som nevnt ovenfor spilte det amerikanske forsvaret en stor rolle i utviklingen av metode og teknologi for tilgangskontroll. Forskningen ledet først til to fundamentale modeller for tilgangskontroll: Discretionary Access Control (DAC) og Mandatory Access Control (MAC).

Med DAC avgjøres tilgang til ressurser basert på brukerens identitet. En bruker gis tilganger til en ressurs ved å legges til i en tilgangsliste (ACL) som er assosiert med aktuell ressurs.

Ved bruk av MAC-modellen blir brukere gitt tilgang til ressurser av en administrator. Kun en administrator kan gi tilganger. Tilgangene baseres på objektenes sikkerhetsnivå.

En av de største utfordringene med å administrere store nettverk er kompleksiteten til administrasjonen rundt sikkerhet. Role Based Access Control (RBAC) ble formalisert i 1992 av David Ferraiolo og Rick Kuhn[21], og har blitt den foretrukne modellen for avansert tilgangskontroll fordi den reduserer kostnader knyttet til dette i form av mindre og enklere forvaltning. Den sentrale ideen med rollebasert tilgangsstyring er at brukerne ikke har diskret tilgang til objekter, men blir isteden assosiert med roller, og brukere blir lagt til som medlemmer i aktuelle roller. Roller kan igjen både gis nye tilganger når nye applikasjoner og hendelser inkorporeres samtidig som de kan tilbakekalles ved behov.

3.1.2.1 Roller og rolle hierarkier:

Med RBAC kan roller ha overlappende ansvar og privilegier hvilket betyr at brukere som tilhører forskjellige roller kan ha behov for å utføre felles operasjoner. Noen operasjoner kan utføres av alle ansatte. I denne situasjonen ville det være ineffektivt å administrere og repetere spesifikasjonen for hver rolle som blir opprettet. Rolle hierarkier kan opprettes for å støtte en organisasjons naturlige struktur.

Et rolle hierarki definerer roller som har unike attributter og som kan inneholde andre roller. Som et eksempel gitt i et sykehus-setting kan en spesialist ha rollen som lege og intern arbeider. Dette betyr at medlemmer i spesialistrollen er implisitt assosiert med operasjonene som igjen assosieres med rollene lege og internarbeider. Tar vi den videre kan eksempelvis rollene Kardiolog og Revmatolog begge inneholde rollen Spesialist.

3.1.2.2 Roller og operasjoner:

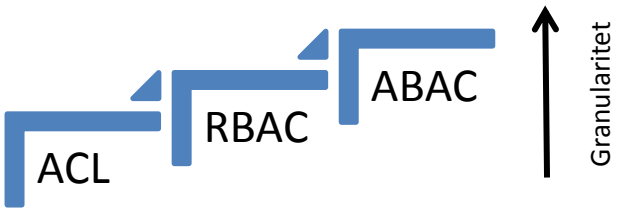
Organisasjoner kan etablere regler for hvilken assosiasjon som er hensiktsmessig mellom operasjoner og roller. For eksempel så kan en helsetilbyder bestemme at klinikerrollen kun skal kunne publisere spesifikke lab tester, men ikke kunne distribuere de til steder som en pasients personvern vil bli krenket. Operasjoner kan også spesifiseres på en måte som kan demonstrere eller håndheve lover og forskrifter. Et eksempel kan være en apoteker som gis tillatelse til å gi men ikke foreskrive legemidler.

3.1.3 ABAC

Rolledefinisjoner og forvaltningen av dem kan fort vokse ut av proporsjoner. I store organisasjoner kan det i mange tilfeller være like mange roller som det finnes brukere. Skal det aksesseres informasjon på tvers av sikkerhetsdomener er det sjelden at de ulike partene som inngår i samhandlingen besitter samme rolledefinisjon i sine respektive system hvis de i det hele tatt har rolledefinisjoner. En annen ting som også gjør at RBAC ofte i slike tilfeller ikke er godt nok er at det ofte finnes flere kontekstuelle parametere som også må være med i tilgangskontrollprosessene utenom rolle. Attribute Based Access Control (ABAC)[24] legger grunnlag for dynamisk, kontekst-basert tilgangskontroll[33][34] og benytter attributter som byggeklosser formalisert i et strukturert språk (XML[15]). Attributtene avgjør tilgang og nivået av tilgang. En kan se dette som at brukeren som skal ha tilgang formaliserer en påstand om seg selv og sine omgivelser i form av attributter. Et attributt kan være rolle, og viser dermed at ABAC er et mye mer dynamisk rammeverk for tilgangskontroll. Selve kontrollen av attributtene utføres ved bruk av definerte regler som formaliseres i policyer. Dette legger også grunnlag for semantisk interoperabilitet da attributt og regeldefinisjonene defineres ut i fra behov og blir således dynamisk. Et eksempel kan være en bruker som vil ha tilgang må være:

- Helsepersonell registrert i HPR-registeret.
- Over 18 år.
- Ha rollen “Lege”.
- Ha en spesifikk strukturell rolle.
- Ha ansattnummer som er registrert i personalsystem.
- Etc.

Figur 12 illustrerer at nivået av granularitet eller hvor "finkornet" autorisasjonen skal være øker ved bruk av RBAC og er mest dynamisk og fleksibel ved bruk av attributtbasert autorisasjon:



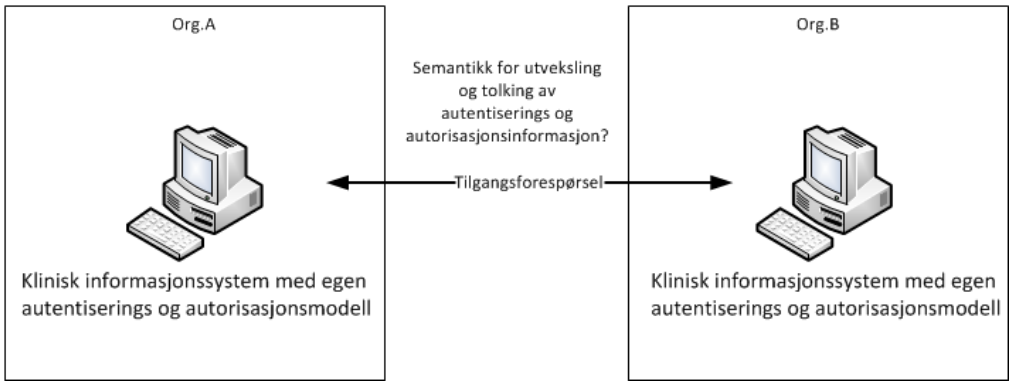
Figur 12: Granulariteten er best ved ABAC.

ABAC blir ofte realisert ved bruk av standarder som eXtensible Access Control Markup Language (XACML)[25] som er et generisk autorisasjonsrammeverk som ved bruk av XML definerer tilgangsregler og Security Assertion Markup Language (SAML 2.0)[22] som bærer av attributter over kommunikasjonsnettverk. Disse standardene vil bli beskrevet lengre ned i teorikapittelet og vil bli benyttet som en sentral standard for å besvare forskningsspørsmålet.

3.2 Tilgangskontroll i kliniske informasjonssystemer

Videre gis en oversikt over tilgangskontroll for kliniske informasjonssystemer. Dette for å vise kompleksiteten i dagens situasjon i tillegg til de standarder og lover som er gjeldende for dette formålet.

Dagens kliniske applikasjonslandskap i helsevesenet i Norge består av høy grad installert base og heterogenitet. Interoperabilitet mellom systemene er svært lite utberedt, både teknisk og semantisk både med tanke på informasjonsutveksling og tilgangskontroll (Figur 13). Dette skyldes historiske grunner som at systemene har blitt anskaffet og forvaltet som "siloer" hvilket betyr at de ikke hadde interoperabilitets- og samhandlingskrav utover funksjonelle krav. En annen viktig faktor er inndelingen av helsevesenet i regioner og helseforetak der hvert helseforetak til nylig har hatt egne anskaffelser av IT-verktøy uten samhandlingsperspektiv i øyemed.



Figur 13: Fravær av semantisk informasjonsmodell på tvers av kliniske informasjonssystemer.

Personvern og informasjonssikkerhet er svært viktig i helsevesenet generelt og det må også gjenspeiles i tilgangskontrollen til informasjonen som er lagret i de ulike kliniske informasjonssystemene.

3.2.1 Standard for EPJ og tilgangsstyring

EPJ Standard del 2: Tilgangsstyring, redigering, retting og sletting[8]

Denne standarden er sentral i hvordan arkitekturen for tilgangskontroll skal realiseres i EPJ-systemer og definerer tekniske og generelle funksjonelle krav til innhold i tillegg til prinsipp beslutningsstyrt tilgangskontroll, samtykke og redigering, retting og sletting. Standarden er utarbeidet av Kompetansesenteret for Informasjonsteknologi i Helsesektoren (KITH) i 2007.

Beslutningsstyrt tilgang er et sentralt begrep for denne oppgaven da det setter krav i form av føringer og forskrifter. Begreper og krav fra standarden vil være gjennomgående og førende for arkitekturen i oppgaven. Dette fordi lover og forskrifter henviser til standarden, men også for å kunne etablere et omforent begrepsapparat for å støtte semantisk interoperabilitet. Dersom sømløs samhandling mellom ulike kliniske informasjonssystemer skal kunne utføres er det et basalt krav at det utarbeides arkitekturer basert på standarder som dekker alle aspekter ved tilgangskontroll til kliniske systemer.

Noen sentrale begreper fra standarden som er viktige:

3.2.1.1 Tjenesteyter

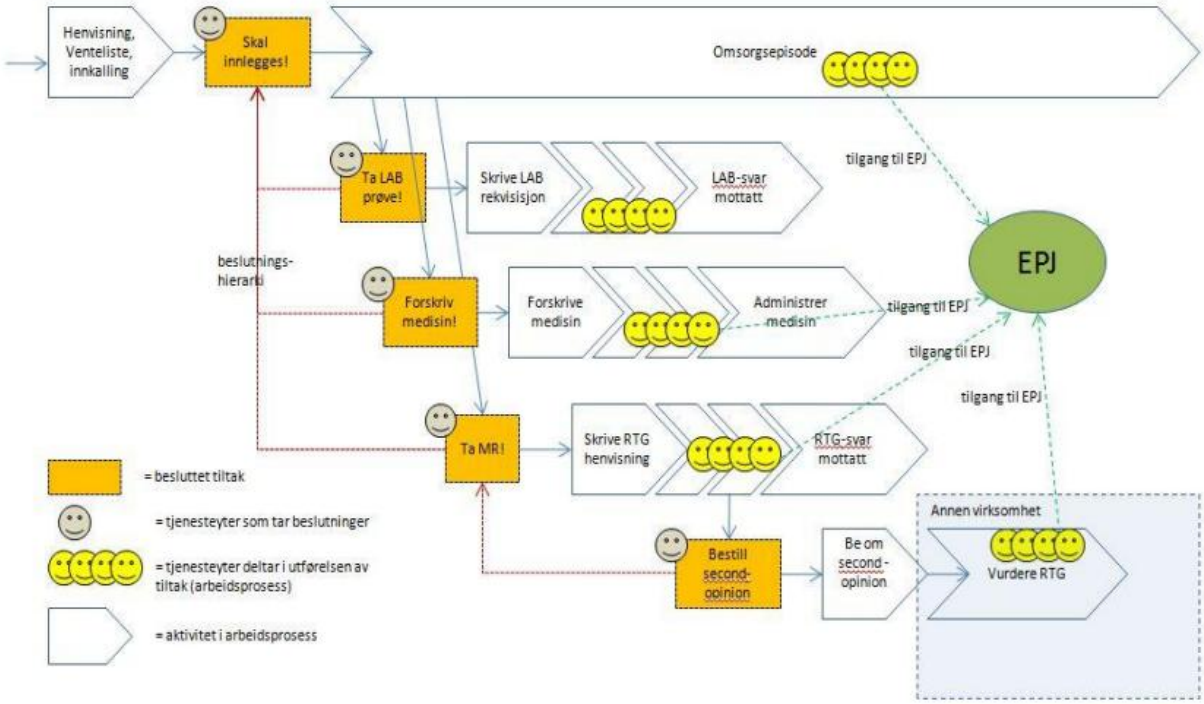
Tjenesteyterbegrepet i EPJ Standard Del 2 – *Tilgangsstyring, redigering og sletting*: "*En Person som opptrer i en rolle er betegnet som en tjenesteyter"[8], der en tjenesteyter er "en person som i kraft av sin rolle er gitt tilgang til pasientens journal i forbindelse med gjennomføring av et besluttet tiltak*". Med en tjenesteyter menes her altså personen og dens tilknytning til organisasjon og rolle.

3.2.1.2 Beslutningsstyrt tilgang

Beslutningsstyrt tilgangskontroll (BT) hvilket er å betrakte som en ontologi for gjeldende lover og forskrifter. Det går frem fra EPJ-standarden Del 2 at "*enhver tilgang til helseopplysninger skal ha et uttrykkelig angitt og saklig begrunnet formål*"[8]. Et formål kan oppsummeres til å være at det "*er en konkret relasjon mellom tjenesteyter og pasient*"[8] da med utgangspunkt i et **besluttet tiltak**. Tilgangsstyringen er samtykkebasert; hovedregelen er at pasienten skal ha gitt sitt samtykke til å motta helsehjelp og med dette dermed gitt sitt samtykke til at tjenesteyter kan dokumentere i aktuelle pasients journal.

Standarden sier *ikke* noe om modellen for tilgangskontroll med tanke på om den skal være rollebasert eller attributtbasert, men at tilgangen utover dette må innebefatte et behandlerforhold til pasienten. Behandlerforholdet etableres ut i fra at det etableres en beslutning/tiltak om innleggelse/behandling.

De rettigheter som skal følge med gjennomføring av de forskjellige typer tiltak vil kunne variere. Det må derfor finnes en mulighet for beskrive typer av tiltak og de rettigheter som er nødvendige for å gjennomføre slike tiltak. I standarden kalles en slik beskrivelse **"Tiltaksmal". Tiltaksmal som knyttes sammen med rollebeskrivelse og organisasjonstilhørighet for tjenesteyter** vil en eller flere tjenesteytere rett til å lese pasientens informasjon. Figur 14 illustrerer eksempler på hvordan den enkelte besluttede tiltak genereres:



Figur 14: Eksempel på generering besluttede tiltak [35].

3.2.1.3 Rollemaler og tiltaksmaler

Rollemaler

Ethvert EPJ-system skal inneholde eller ha mulighet for å opprette det antall rollemaler som er nødvendig for å dekke de opp-gaver som tilligger virksomheten. (Krav K7.42) Rollemalen beskriver datastrukturen for rolle.

Enhver rolle i virksomheten skal baseres på en rollemal (Krav K7.44).

Tiltaksmaler

Det skal finnes mulighet for registrering av Tiltaksmaler. En slik tiltaksmal skal inneholde en overordnet beskrivelse av tiltaket, hvilke kategorier helsepersonell som kan gjennomføre denne typen tiltak samt hvilke rettigheter i forhold til informasjon i journalen som er nødvendig (Krav K7.104).

Tiltaksmaler benyttes for å registrere maler for de typer besluttede tiltak som skal kunne benyttes i forbindelse med styring av tilgang til journalopplysninger innenfor en virksomhet i helsevesenet. Tiltaksmalen beskriver datastrukturen for tiltak.

Standarden beskriver kun et sett av minimumskrav som må være til stede i definisjonen av tiltaksmaler[8]:

1. Registrere helsehjelprelatertbeslutning. (Registrering av Besluttet tiltak.)

2. Helsehjelp. Tiltaket skal både gi mulighet til å nedtegne opplysninger i journalen (jf. helsepersonelloven § 39) og tilgang til opplysninger som er nødvendig for å gi forsvarlig helsehjelp (jf. helsepersonelloven § 25).

3. Pasientadministrasjon, jf. helsepersonelloven § 26.

4. Pasientinnsyn, jf. helsepersonelloven § 41 og pasientrettighetsloven § 5-1.

5. Informasjon til pasienten, jf. pasientrettighetsloven §§ 3-2 og 3-5.

6. Retting av opplysninger, jf. helsepersonelloven § 42.

7. Sletting av opplysninger, jf. helsepersonelloven § 43.

8. Redigering av journal, jf. journalforskriften § 13.

9. Tilsyn med helsepersonellets virksomhet, jf. helsepersonelloven § 30.

10. Akutt helsehjelp. Skal kun benyttes i akuttsituasjoner hvor tilgang til journalen er nødvendig og det ikke er tid til å benytte normal prosedyre for å få slik tilgang.

3.2.2 Identiteter i kliniske informasjonssystemer

Å kunne entydig identifisere personer og subjekter som skal benytte IT-verktøy er en absolutt nødvendighet for å kunne utføre autentisering (hvem) og videre autorisere (hva har subjektet lov til å utføre) for tilgangen til informasjon. Likevel er det utfordringer med tanke på dette i en nasjonal sammenheng. Dette har historiske grunner som videre blir forklart her. Jeg har valgt å beskrive Helse Sør-Øst sin modell for forvaltning av identiteter i spesialisthelsetjenesten for å gi en oversikt over identitetshåndtering

Helsevesenet i Norge er delt inn i 4 regioner. Spesialisthelsetjenesten i de ulike regionene har hvert sitt adskilte system for opprettelse og forvaltning av identiteter som benyttes til lønns- og personalsystem i tillegg til brukeridentiteter i informasjonssystemer. Historisk sett har hvert helseforetak sine egne brukerkataloger der identitetene til de ulike brukerne er registrert. Dette betyr at det ikke finnes en omforent og enhetlig **nasjonal** tilnærming for identitetsforvaltning i skrivende stund for spesialisthelsetjenesten hvilket betyr at I et samhandlingsperspektiv gir dette utfordringer med tanke på autentisering og autorisasjon fordi en identitet i Helse Sør-Øst ikke er semantisk lik en identitet i en annen region. Det må altså utformes strategi for identiteter i et nasjonalt perspektiv. Dette understøttes også i St. meld. 9 (2012-2013) "Én innbygger – én journal i avsnitt 6.1 Infrastruktur, omtales Norsk Helsenetts ulike administrative registre og behovet for en bedre samordning av innholdet i disse. Under avsnittet Informasjonssikkerhet presenteres følgende forslag:

"… Det foreslås å etablere sikker identifisering av helsepersonell. En mulig løsning kan være etablering av et profesjonskort med elektronisk ID. Løsningen må etableres i henhold til en nasjonal sikkerhetsinfrastruktur og omfatte alle aktørene i sektoren. Løsningene skal understøtte både lokale og nasjonale behov, for eksempel e-resept, nasjonal kjernejournal og tilgang til opplysninger på tvers av virksomhetsgrenser..".

Helsepersonell som har flere arbeidsforhold er en stor utfordring i forhold til juridiske knytninger. En lege som har flere roller i forskjellige organisasjoner må kunne autentiseres og gis tilgang til ressurser for den rollen hun opptrer som i øyeblikket. Det finnes i dag ingen omforent modell for dette på tvers av systemer og helseforetak hvilket er en stor utfordring.

3.2.3 Masterdatakilder som er viktige for å understøtte nasjonal elektronisk samhandling

I dag finnes følgende nasjonale registre som er viktige kapabiliteter som er med å understøtte deler ved elektronisk samhandling:

- Helsepersonellregisteret (HPR) – register over alt helsepersonell med autorisasjon og lisens etter helsepersonelloven.
- Adresseregisteret – register over virksomheter og personer (kun for primærhelsetjenesten) som får betegnelsen kommunikasjonsparter og får en unik identifikator som kalles HER-ID (Helse Enhets Register-ID). HER-ID brukes til å identifisere avsendere og mottakere av alle elektroniske meldinger med pasientinformasjon. En kommunikasjonspart er en avsender/mottaker av meldinger i Norsk Helsenett.
- RESH – register over enheter i spesialisthelsetjenesten (RESH) er den autorative kilden for organisasjonsstruktur i spesialisthelsetjenesten med detaljert beskrivelse av tjenestene som tilbys i kliniske enheter ved hjelp av et kodeverk for spesialisthelsetjenesten (OK2007 versjon 2.0). RESH benyttes primært for innmelding til myndigheter om aktivitet, kvalitet og ventelister til NPR der en RESH-ID identifiserer enheten det gjelder. HER-ID benyttes også i RESH-registeret for identifisering av elektronisk tjenester i spesialist- og kommunehelsetjenesten.

Primærhelsetjenesten benytter foruten manuelle registreringer av identiteter og brukere det nasjonale adresseregisteret for å kunne identifisere kommunikasjonsparter i samhandlingsprosesser både på virksomhets og personnivå. Norsk Helsenett omtaler selv Adresseregisteret:

"...*Ved registrering i Adresseregisteret, blir den enkelte virksomhet og dens egne kommunikasjonsparter (avsendere/mottakere) knyttet til en unik identifikator som kalles HER-id. HER-id brukes til å identifisere avsendere og mottakere av alle elektroniske meldinger med pasientinformasjon…*"

3.3 Tjenesteorientert arkitektur

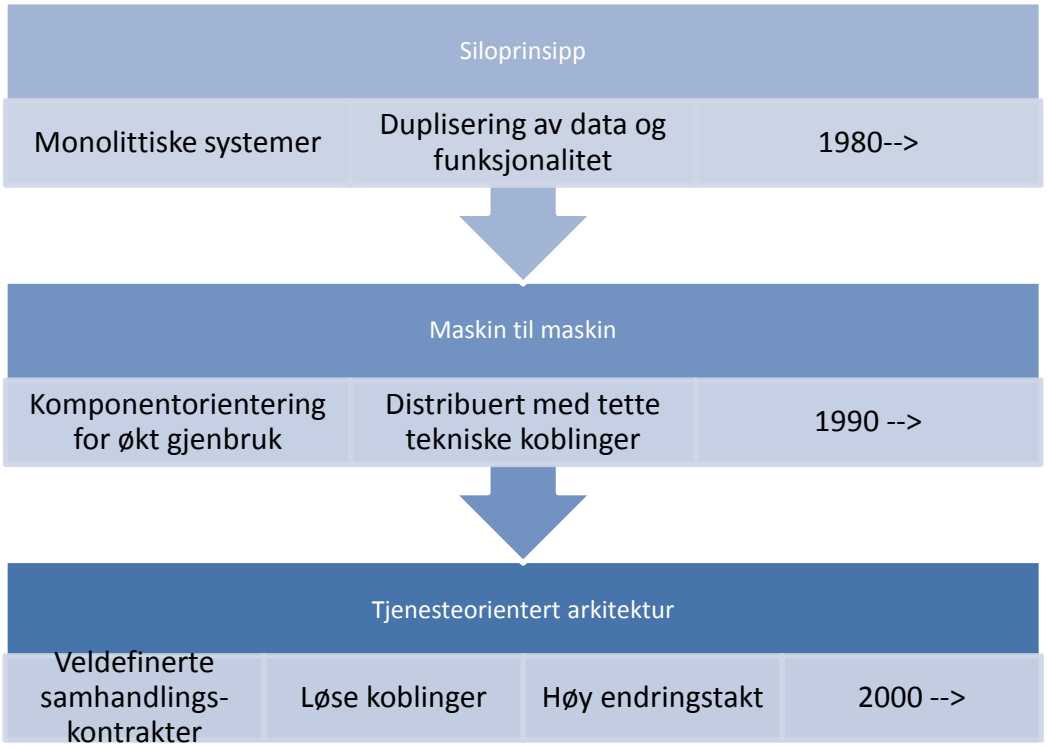
Det foreligger føringer i form av styringsdokumentet "Tjenesteorientert arkitektur i spesialisthelsetjenesten"[32] om å etablere en felles systemarkitektur for spesialisthelsetjenesten. Dette betyr at Intern og ekstern elektronisk samhandling mellom enheter i spesialisthelsetjenesten skal utføres på tjenesteorientert arkitektur. Det er derfor nødvendig å gi en teoretisk innføring i dette emnet fordi tjenesteorientert arkitektur ligger i bunn for besvarelsen av forskningsspørsmålet.

Tjenesteorientert arkitektur åpner muligheter for hele verden til å utføre forretninger og elektronisk samhandling via standarder som legger grunnlag for støtte av interoperabilitet og benytter begrepet "tjeneste" som fundamentale elementer når det skal utvikles applikasjoner. En tjeneste kan defineres som "å utføre noe for andre". Bedrifter og organisasjoner tilbyr gjerne sine tjenester elektronisk ved bruk av tjenesteorientert arkitektur og web services.

Utvikling av kompleks programvare er dyrt og tidkrevende. Prosessen rundt programvareutvikling har i mange år hatt fokus på hvordan kode kan gjenbrukes. Grovt sett kan vi se en 3-delt utvikling av dette. Programmerere på 80-tallet begynte å ta i bruk objekt-orientering for å kunne gjenbruke deler av interne strukturer. Utfordringen med det var at i det applikasjonen var laget så var den statisk og det var ikke noen god måte å gjenbruke eller endre funksjonalitet.

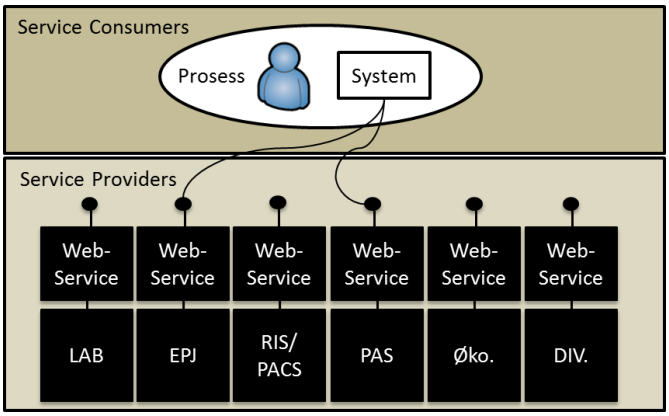
På 90-tallet kom begrepet "komponentbasert utvikling"[9]. Med denne utviklingsmetoden begynte man å benytte grensesnittsom definerte hva komponenten kunne utføre (Interface). Pendelen svingte tilbake fra stormaskiner til distribuert databehandling ved bruk av DCOM og CORBA[10] Det betydde at store datastrukturer ble logisk inndelt i komponenter som kunne fysisk plasseres distribuert hvilket tilgjengelig gjorde gjenbrukbar funksjonalitet. Remote Procedure Call (RPC)[10] ble hovedsakelig benyttet for eksekvering av funksjoner på distribuerte objekter/komponenter. På 2000-tallet dukket begrepet "tjenesteorientering" opp. Det ble da fokus på plattformuavhengighet og selv-beskrivende applikasjoner. I stedet for å aktivere metoder på objekter ble abstraksjon viktig ved og i stedet fokusere på meldingsutveksling som også la grunnlaget for skalerbare, løst koblede og interopererbare tjenester basert på standarder. Med andre ord ble funksjonalitet og plattform abstrahert ut til tjenester som hadde standarder for både eksponering og konsumering av denne funksjonaliteten.

I store organisasjoner i dag har man et stort antall applikasjoner kjørende på ulike plattformer, teknologier, programmeringsspråk og versjoner. Disse små eller store siloene av enkeltapplikasjoner må kunne snakke sammen og utveksle data for å kunne støtte stadig større krav til forretningsprosessene. Figur 15 viser utviklingen av dette fra monolittiske siloer til tjenesteorientert arkitektur.



Figur 15: Fra siloer til tjenester.

Figur 16 illustrerer den logiske oversikten for tjenesteorientert arkitektur fra spesialisthelsetjenesten der den underliggende plattform og tekniske proprietære implementasjonen skjules for tjenestekonsumenter ved å eksponere funksjonaliteten via standardiserte grensesnitt



Figur 16: Logisk oversikt tjenesteorientert arkitektur.

Don Box kom i 2004 med sin definisjon av tjenesteorientert arkitektur med “Four tenets of service orientation som er et formalisert syn på hvilke av hvilke krav som ligger i bunn for hva som kan kalles tjenesteorientert arkitektur [11]:

- Service boundaries are explicit.
    - Tjenester interagerer gjennom meldingsutveksling via SOAP-standarden[12] over veldefinerte grenser. En tjenestegrense representerer grensen mellom en tjenestes offentlige grensesnitt skjematisk ved bruk av WSDL[13].
    - Data utveksles via meldinger.
- Services are autonomous.
    - Tjenester er entiteter som individuelt blir produksjons satt, versjonert og håndtert og er dynamisk adresserbare via URI ‘er[14].
- Services share schema and contract, not class.
    - Interaksjon med tjenester skjer ved bruk av:
        - Skjema for transport av data (XSD)[15].
        - WSDL for tjenestebeskrivelse.
        - Orkestreringer (aggregering) er beskrevet med BPEL[16].
- Service compatibility determined by policy.
    - WSDL inneholder WS-Policys[17] for å beskrive interoperabilitet.

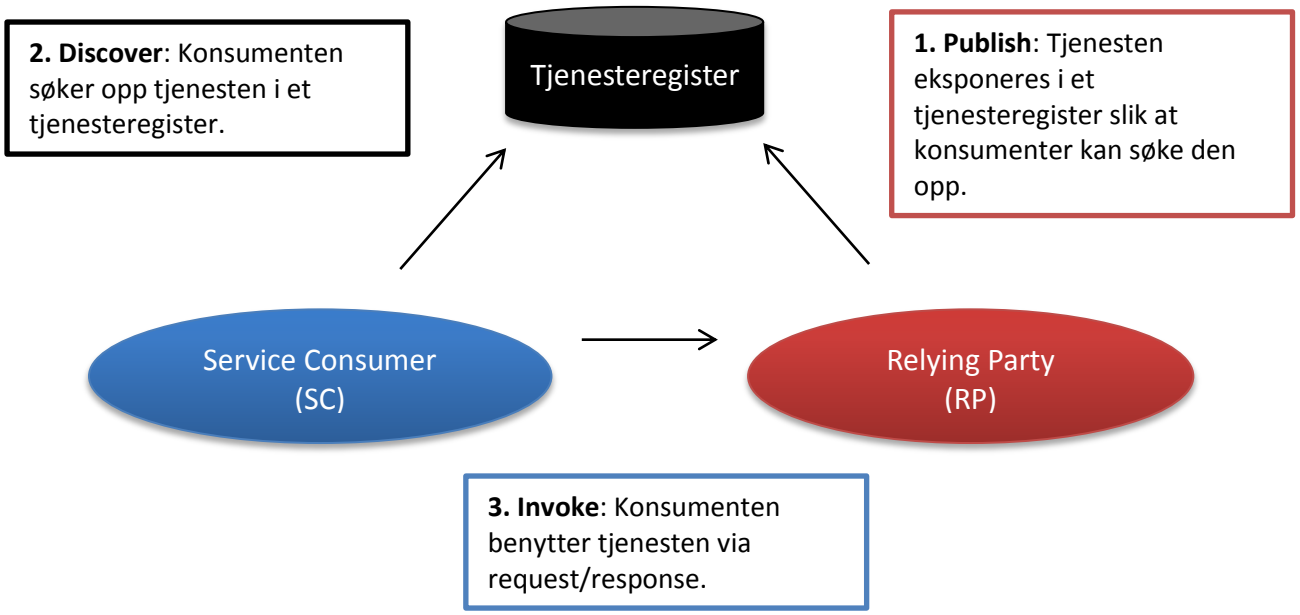
Noen viktige begreper og aktører i tjenesteorientert arkitektur (De enkelte elementene omtales videre i de påfølgende kapitlene):

Begrep	Forklaring
Identity Provider (IdP)	IdP er den enkeltes organisasjons system for identitetshåndtering og kan eksponeres som brukerkataloger (LDAP, Active Directory etc.). IdP er identitetsgrunnlaget for STS.
Security Token Service (STS)	STS er et web-service grensesnitt mot brukerkataloger som for eksempel LDAP/Active Directory som har som oppgave å generere, signere og utstede Sikkerhetstokens som typisk er SAML. Baseres på standarder som støtter interoperabilitet beskrevet i WS-Security som WS-Trust, WS-Federation
Service Provider (SP) /Relying Party (RP)	Er selve web-servicen som utfører forretningslogikk for service consumer(er). Ofte også kalt relying party fordi den baserer seg på SAML-sikkerhetstokens for autentisering og/eller autorisering
Service Consumer	Klient som benytter web-service (Service Provider)
SOAP	Simple Object Transfer Protocol (SOAP) er en web-standard som definerer formatet til meldinger som benyttes i web-services
WSDL	Web Service Description Language (WSDL) er metadata som beskriver web-services funksjonalitet og hvordan de skal konsumeres på funksjons og datanivå.
Assertions	Sikkerhetstoken med påstander om hvem du er og hva du kan utføre. Formalisert ved bruk av SAML-sikkerhetstokens. Utstedes og valideres av STS der den signeres. Sikkerhetstokens legges i header på SOAP-meldingen ved bruk av WS-Security
SAML	Security Assertion Markup Language (SAML) er et standardisert dataformat som benyttes for å definere Sikkerhetstoken
WS-Security	Rammeverk for sikkerhet som består av et sett protokoller som skal understøtte sikring av Web-services som benytter SOAP
WS-Trust	Standardprotokoll i WS-Security som gir web services standardiserte metoder og grensesnitt for å etablere tillit (eng: trust) mellom identitetstilbydere/sikkerhetsdomener i tillegg til utstedelse og validering av Sikkerhetstokens
WS-Federation	Standardprotokoll i WS-Security som definerer mekanismer for å bringe påstander (SAML) mellom identitetstilbydere/sikkerhetsdomener
WS-Policy	Standardprotokoll som definerer hvordan web-services kan definere krav til sikkerhet for konsumenter av web-services. Denne standarden er sentral i SAML-basert tilgangskontroll da den definerer hvilke type sikkerhetsmekanismer som er påkrevd for å benytte aktuelle tjenester som protokoller, adresser (URL) og forventet innhold i Sikkerhetstokens.

WS-Addressing	WS-Addressing er en egen standard definert av OASIS. WS- Addressing er en utvidelse av SOAP på lik linje med WS-Security med elementer som deklarer slutt endepunkt mens http-header beskriver neste hopp endepunkt.
Digital signatur	Krypteringsalgoritme som støtter bevis på at meldingens avsender er autentisk og at meldingsinnhold (SOAP) ikke har blitt modifisert under transport. En forutsetning for etablering av trust mellom sikkerhetsdomener.
Kerberos	Autentiseringsprotokoll som benyttes i AD (Active Directory) LDAP brukerkatalog. Typisk er dette autentiseringsprotokollen som benyttes av Windows-maskiner for pålogging til lokalt nettverk (AD)
PKI	Public Key Infrastructure (PKI) er et rammeverk for sikring av informasjonsutveksling ved bruk av digitale sertifikater og bygger på krypteringsnøkler som opptrer i par der den ene er offentlig tilgjengelig (eng: public) og den andre er privat

.

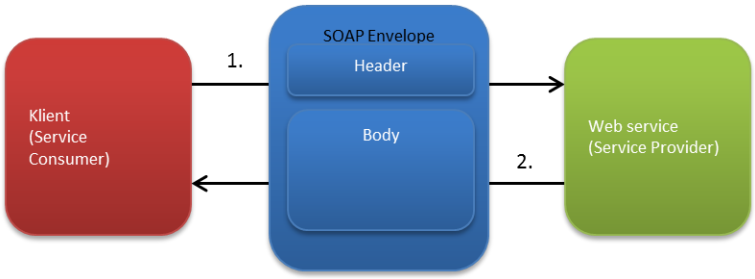
W3C definerer tjenesteorientert arkitektur som: *"A set of components which can be invoked, and whose interface descriptions can be published and discovered"* [11]. Figur 17 illustrerer hvordan den logiske oppbyggingen av arkitekturen er:



Figur 17: Web service modell.

3.3.1 SOAP

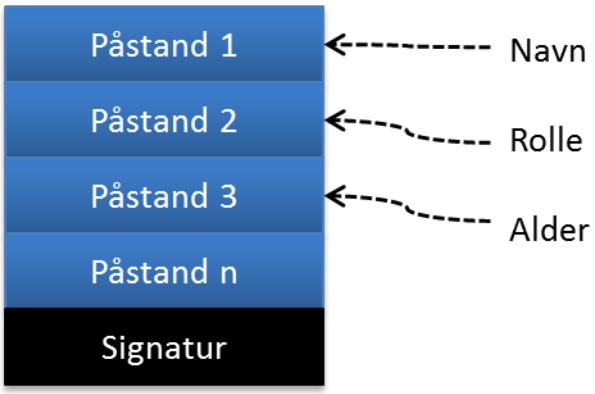
En av de viktigste åpne web-service standarder er Simple Object Access Protocol (SOAP)[12] som er meldingsstandarden som benyttes for interaksjon med tjenester. SOAP er en plattformuavhengig protokoll for utveksling av XML-baserte meldinger og danner grunnlaget for web services. SOAP bruker eksisterende standardiserte transportprotokoller som både HTTP og SMTP. Figur 18 illustrerer en logisk oversikt over SOAP-standardens hovedoppgave, nemlig å frakte data og tjenestekall mellom web-service klient og tjenester.



Figur 18: SOAP melding mellom klient og web service.

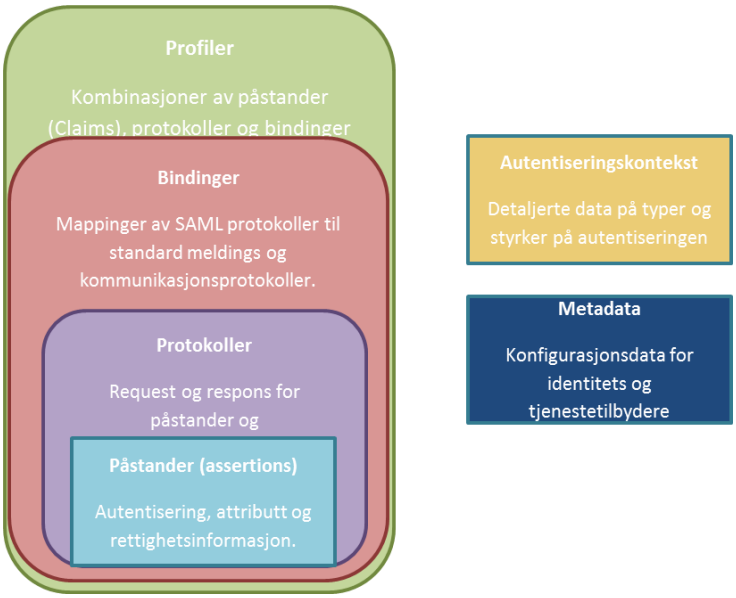
3.3.2 SAML 2.0

SAML er en utvidelse av SOAP-standarden som blir benyttet til å utveksle autentiserings og autorisasjonsattributter mellom sikkerhetsdomener, mer spesifikt mellom en identitetstjeneste og en service provider. Attributtene fungerer som **påstander** om hvem du er og hva du kan utføre. Da både websider og web-services ofte beveger seg over flere virksomhetsgrenser og domener er det viktig å kunne bringe hvem, hva og hvor vi er fra domene til domene uten å ta hensyn plattform og implementasjon. Eksempel på Sikkerhetstoken illustreres i figur 19. Legg merke til at det er et element der for signering. Dette betyr at SAML-sikkerhetstokenet signeres med sertifikat av avsender og verifiseres av mottaker for å sikre at dataene ikke har blitt endret. Føderering (eng: federation)omhandler det å linke en persons elektroniske identitet og attributter som er lagret over flere sikkerhets- og policy domener for å støtte sømløs interaksjon[23]. Identity federation vil bli omtalt grundig senere i kapittel 3.3.3.4. SAML arkitektur illustreres i figur 20.



Figur 19: Eksempel på Sikkerhetstoken.

3.3.2.1 SAML 2.0 Arkitektur



Figur 20: SAML 2.0 arkitektur.

Noen viktige punkter rundt SAML 2.0 arkitektur:

- SAML- Sikkerhetstokens inneholder identifiserende informasjon som er utstedt av en SAML utsteder (Identity Provider(IdP)). SAML skiller mellom tre hovedkategorier:
    1. Autentisering: Validerer at det spesifiserte subjektet er autentisert via IdP på et gitt tidspunkt ved bruk av en valgt metode.
    2. Autorisering: Beskriver hva det spesifiserte subjektet er autorisert til å utføre.
    3. Attributt: Inneholder spesifikk informasjon vedrørende det spesifikke subjektet.'
- Protokoller: Definerer en rekke request/response-protokoller. Disse protokollene gir Service Providere muligheten til å:
    1. Spørre etter en påstand
    2. Spørre om å få autentisert et subjekt
    3. opprette og håndtere navnemappinger
    4. Spørre etter single logout.
- Bindinger: Definerer hvordan SAML request/response meldingsutveksling mappes til kommunikasjonsprotokoller som SOAP. SAML fungerer også sammen andre typer kommunikasjonsprotokoller som Hypertext Transfer protocol (http), Simple Mail Transfer Protocol (SMTP) og File Transfer Protocol (FTP) etc.
- Profiler: SAML-profiler definerer begrensninger og/eller utvidelser for å understøtte konteksten og spesifiserer hvilke SAML-bindinger som kan benyttes.
- Metadata: Definerer en måte og uttrykke og dele konfigurasjonsinformasjon mellom SAML-entiteter.
- I enkelte situasjoner har en service provider behov for detaljert informasjon om hvilke type og styrken på autentisering som en bruker benyttet når de autentiserte hos en identity provider. En SAML-autentiserings kontekst benyttes i en påstands autentiserings

3.3.2.2 Hvorfor er SAML viktig?

- Plattformnøytralitet. SAML abstraherer sikkerhetsrammeverket vekk fra spesifikk implementasjon og arkitektur.
- Løs kobling. SAML krever ikke at brukerinformasjon synkroniseres mellom brukerkataloger.
- Økt kvalitet i på og avloggingsprosesser. SAML-sikkerhetstokens gir mulighet for Single Sign On ved å tillate brukere å autentisere seg ved en identity provider for så og aksessere tjenester/ressurser hos service providers uten å gjenta på og avloggingsprosessen mer enn en gang.

3.3.2.3 Bruken av SAML

Som et generelt rammeverk for kommunikasjon av sikkerhets og identitetsinformasjon kan SAML benyttes på flere måter. Viktige punkter:

- Web Single Sign-On (SSO)
    - Med SSO autentiserer en bruker seg til en webside for så å kunne navigere til andre websider uten å behøve og autentisere seg på nytt.
- Attributtbasert autorisasjon
    - På lik linje med SSO beskrevet over benytter attributtbasert autorisasjon modellen med at en webside kommuniserer identitets-informasjon om et subjekt til en annen webside. Men med denne modellen kan identitetsinformasjonen bestå av karakteristikker som beskriver subjektet. Eksempel kan være en persons rolle eller lokasjon i stedet for eller i tillegg til informasjon om når og hvordan personen ble autentisert.
- Sikring av web services
    - SAML-sikkerhetstokens kan brukes i SOAP-meldinger for å transportere sikkerhets og identitetsinformasjon mellom web service-aktører.

Oppsummert kan vi si at SAML-sikkerhetstokens gir mulighet for å distribuere sikkerhetsrelatert informasjon som input for tilgangskontroll som når og hvordan en bruker blir autentisert eller hvilke attributter som benyttes for å avgjøre om en request skal tillates. SAML spesifiserer derimot ikke hvordan denne informasjonen skal benyttes eller hvordan tilgangskontroll-policyer skal brukes for å foreta valg. For det formålet har OASIS spesifisert en annen standard som heter Extensible Access Markup Language (XACML)[25].

3.3.3 Sikkerhet i tjenesteorientert arkitektur

Å sikre tilgang til informasjon er viktig for enhver person organisasjon som er involvert i elektronisk samhandling. Tjenesteorientert arkitektur har prinsipp om løs kobling[11]. Med løs kobling menes graden av avhengighet mellom kommuniserende systemer og deres operasjoner på tvers av grenser. Med dette prinsippet blir også sikring av innhold og transport enda mer viktig. Tradisjonelt har sikkerhetsmodeller blitt hardkodet inn i systemer hvilket er uegnet i en setting der det kreves tjenesteorientert arkitektur. Figuren under viser den historiske utviklingen i forbindelse med paradigmer med tanke på sikkerhet:

Paradigme:	Objektorientert	Komponentbasert	Tjenesteorientert med web services
Sikkerhetsaspekter	Leverandør eller implementasjon sørger for sikkerhetsmekanismer, autentisering, autorisering, logging etc.	Komponentmodellen sørger for implementasjonsspesifikk sikkerhetsmodell som ikke er interopererbar mellom tjenester og grenser. Altså sørget systemene selv for implementasjon av sikkerhet. Ingen åpne standarder.	Interopererbare sikkerhets industristandarder som WS-Security, XACML, SAML.

Figur 21: Sikkerhetsparadigmer innen sikkerhet for applikasjonsutvikling.

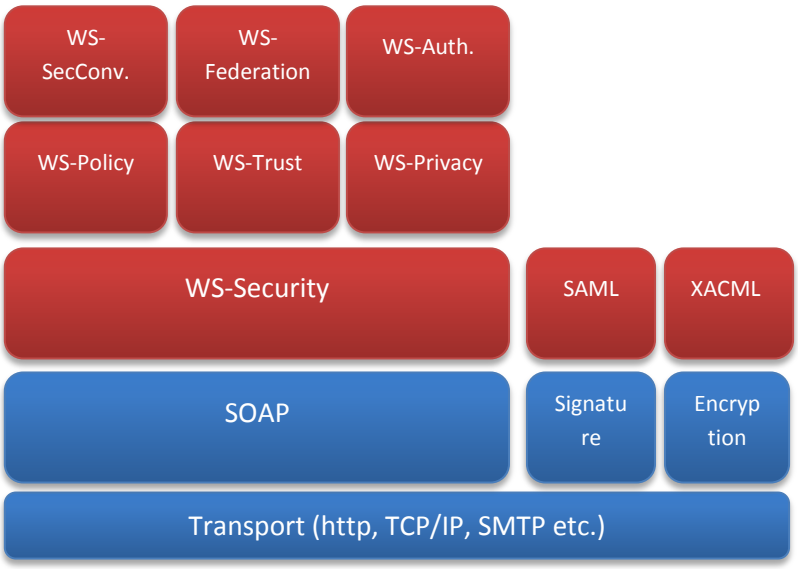
Vi skiller mellom to typer sikkerhet:

1. Meldingssikkerhet: Med meldingssikkerhet menes at meldingen skal kunne overføres fra start til endepunkt med konfidensialitet og integritet. Dette sikres ved standarden WS-Security.
2. Transportsikkerhet. Selve linjen sikres. Eksempelvis kan HTTPS/SSL benyttes.

3.3.3.1 WS-Security

I 2002 sendte Microsoft, IBM og Verisign inn et standardforslag til OASIS (Organization for the Advancement of Structured Information Standards), for web service sikkerhet kalt WS-Security[18].

Spesifikasjonen er et rammeverk for meldingssikkerhet (SOAP) og definerer utvidelser av SOAP-standarden for å støtte integritet og konfidensialitet ved informasjonsutveksling i en tjenesteorientert arkitektur. Figur 22 viser de ulike elementene som inngår i ws-security rammeverket:



Figur 22: WS-Security.

3.3.3.2 PKI

Integritet og konfidensialitet er en forutsetning for å utveksle informasjon slik at ikke innholdet er synlig for uvedkommende eller at den endres underveis. Bruk av PKI er en forutsetning for tjenesteorientert arkitektur der deler av arkitekturen baserer seg på tillit (eng: trust) ved autentisering og utstedelse av attributter. Det er derfor nødvendig først å gi en oversikt over PKI og dets bestanddeler før jeg presenterer hvordan dette benyttes i praksis i tjenesteorientert arkitektur som denne oppgaven baserer seg på.

PKI omfatter infrastruktur for sikring av informasjonsutveksling ved bruk av digitale sertifikater og bygger på krypteringsnøkler som opptrer i par der den ene er offentlig tilgjengelig (eng: public) og den andre er privat[48]. Den offentlige nøkkelen har den fordelen at den kan gis i praksis til hvem som helst. Nøklene består av store primtall som har den egenskapen at det som krypteres med den ene nøkkelen kan dekrypteres med den andre. Som et eksempel kan det offentlige sertifikatet benyttes til kryptering og det private sertifikatet benyttes til dekryptering. Dette fordi det kun er innehaver av privat nøkkel som kan "låse opp" krypteringen. Dette kalles også asymmetrisk kryptografi. Vi skiller mellom kryptering, autentisering og signering i PKI.

En PKI består av følgende elementer:

- Sertifikat-autoritet (eng: Certificate authority (CA))
    - CA har ansvaret for utstedelse og verifiseringen av digitale sertifikater.
- Registrerings-autoritet (eng: Registration authority (RA))
    - RA har ansvaret for å verifisere identiteten til brukerne før det skal utstedes fra CA.
- Katalogtjenester (eng: Central directory)
    - Har ansvaret for å indeksere og gjøre sertifikatene tilgjengelige via sikrede katalogtjenester.
- Endesystemer og personer som benytter sertifikatene for kryptering, autentisering og signering).

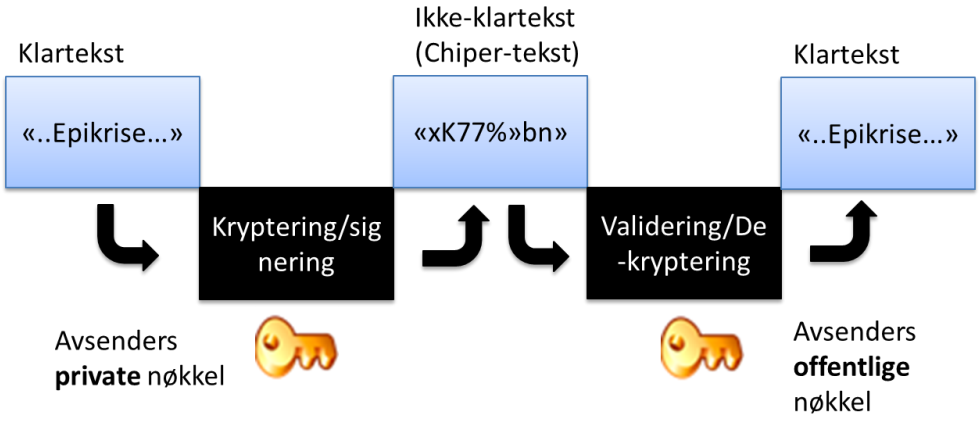
Figur 23 viser de ulike anvendelsesområdene for PKI.

PKI anvendelsesområde	Beskrivelse
Autentisering	Etablering av tillit til en person, organisasjon eller subjekts identitet.
Kryptering	Gjøre data ikke gjenkjennbart.
Signering	Verifisering av dataintegritet og ikke-avviselighet. Sistnevnte betyr at man ikke kan benekte at man har signert. En signatur er et tall som er beregnet matematisk fra dataene, en såkalt "hash". Dette tallet benytter så mottakeren av dataene ved bruk av sertifikatet for å sjekke om tallet er det samme. Er de ikke det har dataene blitt endret og signaturen er brutt hvilket betyr at dataene ikke er gyldige. Prosessen for å generere en digital signatur er som følger: 1. Algoritme benyttes for å generere hash-verdi fra de aktuelle dataene. 2. Hash-verdien krypteres med avsenders private nøkkel. 3. Dataene (som også kan krypteres før hash-verdi genereres), hash-verdien og informasjon rundt hash-algoritmen sendes til mottaker. 4. Mottaker benytter avsender sin offentlige nøkkel for å dekryptere hash-verdien.

5. Mottaker benytter den samme hash-algoritmen på oversendt data for å generere ny hash-verdi.
6. Mottaker sammenligner dekryptert hash-verdi med egengenerert hash-verdi for å sjekke om de er like og dermed ikke blitt endret underveis.

Figur 23: PKI anvendelsesområder.

PKI baserer seg på en nøytral og tiltrodd tredjepart som utsteder sertifikatene. Utstederne må være registrert hos Post- og teletilsynet for å være kvalifiserte. Som et eksempel på bruk av PKI viser figur 24 fra venstre side klartekst som krypteres og signeres ved bruk av avsenders private nøkkel for så å verifisere signaturen på andre siden og til slutt de-kryptere teksten tilbake til klartekst ved bruk av avsenders offentlige nøkkel.



Figur 24: Prinsipp ved PKI.

Her vises en tabell som viser hvilke nøkler som skal benyttes når:

For å gjøre følgende	Benyttes	Type nøkken
Sende krypterte data	Mottakers	Offentlige nøkkel
Sende kryptert signatur	Senders	Private nøkkel
Dekryptere krypterte data	Mottakers	Private nøkkel
Dekryptere en kryptert signatur (og autentisere senderen)	Senders	Offentlige nøkkel

3.3.3.2.1 Sertifikattyper

Det skilles mellom to ulike sertifikattyper:

- Personlig: Et personsertifikat for en bestemt fysisk person som entydig identifiseres i sertifikatet med en privat kode (pinkode). Eksempler på personlige sertifikater kan være:
    - BankID
    - Smartkort (ID-kort med SIM)
    - USB-enhet
    - Installert på PC
- Virksomhet: Et virksomhetssertifikat for en enhet (virksomhet) som entydig identifiseres i sertifikatet. Eksempel på virksomhetssertifikat kan være et digitalt sertifikat utstedt av godkjent sertifikatutsteder.

Hva er så forskjellen mellom disse i praksis? Virksomhetssertifikater representerer virksomheten og skal sikre nettopp kommunikasjonen til og fra virksomheter og enheter og inneholder ikke personinformasjon. Personlige sertifikater benyttes der det er behov for å knytte personer til digitale signaturer og data. Vanligvis knyttes en unik ID som personnummer etc. opp mot sertifikatet.

3.3.3.2.2 Sikkerhetsnivå for digitale sertifikat

Digitale sertifikater inndeles i ulike sikkerhetsnivåer. Dokumentet "Kravspesifikasjon for PKI i offentlig sektor[51] har laget en egen inndeling ut i fra hva myndighetene har definert. Under vises utdrag fra dokumentet:

"I april 2008 publiserte Fornyings- og administrasjonsdepartementet "Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor" [52] hvor det brukes 4 sikkerhetsnivåer. Disse 4 sikkerhetsnivåene har etter hvert blitt innarbeidede begreper i offentlig sektor. Sikkerhetsnivåene i kravspesifikasjonen forholder seg til de to øverste sikkerhetsnivåene i rammeverket: nivå 3 og 4. "Person-Standard" er tilpasset krav til nivå 3, og "Person-Høyt" er tilpasset krav til nivå 4"[51].

Kravspesifikasjon for PKI i offentlig sektor[51] har definert tre ulike sikkerhetsnivåer, to for privatpersoner og et for virksomheter:

- Person-Høyt
    - Et personsertifikat for en bestemt fysisk person som entydig identifiseres i sertifikatet. Person-Høyt er basert på kvalifiserte sertifikater, jf. esignaturloven § 4. Eksempel på Person-Høyt kan være BankID og ID-Porten og bruk av smartkort.
- Person-Standard
    - Et personsertifikat for en bestemt fysisk person som entydig identifiseres i sertifikatet. Eksempel på Person-Standard sertifikat kan være MinID.
- Virksomhet
    - Et virksomhetssertifikat for en enhet (virksomhet) som entydig identifiseres i sertifikatet.

3.3.3.3 Identitetshåndtering

Det er nødvendig å beskrive litt om identiteter generelt, hvordan de forvaltes og til slutt hvordan dette passer inn i en tjenesteorientert arkitektur da det tross alt er identiteten som er med på å gi tilgang til elektroniske tjenester.

Hva er egentlig en identitet? En identitet er en representasjon av en entitet, vanligvis en bruker, som inneholder et sett med attributter[36].

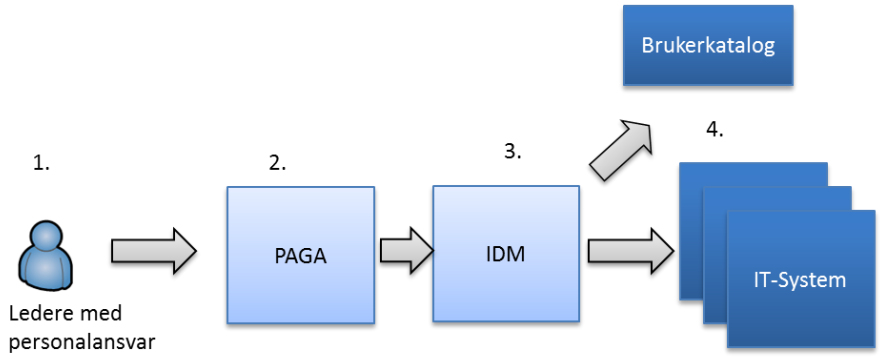
Regler for tilgang til ressurser er basert på identitetens attributter og relasjoner. For en gitt identitet og en gitt ressurs er det derfor en rekke attributter og relasjoner det kan være relevant å samle inn avhengig av hva slags anvendelse som er aktuell. For identitets- og tilgangsstyring påvirkes dette av to sentrale forhold:

1. Hvordan skal identiteten identifisere seg
2. Hvilke attributter trenger de ulike ressursene for å gi aktuell tilgang

I tillegg til disse statiske attributtene kan det også være situasjonsbestemte parametere som lokasjon og omgivelser, hvilket utstyr en bruker benytter, hvilken dato eller tid, etc., som styrer tilgangen.

Sikkerhetsdomener benyttes for å holde styr på en organisasjons datamaskinpark, brukere, nettverk og definerer ofte de juridiske virksomhetsgrensene. Hvert sikkerhetsdomene definerer ofte sin egen brukerkatalog (ikke delt). Brukerkataloger populeres av identitetshåndteringssystem (IDM) der leder og HR-avdelinger etc. registrerer nyansatte eller oppdaterer informasjon vedrørende ansatte. En brukerkatalog består av informasjon rundt brukere som identitet og gruppetilhørighet som igjen er avgjørende for tilgang til ressurser og autentisering i systemer innen aktuelt sikkerhetsdomene. Katalogen er tilgjengelig på en server via standard teknologi som for eksempel Leightweight Directory Access Protocol (LDAP). Programvareleverandøren Microsoft har sin implementasjon av denne standarden i et produkt som heter Active Directory (AD) og er den katalogtjenesten som er svært vanlig i organisasjoner. Strategien rundt prosessene for å registrere brukere i Helse Sør-Øst er

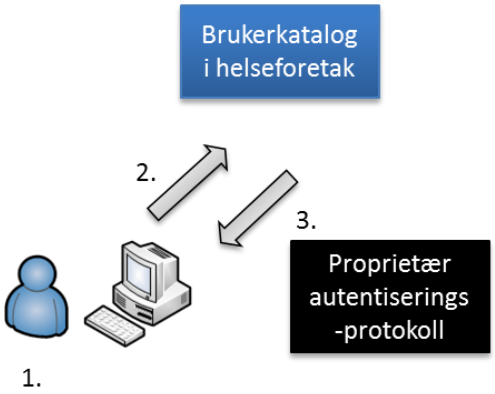
formålstjenlig å beskrive her forenklet da det er med på å gi en god oversikt over de ulike elementene i identitetsforvaltning (Figur 25).



Figur 25: Prinsipp ved brukerregistrering i Helse Sør-Øst.

1. Ledere med personalansvar i Helse Sør-Øst registrerer og vedlikeholder informasjon om medarbeidere i Personalportalen
2. Brukeren registreres i Helse Sør-Øst sitt lønns og personalsystem PAGA
3. Brukeren overføres til identitetshåndteringssystemet
4. Identitetshåndteringssystemet provisjonerer ut brukeren til aktuell brukerkatalog i sikkerhetsdomenet der brukeren skal ha en rolle i tillegg til aktuelle IT-systemer brukeren skal ha tilgang til. Merk at det i skrivende stund er en prosess i Helse Sør-Øst for å etablere nytt felles IDM-system som skal dekke hele regionen, men prinsippet er som beskrevet.

Applikasjoner og andre ressurser som tilbyr tjenester, funksjoner og informasjon må ha kontroll med brukere. Ressursen må vite hvem brukeren er, må få vite eller selv avgjøre hva slags rettigheter brukeren skal ha, og kan også ønske å registrere hvilke handlinger brukeren utfører. Et eksempel kan være en bruker som logger seg på lokal PC i et helseforetak noe som igjen gir tilgang til forhåndskonfigurerte filområder. Selve påloggingen skjer som følger:



1. Bruker logger seg på lokal PC med brukernavn og passord
2. Brukernavn og passord sendes over nettverket til aktuell brukerkatalog for autentiseringssjekk.
3. Ved suksessfull autentisering sender brukerkatalog tilbake autentiserinstoken. Denne billetten er proprietær hvilket betyr at den er plattformavhengig og kan ikke deles mellom ulike teknologier og plattformer. Ved bruk av Microsoft AD som brukerkatalog (noe som er svært vanlig i organisasjoner der Microsoft servere benyttes) heter denne autentiseringsprotokollen Kerberos[53].

Etter å ha logget seg på lokal PC med suksess logger brukeren seg på et system, la oss si EPJ med samme bruker. På bakgrunn av identitet kan EPJ-systemet så autentisere aktuell pålogget bruker for innlogging. Autorisasjon for tilgang til ulik funksjonalitet og data avgjøres lokalt i EPJ også på bakgrunn av brukerens identitet og oppsatte tilganger/autorisasjoner.

Hvordan passer så dette inn i tjenesteorientert arkitektur?

Tilgangskontroll i tjenesteorientert arkitektur innebærer autentisering og autorisasjon av identiteter i prinsippet over flere sikkerhetsdomener. *Det er da ingen garanti for at teknologi og plattform er lik i de ulike domenene*. Hvordan adresseres så dette? Det er her prinsippet om nettopp plattformuavhengighet kommer inn i bildet. Standardene under WS-Security er basert på XML med teknisk interoperabilitet som et av målene. De neste avsnittene tar for seg disse standardene for å beskrive hvordan tjenesteorientert arkitektur adresserer autentisering internt eller mellom flere sikkerhetsdomener med forskjellige brukerkataloger, plattformer og teknologier.

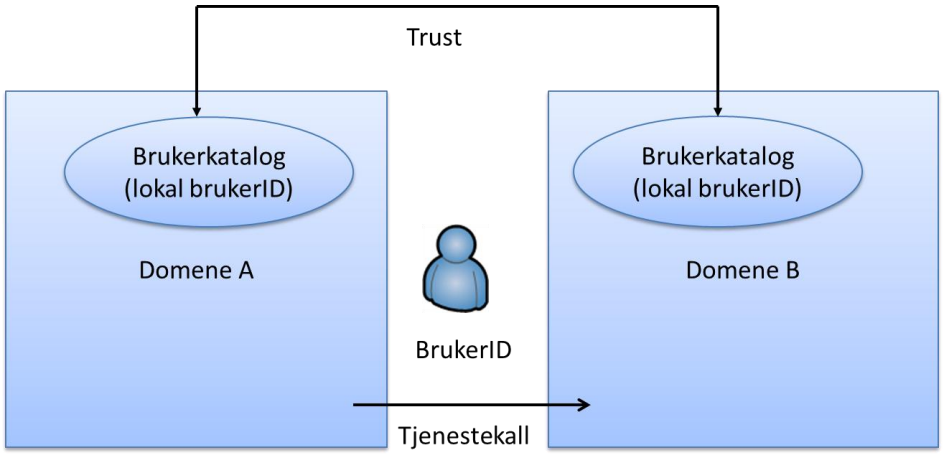
3.3.3.4 Identitetsføderering (eng: identity federation) og tillit (eng: trust)

Å føderere brukere over flere sikkerhetsdomener betyr ikke at aktuelle sikkerhetsdomener faktisk har aktuell bruker registrert i sine brukerkataloger. Hvordan får man da autentisert vedkommende i et annet sikkerhetsdomene? For å illustrere denne problemstillingen for spesialisthelsetjenesten der hvert helseforetak er egne juridiske enheter og med egne sikkerhetsdomener og brukerkataloger er det nettopp en utfordring å autentisere brukere på tvers av helseforetak. Sikkerhetsdomene A må ha kjennskap til brukeren i sikkerhetsdomene B dersom tilgangen på tvers skal kunne autentiseres i aktuell tjeneste.

Identitetsfederering omhandler standarder (WS-Federation og WS-Trust) og PKI. For å utstede autetiseringsbillett fra STS brukerkatalog (SAML), frakte denne informasjonen over et eller flere sikkerhetsdomener for så å benytte samme autetiseringsbillett for og nettopp autentisere brukeren i aktuelt sikkerhetsdomene. Autentiseringsbilletten signeres ved bruk av PKI for å sørge for at den ikke endres underveis. Dette gjøres via en såkalt Security Token Service som er et tjenesteorientert teknisk grensesnitt til brukerkatalogen i aktuelt sikkerhetsdomene.

Tjenesteorientert arkitektur baserer seg på at det etableres *tillit* (eng: trust) mellom sikkerhetsdomener. Dette er en nødvendighet fordi som det innledningsvis i avsnitt 3.3.3.3 ble beskrevet ofte ikke finnes en brukerkatalog for alle brukere i en samhandlingskjede, men hvert sikkerhetsdomene har egne brukerkataloger. Det som da gjøres er å si at "vi stoler på at alle brukere fra domene faktisk er de de utgir seg for å være. Med andre ord, det etableres et tillitsforhold på et organisatorisk og teknologisk plan. For å kunne etablere trust mellom to sikkerhetsdomener må det

finnes mekanismer som gjør det mulig å validere at etablert trust faktisk er gyldig. Den underliggende trust-modellen som benyttes er PKI[48]. Figur 26 viser logisk prinsipp ved etablering av trust.

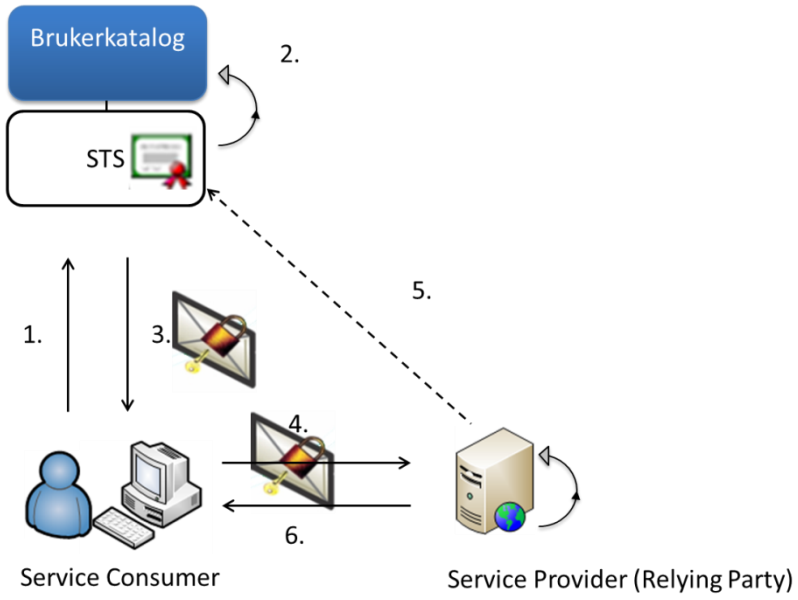


Figur26: Logisk prinsipp ved trust mellom to sikkerhetsdomener.

Hvordan fungerer så dette i praksis? Det er hensiktsmessig å vise hvordan dette fungerer både ved autentisering innen eget domene i tillegg til mellom to ulike domener med hver sin brukerkatalog.

3.3.4 Viktige begreper i tjenesteorientert arkitektur

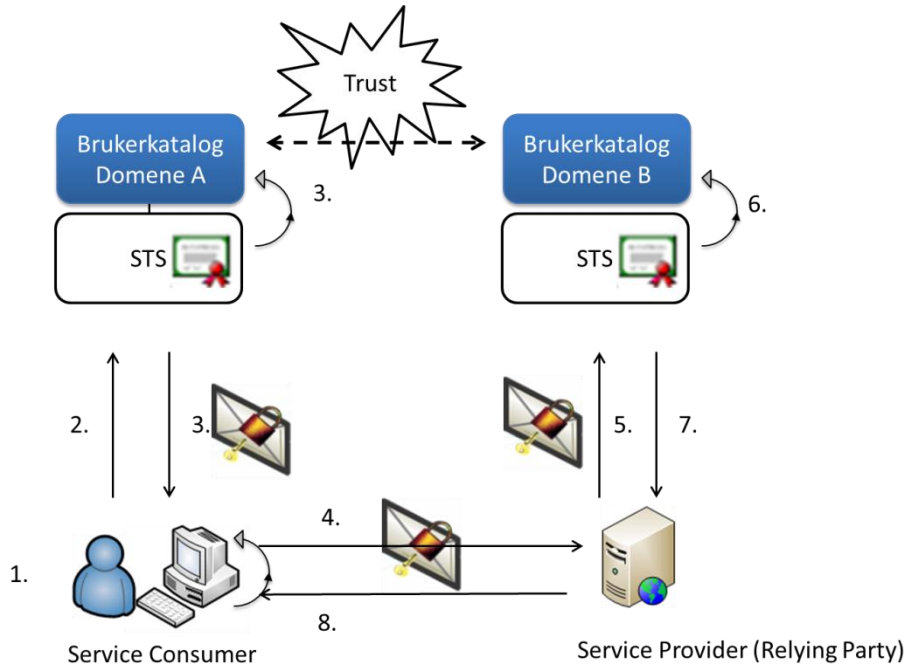
Det er nødvendig med et omforent begrepsapparat når vi snakker om tjenesteorientert arkitektur for forståelsen de ulike teknologiske bestanddelene. Her gis en innføring i de viktigste begrepene slik at leseren har en forforståelse av teori og diskusjoner videre i oppgaven. Figur 27 viser hovedprinsippet ved autentisering i tjenesteorientert arkitektur innen eget domene:



Figur27: Referansearkitektur ved autentisering i tjenesteorientert arkitektur innen samme domene.

1. Klient (bruker) forespør tjeneste (web-service) fra klientapplikasjon som er fysisk plassert i samme domene som klienten befinner seg i. Forespørselen blir da dirigert til STS.
2. STS foretar autentiseringskontroll mot brukerkatalog.
3. Ved suksessfull autentisering genererer STS en SAML-billett som signeres med PKI og returnerer denne til klienten.
4. Klientapplikasjonen legger ved SAML-billett i forespørselen til tjenesten.
5. Tjenesten validerer SAML-billett fra forespørselen opp mot STS. Her vil signatur valideres med PKI.
6. Ved suksessfull autentisering kalles så tjenesten for så og returnere resultatsettet tilbake til klientapplikasjon.

Ved autentisering mellom to ulike domener opprettes det først trust mellom domenene. Referansearkitekturen ser slik ut:



Figur 28: Referansearkitektur ved autentisering i tjenesteorientert arkitektur mellom to forskjellige domener.

1. Klient (bruker) forespør tjeneste (web-service) fra klientapplikasjon som er fysisk plassert i samme domene som klienten befinner seg i (domene A). Forespørselen blir da dirigert til STS.
2. STS foretar autentiseringskontroll mot brukerkatalog.
3. Ved suksessfull autentisering genererer STS en SAML-billett som signeres med PKI og returnerer denne til klienten.
4. Klientapplikasjonen legger ved SAML-billett i forespørselen til tjenesten.
5. Tjenesten i domene B validerer SAML-billett fra forespørselen opp mot lokal STS. Her vil signatur valideres med PKI.
6. Ved suksessfull autentisering kalles så tjenesten for så og returnere resultatsettet tilbake til klientapplikasjon.

3.3.4.1 Egendefinert STS

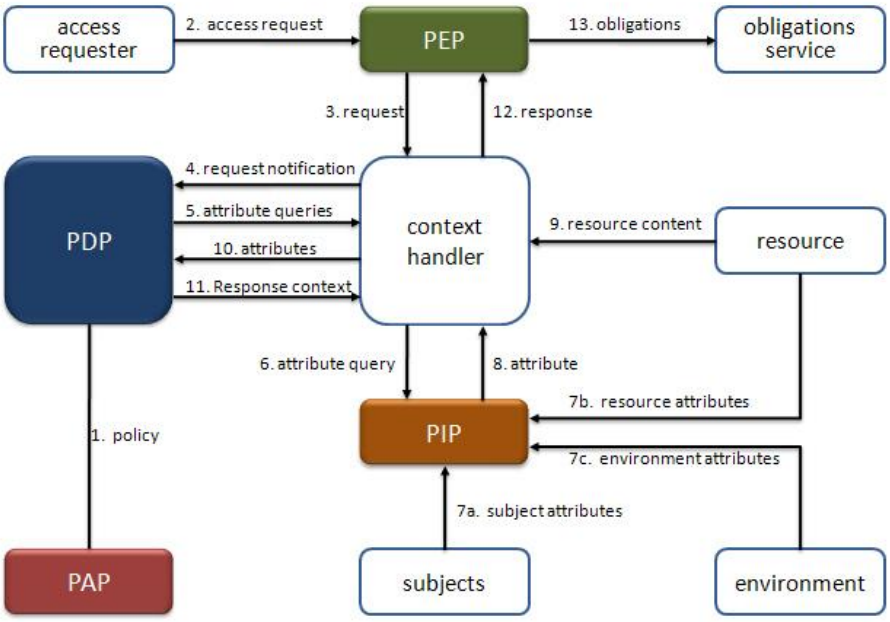
Brukerkatalogers (typisk AD) grensesnitt mot tjenesteorientert arkitektur og validering/signering utstedelse av SAML-sikkerhetstokens dreier seg om identiteten til brukeren. Hva om det er nødvendig med egendefinerte attributter ut over de som brukerkataloger kan støtte? I de tilfeller er det vanlig å utvikle egendefinert(e) STS der målet er og populere SAML-sikkerhetstokens med spesielle attributter som måtte være nødvendige for tilgangsforespørselen for eksempel dynamiske attributter utover identitet.

3.3.5 Tilgangskontroll i tjenesteorientert arkitektur.

3.3.5.1 XACML 2.0

XACML [25]er kompletterende standard utover SAML som omhandler det å utføre valgene rundt tilgangskontroll[18]. Dette betyr at når en service provider blir forespurt av en service consumer må tjenesten sørge for at den spesifiserte sikkerhetspolicy gjennomføres. Et eksempel kan være: Straks en leges identitet blir verifisert av det aktuelle systemet ved bruk av SAML kan det ved bruk av XACML utføres valg hvorvidt den samme legen har rett til spesifikke data til en pasient.

3.3.5.2 XACML 3.0 Arkitektur



Figur 27: XACML sikkerhetsmodell for tilgangskontroll i tjenesteorientert arkitektur[26]

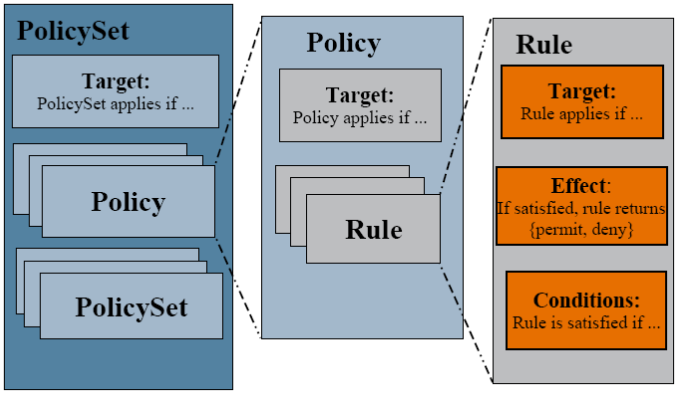
XACML virker på følgende måte[26]:

XACML profilen spesifiserer fem entiteter som håndterer tilgangsstyring: Policy Enforcement Point (PEP), Policy Administration Point (PAP), Policy Decision Point (PDP), Policy Information Point (PIP) i tillegg til en kontekstbehandler.

- PAP fungerer som lagringspunkt for policyer og tilbyr disse policyene til PDP.
- PDP fungerer som hovedpunkt for tilgangssyring ved å samle inn nødvendig informasjon fra andre aktører for så å konkludere resultat.
- PEP er et grensesnitt og fasade mot hele miljøet til verden utenfor. PEP mottar tilgangsforespørsler og evaluerer de ved hjelp av de andre aktørene og tillater eller avslår tilgang til ressursene.
- PIP er punktet hvor de nødvendige attributtene for evaluering av policyene samles inn fra de ulike interne og eksterne aktørene. Attributtene kan samles inn fra ressursen som skal aksesseres, miljøet (tid, sted), subjekter osv.

XACML – modellen består av tre hovedkomponenter:

- Rule (Regel): Et regelelement er det grunnleggende elementet for en policy. Det definerer såkalte "target elements" som beskriver hvem regelen gjelder for og setter betingelser for å bruke den. En regel består av tre komponenter:
    - Target – definerer ressurser, subjekter, aksjoner og miljøet for der regelen skal brukes. Et eksempel kan være en lege som skal aksessere en pasients sammenstilling av kliniske data.
    - Effect – definerer konsekvensen av regelen.
    - Condition – definerer betingelser som skal gjelde for regelen.
- Policy (Polise): Policyer er de ulike settene med regler som kombineres ved hjelp av algoritmer.
- PolicySet: Et sett med policyer som kan kombineres.

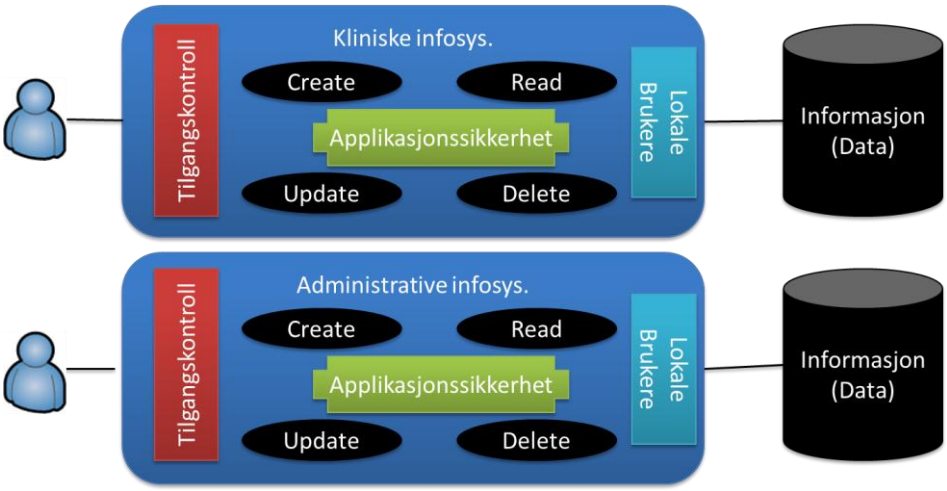


Figur 28: XACML modell.

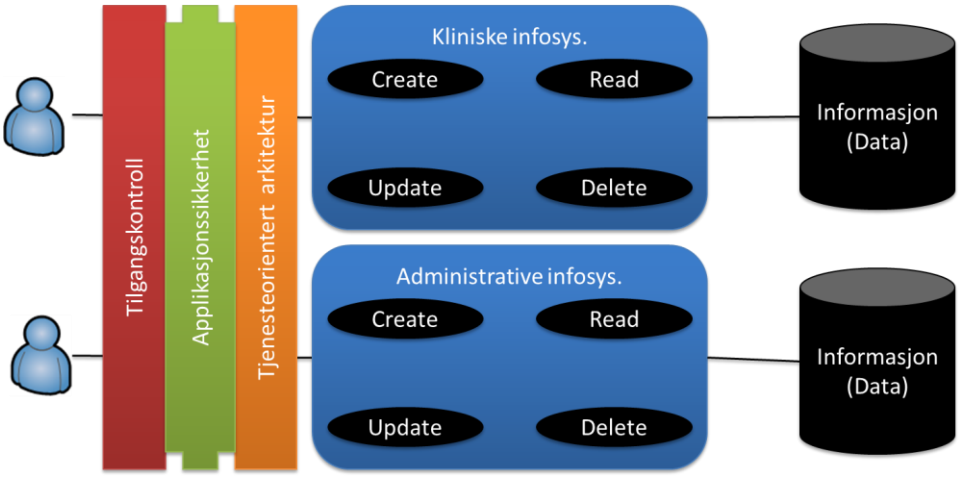
3.3.5.3 Hvorfor er XACML viktig?

Ved første øyekast kan det kanskje ikke være helt innlysende hvilket problem XACML forsøker å løse. Med SAML blir informasjonsattributter sendt mellom de ulike aktørene. Disse aktørene må derfor enes om formatet for dataene i tillegg til å enes om hvordan autorisasjon skal utføres. Dersom to aktører er uenig i hvordan de skal beskrive autorisasjonsprosesser på, blir egenskaper som Single Sign On (SSO)[23] umulig å gjennomføre fordi de ikke er i stand til å uttrykke informasjon om sikkerhetsstatus for respektive brukere til hverandre. XACML er et plattformuavhengig *policy-utvekslingsformat* som systemer skal kunne bruke for utveksle eller dele autorisasjonspolicyer-selv om policyene oversettes til et proprietært eller lokalt format. Bruk av XACML betyr at policyer for tilgangskontroll ikke har behov for å være tett koblet til systemene som styrer tilgangskontrollen., men kan fungere på tvers av systemer og organisasjoner, ressurser, databaser og applikasjoner. XACML kan også forstås ut i fra SAML arkitekturen der SAML protokoller bruker autoriserings-spørring for å spørre om autorisasjon for tilgang. I tillegg kan en attributt-spørring utføres for å finne informasjon som benyttes for å foreta autorisasjonsvalg (ABAC).

Tradisjonelt har autentiserings og- autorisasjonsfunksjonalitet i applikasjoner blitt laget med tette knytninger hvilket betyr at de er innbakt i kildekoden uten støtte for interoperabilitet mellom andre systemer. XACML lar tjenesteleverandører og applikasjonsutviklere eksternialisere autorisasjonsprosessene og beskrivelsene av de ut fra applikasjonene. Dette betyr sentralisert forvaltning av autorisasjonsdefinisjoner. Dette passer svært godt til tjenesteorientert arkitektur da det ofte involverer flere samhandlingsparter som benytter heterogene plattformer (applikasjoner) som alle trenger et felles autorisasjonsrammeverk. Figur 29 under viser arkitekturprinsippet med tett knyttet og proprietær tilgangskontroll, mens figur 30 viser arkitekturprinsippet med eksternialisert tilgangskontroll:



Figur 29: Tett knyttet og proprietær tilgangskontroll.



Figur 30: Eksterialisert tilgangskontroll.

3.4 Formalisert bruk av standarder rettet mot tilgangskontroll og informasjonsutveksling i kliniske informasjonssystemer

Standardene SAML.20 og XACML 3.0 beskrevet over sier ingenting om informasjonsinnhold, hvordan informasjon skal utveksles eller definerer regler for tilgangskontroll. Det finnes derimot noen organisasjoner og standardiseringsorgan som ved formalisert bruk av eksisterende standarder har satt sammen disse for bruk i kliniske informasjonssystemer for rammeverk for tilgangskontroll og informasjonsutveksling.

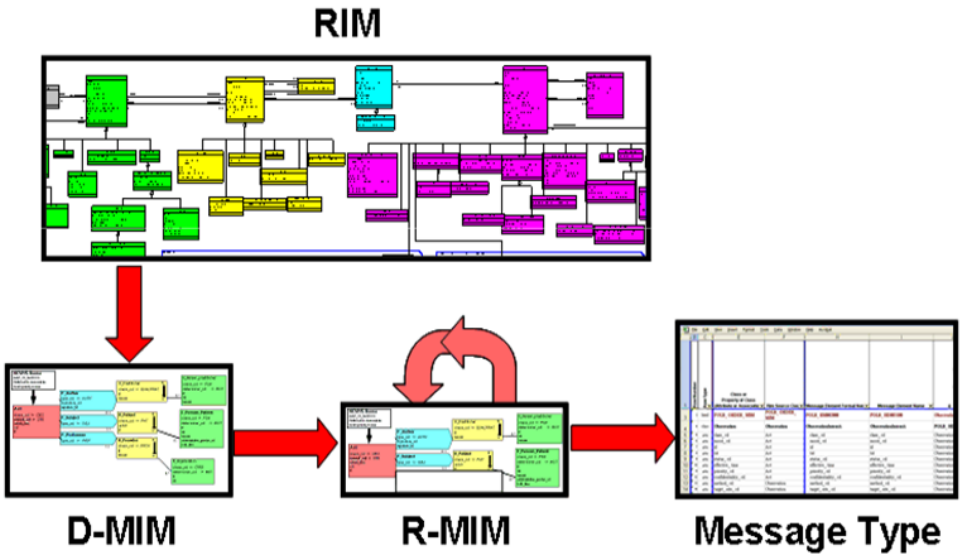
3.4.1 HL-7v3

HL-7 (Health Level Seven) ble stiftet i 1987 og er en organisasjon akkreditert av American National Standards Institute (ANSI) som involverer seg i å utvikle internasjonale interoperabilitetsstandarder og rammeverk for utveksling, integrering, deling og innsamling av elektronisk helseinformasjon[37]. HL-7 Standardene definerer hvordan informasjon struktureres og kommuniseres fra en enhet til en annen der påkrevde språk, informasjonsstruktur og datatyper for sømløs elektronisk samhandling. HL-7 v3 er basert på XML.

Nyeste versjon av HL-7-standardene er versjon 3 som er en modellbasert spesifikasjon hvilket betyr at det baserer seg på å utvikle domenemodeller som er abstrakte representasjoner av virkeligheten. I hjertet av dette ligger en felles statisk informasjonsmodell – RIM (Reference Information Model) som er en objektorientert, stor og svært detaljert representasjon over kliniske data. RIM definerer livssyklusen til meldinger som skal utvikle og fungerer som en delt modell mellom alle kliniske helsedomener.

Ut i fra RIM velger en så aktuelle informasjonselementer som er aktuelle for domenet det skal utvikles konkret informasjonsmodell for og blir dermed et spesifikt subsett av RIM og vil få betegnelsen D-MIM (Domain Message Information Model).

Ved å fingranulere informasjonsstrukturene i D-MIM slik at modellen passer inn i ønsket klinisk domene blir den et subsett av D-MIM og få benevnelsen R-MIM (Refined Message Information Models). Dette utføres iterativt til meldingstype er tilfredsstillende.



Figur 31: Utviklingsprosess for meldingstyper basert på HL-7 v3.

3.4.2 CDA (Clinical Document Architecture)

CDA er en sentral standard i HL-7 som spesifiserer struktur og semantikk for kliniske elektroniske dokumenter med det formål å utveksle de mellom kliniske informasjonssystemer[39]. Denne standarden passer godt til dagens dokumentbaserte elektroniske pasientjournalsystemer (EPJ) og kan inkludere tekst, bilde, lyd og annet multimediainnhold. Eksempler på bruk av denne standarden kan være henvisning, epikrise, observasjoner og medisinsk historikk. Hovedkomponentene i et CDA-dokument er som følger[39]:

- **Header** – identifiserer og klassifiserer dokumentet i tillegg til å gi informasjon om autentisering, pasient og eventuelle involverte parter.
- **Body** – består av den kliniske informasjonen og har 3 grader av semantisk interoperabilitet. Dette betyr med andre ord hvor strukturert informasjonen er:
    - Level 1: Lavest grad av interoperabilitet og struktur. Inkluderer CDA Header i tillegg til body bestående av ustrukturerte data i form av et vedlegg som PDF, DOCX eller annet.
    - Level 2: Høyere grad av interoperabilitet og struktur. Inkluderer CDA Header og Body bestående av XML-deklarasjon med beskrivende felter som er identifisert med koder.

- Level 3: Høyest grad av interoperabilitet og struktur. Inkluderer CDA Header og Body bestående av XML-deklarasjon med beskrivende felter som er identifisert med koder som eksisterer i RIM. Eksempler på dette kan være:
  - LOINC
  - SNOMED
  - CPT

```
<ClinicalDocument>
  ... CDA Header ...
  <StructuredBody>
    <section>
       <text>...</text>
      <Observation>...</Observation>
      <Observation>
        <reference>
          <ExternalObservation>...</ExternalObservation>
        </reference>
      </Observation>
    </section>
    <section>
       <section>...</section>
    </section>
  </StructuredBody>
</ClinicalDocument>
```

Figur 32: Overordnet struktur i et CDA-dokument.

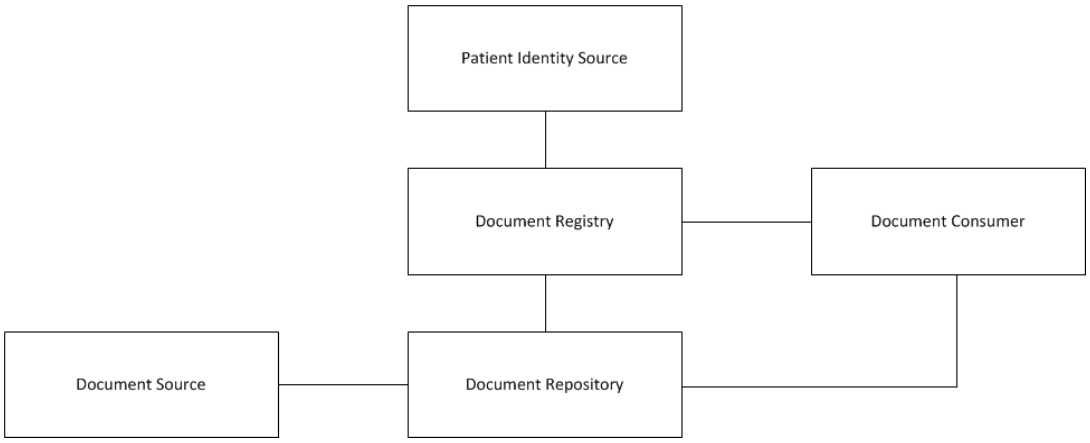
3.4.3 IHE

Integrating the Healthcare Enterprise (IHE) er en organisasjon som formaliserer bruken av eksisterende standarder for å legge til rette for elektronisk samhandling mellom kliniske informasjonssystemer[45]. IHE definerer ulike profiler i form av tekniske rammeverk for arkitektur av dokumentutveksling og integrasjonsprofiler for ulike domener innen kliniske enheter. Integrasjonsprofilene definerer det semantiske innholdet. Eksempler på domener kan være:

- Patologi
- Lab
- Apotek
- Radiologi

IHE Cross-Enterprise Document Sharing (XDS)[44] er et teknisk rammeverk basert på eksisterende standarder for å håndtere utveksling av dokumenter mellom kliniske informasjonssystemer i helseenheter. Dette håndteres gjennom sentraliserte eller distribuerte dokumentlagre i tillegg til et indeksert dokumentregister som inneholder metadata rundt selve dokumentene. Dokumentene kan være av typen HL-7 CDA. XDS består av følgende entiteter med hver sitt ansvarsområde:

- Dokument Repository. Lagrer dokumenter. Kan være sentralisert eller distribuert.
- Document Registry. Lagrer informasjon om dokumentene som versjoner og hvor de fysisk befinner seg.
- Document Sources. Dokumenter kan være fysisk lokalisert i en eller flere dokumentlagre.
- Document Consumers. Dokumenter aksesseres av en eller flere konsumenter.



Figur 33: Aktører i XSD.

3.4.4 OASIS

Organization for the Advancement of Structured Information Standards (OASIS) er en non-profit internasjonalt standardiseringsorgan som produserer standarder for informasjonssikkerhet, nettskyen, tjenesteorientert arkitektur og web services etc. I et initiativ på å oppnå interoperabilitet for tilgangskontroll mellom kliniske informasjonssystemer og enheter i helsevesenet, har OASIS etablert en teknisk komite kalt Cross-Enterprise Security and Privacy Authorization (XSPA)[40] med det formål å utvikle profiler som definerer semantikk for tilgangsstyringen. Profilene er basert på de eksisterende standardene SAML 2.0 og XACML 3.0. XSPA er tilpasset det amerikanske helsevesenet og dets krav til klinisk tilgangskontroll og ved Health Insurance Portability and Accountability Act (HIPAA). Videre følger en beskrivelse av disse standardene:

3.4.4.1 Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of Security Assertion Markup Language (SAML) for Healthcare v1.0[40]

Profilen baserer seg på SAML 2.0-standarden og definerer et minimum sett med vokabular i form av attributter som er nødvendig for å oppnå semantisk interoperabilitet for igjen å kunne foreta tilgangskontroll til ressurser og funksjonalitet mellom kliniske informasjonssystemer. Følgende attributter er definert i profilen:

Attributt (Gjengitt med namespace)	Datatype	Gyldige verdier
urn:oasis:names:tc:xacml:2.0:subject:subject-id	String	Unik identifikator for subjektet som påkrevd av HIPAA.
rn:oasis:names:tc:xpsa:1.0:subject:organization	String	Organisasjonstilhørighet for subjekt.
urn:oasis:names:tc:xspa:1.0:subject:organization-id	anyURI	Unik identifikator for organisasjon.
urn:oasis:names:tc:xspa:1.0:subject:hl7:permission	String	Refererer til [HL-7 PERM] for rettigheter. (Operation Definitions)
urn:oasis:names:tc:xacml:2.0:subject:role	String	Definerer brukerens strukturelle rolle [ASTM E1986-98 (2005)].
urn:oasis:names:tc:xspa:1,0:subject:purposeofuse	String	Definerer konteksten for tilgangsforespørselen. Gyldige verdier: TREATMENT, PAYMENT, OPERATIONS, EMERGENCY, SYSADMIN, MARKETING, RESEARCH, REQUEST, PUBLICHEALTH
urn:oasis:names:tc:xacml:1.0:resource:resource-id	String	Unik identifikator over ressursen som skal aksesseres. I følge profilen er dette en unik identifikator for pasienten.
urn:oasis:names:tc:xspa:1.0:resource:hl7:type	String	Refererer til [HL-7 PERM] for hva som skal utføres (Object Definitions).

urn:oasis:names:tc:xspa:1.0:environment:locality	String	Unik identifikator som representerer tjenesteyters organisasjon.
urn:oasis:names:tc:xspa:2.0:subject:npi	String	National Provider ID (U.S. Goverment for all active providers).

3.4.4.2 Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of XACML v2.0 for Healthcare Version 1.0[41]

Profilen baserer seg på XACML 2.0-standarden[25] som autorisasjonsrammeverk og definerer semantisk interoperabilitet for tvers av helseenheter i form av mekanismer for å autentisere, administrere og benytte regler for autorisasjoner for tilgangsforespørsler til beskyttede (kliniske) data[42].

3.5 Relatert arbeid for teori

En rekke initiativ er gjort i andre forskningssammenheng der det er designet forslag på arkitektur for kommunikasjon mellom helseenheter basert på tjenesteorientert arkitektur. Gritzalis og Lambrinoudakis[46] skrev i 2004 "A security architecture for interconnecting healthcare information systems" der de omtaler problemstillingen rundt fragmentert pasientdata for kronisk syke. De presenterer en arkitektur for tilgang til pasientdata lagret hos ulike helseenheter som baserer seg på bruk av regler. Reglene blir uttrykt i form av XACML-rammeverket.

Namli og Dognac[49](2008) presenterer en løsning for tilgangskontroll for prosjektet "SAPHIRE"[49] som er en arkitektur for klinisk beslutningsstøttesystemer. Tilgangskontrollen benytter seg av tjenesteorientert arkitektur der XACML benyttes som standard for regeldefinisjoner og SAML benyttes som standard for attributter for federering av mellom enhetene som benyttes til autentisering og autorisasjon.

Et fellestrekk for alle initiativ er semantisk interoperabilitet mellom aktørene. Dette betyr at det i hvert enkelt case må utarbeides et sett med attributter som alle involverte parter skal benytte for autentisering og autorisasjon. I den norske spesialisthelsetjenesten er denne typen av semantisk interoperabilitet nærmest fraværende systemene seg i mellom og ikke minst mellom helseforetakene både regionalt og nasjonalt. Hvert enkelt helseforetak har sine rolledefinisjoner i sine systemer hvilket er helt ukjente for andre helseforetak.

4 Metode

Dette kapittelet beskriver metode for hvordan oppgaven er utarbeidet for forskningsspørsmålet. Det benyttes "design research"[50] som metode for gjennomføring. Design research fokuserer på problemløsning med det formål å forstå og forbedre designprosesser, spesielt innen design av informasjonssystem, utvidelser av dets kapabiliteter samt design av tjenester, og består av mennesker, organisasjoner og teknologi. Resultatet av designet presenteres ved å benytte IT-artefakter som kan defineres som konstruksjonselementer bestående av vokabular og symboler, modeller, metoder og instansieringer av implementerte prototyper og systemer. I artikkelen "Design Science in Informations Systems Research"[50] presenteres retningslinjer for forskning på informasjonssystemer (Figur 34). Retningslinjene er et verktøy for å forstå, utføre og evaluere forskning på informasjonssystemer.

Guideline	Description
Guideline 1: Design as an Artifact	Design-science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation.
Guideline 2: Problem Relevance	The objective of design-science research is to develop technology-based solutions to important and relevant business problems.
Guideline 3: Design Evaluation	The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods.
Guideline 4: Research Contributions	Effective design-science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies.
Guideline 5: Research Rigor	Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact.
Guideline 6: Design as a Search Process	The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment.
Guideline 7: Communication of Research	Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences.

Figur 34: Design Research Guidelines fra artikkelen *Design Science in Informations Systems Research*.

Tre av retningslinjene fra artikkelen benyttes som metodikk for å beskrive hvordan oppgaven er organisert og utført. Retningslinjene diskuteres i de neste kapitlene og forklarer hvordan oppgaven relaterer til de enkelte retningslinjene:

1. Retningslinje 1: Design as an artifact
2. Retningslinje 2: Problem relevance
3. Retningslinje 3: Design evaluation

4.1 Design as an artifact

Tjenesteorientert arkitektur er samhandlingsplattformen internt og eksternt mellom enheter spesialisthelsetjenesten. Tjenester formaliseres teknisk som web-services som også har som formål å kunne være tjenester som kan i praksis kan benyttes av alle helseregionene. Samtidig kommer det fra myndighetenes side nye føringer og endringer i gjeldende lovverk og forskrifter noe som krever stor endingsevne. Erfaringsmessig tar det lang tid å innføre nye tjenester i helse-Norge grunnet heterogenitet og minimal interoperabilitet både teknisk og semantisk. Tjenesteorientert arkitektur kan i denne sammenheng sees på som et verktøy som er med på å løse dette. Å løse forskningsspørsmålet med en fungerende teknisk løsning for tilgang på tversinnebærer mye mer arbeid og involvering av interessehavere enn tiden og omfanget denne masteroppgaven har til disposisjon. Derfor er det et godt valg med design research der det benyttes artefakter for og på et mer overordnet nivå kunne utarbeide en arkitektur. Arkitekturen vil enkelt kunne etterprøves og evalueres med scenarioer fra den virkelige arbeidshverdagen til helsepersonell. De ulike artefaktene er også utarbeidet i samråd med kollegaer i arkitekturgruppen der jeg jobber.

Å designe en arkitektur i form av artefakter for en problemstilling er ofte en metodikk som benyttes før den instansieres. På denne måten kan den endres og forfines til den tilfredsstiller kravene, både funksjonelle og ikke-funksjonelle som juridiske og kvaliteter. Artefaktene som er produsert i denne oppgaven fungerer som et vokabular for å definere forskningsspørsmålet, problemstillinger og løsninger rundt det. Kapittel 6 beskriver løsningsdesign ved først å bruke artefakter for en generell beskrivelse av informasjon og teknologi for tilgangskontroll for så og presentere artefakter for løsning der tilgang på tvers i en tjenesteorientert arkitektur kan være. Tilleggstjenester som er nødvendige kapabiliteter for å understøtte arkitekturen er også beskrevet som artefakter.

4.2 Problem relevance

Hvilke informasjonselementer må forstås for å kunne foreta autentisering og autorisasjon for tilgang etter klinisk informasjon på tvers av juridiske virksomhetsgrenser i spesialisthelsetjenesten slik at Helseinformasjonssikkerhetsforskriftens § 11c oppfylles?

Relevansen av forskningsspørsmålet var viktig i valg av problemstilling. Tilgang på tvers mellom enheter i helsesektoren er et svært aktuelt tema i skrivende stund med tanke på krav om økt elektronisk samhandling internt og mellom enheter og omsorgsnivå. De ulike føringer og forskrifter fra myndighetene styrker også relevansen til denne oppgavebesvarelsen sterkt.

Et av Samhandlingsreformens strategiske virkemidler for å få ned kostnader i form av liggedøgn på sykehus er å la kommunene få større del av ansvaret for både forebygging og behandling. Kronikerpasienter mottar typisk hoveddelen av pasientbehandlingen på et lokalsykehus mens den avanserte behandlingen mottas på et eller flere universitetssykehus. Økt spesialisering og pasienter som vandrer mellom omsorgsnivå er også viktige elementer som er med å underbygge det store behovet for innhenting av pasientinformasjon fra overnevnte enheter slik at helsepersonell kan danne seg et godt bilde av pasientforløp og dermed kunne gi adekvat behandling.

Som ansatt i arkitekturgruppen i Sykehuspartner IT har jeg deltatt i et regionalt strategiprosjekt for tilgangsstyring til kliniske informasjonssystem. Dette har vært svært nyttig både for forståelsen av teorien rundt, men også på grunn av relevansen for dette prosjektet generelt. Et stort antall artikler og aktuell litteratur er benyttet for å få et godt fundamentert overblikk over hvordan andre organisasjoner har løst denne typen problemstilling. Som samarbeidspartner for case har jeg hatt et godt samarbeid med DIPS og deres løsningsarkitekt og leder for forskning og utvikling (FOU) Trond Elde. Sistnevnte har fungert som ekstern veileder. DIPS er også et svært relevant case da det er det klart største og mest brukte systemet for elektronisk pasientjournal i spesialisthelsetjenesten. Med utgangspunkt i DIPS vil det være nødvendig å beskrive DIPS sin arkitektur for tilgangskontroll. Det vil være en del forutsetninger og avgrensinger som tas, dette for å tilpasse innholdet i oppgaven til tid og forskningsspørsmål. Kapittel 1, 2 og 3 legger det teoretiske grunnlaget for å kunne besvare forskningsspørsmålet som er definert i kapittel 2.4.3.

Kapittel 6 presenter løsningsdesign som skal løse forskningsspørsmålet. Arkitekturen består av diagramartefakter som et resultat av kravspesifikasjon der funksjonelle og ikke-funksjonelle krav beskrives. Kravene er formalisert ut i fra identifiserte behov fra brukstilfeller og forskningsspørsmålet. DIPS som er Norges største leverandør av EPJ vil benyttes som case for foreslått arkitektur. Det er i skrivende stund ikke laget modeller for tilgangskontroll mellom kliniske informasjonssystemer som dekker norske lover og forskrifter inklusive beslutningsstyrt tilgang.

Kapittel 7 presenterer evaluering av foreslått løsningsdesign. Det er et viktig poeng å vise at foreslått løsningsdesign virker som antatt. Brukstilfellene som ble beskrevet i kapittel 5 benyttes som bakgrunn for beskrivende evaluering (eng: descriptive evaluation) som er en av evalueringsmetodene for design research[50].

4.3 Design Evaluation

Evaluering av løsningsdesign vil skje i tråd med retningslinje 3 “design evaluation”. Realistiske scenarioer vil benyttes som testbenk for artefakter og løsningsdesign fra en reell problemstilling i spesialisthelsetjenesten. For infrastruktur benyttes to DIPS EPJ-instanser med hver sin database som er lokalisert henholdsvis i Oslo Universitetssykehus (OUS) og Kongsvinger Sykehus (SIHF).

Artefaktene vil benyttes som modeller hvor data og funksjonalitet fra DIPS vil være input. Målet er å bevise teoretisk empirisk at løsningsdesignet vil fungere.

5 Kravspesifikasjon

Løsningsdesignet presentes med fire diagram-artefakter som er løsningsdesign på kravspesifikasjon basert på brukstilfeller

5.1.1 Funksjonelle krav

Brukstilfelle

Det vil her presenteres to brukstilfeller som beskriver hvordan et målbilde for funksjonelle krav for elektronisk tilgang på tvers mellom enheter i helsesektoren kan være. Brukstilfelle 1 beskriver hvordan en tjenesteyter velger aktuell rolle når hun logger seg inn i EPJ-systemet. Dette må utføres da en tjenesteyter ofte har mange roller og det må velges hvilken rolle som skal benyttes i konteksten.

Brukstilfelle 2 beskriver hvordan søk etter pasientdata kan utføres fra EPJ-system. I søket velger lege ønsket sykehus og blir presentert med en dokumentliste hvor det velges ønsket dokument. Valgt(e) dokument(er) returneres så tilbake. Hensikten er å dekke det funksjonelle behovet i tillegg til de ikke-funksjonelle behovene for elektronisk tilgang på tvers. De ikke-funksjonelle kravene har stort fokus rundt sikkerhet og hvilke sikkerhetsmekanismer og nivå som er påkrevd fra myndighetenes side.

Forutsetninger:

1. Behandlende lege (Tjenesteyter) er i en situasjon der det er nødvending med komplettering av en aktuell pasients helseopplysninger som er registrert i andre helseforetak.

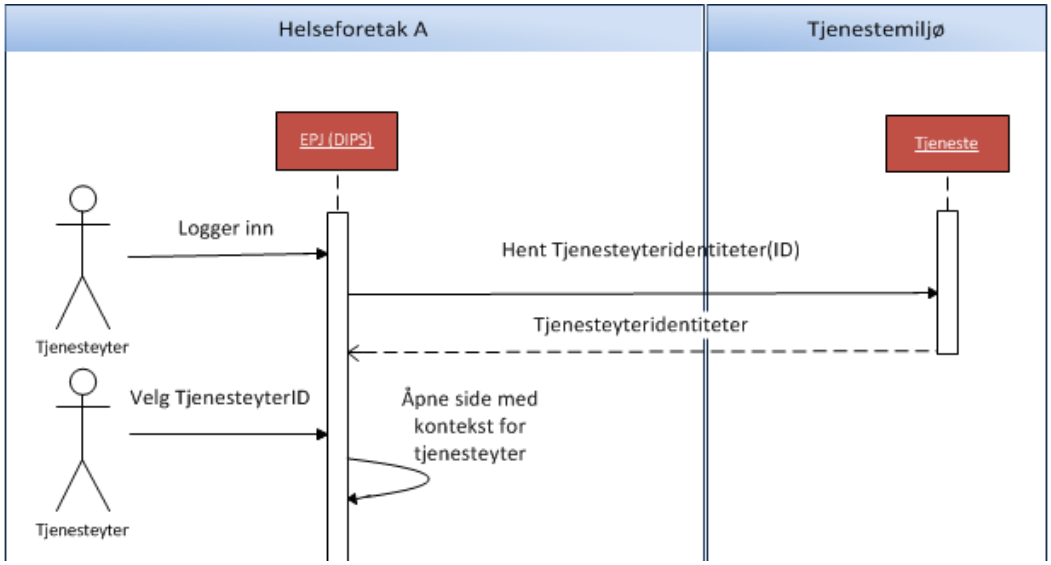
Steg brukstilfelle 1 – Tjenesteyter velger rolle:

1. Tjenesteyter logger seg på lokal maskin og inn i EPJ med brukernavn og passord og velger rolle i EPJ. I bakgrunnen henter EPJ en liste over aktuelle tjenesteyteridentiteter hun er tilknyttet fra en tjeneste og presenterer de i en liste som tjenesteyter velger fra. Rolle er nå valgt.

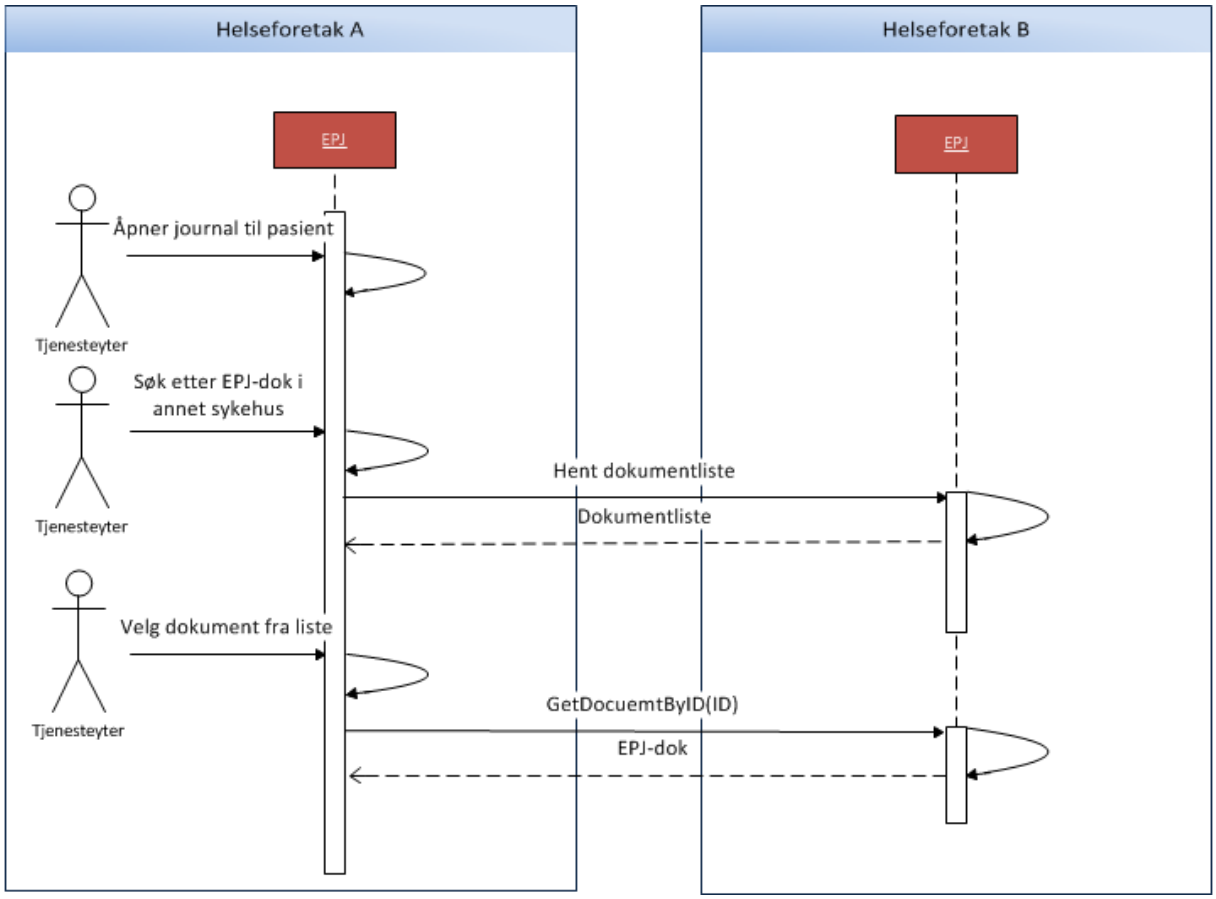
Steg brukstilfelle 2 – Tjenesteyter skal hente pasientopplysninger fra annen helseorganisasjons EPJ:

1. Tjenesteyter velger aktuell pasient i EPJ. Pasienten er nå aktiv pasient i EPJ
2. Tjenesteyter velger så å gå inn i skjermbildet for innhenting av pasientopplysninger fra andre EPJ ved å klikke på knapp merket “Hent journaldokument fra annen helseinstitusjon”. Tjenesteyter presenteres da med en rullgardinliste i skjermbildet der hun velger ønsket sykehus søket skal gjelde for i tillegg til dato fra/til som søket skal gjelde for og klikker “Søk”
3. Tjenesteyter presenteres så med en dokumentliste i skjermbildet bestående av tilgjengelige dokumenter for aktuell pasient i for gitt tidsperiode søket ble satt til.

4. Tjenesteyter velger så ønskede dokument fra dokumentlisten og klikker knapp merket “Hent valgt dokument”.
5. Valgt sykehus returnerer valgte dokumenter som tjenesteyter benytter til å danne seg et oversiktlig pasientforløp.



Figur 35: Sekvensdiagram - brukstilfelle 1.



Figur 36: Sekvensdiagram - brukstilfelle 2

5.1.2 Ikke-funksjonelle krav

De ikke-funksjonelle kravene er svært viktige i denne sammenheng. Dette fordi de juridiske informasjonssikkerhetskravene ved en slik løsning må oppfylles.

Ikke-funksjonelt krav ID	Beskrivelse
IFK-1	Løsningen skal ivareta krav til informasjonssikkerhet iht. norske lover og forskrifter, herunder også Helseinformasjonssikkerhetsforskriften og krav om beslutningsstyrt tilgang som beskrevet i EPJ-Standarden Del 2, Tilgangsstyring, redigering, retting og sletting.
IFK-2	Løsningen skal ivareta føringer og krav fra Helse-Sørøst sin IKT-langtidsplan, Samhandlingsreformen og Nasjonal-Ikt's strategidokument "Tjenesteorientert arkitektur i spesialisthelsetjenesten".
IFK-3	Løsningen skal ivareta føringer definert i Helse-Sørøst sine arkitekturprinsipper.

6 Løsningsdesign

Forskningsspørsmålet omhandler hvilke attributter/dataelementer som må inngå i en tilgangsforespørsel for pasientdata på tvers av enheter i spesialisthelsetjenesten. I dette spørsmålet skjuler det seg en del store utfordringer med tanke på interoperabilitet. Dette gjenspeiler i grunn situasjonen for elektronisk samhandling i helsevesenet i dag, nemlig at det ikke foreligger et omforent begrepsapparat. Løsningsdesignet vil adressere to hovedpunkter som må ligge til grunn for å kunne utføre dette:

1. Semantisk interoperabilitet for elektronisk samhandling:

   Konstellasjonen av person, roller, enheter og hvilke beslutning som ligger til grunn for tilgangsforespørselen mellom enheter i helsevesenet i dag støtter liten grad av interoperabilitet fordi det ikke foreligger harmonisering og standardisering for begrepsapparatet/semantikken rundt data for tilgangskontroll. For å understøtte elektronisk tilgang på tvers må dette harmoniseres. Løsningsdesignet adresserer disse utfordringene og vil foreslå etablering av ulike registre realisert som tjenester for å understøtte dette kravet.

2. Teknisk interoperabilitet for elektronisk samhandling:

   Som beskrevet i kapittel 3.3 er tjenesteorientert arkitektur samhandlingsplattformen internt og mellom enheter i spesialisthelsetjenesten og dette baseres løsningen på. Det er for øvrig uløste utfordringer med tanke på den tekniske delen ved autentisering og autorisering av tjenesteytere som benytter tjenester. Autentisering ved elektronisk tilgang på tvers som oppfyller Helseinformasjonssikkerhetsforskriften (Person-Høyt) er ikke etablert i dag noe som adresseres i løsningsdesignet i form av nye tjenester og infrastruktur.

Det er lagt vekt på at beskrivelsene skal være pedagogiske fremfor for detaljerte hvilket betyr at det som presenteres i dette kapittelet er av konseptuell karakter ved at det er gjort noen forenklinger i forhold til detaljer med elektronisk samhandling.

6.1 Forutsetninger

Følgende forutsetninger for oppgaven er identifisert og ligger til grunn for foreslått løsningsarkitektur:

- Begrenser seg til semantisk innhold i attributter som er nødvendige for å kunne utføre tilgangskontroll inkludert beslutningsstyrt tilgangsinformasjon.
- Ikke autorisasjonsregler ved bruk av XACML-rammeverket.
- Samtykke fra pasient vedrørende innsyn i pasientdata forutsettes etablert.
- Avtaler mellom helseforetakene vedrørende tilgang på tvers av EPJ er opprettet.

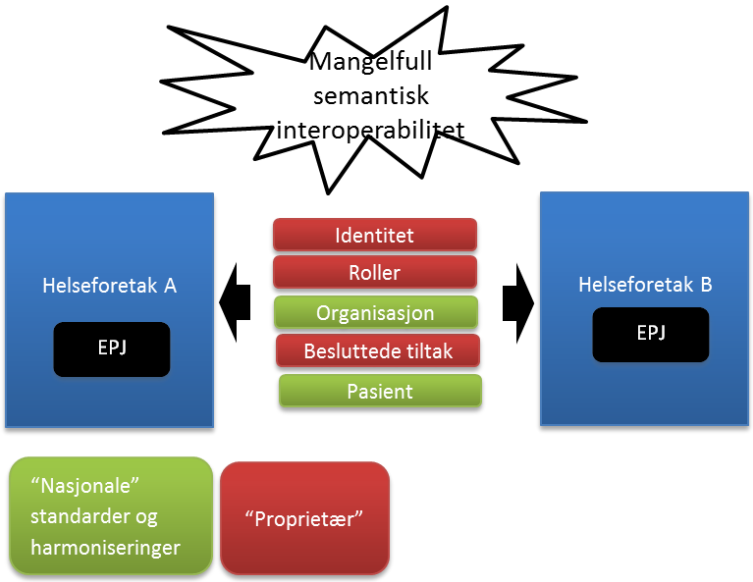
6.2 Semantisk interoperabilitet

Status i helsevesenet i dag for interoperabilitet mellom systemer er lav. Elektronisk tilgang på tvers synliggjør dette ytterligere da det ikke finnes et omforent begrepsapparat for data og betydningen av de. En rolle i et system heter og betyr som oftest noe annet i et annet system. Det samme gjelder beskrivelsen av identiteter. Et system kan benytte kun lokalt brukernavn mens et annet benytter HPR-nummer. Det foreligger standardisering på organisasjon med RESH og adressering med Adresseregisteret.

Som de ikke-funksjonelle kravene beskriver så skal norske lover være gjeldende i tillegg til EPJ-Standarden del 2 og styringsdokumentet "Tjenesteorientert arkitektur i spesialisthelsetjenesten". For elektronisk tilgang på tvers er Helseinformasjonssikkerhetsforskriften lovverket som er dekkende utover Normen for Informasjonssikkerhet. Overordnet må følgende data utveksles for å kunne utføre tilgangskontroll mellom kliniske systemer som involverer pasientsensitiv informasjon: tilgangsforespørsel:

- Identitet – hvem skal ha tilgang?
- Rolle – hvilken rolle har identiteten i øyeblikket?
- Organisasjon – hvilken organisasjonstilhørighet har identiteten?
- Besluttet tiltak – hvilket besluttet tiltak er tilknyttet pasienten, identiteten og rollen?

På bakgrunn av identifiserte elementer som må inngå i en tilgangskontrollprosess er som nevnt innledningsvis utfordringen semantikken for disse. Figur 37 illustrerer utfordringen:



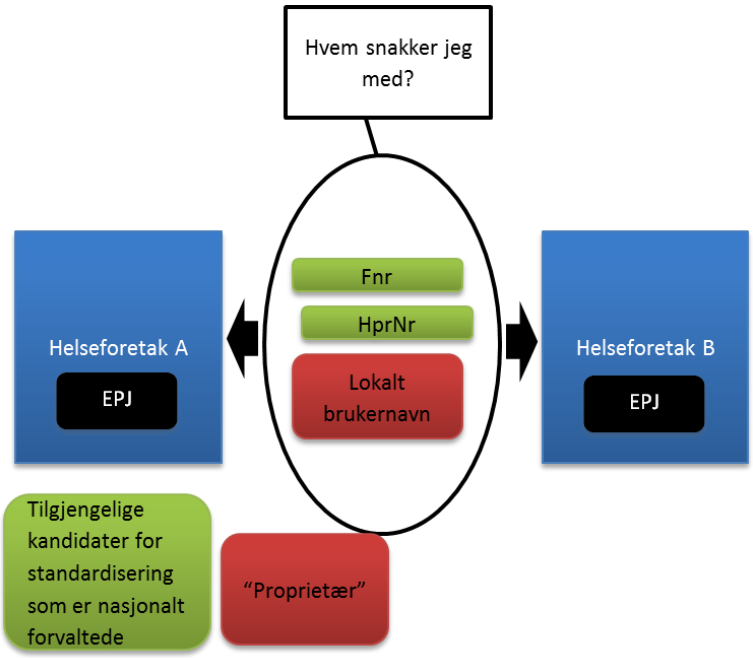
Figur 37: Liten grad av harmonisering på data for tilgangskontroll.

De påfølgende kapitlene vil diskutere hvert enkelt element og muligrommet som finnes i dag for hver av dem og hvilke løsninger som er gunstige for harmonisering.

6.2.1 Identiteter

For å autentisere hvem brukeren er kan brukernavn, fødselsnummer, hpr-nummer eller personlig sertifikat benyttes som er vanlig i kliniske systemer i dag. Noen identiteter er nasjonalt forvaltet og kan i praksis benyttes, men det foreligger i dag ingen formell bestemmelse for ***hvilke***t attributt for identitet som skal benyttes for elektronisk samhandling.

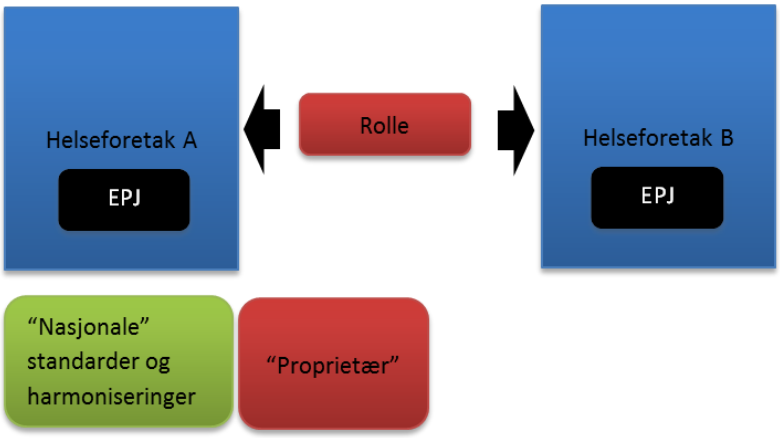
I en løsning der brukernavn knyttet til system benyttes sier det seg selv at dette ikke er særlig formålstjenlig i et nasjonalt perspektiv der denne typen forespørsler i prinsippet skal gå på tvers av systemer og regioner. Fødselsnummer eller hpr-nummer vil være bedre kandidater som inngår i en formell harmonisering da dette er identiteter som i praksis fungerer i et nasjonalt perspektiv med forvaltede registre. Figur 38 illustrerer valgmulighetene:



Figur 38: Kandidater for attributter som kan inngå i en harmonisering av identiteter.

6.2.2 Roller

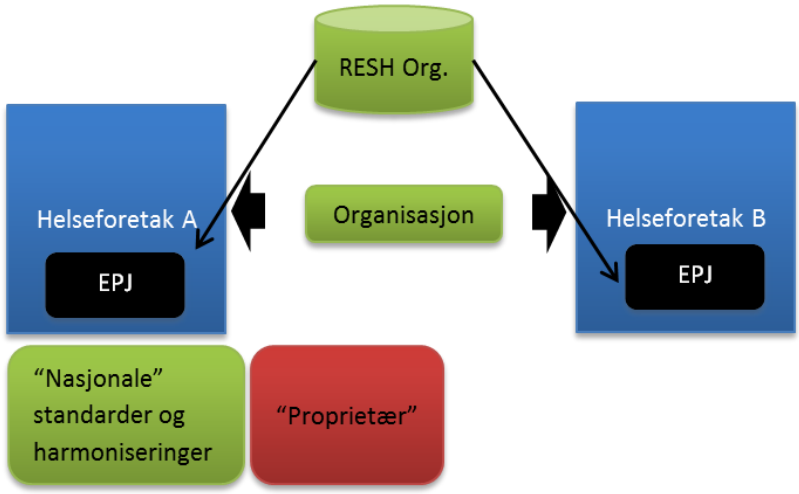
Identiteter i seg selv er ikke nok til å avgjøre tilgang. Identiteten må settes i en kontekst for hvilke funksjon vedkommende har i øyeblikket. Eksempel på funksjonell rolle kan være "Kirurg". Rollen er med på å avgjøre om identiteten har lov til å aksessere ressurser og data. Attributter for roller og definisjonen av dem er i skrivende stund ikke standardisert i helse-Norge for elektronisk samhandling. KITH (nå Helsedirektoratet) har definert kodeverk 9034 "*Helsepersons roller i forhold til pasient*", men dekker ikke behovet for den grad av granulering som er nødvendig for å kunne bruke det som grunnlag. (Se figur 39):



Figur 39: Det eksisterer i dag ingen standardisert kodeverk som kan benyttes til rolleattributt.

6.2.2.1 *Organisasjonstilhørighet*

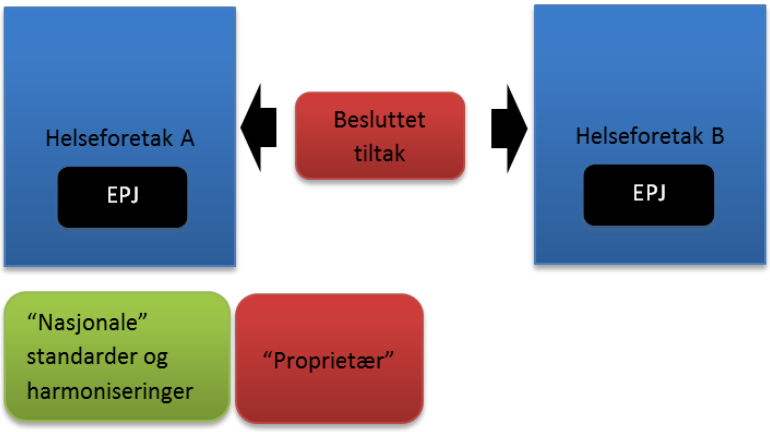
På lik linje som rolle må organisasjonstilhørighet for tjenesteyter defineres. Roller er knyttet til organisasjon og identitet som legger grunnlag for autorisering. Hvilken organisasjon er pasienten tilknyttet og hvilke organisasjon er forespørrende lege tilknyttet? Organisasjoner er i dag standardisert i RESH (kapittel 3.2.3), og er et naturlig register å benytte i denne sammenheng da dette er et etablert register som forvaltes av det enkelte helseforetak. Identiteten for dette er RESH-ID. Figur 40 illustrerer nasjonalt definert attributt for organisasjon:



Figur 40: Attributt "Organisasjon" og harmonisering på tvers av helseforetak.

6.2.2.2 *Besluttede tiltak*

Helseinformasjonssikkerhetsforskriften § 10 sier: *"Retten til tilgang til helseopplysninger skal følge av en konkret **beslutning** om å yte helsehjelp til pasienten og være tilpasset pasientens behov for helsehjelp. Beslutningen skal **dokumenteres**."* Det må altså foreligge et besluttet tiltak på lik linje som når tilgangen til pasientinformasjon som forespørres i EPJ er lokal eller på tvers. Det finnes i dag ingen formell standardisering av besluttede tiltak noe som må adresseres for denne løsningen. Det er heller ikke utvekslet denne typen data i noen samhandlingsprosesser i skrivende stund i helse-Norge. Dette behovet har kommet til syne nå som elektronisk tilgang på tvers kan realiseres. I dag er beslutningsstyrt tilgang implementert forskjellig i EPJ-systemene i de ulike helseforetakene på lik linje med rolledefinisjoner. Figur 41 illustrerer problemstillingen:



Figur 41: Attributt for utveksling av tiltak har ingen etablert standardisering (merk at det i skrivende stund ikke har vært utveksling av denne typen data da tilgang på tvers ikke har vært aktuelt før nå)

6.2.3 Arkitektur basert på EPJ-standarden

Overnevnte diskusjoner rundt attributter for tilgangskontroll beskrev et bilde av dagens situasjon som er preget av et fragmentert begrepsapparat og ingen formell omforent standardisering. Noen attributter som organisasjon er standardisert (RESH) og benyttes isolert som masterdatakilde for nettopp organisasjon i en rekke kliniske systemer, men det finnes ingen etablerte registre og tjenester der autoriseringsdata er standardisert.

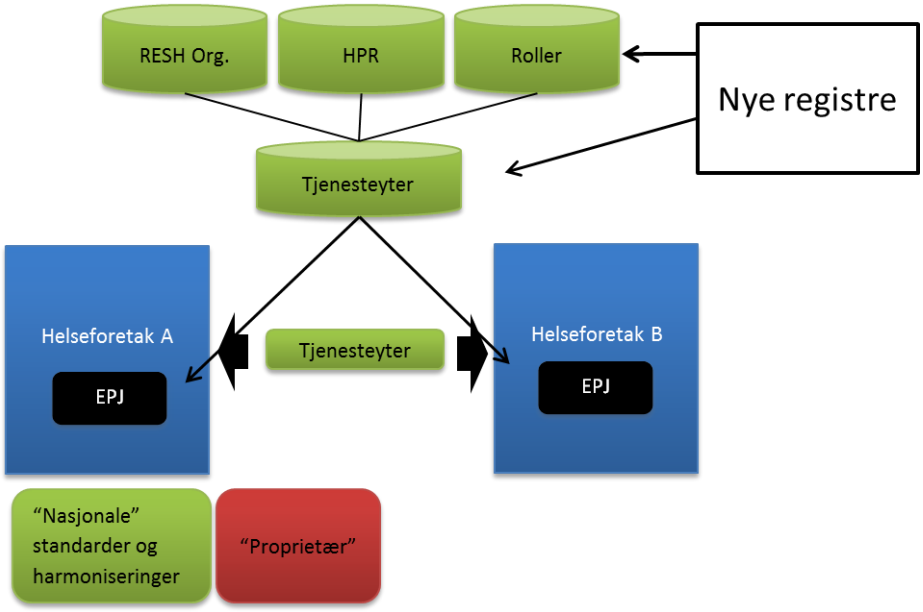
Det vil være formålstjenlig å harmonisere identitet, rolle og organisasjon inn i en enhet slik at det etableres en standardisert omforent semantikk rundt attributter for tilgangskontroll.

6.2.3.1 Tjenesteyter

EPJ-standarden del 2 definerer begrepet "Tjenesteyter" (kapittel 3.2.1.1) og setter krav til tilgangskontroll basert på **rollemaler** og **tiltaksmaler**. For å eksemplifisere dette kan følgende scenario beskrives[8]:

"*Dr. Jensen er lege og når han er på jobb, opptrer han som **Tjenesteyter** i **Rollen** lege ved kirurgisk avdeling, en **Organisatorisk** enhet ved Kongsvinger sykehus. **Rollen** er basert på en **Rollemal** for Lege som gir tilgang til et sett av **Tiltaksmaler** som dekker de oppgaver en lege ved kirurgisk avdeling skal kunne utføre*".

På bakgrunn av EPJ-standarden og kravene den stiller kan det standardiseres på begrepet "Tjenesteyter" der det etableres et tjenesteyterregister som **knytter sammen identitet, rolle og organisasjon**. Dette vil da være med på å understøtte autorisering av tjenesteyter mellom systemer. Dette finnes ikke i helsevesenet i dag og vil være et svært nyttig og etterlengtet register fordi det vil kunne understøtte interoperabilitet for autorisasjon på tvers av systemer og i praksis fungere nasjonalt. Registeret baserer seg på etablerte masterdatakilder for organisasjonstilhørighet (RESH) og register for helsepersonell (HPR). Logisk arkitektur for dette vises i figur 42:



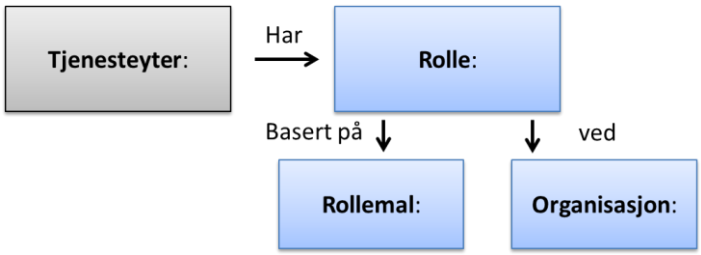
Figur 42: Attributt "Tjenesteyter". Etablering av nasjonalt register over roller og tjenesteytere.

6.2.3.2 Tjenesteyterregister

En tjenesteyter-identifikator etableres for hver rolle tjenesteyter har. En tjenesteyter har ofte flere arbeidsforhold både innen samme helseforetak og andre helseforetak. Basert på krav i EPJ-standarden del 2 må løsningen basere seg på følgende:

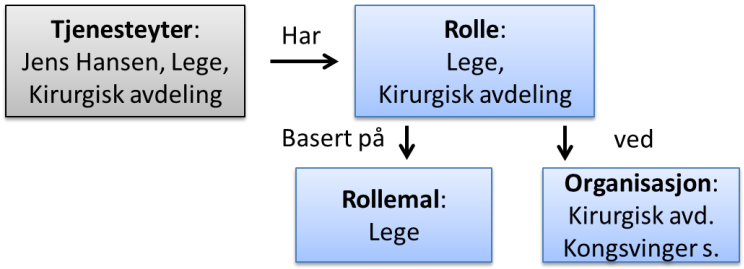
Krav nr.	Kravbeskrivelse
K 7.42	Ethvert EPJ-system skal *inneholde* eller *ha mulighet* for å opprette det antall **Rollemaler** som er nødvendig for å dekke de opp-gaver som tilligger virksomheten.
K 7.43	Enhver *rolle* i virksomheten skal baseres på en **Rollemal**
K 7.44	Enhver rolle skal kunne knyttes opp mot en eller flere **organisatoriske** enheter
K 7.45	Flere tjenesteytere skal kunne inneha samme Rolle

En logisk datamodell benyttes for tilknytning til rolle og organisasjon som kan benyttes i etableringen av et tjenesteregister ser slik ut[8]:

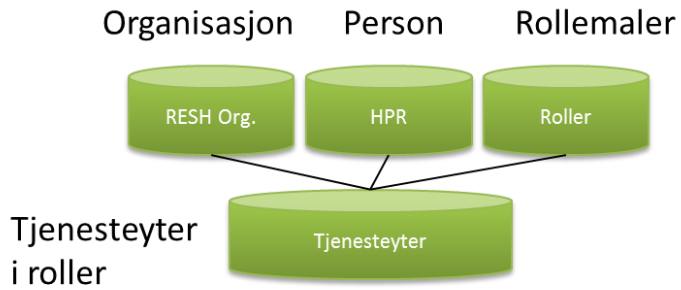


Figur 43: EPJ-standarden del 2 tjenesteyter og dens knytning mellom rolle og organisasjon.

Eksempel på dette kan være:



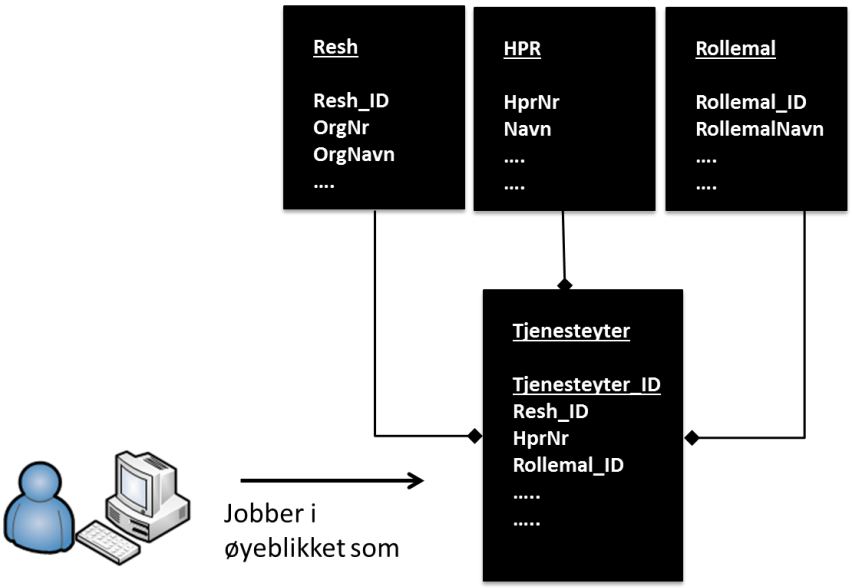
Et tjenesteyterregister vil kunne se slik ut ved bruk av EPJ-standarden (Vist med tilhørende masterdatakilder):



Figur 44: Bestanddeler i et tjenesteyterregister.

Datamodell for tjenesteyterregisteret

Basert på overnevnte masterdatakilder kan en datamodell for tjenesteyterregisteret som illustrert i figur 45. Det viktige her er at ved bruk av "Tjenesteyter_ID "ved generell elektronisk samhandling vil kunne identifisere en tjenesteyter i gitt rolle. Vi kan si det har blitt harmonisert på begrepet "Tjenesteyter" og definert semantikken rundt den som igjen legger grunnlaget som et omforent begrepsapparat på tvers av systemer.



Figur 45: Datamodell for tjenesteyterregisteret.

6.2.3.3 Besluttede Tiltak

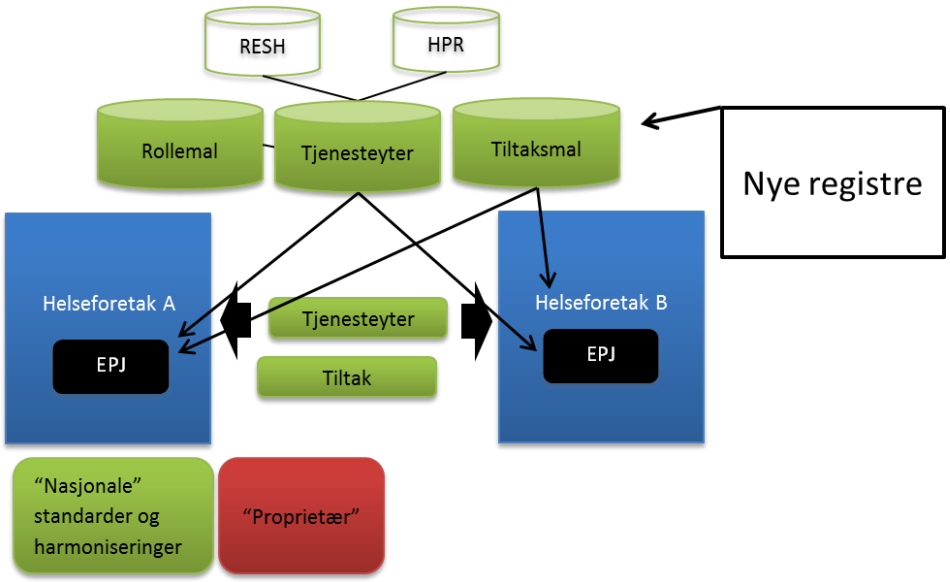
Med tjenesteyter definert som knytter person til rolle basert på rollemal og organisasjonsenhet gjenstår et viktig element i tilgangsforespørsel, nemlig "**Besluttet tiltak**" som beskrevet i kapittel 3.2.1.2.

Krav nr.	Kravbeskrivelse
K 7.8	Tilgang til helseopplysninger i EPJ skal kun gis i forbindelse med gjennomføringen av **et Besluttet tiltak**.
K 7.104	Det skal finnes mulighet for registrering av Tiltaksmaler. En slik tiltaksmal skal inneholde en overordnet beskrivelse av tiltaket, hvilke kategorier helsepersonell som kan gjennomføre denne typen tiltak samt hvilke rettigheter i forhold til informasjon i journalen som er nødvendig.
K 7.46	Hver Rollemal skal kunne assosieres med det sett tiltak som alle som innehar rollen skal være autorisert for å beslutte og/eller utføre.

Besluttede tiltak baseres i følge EPJ-standarden altså på tiltaksmaler på lik linje som rollemaler, men sier samtidig at det er opp til virksomhetene selv å detaljere de.

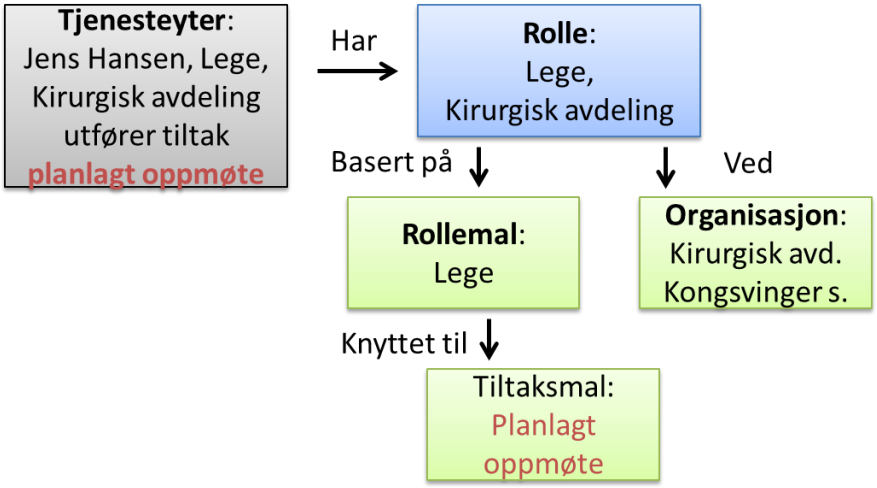
I et interoperabilitets- og samhandlingsperspektiv er det lite gunstig å la de enkelte organisasjoner selv definere innholdet i standarder.

Basert på minimumskravene vil det kunne være formålstjenlig å opprette et nasjonalt register for tiltaksmaler som harmoniserer tiltaksmaler basert på minimumskravene EPJ-Standarden definerer. Figur 46 illustrerer alle 3 nye registrene som foreslås innført. **Verd å merke seg at rollemal_ID og organisasjon (RESH-ID) ikke må overføres da denne knytningen er definert i tjenesteyterregisteret**. Kun tjenesteyter-ID sammen tiltaksmal_ID er attributtene som er nødvendige. Vi kan nå begynne å se nytten:



Figur 46: Attributt "Tiltaksmal_ID". Utveksling av besluttet tiltak basert på nasjonale harmoniseringer.

En logisk datamodell for tjenesteyter tilknyttet rolle og tiltak som kan benyttes i en harmonisering mot standardisering av attributter for tilgangskontroll illustreres i figur 47:



Figur 47: Logisk datamodell for innhold i attributter for utveksling av tilgangskontrolldata basert på EPJ-standarden del 2.

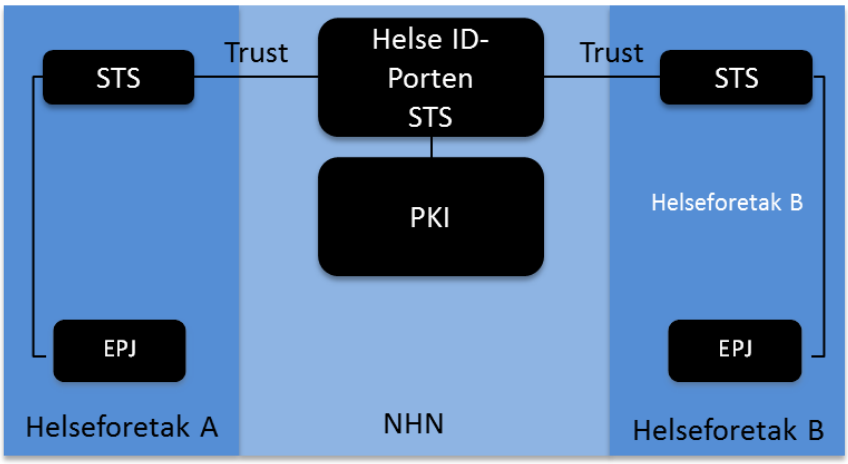
6.3 Teknisk interoperabilitet

Dette kapittelet vil beskrive tekniske løsninger for interoperabilitet basert på tjenesteorientert arkitektur og fokuset er funksjonalitet og infrastruktur. Teknisk interoperabilitet støttes i form av web-service standardene som omtalt i kapittel 3.3. Registrene som ble foreslått innført i foregående kapittel (Tjenesteyterregisteret og Tiltaksmalregisteret) vil her beskrives som et sett med tjenester. Det vil også her foreslås innført nye kapabiliteter som kan være med å understøtte samhandling mellom parter i form av autentiseringstjenester.

6.3.1 Helse ID-Porten og PKI infrastruktur

Norsk Helsenett (NHN) er et naturlig punkt for helse-Norge å etablere og forvalte fellestjenester. En rekke tjenester som RESH, Adresseregisteret benyttes intensivt i dag som grunnleggende kapabiliteter for elektronisk samhandling. Etablering av tjenesteyterregistertjeneste er en viktig kapabilitet for samhandlingen som standardiseres i henhold til EPJ-standarden. Nasjonale fellestjenester for autentisering og autorisering er i dag ikke etablerte, men det er i skrivende stund initiativ for å forsøke å etablere dette spesielt med tanke på autentisering i en tjenesteorientert plattform (STS). Alternativet til og ikke å innføre en delt tjeneste for dette er at hvert helseforetak eller helseregion anskaffer og forvalter hver sin plattform for autentisering med "Person-Høyt". Dette er lite "samhandlingsvennlig" og økonomisk. Poenget er at det må finnes et felles multiplum som alle parter kan stole på (trust). Jeg har valgt å innføre "Helse ID-Porten" i denne arkitekturen fordi det er et behov for denne typen tjeneste og vil nettopp fungere som et nasjonalt punkt for behovet av å

autentisere med sikkerhetsnivå “Person-Høyt”. Dette finnes ikke i skrivende stund i helse-Norge. Tjenesten vil også fungere som et nav i etableringen av trust mellom tjenestetilbydere i helse-Norge på tvers av omsorgsnivå. NHN er også et naturlig punkt å etablere en PKI-infrastruktur og fungere som godkjent kortutsteder. Figur 48 illustrerer logisk arkitektur for overnevnte:



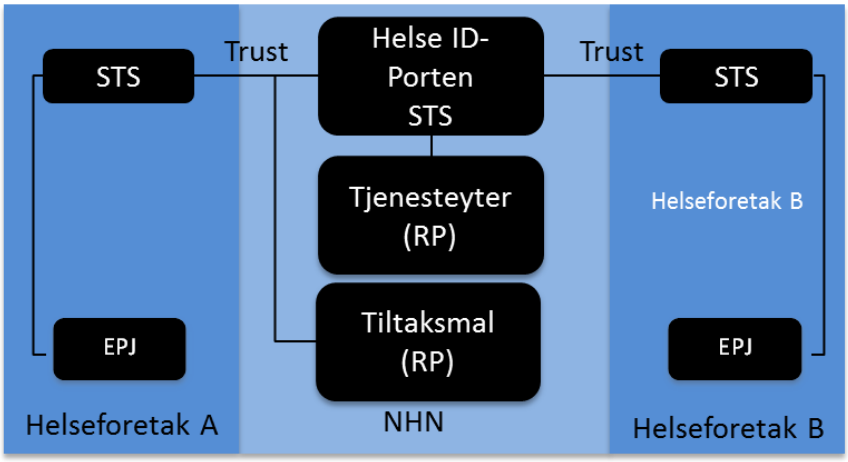
Figur 48: Etablering av NHN STS "Helse ID-Porten" og PKI.

I praksis vil etablering av en slik kapabilitet støtte følgende:

1. Autentisering med sikkerhetsnivå “Person-Høyt”. Denne tjenesten kan benyttes som kapabilitet for andre tjenester og fungerer nasjonalt.
2. PKI er en forutsetning for punkt 1. NHN vil da måtte fungere som kortutsteder av personlige sertifikat og fungere som godkjent CA.

6.3.2 Tjenesteyterregister as a service

Etableringen av registrene som foreslått i kapittel 6 er naturlig å eksponere som tjenester lokalisert i NHN. Dette er i tråd med føringer om plattform for elektronisk samhandling. Tilgangskontroll til tjenestene vil reguleres av Helse ID-Porten som STS. Figur 49 illustrerer etableringen av tjeneste for tjenesteytere og tiltaksmaler:

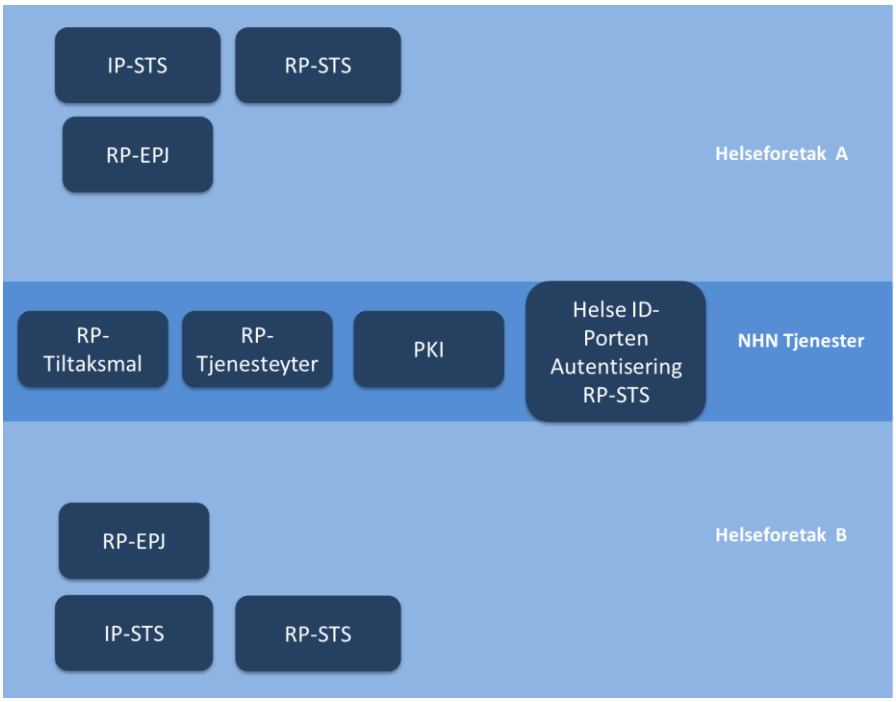


Figur 49: Tjenesteyterregisteret og Tiltaksmalregisteret som tjenester. (Merk registre som RESH og HPR er ikke vist her da de fungerer som masterdatakilder for tjenestene.

6.4 Valgt løsning - arkitektur

Kapittel 6 illustrerte en rekke problemstillinger og løsningsforslag for de tekniske og semantiske aspektene av løsningen, nemlig attributter og tjenester på et overordnet logisk nivå for tilgangskontroll i tillegg til hvordan autentisering mellom sikkerhetsdomener kan utføres i henhold til krav i EPJ-standarden del 2 og Helseinformasjonssikkerhetsforskriften. Dette kapittelet vil presentere valgt løsning der elementene er satt sammen. Attributter vil også spesifiseres som skal dekke og tilfredsstille forskningsspørsmålet.

6.4.1 Logisk overordnet arkitektur



Figur 50: Artefakt 1: Logisk overordnet arkitektur.

Figur 50 viser overordnet logisk arkitektur for løsningen. Forklaring av de forskjellige elementene:

- IP-STS (Identity Provider-STS) er de ulike organisasjonenes lokale web-service grensesnitt mot brukerkatalogen (AD).
- RP-STS (Relying Party-STS) er de ulik EPJ-instansenes lokal web-service grensesnitt mot egen utsteder av SAML-sikkerhetstokens. Dette benyttes der custom attributter må legges ved tilgangsforespørselen som ikke dekkes av IP-STS.
- RP-Tiltaksmaltjenesten (Relying Party)er tjeneste som støtter seg til SAML-sikkerhetstokens for autentisering for tilgang og har web-service grensesnitt for nedlasting av tiltaksmaler til lokale registre.
- RP-Tjenesteytertjenesten (Relying Party) er tjeneste som støtter seg til SAML-sikkerhetstokens for autentisering av tilgang og har web-service grensesnitt for nedlasting av tjenesteytere til lokale registre. Kan også gjøre oppslag dynamisk for å verifisere en tjenesteyters rolle og organisasjonstilhørighet.
- PKI er etableringen av PKI-infrastruktur som omfavner godkjent sertifikatutsteder og forvaltning av personlige sertifikat.
- RP-STS Helse ID-Porten er nasjonal STS som fungerer som et nav der STS i de ulike organisasjonene i helse-Norge kan etablere trust mot slik at federering kan støttes. Har også funksjonalitet for signering av SAML-sikkerhetstokens med personlige sertifikat.
- RP-EPJ (Relying Party) er instanser av elektroniske pasientjournaler med egne databaser som er installert i infrastruktur i de ulike helseforetakene og har web-service grensesnitt for spørring på dokumentliste for pasienter samt for uthenting av journaldokumenter.

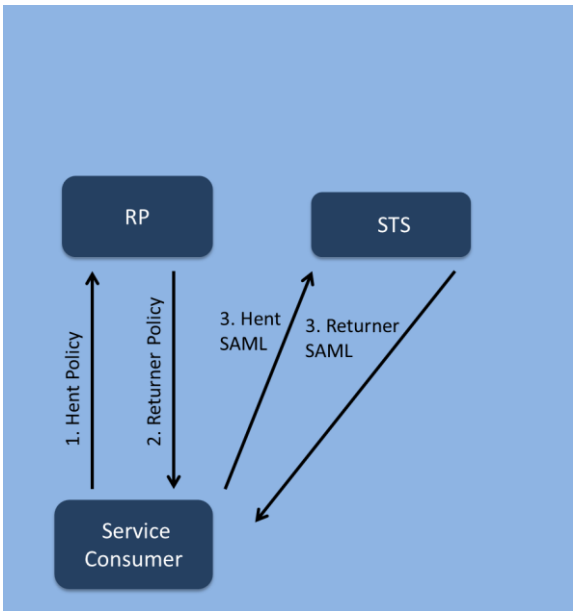
6.4.2 Attributter for utveksling av data for tilgangskontroll

Basert på diskusjoner rundt attributter i kapittel 6.2 velges følgende attributter som skal inngår i en tilgangsforespørsel:

Attributt	Datatype	Beskrivelse
Tjenesteyter_ID	String	Identifiserer tjenesteyter. Tjenesteyter_ID er tilknyttet Rollemal_ID og RESH-ID
Tiltaksmal_ID	String	Identifiserer tiltaksmal som ligger til grunn for besluttet tiltak
Pasient_ID	String	Fødselsnummer

6.4.3 Autentisering av tjenesteyter

Bruk av policy (WS-policy) som omtalt i kapittel 3.3.3.1 benyttes av service providers for å beskrive kravene til sikkerhetsmekanismene som er påkrevd for å konsumere tjenesten i form av forventede SAML-sikkerhetstokens, sertifikater (trust) og adresser til STS. I løsningsdesignet er ikke dette beskrevet i de ulike artefaktene hvilket betyr at det er utvekslet policy i første kall mot tjenesten. Jeg velger likevel å illustrere dette med en figur slik at oversiktsbildet blir enklere:



Figur 51: Service Consumer mottar policy for konsumering av tjeneste.

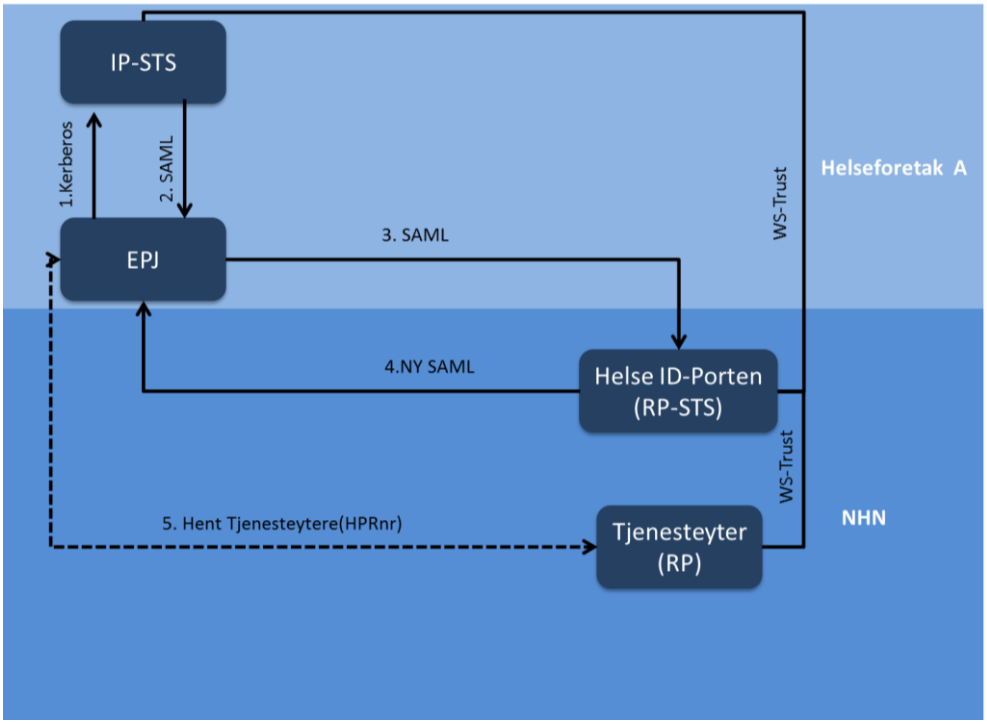
Som beskrevet i kapittel 3.3.3.4 blir personer implisitt autentiserte ved etablering av trust mellom sikkerhetsdomener i tjenesteorientert arkitektur, derav ordet "trust". Virksomhetssertifikater benyttes for denne etableringen der SAML-sikkerhetstokens som inneholder attributtene som skal utveksles signeres (ved bruk av virksomhetssertifikat).

Utfordringen med den lokale autentiseringen før konsumering av tjeneste på tvers av sikkerhetsdomene er sikkerhetskravene i Helseinformasjonssikkerhetsforskriftens § 9 *Krav om autentisering:*

"*..Den som gis elektronisk tilgang til helseopplysninger i et behandlingsrettet helseregister, skal autentisere seg ved bruk av* ***personlig kvalifisert sertifikat*** *eller en annen tilsvarende sikker autentiseringsløsning..*"

Personlige sertifikat er som kapittel 3.3.3.2 beskriver personlige kvalifiserte sertifikat som sikkerhetsklasse "Person-Høyt" noe som tilsier at autentisering må skje ved bruk av type smartkort der i denne sammenheng tjenesteyter må taste inn en pin-kode. Dette er høyere krav til sikkerhet enn hva de fleste helseforetak kan skilte med i skrivende stund. Kapittel 5.1.15.1.1, funksjonelle krav presenterte 2 brukstilfeller og det vil her presenteres løsningsdesign for autentiseringsprosessene.

6.4.3.1 Autentisering for brukstilfelle 1 – Tjenesteyter velger rolle:



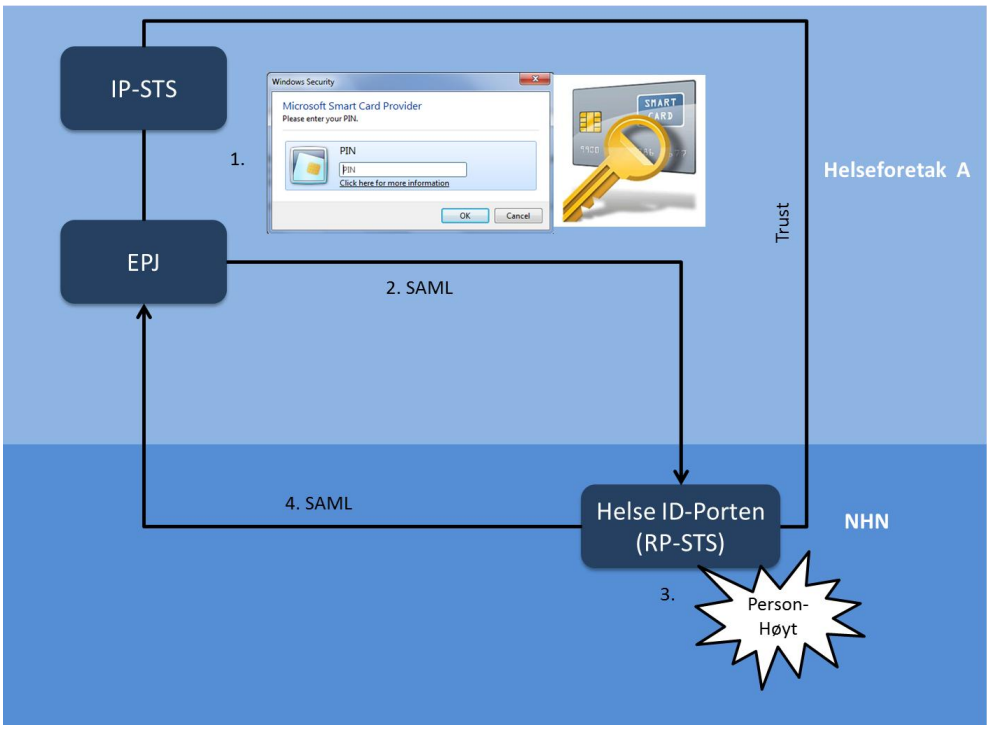
Figur 51: Artefakt 2: Autentisering med lokal STS og Helse ID-Porten for konsumering av tjenesteytertjenesten.

Forklaring artefakt 2:

Tjenesteyter skal velge rolle ved innlogging i EPJ. Basert på autentiseringen som ble utført da tjenesteyter logget seg inn i EPJ vil EPJ automatisk koble seg til tjenesteytertjenesten for å hente alle tjenesteyteridentiteter hun er tilknyttet. EPJ opptrer da som tjenestekonsument og vil utføre autentisering mot tjenesten i følgende sekvens (se artefakt 2 for detaljer):

1. Når tjenesteyter logger seg inn i EPJ med brukernavn og passord vil EPJ-web service klient (Service Consumer) eksekverer forespørsel mot tjenesten og foretar først autentisering mot IP-STS basert på kerberos-billett som ble utstedt av lokal brukerkatalog (AD) når innlogging på lokal maskin ble utført. IP-STS utsteder SAML-sikkerhetstoken.
2. Service Consumer mottar SAML-sikkerhetstoken.
3. Service Consumer sender SAML-sikkerhetstoken i en WS-Trust Request Security Token (RST) signert av virksomhetssertifikatet til Helseforetak A til Helse ID-Porten (RP-STS) som validerer dette basert etablert trust fra Helse ID-Porten til Helseforetak A IP-STS.
4. Helse ID-Porten responderer med WS-Trust Request Security Token Response (RSTR) SAML-sikkerhetstoken som er signert med Helse ID-Porten sitt virksomhetssertifikat.
5. EPJ Service Consumer er nå autentisert for tilgang til tjenesteytertjenesten og kan hente tjenesteytere (i web-service request).

6.4.3.2 Autentisering for brukstilfelle 2 – Tjenesteyter skal hente pasientopplysninger fra annen helseorganisasjons EPJ:



Figur 52: Artefakt 3: Autentisering med lokal STS og Helse ID-Porten STS for konsumering av tjeneste fra EPJ i annen helseorganisasjon ("elektronisk tilgang på tvers").

Forklaring artefakt 3:

Tjenesteyter skal søke etter pasientdokumenter fra EPJ i annen helseorganisasjon. Etter å ha valgt aktuell rolle (Tjenesteyteridentitet), aktuell pasient og ønsket tidsrom søket etter journaldokumenter skal gjelde for, klikker tjenesteyter på "Søk".

Følgende sekvens finner sted (Baseres på at stegene i artefakt 2 er utført hvilket betyr at SAML fra steg 2 ligger i sesjonen og benyttes videre):

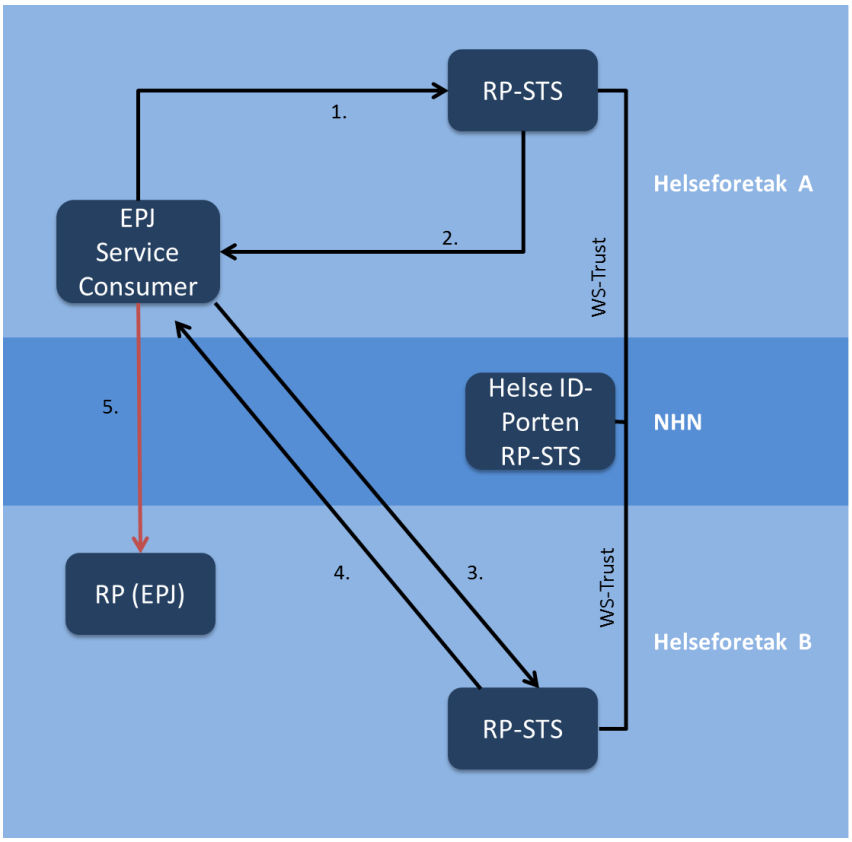
1. EPJ Service Consumer starter lokal Smart Kort Provider for signering av SAML-sikkerhetstoken utstedt i steg 2 i artefakt 2. Tjenesteyter må taste inn pin-kode etter å ha satt smartkortet (personlig sertifikat) i kortleseren.
2. Service Consumer sender SAML-sikkerhetstoken signert med tjenesteyters personlige kvalifiserte X.5093 sertifikat til Helse ID-Porten (RP-STS) med protokoll WS-Trust Request Security Token (RST)
3. Helse ID-Porten foretar validering av den personlige signaturen.
4. Helse ID-Porten genererer og utsteder nytt signert SAML-sikkerhetstoken med protokoll WS-Trust Request Security Token Response (RSTR). Signeringen blir utført med Helse ID-Porten sitt virksomhetssertifikat.

5. Service Consumer kan nå bruke SAML-sikkerhetstoken sikkerhetstoken fra steg 4 for tilgang til tjeneste i RP-EPJ i annen helseorganisasjon fordi tjenesteyter nå er autentisert med sikkerhetsnivå “Person-Høyt”.

6.4.4 Autorisering av tjenesteyter

SAML-sikkerhetstoken som utstedes fra Helse ID-Porten etter suksessfull autentisering med sikkerhetsnivå “Person-Høyt” inneholder kun en signert påstand om at tjenesteyter er den hun utgir seg for å være. Attributter for autorisering må også legges ved i SAML-påstanden. Det er nødvendig å etablere egendefinert RP-STS for EPJ ved helseforetakene som kan generere SAML-sikkerhetstoken inneholdende autorisasjonsattributter. Autorisasjonsattributter kan normalt ikke utstedes fra IP-STS fordi den inneholder kun data om identiteter og ikke autorisasjoner.

Attributtene **Tjenesteyter_ID**, **Pasient_ID** og **Tiltaksmal_ID** må legges ved i SAML-sikkerhetstoken som genereres av EPJ. Videre følger en overordnet beskrivelse av de enkelte attributter som må legges ved i en autoriseringsprosess. Dette beviser at tjenesteyter er involvert i behandling av pasienten under et gitt tiltak (identifisert med tiltaksmal ID).



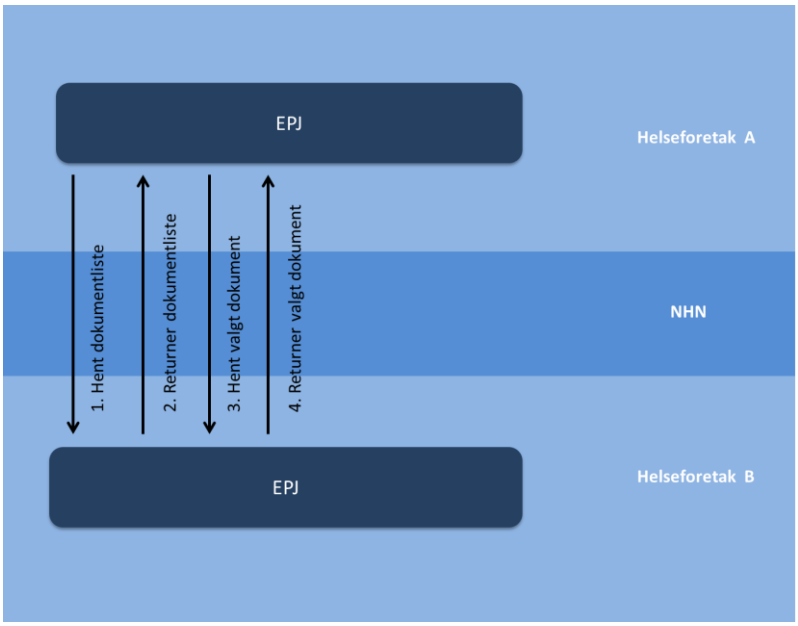
Figur 53: Artefakt 4: Modell for autorisering av tjenesteyter.

Følgende sekvens finner sted (Baseres på at stegene i artefakt 3 er utført) autorisering av tjenesteyter:

1. EPJ Service Consumer gjør et WS-Trust Request Security Token (RST) tjenestekall til RP-STS med SAML-sikkerhetstoken fra steg 2 i artefakt 2. (IP-STS).
2. RP-STS for EPJ genererer signert SAML-sikkerhetstoken for autorisasjon og sender den med Request Security Token Response (RSTR). SAML-sikkerhetstoken er signert med virksomhetssertifikatet til helseforetak A og inneholder:
    1. Tjenesteyter_ID
    2. Pasient_ID
    3. Tiltaksmal_ID (identifiserer type besluttet tiltak)
3. Med utgangspunkt i SAML-sikkerhetstoken som ble generert i punkt 2 samt SAML-sikkerhetstoken fra Helse ID-Porten RP-STS (2 sikkerhetstoken), sendes i ny WS-Trust request til RP-STS hos helseforetak B.
4. RP-STS hos helseforetak B validerer begge sikkerhetstokens, og lager en ny SAML-sikkerhetstoken der Tjenesteyter_ID, Pasient_ID, og Tiltaksmal_ID blir pakket og signert med helseforetak B sitt virksomhetssertifikat.

   Alle WS-Trust request meldinger fra EPJ Service Consumer i Helseforetak A (tilgang på tvers scenario), til RP-STS i helseforetak B, vil kreve SAML-sikkerhetstoken fra Helse ID-Porten hvor sikkerhetsnivå "Person-Høyt" autentisering med kvalifisert personlig sertifikat ble benyttet. Det gjelder ikke for WS-Trust requests som kommer fra en lokal EPJ Service Consumer i helseforetak B.
5. SAML-sikkerhetstoken generert av helseforetak B sin RP-STS benyttes til å kalle tjenesten RP-EPJ i helseforetak B der dokumentene returneres fra.

Sekvensen i Artefakt 4 benyttes også når selve journaldokumentet skal hentes. Figur 54 illustrerer de funksjonelle sekvensene for selve uthentingen av dokumentlisten og journaldokumentene:



Figur 54: Modell for henting av journaldokumenter.

6.5 Diskusjon rundt løsningsdesign

Dette kapittelet innledet med diskusjon rundt hver enkelt av dataattributtene som er nødvendige i en prosess der tilgangskontroll mellom kliniske systemer skal utføres. For å kunne utføre elektronisk samhandling må begrepsapparatet være likt hos alle samhandlingsparter, både kliniske begreper og begreper for tilgangsstyring. I dag opererer hvert helseforetak som autonome enheter der egne definisjoner for roller, brukere, og identiteter benyttes. Dette er lite samhandlingsvennlig og det ble klart at det ble viktig å etablere et omforent begrepsapparat for dette. En kunne tatt en "standard" som et av helseforetakene hadde definert for sitt bruk og benyttet det som standard for alle, men det er av erfaring en dårlig ide å bygge på proprietære løsninger.

Basert på EPJ-Standarden etablerte jeg et felles begrepsapparat for helsepersonell, nemlig tjenesteyter og designet fellestjenester for dette der helsepersonell registreres med tilhørende rolle og organisasjonstilknytning. Dette legger grunnlaget for tilgangskontroll i praksis alle kliniske informasjonssystem fordi det er et felles begrepsapparat.

En ny dimensjon for tilgangskontroll på toppen av tradisjonell tilgangskontroll der roller og organisasjonstilhørighet er de viktigste ble identifisert med beslutningsstyrt tilgangskontroll. Denne dimensjonen måtte også adresseres for tilgang mellom kliniske system der det er pasientbehandling som formål. Semantikken for denne dimensjonen ble også adressert ved å etablere felles register for definisjonene eksponert som en tjeneste.

Teknologien for å samhandle elektronisk er tjenesteorientert arkitektur. Dette er i tråd med føringer som styringsdokumentet "Tjenesteorientert arkitektur i Spesialisthelsetjenesten". Dokumentet "IKT Strategi og Handlingsplan HSØ" har stor fokus på samhandling og fellestjenester. Trenden er at tjenester etableres som nasjonale tjenester som for eksempel RESH og Adresseregisteret.

Tjenesteorientert arkitektur er en god plattform for samhandling da den baserer seg på etablerte standarder, noe som er en forutsetning for å kunne samhandle sømløst. Det var derfor naturlig å etablere konseptet "Helse ID-Porten" "PKI", "Tjenesteytertjenesten" og "Tiltaksmaltjenesten" med en slik arkitektur. Semantikken som ble etablert innledningsvis ble innholdet i tjenestenes funksjonskall for å kunne forespørre tilgang.

7 Evaluering - demonstrasjon av nytteverdi

En arkitekturmodell er ikke verdt noe dersom den ikke kan implementeres. Derfor er neste steg å teste modellen mot et realistisk brukerscenario. I scenarioet benyttes DIPS EPJ som testobjekt som har hver sin separate installasjon og database i henholdsvis Kongsvinger Sykehus (Sykehuset Innlandet HF) og Oslo Universitetssykehus (OUS HF). Evalueringen vil basere seg på bruk av artefaktene som ble produsert i løsningsdesignet. Siden funksjonalitet for tilgang på tvers ikke er realisert i DIPS EPJ i dag vil det med sikkerhet identifiseres gap i begrepsapparat og funksjonalitet. Gapet vil kunne være med å sette søkelyset på hva som må til for å sette DIPS (og i praksis andre kliniske informasjonssystem) i stand til å utføre elektronisk tilgang på tvers i forhold til lovkrav, føringer, infrastruktur, teknologi og arkitektur. Innledningsvis er det nødvendig å presentere en forenklet oversikt over arkitektur for tilgangskontroll i DIPS. Deretter vil det settes en del forutsetninger og en begrepsoversikt for DIPS sine attributter og hva EPJ-standarden definerer.

7.1 Tilgangskontroll i DIPS EPJ

DIPS (Distribuert Informasjons og Pasientdatasystem i Sykehus) er Norges største leverandør av elektronisk pasientjournal (EPJ) og brukes av Helse Sør-Øst RHF, Helse Vest RHF og Helse Nord RHF i tillegg til en rekke private sykehus. Sikring av kliniske personsensitive data og tilgangen til den er svært viktig. DIPS har en tilgangskontrollarkitektur som sikrer alle aspekter ved dette herunder også beslutningsstyrt tilgang. Utgangspunktet for tilgangskontrollen i DIPS er brukerens rettigheter som styres av en rekke tilstander og parametere som igjen skal sørge for datasikkerhet og understøtte personvern for pasienter. Et viktig aspekt er at kun de som har rett og behov for å se pasientinformasjon skal kunne gjøre det. Videre presenteres et forenklet bilde for tilgangskontroll i DIPS.

7.1.1 Bruker og tilganger i DIPS

DIPS har en grundig og granulert tilgangskontrollarkitektur. Under gis en oversikt over dette der først standard tilgangskontroll beskrives for deretter å legge på en dimensjon til som innbefatter beslutningsstyrt tilgangskontroll:

Bruker og autentisering:

Brukere i DIPS må registreres med en såkalt “DIPSSignatur“ som er et brukernavn som igjen blir knyttet med et passord for innlogging. DIPS støtter innlogging og autentisering med ekstern brukerkatalog Active Directory (AD).

Bruker og autorisasjoner:

En bruker må knyttes til minimum en brukerrolle. En brukerrolle i DIPS kan knyttes til en rekvirent. En rekvirent er et begrep som av begrepet "Tjenesteyter" som beskrevet i kapittel 3.2.1.1. Alle rettigheter til funksjoner og data tildeles til brukerrollen. Dersom brukeren har flere arbeidsforhold vil det opprettes en brukerrolle pr arbeidsforhold. Valgt rolle velges ved innlogging. Brukerrollen knyttes så til en eller flere brukertyper som er et navngitt sett med autorisasjoner som eksempelvis kan være "Behandler", IT ansvarlig" etc.

Det må også tildeles tilganger på ulike nivåer både fra organisatorisk og gruppenivåer. Gruppenivåer innbefatter:

- Avdelingstilgang
    - Avdelinger som brukerrollen skal ha tilgang til.
- Posttilgang
- Seksjonstilgang
    - Seksjonene på de avdelingene brukerrollen har tilgang til.
- Journalgruppe tilgang
    - Styrer tilgang på journaldokumentnivå.

Under gis en oversikt over de ulike begrepene som innbefattes av autorisasjoner i DIPS:

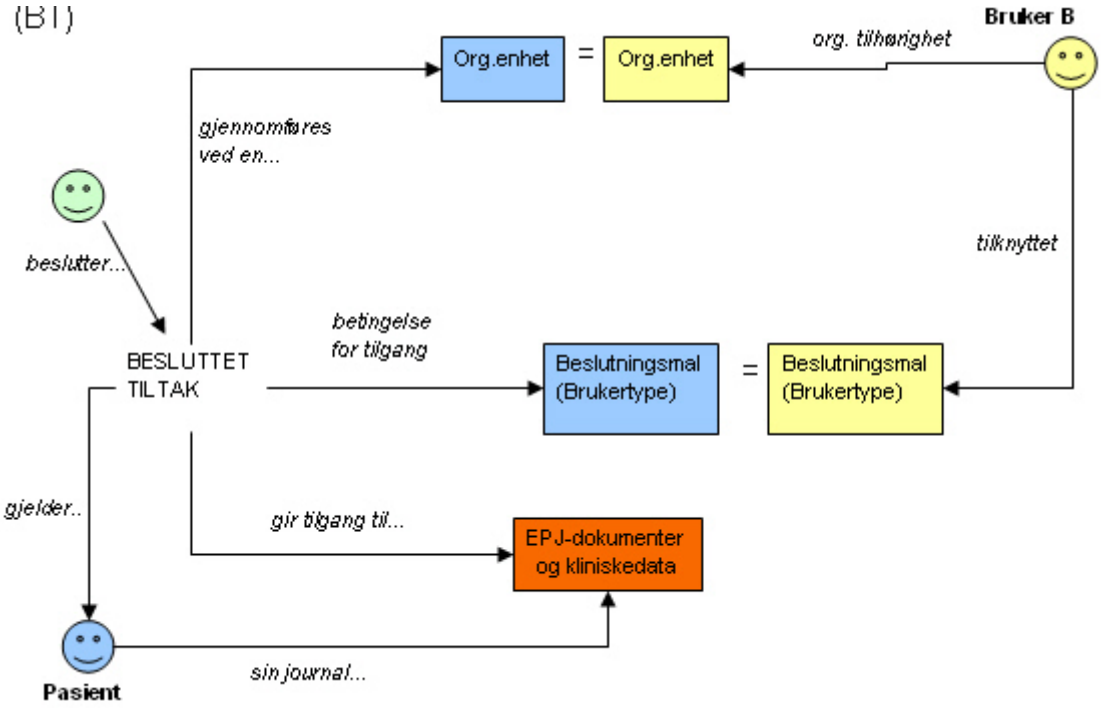
Begrep/entitet	Beskrivelse
Brukerrolle	Knyttes til brukernavn og organisasjon. Kan ha flere brukerroller
Rekvirent	Definerer en behandler som rekvirerer en tjeneste fra sykehuset, for eksempel en blodprøve. (DIPS definisjon). DIPS har eget register over rekvirenter. En Brukerrolle i DIPS kan tildeles begrepet rekvirent og brukeren får da mulighet til å rekvirere tjenester og fungere som mottaker og avsender av meldinger.
Brukertype	Knyttes til brukerrolle. Brukertype er et navngitt sett med autorisasjoner som består av en eller flere elementtyper. Eksempel kan være: "Behandler", "IT Ansvarlig".
Elementtype	Elementtyper beskriver klassifiseringen av data og funksjoner i DIPS. Eksempel kan være

	"Journal data" som er en basis elementtype som må tildeles brukertypen for å få tilgang til data i journalen. Andre elementtyper tildeles i henhold til behov for tjenesteyter

7.1.2 Beslutningsstyrt tilgang i DIPS

DIPS benytter også beslutningsstyrt tilgang som EPJ-standarden Del 2 definerer. Dette er i praksis en enda mer fingranulering av den generelle tilgangskontrollen ved at det må foreligge et besluttet tiltak og baseres på tiltaksmaler. Det er hensiktsmessig å utdype hvordan DIPS har implementert modellen for beslutningsstyrt tilgang:

Når ***tjenesteyter*** aksesserer skjermbilder der det er tilknyttet pasientdata vil DIPS sjekke at det foreligger riktig ***Tiltaksmal*** i tillegg til ***organisasjonstilhørighet***, ***rollemaler*** og ***journalgrupper***. Figur 55 viser prinsippet med beslutningsstyrt tilgangskontroll i DIPS basert på tiltak:



Figur 55: (Brukerdokumentasjon Beslutningsstyrt tilgang DIPS[54]), Beslutningsstyrt tilgangsprinsipp i DIPS basert på tiltak.

7.1.2.1 Tiltaksmaler i DIPS

DIPS sin implementasjon av beslutningsstyrt tilgang består av to typer overordnede tiltaksmaler og skiller mellom ***implisitt*** og ***eksplisitt*** tilgang[54]:

1. Implisitt tilgang
2. Eksplisitt tilgang

7.1.2.2 Implisitt tilgang

Med implisitt tilgang menes de tilganger en bruker får tilknyttet stilling og arbeidssted. Implisitte tiltaksmaler er formalisert i form av tiltaksmaler som illustreres her:

- Bruker er informasjonsansvarlig for pasienten
- Bruker er journalansvarlig for pasienten
- Bruker er pasientansvarlig for pasienten
- Bruker er pasientens primærkontakt
- Bruker har behandlingsansvar for pasienten
- Data i arbeidsflyt
- Henvisning til vurdering
- Vurdert henvisning
- Inneliggende pasient
- Planlagt oppmøte
- Poliklinisk besøk
- Pasienten finnes på operasjonsoversikten
- Ventende pasient
- Åpen henvisningsperiode
- Åpen konsultasjonsserie
- Inneliggende ledsager

7.1.2.3 Eksplisitt tilgang

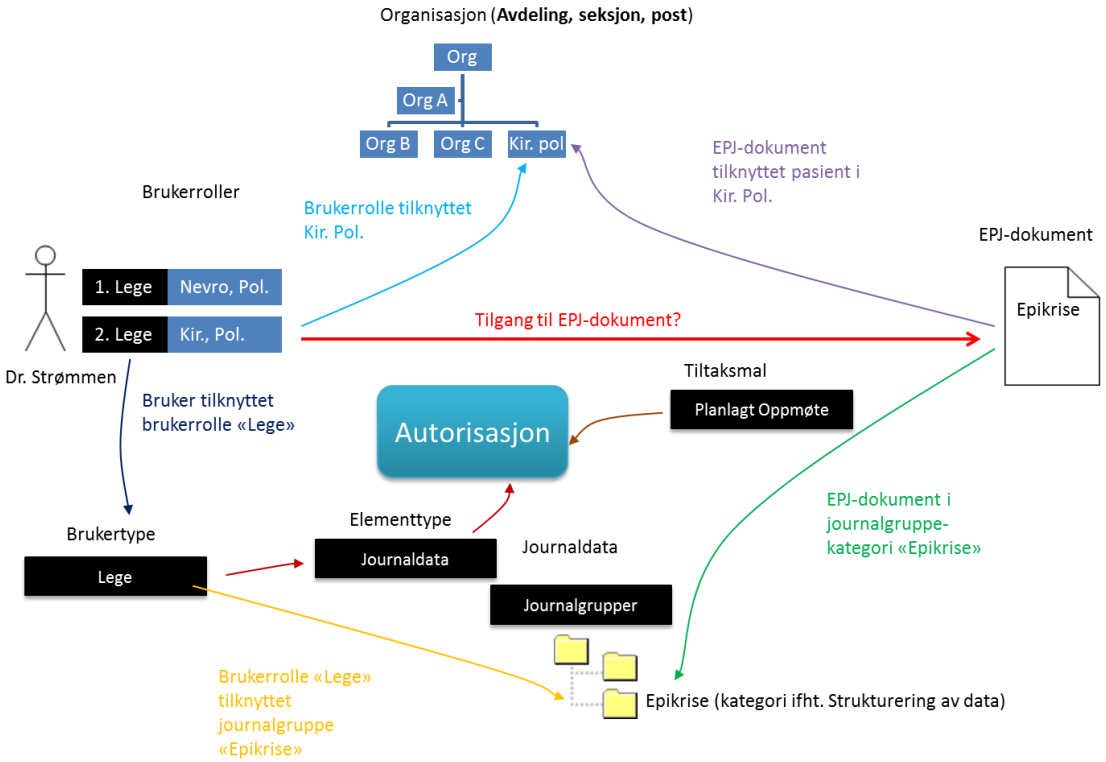
I de tilfeller en bruker ikke har gyldig implisitt tilgang til informasjon og tilgang er ønskelig blir eksplisitte tiltaksmaler påtvunget. Dette for å kunne dokumentere hvorfor det var nødvendig for tilgangen. DIPS benytter følgende eksplisitte tiltaksmaler:

- Bestilling av dokumenter fra offentlige og juridiske instanser og forsikringsselskap
- Eksternt prøvesvar/notat til vurdering
- Etterarbeide
- Forskning
- Henvendelse fra pasienten
- Henvendelse fra pasientens behandler
- Henvendelse fra pasientens pårørende
- Internkontroll/Kvalitetssikring
- IT-Systemarbeid
- Meldt pasient
- Pasientinnsyn
- Tilsyn med helsepersonellets virksomhet
- Tilsyn på annen avdeling.
- Undervisning
- Åpne sperret journal i nødverge

DIPS har definert tre ulike scenarioer der eksplisitte tiltaksmaler må benyttes:

1. Brukeren gir seg selv tilgang ved å velge tiltaksmal
2. Brukeren gir andre tilgang ved å velge tiltaksmal
3. Brukeren gir seg selv og andre tilgang ved å velge tiltaksmal

Komplett oversikt over DIPS tilgangskontroll er oppsummert i figur 56:



Figur 56: Logisk oversikt DIPS tilgangskontroll med beslutningsstyrt tilgang basert på tiltaksmal.

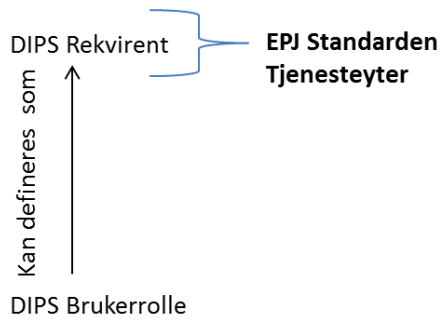
7.1.3 Harmonisering av DIPS begrepsapparat mot løsningsdesign

Løsningsdesignet etablerer nye begreper, krav om funksjonalitet, infrastruktur og semantikk for data og begreper som naturlig nok ikke er på plass i dagens versjon av DIPS. Evalueringen vil identifisere gapet som skiller design fra realitet med tanke på det viktigste – informasjonen som også denne oppgaven har som forskningsspørsmål. Det er en del likheter i begrepsapparatet til DIPS og løsningsdesignet som direkte kan mappes over til EPJ-standardens og løsningsforslagets begreper for harmonisering mot omforent semantikk på tvers av systemer. DIPS benytter begrepet “Rekvirent” om det EPJ-Standarden omtaler som “Tjenesteyter” som er benyttet i løsningsdesignet. En Brukerrolle i DIPS kan tildeles begrepet “Rekvirent” og benyttes der tjenesteytere skal for eksempel rekvirere laboratorieprøver eller være mottaker av kliniske meldinger. Tabellen under lister opp denne mappingen:

DIPS EPJ begrep	EPJ-Standarden del 2 begrep
Rekvirent	Tjenesteyter. DIPS EPJ benytter begrepet "Rekvirent" om behandlere i roller som er tilknyttet organisasjoner slik EPJ-standarden del 2 definerer tjenesteyter.
Brukertype	Rollemal
Beslutningsmal	Tiltaksmal

Figur 57: Mappingtabell for tilgangsattributter i DIPS og EPJ-Standarden som løsningsdesign er basert på.

På bakgrunn av sammenligning av begrepsapparat kan vi trekke følgende konklusjon at rekvirentbegrepet i DIPS korresponderer med tjenesteyterbegrepet i løsningsforslaget:



Figur 58: DIPS Rekvirent vs. EPJ-Standarden tjenesteyter.

På bakgrunn av denne begrepsmappingen kan vi i scenarioet benytte DIPS sitt rekvirentbegrep for tjenesteyterbegrepet. En ytterligere forfining av attributter for rekvirent i DIPS som er interessant her kontra tjenesteyter i løsningsdesign:

DIPS attributt	Tjenesteyterregister basert på EPJ-Standarden
Rekvirentkode	Tjenesteyter_ID
Rollenavn_ID	Rollemal_ID
Organisasjon_ID	RESH_ID
Beslutningsmal_ID	Tiltaksmal_ID

7.1.4 DIPS rammeverk for dokumentutveksling

For dokumentindeksering og rammeverk for dette benytter DIPS IHE-XDS som beskrevet i kapittel 3.4.3. og HL-7 CDA som beskrevet i kapittel 3.4.2. Dette er rammeverk som er bygget for standarder i dokumentutvekslingsprosesser der IHE definerer indekseringen og hvor journaldokumentene er fysisk lokaliserte. HL-7 CDA definerer strukturen i selve journaldokumentene. Dette passer godt inn i løsningsdesignet og tjenesteorientert arkitektur. Dette betyr for DIPS og dette scenarioet at journaldokumentene som utveksles er strukturert i henhold til HL-7 CDA som er indekserte i IHE-rammeverket.

7.2 Testing av løsningsforslag mot scenario

Kronikerpasienten mottar typisk hoveddelen av pasientbehandlingen på et lokalsykehus mens den avanserte behandlingen mottas på et eller flere universitetssykehus. Et av Samhandlingsreformens strategiske virkemidler for å få ned kostnader i form av liggedøgn på sykehus er å la kommunene få større del av ansvaret for både forebygging og behandling. Scenarioet er tilpasset et slikt pasientforløp for å understreke nødvendigheten av elektronisk tilgang på tvers.

DIPS har i dag ikke tjenesteyterbegrepet etablert mellom helseforetak. Som nevnt i foregående kapittel er rekvirentbegrepet i DIPS overførbart til tjenesteyterbegrepet. Det vil i testen av løsningsforslag etableres en mapping mellom de to begrepene slik at tjenesteyterdefinisjonen benyttes her.

Forutsetninger:

Forutsetning	Kommentar
Etablert infrastruktur i NHN	For at DIPS skal kunne benyttes som testobjekt i arkitekturen forutsettes det at Helse ID-Porten, Tjenesteytertjenesten, Tiltaksmaltjenesten og PKI er etablert i NHN. Tjenesteyter er tildelt personlig sertifikat fra NHN og etablering av trust mellom de aktuelle Identity Providers i helseforetakene er etablert.
Etablert infrastruktur i helseforetakene	Det forutsettes at det er etablert STS-grensesnitt for Identity Providers i helseforetakene slik at SAML-sikkerhetstokens kan utstedes til samhandlingspartene.
Etablert funksjonalitet i helseforetakenes DIPS EPJ	Det forutsettes at DIPS EPJ har utviklet og implementert web-service grensesnitt med tilhørende funksjonalitet: • Søk etter dokumenter for gitt tidsintervall der dokumentliste returneres som inneholder en liste over tilgjengelige dokumenter. • Hente dokument(er) på bakgrunn av valgt dokumentID valgt fra listen i punktet ovenfor.
Etablert funksjonalitet i helseforetakenes DIPS EPJ	Det forutsettes at DIPS har utviklet funksjonalitet for konsumering av Tiltaksmaltjenesten og databasene er oppdatert med disse dataene slik at tiltaksmaler er harmonisert på tvers av systemer.
Etablert funksjonalitet i helseforetakenes DIPS	Det forutsettes at DIPS har harmonisert sine

EPJ	databaser med tanke på Rollemaler, Organisasjoner (RESH), Tjenesteytere, til lokal database slik at semantisk interoperabilitet oppnås på tvers av systemer.
Etablert funksjonalitet i helseforetakenes DIPS EPJ	Det forutsettes at DIPS har utviklet funksjonalitet for konsumering av tjenesteytertjenesten for nedlasting av tjenesteytere ved valg av roller under innlogging.
Trust mellom Identity Providers	Det forutsettes at det er etablert trust i form av sertifikatutveksling og protokollen WS-Trust
Tjenesteyter må være registrert i EPJ-system det skal spørres etter journaldokumenter fra. Dette for	Følgende må registreres: Tjenesteyter_ID, Rollemal_ID, RESH-ID (for der tjenesteyter jobber i øyeblikket) og Tiltaksmal_ID. Dette betyr at det må settes opp autorisasjoner i DIPS manuelt.

7.3 Aktører, begreper og forutsetninger

Aktører

Aktør	Forklaring
Service Provider: Oslo Universitetssykehus (OUS).	Dette er helseforetaket som skal ta i mot forespørselen etter kliniske pasientdata fra service consumer.
Service Consumer: Kongsvinger Sykehus – Sykehuset Innlandet HF.	Dette er helseforetaket der tjenesteyter skal forespørre kliniske pasientdata på tvers av de juridiske virksomhetsgrensene.

Pasient Lise jensen	Dette er pasienten som har registrert data i flere EPJ-instanser
Dr. Hansen	Tjenesteyter som skal behandle pasient ved Kongsvinger Sykehus og har behov for å innhente opplysninger i EPJ ved Oslo Universitetssykehus

7.3.1 Scenario

Pasienten har diagnosen diabetes mellitus Type 1 og mottar storparten av behandlingen ved poliklinikken ved Kongsvinger sykehus, men det hender at hun reiser til OUS for å motta behandling der også. Dette gjør at pasienten har registrert EPJ-opplysninger begge steder. Pasienten har ved flere anledninger opplevd både smerter og nedsatt følsomhet i føttene når hun har vært på besøk i Oslo og oppsøkt både legevakt og ved en anledning akuttenheten ved OUS og har mottatt behandling i form av kirurgi og medisinering. Pasienten opplever forverring av smertene i føttene og oppsøker behandlende lege ved Kongsvinger sykehus. Legen er i tvil over hvilken behandling han skal gi da pasientforløpet er uoversiktlig.

Dette betyr i dagens situasjon at det må foretas tidkrevende ringerunder eller transport av journaldokumenter med taxi, fax eller lignende. Pasienten kan også ha mottatt relevant behandling i forskjellige helseforetak og regioner i tillegg hvilket gjør det tidkrevende og usikkert å innhente riktig informasjon. Informasjon som kan være livsviktig for videre behandling. Behandlende lege logger seg på lokal PC og så inn i DIPS. Rollene hentes dynamisk ned fra tjenesteytertjenesten og presenteres i listeform i DIPS. Brukstilfellene fra funksjonelle krav definert i kapittel 5.

Tildeling av data til aktører i scenario: Dr. Hansen:

DIPS attributt	Verdi	Tjenesteyterregister attributt	Verdi
Rekvirentkode	HANTES	Tjenesteyter_ID	444898

Tildeling av data til aktører i scenario: Pasient:

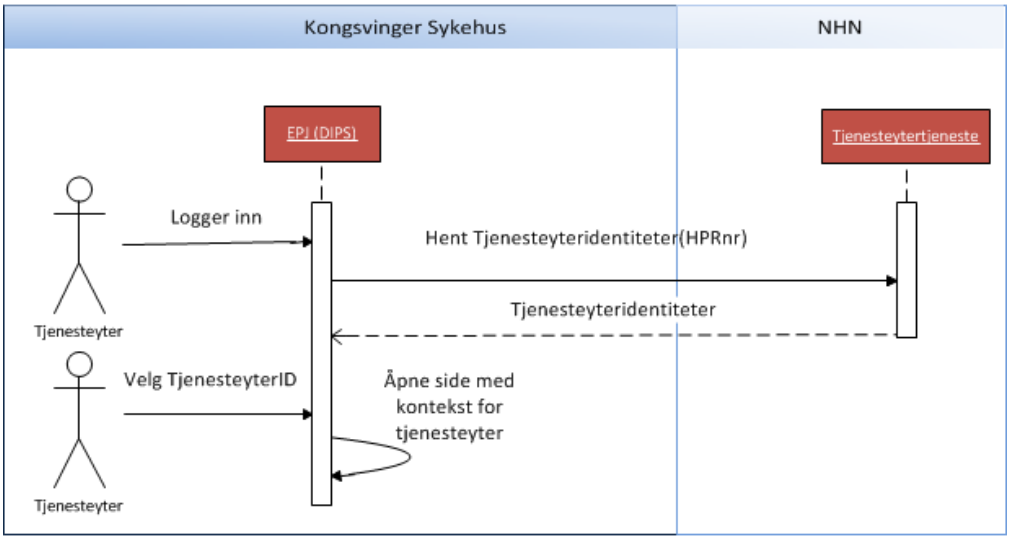
DIPS attributt	Verdi

Pasient_ID	04017329354
Fornavn	Lise
Etternavn	Jensen
….	

Mapping av DIPS attributter mot tjenesteyterregisterets begrep:

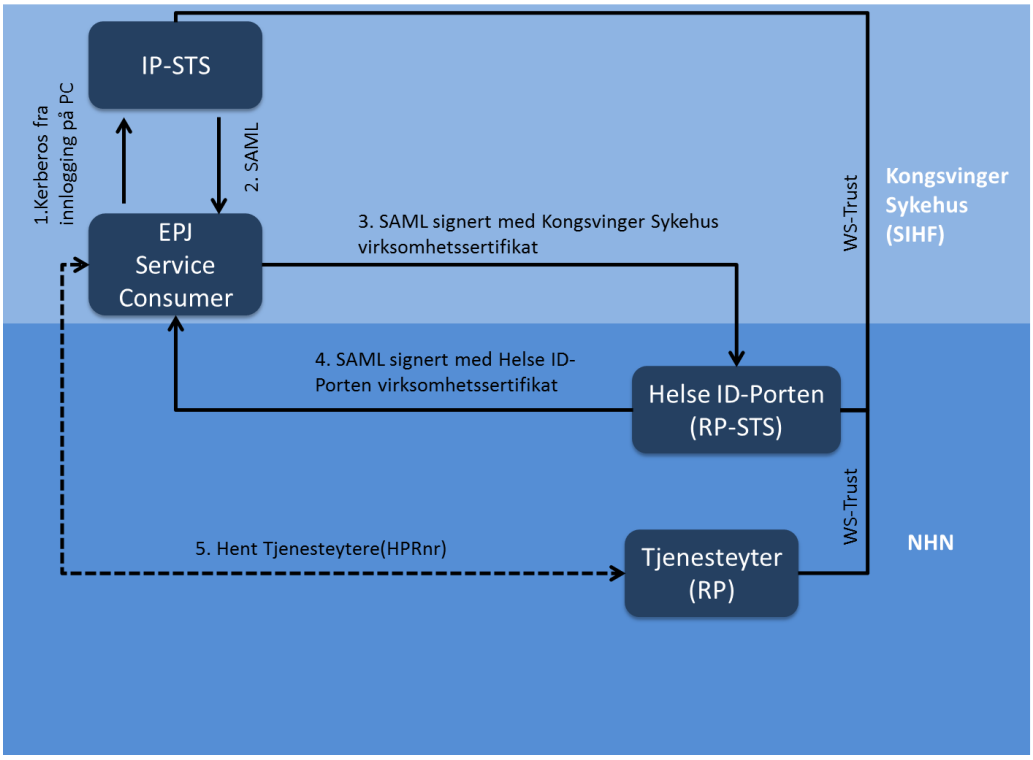
DIPS attributt	Verdi	Tjenesteyterregister attributt	Verdi
Rekvirentkode	HANTES	Tjenesteyter_ID	444898
Beslutningsmal_ID	376765	Tiltaksmal_ID	889988

Brukstilfelle 1 – Tjenesteyter velger rolle:



Figur 60: Sekvens for innlogging i EPJ der tjenesteyteridentiteter for Dr. Hansen hentes ned dynamisk fra tjenesteytertjenesten.

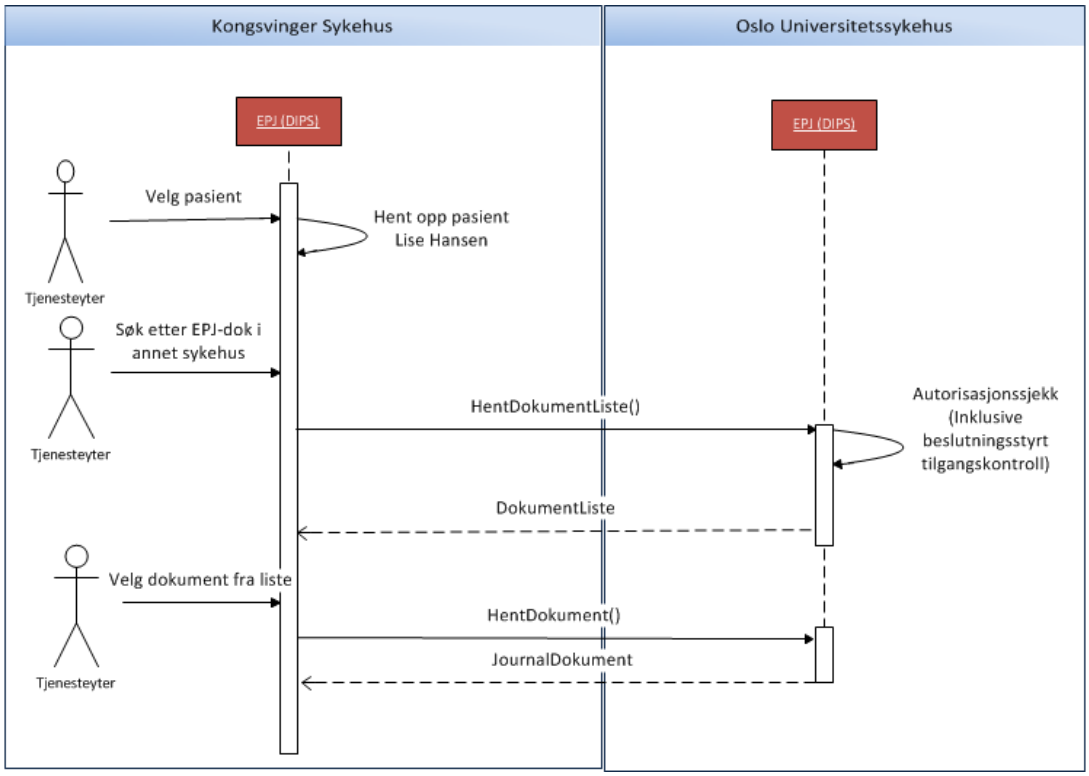
Dr. Hansen har tatt i mot pasient Lise Jensen med fødselsnummer 0401732935 og logger seg inn i EPJ (DIPS) med brukernavn og passord. I bakgrunnen utføres sekvens som beskrevet i Artefakt 2:



Figur 59: Artefakt 2: Autentisering mot tjenesteytertjenesten i brukstilfelle 1.

EPJ Service Consumer henter alle tjenesteyteridentiteter registrert på Dr. Hansen fra tjenesteytertjenesten etter suksessfull autentisering som vist i artefakt 2. Dr. Hansen velger så aktuell tjenesteyterID med verdi “444898” fra listen og dermed er kontekst satt for hvilken rolle hun opererer med i EPJ.

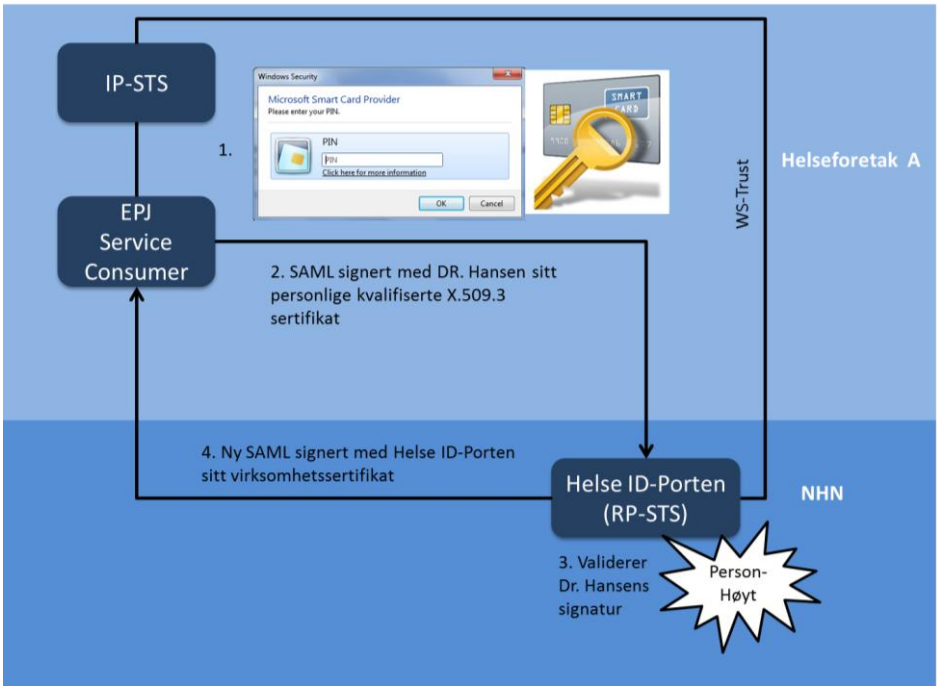
Brukstilfelle 2 – Tjenesteyter skal hente pasientopplysninger fra annen helseorganisasjons EPJ:



Figur 61: Sekvens for henting av dokumentliste og aktuell(e) journaldokumenter.

Dr. Hansen henter opp pasient Lise Jensen i EPJ og bestemmer seg for å hente inn deler av pasientforløpet hennes og velger Oslo universitetssykehus fra listen over tilgjengelige helseforetak med tidsramme fra 1 Jan.2011 til 1 Jan 2013 og klikker “Søk”.

I bakgrunnen utføres sekvens for autentisering som beskrevet i Artefakt 3:

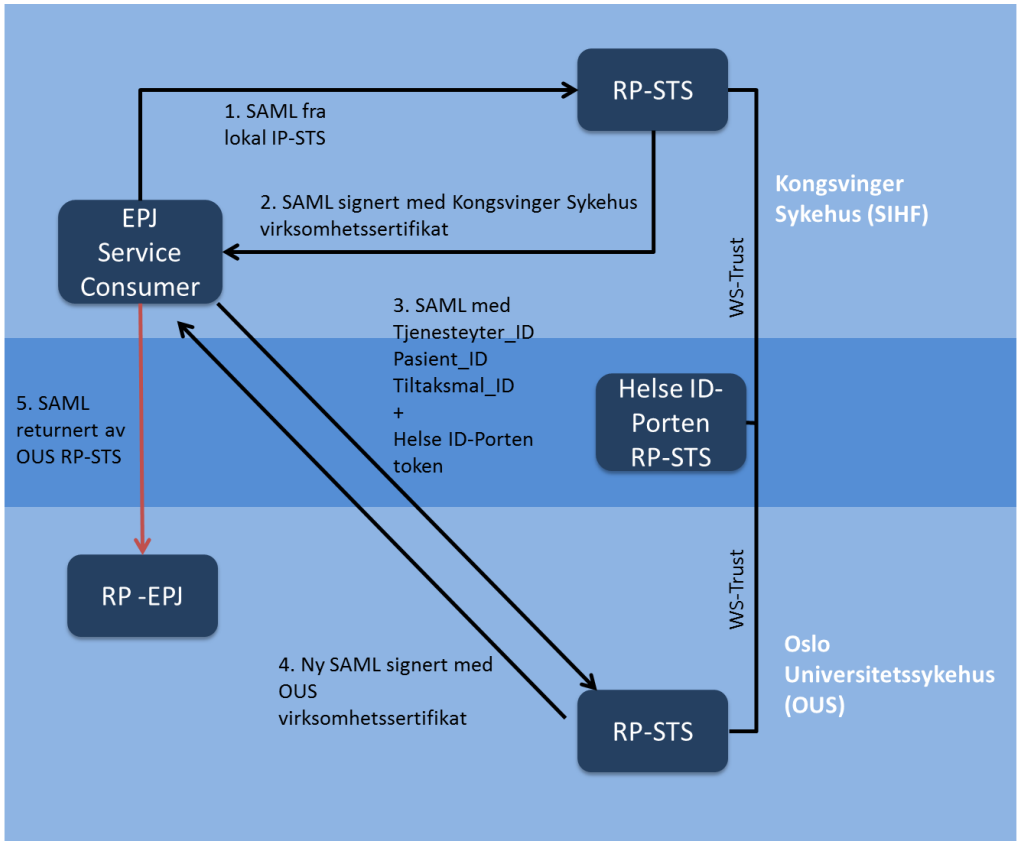


Figur 62: Artefakt 3: Autentisering mot Helse ID-Porten med sikkerhetsnivå "Person-Høyt" for Dr. Hansen.

Dr. Hansen setter inn sitt personlige kvalifiserte X.509.3 sertifikat og taster inn pin-kode (1) og et SAML-sikkerhetstoken sendes til Helse ID-Porten signert med Dr. Hansens personlige sertifikat sendes av Service Consumer til Helse ID-Porten(2) der det valideres (3). Helse ID-Porten sender tilbake til EPJ Service Consumer et nytt SAML-sikkerhetstoken signert med Helse ID-Portens virksomhetssertifikat. Så langt i den tjenesteorienterte prosessen er Dr. Hansen nå autentisert med sikkerhetsnivå “Person-Høyt”.

Etter vellykket autentisering mot Helse ID-Porten vil autorisasjonsprosessen starte. Attributtene som skal benyttes for autorisering er som følger:

Attributt	Verdi
Tjenesteyter_ID	444898
Pasient_ID	04017329354
Tiltaksmal_ID	889988



Figur 63: Artefakt 4: Autorisasjonsprosess for Dr. Hansen.

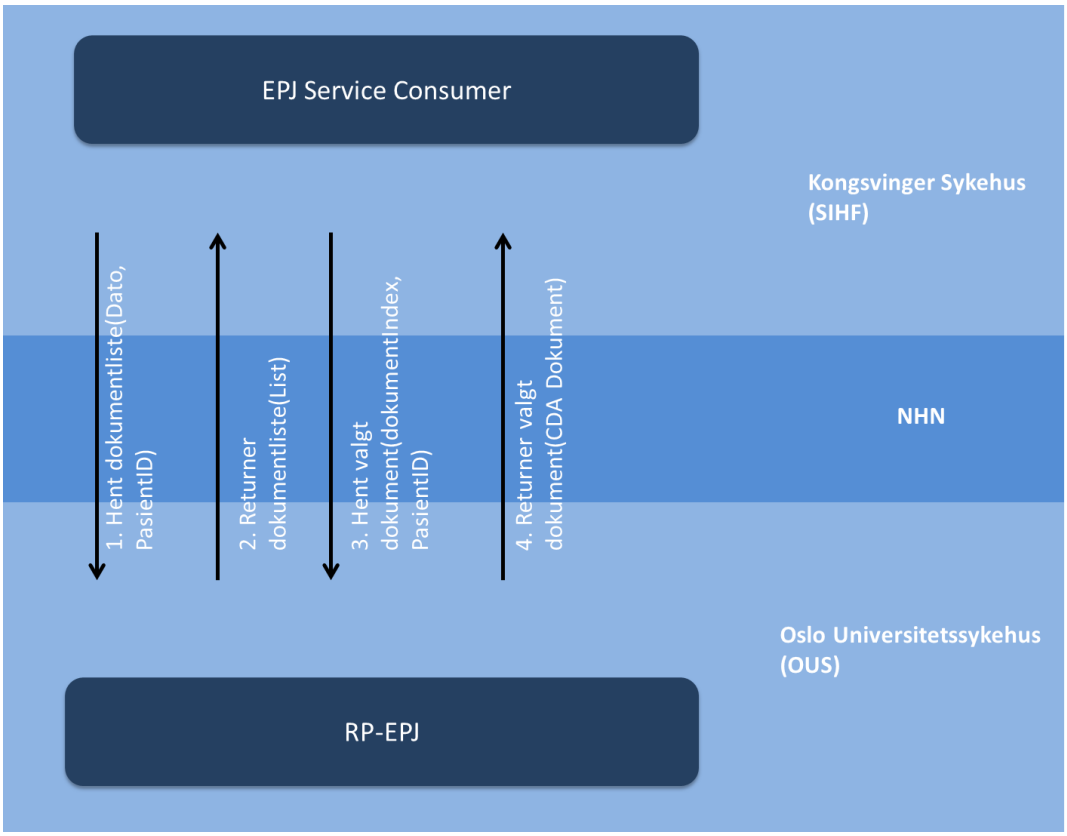
Et SAML-sikkerhetstoken (som ble generert av IP-STS i Kongsvinger Sykehus ved tjenestekall mot tjenesteytertjenesten i artefakt 2) sendes til lokal RP-STS (1) som genererer en ny SAML-sikkerhetstoken signert med Kongsvinger Sykehus sitt virksomhetssertifikat. Sikkerhetstokenet inneholder identifiserte tilgangsattributter (Tjenesteyter_ID, Pasient_ID og Tiltaksmal_ID) som DIPS har hentet opp. (Forutsetter en mapping med begrepet "Rekvirent" i DIPS) og sendes tilbake til EPJ Service Consumer (2).

SAML-sikkerhetstoken som ble generert i punkt 2 samt SAML-sikkerhetstoken fra Helse ID-Porten RP-STS (2 sikkerhetstoken), sendes ny WS-Trust request til RP-STS hos OUS (3).

RP-STS hos OUS validere begge innkommende sikkerhetstokens og genererer ny SAML-sikkerhetstoken signert med OUS virksomhetssertifikat. Denne inneholder attributtene som ble sendt inn (Tjenesteyter_ID, Pasient_ID og Tiltaksmal_ID) og sendes tilbake til EPJ Service Consumer (4).

SAML-sikkerhetstoken fra punkt 4 benyttes i direkte web-service request til RP (EPJ) (5).

Dr. Hansen er nå autorisert og får konsumere tjenesten til RP-EPJ der spørring etter dokumentliste for journaldokumenter eksekveres. Dokumentlisten returneres og presenteres for Dr. Hansen i DIPS. Dr. Hansen velger seg så et journaldokument fra 5. juni 2012 og klikker "Hent Journaldokument". EPJ Service Consumer utfører samme autoriseringsprosess mot RP-EPJ som i stegene over og returnerer ønsket dokument. Se figur 64:



Figur 64: Steg i dokumentuthenting.

8 Konklusjon og diskusjon

Denne oppgaven stilte spørsmålet:

"*Hvilke informasjonselementer må forstås for å kunne foreta autentisering og autorisasjon for tilgang etter klinisk informasjon på tvers av juridiske virksomhetsgrenser i spesialisthelsetjenesten slik at Helseinformasjonssikkerhetsforskriftens § 11c oppfylles?*"

Dette var og er et svært aktuelt tema med stor relevans som var viktig å sette søkelyset mot. I min daglige arbeidssituasjon i Sykehuspartner IKT arbeider jeg med virksomhetsarkitektur de IT-tjenester er en viktig brikke for å støtte opp under strategier og føringer. En gjentakende problemstilling er arkitektur for tilgangskontroll til systemer og tjenester. Helsepersonell med flere arbeidsforhold, lokasjoner og funksjonelle roller må få tilgang til informasjon og ressurser basert på den rollen hun opptrer i det øyeblikket informasjonen etterspørres.

Det har vært en svært interessant prosess å skrive denne oppgaven. Målet var å designe en modell og en kjørbar prototype for elektronisk tilgang på tvers mellom enheter i spesialisthelsetjenesten. Oppgavens omfang ble for stor for å kunne lage en prototype, men metoden for evalueringen viser at modellen fungerer. Det ble avdekket et gap mellom hva DIPS har av funksjonalitet og begrepsapparat og hva arkitekturen i løsningsforslaget definerte noe som kan være med på å peke på hva som må endres i DIPS og i praksis andre kliniske systemer for å kunne utføre elektronisk tilgang på tvers.

Attributtene Tjenesteyter_ID, Pasient_ID og Tiltaksmal_ID ble identifisert som informasjonselementene som ble benyttet i en autentisering- og autorisasjonsprosess for klinisk informasjon på tvers av juridiske virksomhetsgrenser. Kravet om autentisering med sikkerhetsnivå "Person-Høyt" ble også adressert.

Det ble vurdert å designe en utvidelse av Adresseregisteret med tanke på å støtte tjenesteytere da det har en unik identitet på helsepersonell og enheter, men kun for primærhelsetjenesten. Adresseregisteret er lagt for et annet formål, nemlig adressering av kommunikasjonsparter, hvilket er en helt annen intensjon. Å tvinge inn og kombinere nye begreper for det registeret vil ikke være formålstjenlig. Det er et stort behov for å kunne identifisere en tjenesteyter i nasjonal setting for autorisasjoner også med dimensjonen beslutningsstyrt tilgang. Derfor valgte jeg å etablere tjenesteyterregisteret og eksponere det som en tjeneste. Dette vil legge grunnlaget for sømløs elektronisk samhandling med tanke på autorisasjoner i en tjenesteorientert arkitektur.

Med tilgang til spørring etter klinisk informasjon på tvers av virksomheter legges det til en ny utfordring som i praksis gjelder for alle typer kliniske informasjonssystem. Teknologien er klar, det er bare å sette den riktig sammen. Informasjonen er slik jeg ser det viktigst da betydningen og fortolkningen av den må omforenes før samhandlingen kan utføres. Samhandlingskontrakter mellom parter der semantikken er harmonisert mellom samhandlingsparter må etableres.

Det har derfor vært en veldig god øvelse på vei mot målet om semantisk interoperabilitet for elektronisk samhandling med denne oppgaven da begrepsapparatet måtte etableres først før arkitekturen for tjenestene ble utarbeidet. Jeg håper denne oppgaven kan være et steg på veien for

en modell for semantikken rundt tilgangskontrollinformasjon slik at helsepersonell får en enklere hverdag og ikke minst at pasienten kan motta bedre helsetjenester der pasientforløpet kan innhentes noe som gir bedre kvalitet.

8.1 Videre arbeid

Løsningsdesignet i denne oppgaven identifiserte en form for veikart mot sømløs elektronisk samhandling basert på tjenesteorientert arkitektur. Dette betyr ikke at bildet er komplett. Det gjenstår enda en del kapabiliteter i form av funksjonalitet (og realisering av løsningsforslaget) som må på etableres. Her velger jeg å diskutere noen:

8.1.1 Harmonisering av standarder

Som scenarioet i evalueringskapittelet avdekket er ikke begrepsapparatet harmonisert i DIPS med tanke på foreslått arkitektur. Dette gjelder alle kliniske informasjonssystem i helse-Norge i dag. Som tidligere nevnt er dette en forutsetning for å kunne realisere sømløs elektronisk samhandling. Informasjonsarkitektur er slik jeg ser det viktigst. Arkitekturen kan være med på å utarbeide krav til leverandører av fagsystem. Som beskrevet i kapittel 3.4.4 har OASIS utarbeidet en arkitektur for informasjonselementer som skal inngå i en tilgangskontrollprosess til kliniske systemer tilpasset det amerikanske helsevesenet. Et målbilde for det norske helsevesenet burde være å utarbeide en slik standard. Denne masteroppgaven kan være en bidragsyter for dette.

8.1.2 Provisjonering av brukere

For tilgang på tvers scenarioer er det lite brukervennlig og dynamisk å måtte på forhånd registrere en tjenesteyter i aktuell EPJ-instans (eller andre kliniske systemer) før en kan sette i gang en elektronisk forespørsel. Dette må adresseres. I Helse Sør-Øst pågår det i disse dager en konsolidering av identitetshånderingssystem (IdM). Målet er å ha en brukerkatalog for HSØ. IdM-systemet kan da også provisjonere tjenesteytere og tilhørende roller og organisasjoner til tjenesteyterregisteret samtidig som den provisjonerer ut til fagsystem.

Tiltaksmaler er også en dimensjon som bør adresseres med tanke på at disse også må foreligge i aktuelt klinisk system før en tilgangsforespørsel ette pasientdata kan utføres. Tjenesteytertjenesten kan utvides til å støtte dette også ved at rollemalene som er tilknyttet tjenesteyteren også tilknyttes tiltaksmaler dynamisk. Hvordan dette skal utføres og i hvilken sekvens må utredes, men tjenesteytertjenesten vil være et naturlig sted å legge det til da disse begrepene hører tett sammen for tilgangskontroll og semantikken rundt.

8.1.3 Utvidet bruk av tjenesteytertjenesten

Tjenesteytertjenesten vil i praksis kunne fungere som et dynamisk autorisasjonsregister der fagsystem utfører dynamiske oppslag under kjøring for å autorisere tjenesteyter. Som beskrevet i kapittel 3.3.5 er autorisasjonsrammeverket XACML et svært spennende policy-basert språk for opprettelse og utføring av autorisasjoner i tjenesteorientert arkitektur. Ved bruk av denne standarden funksjonalitet for autorisasjoner i prinsippet løftes ut fra fagsystemer og sentraliseres. Dette vil være med på å forenkle forvaltningen og eventuelle endinger av tilgangskontroll både i daglig drift, men også ved juridiske endringer noe som i høy grad skjer i dag. Ved bruk av XACML er det mulig å utføre attributt og policy-basert tilgangskontroll på en svært dynamisk og fingranulert måte. Tjenesteytertjenesten kan være en kapabilitet i et XACML rammeverk i form av attribute-store (attributtlager).

8.1.4 Nettskyen

Det var opprinnelig planlagt å realisere løsningsdesignet for elektronisk tilgang på tvers i en nettskyløsning. Dessverre strakk ikke tiden til, men det er en svært spennende teknologi som ikke ennå har fått fortfeste innen e-helse. Arkitekturen for nettskyen er tjenesteorientert, så selve det å eksponere tjenestene i en nettsky er ikke utfordringen. Det ville heller lettet på kompleksiteten i arkitekturen med tilgangskontroll ved bruk av for eksempel Access Control Service som er en sentral kapabilitet i Microsofts nettskyplattform Microsoft Azure. Denne kunne fungert som en STS slik Helse ID-Portens konsept er.

Nettskyen bringer nye spennende utfordringer inn med tanke på juridiske og bruksmessige aspekter. Personvern er viktigere enn teknologi, men teknologi er ikke et hinder for å opprettholde et godt personvern dersom det brukes riktig, tvert i mot teknologi brukt riktig vil gi bedre helsetjenester til pasienter.

Bruksmessige aspekter ved innføring av nettskyplattform vil på sikt kunne gi store endringer for hvordan vi i dag benytter tjenester og applikasjoner. I stedet for å ha tusenvis av lokale maskiner rundt i helseorganisasjoner vil all funksjonalitet kunne flyttes opp i nettskyen og forvaltes der. Modeller for hvordan de økonomiske aspektene vil bli er også et viktig tema, da det i prinsippet kan være interessant og kun betale for den faktiske bruken av tjenestene i stedet for tradisjonelle lisensavtaler. Tjenestene kan i praksis også settes sammen av flere slik at de i størst mulig grad blir tilpasset både behov og økonomi.

Det viktigste er at vi velger de riktige løsningene slik at vi kan gi pasientene de mest optimale helsetjenestene.

9 Referanser:

1. Samspill 2.0 (2010), Helse- og omsorgsdepartementet
2. Samhandlingsreformen (2008 – 2009), Helse- og omsorgsdepartementet.
3. Rapport fra forprosjekt nasjonal kjernejournal (2010), Helse- og omsorgsdepartementet.
4. Ot. Prp 51 (2008-2009), Helse- og omsorgsdepartementet
5. Helseinformsjonssikkerhetsforskriften (2011), Helse- og omsorgsdepartementet.
6. Innsyn i pasientjournal, Nasjonalt senter for samhandling og telemedisin, (2012).
7. Definisjon-databehandlingsansvarlig: Helseregisterloven § 2.
8. EPJ Standard del 2 (2007): Tilgangsstyring, redigering, retting og sletting, kap 2.4- "Beslutningsstyrt tilgang til journalopplysninger".
9. Component based development, Debayan Bose (2010), Indian statistical institute.
10. An Architectural View of Distributed Objects and Components.
11. Service Oriented Architecture for Enterprise Applications, Shankar Kambhampaty, Satish Chandra, 2006.
12. Simple Object Access Protocol (SOAP), SOAP Version 1.2.
13. Web Services Description Language (WSDL), Version 2.0.
14. Uniform Resource Identifier (URI): Generic Syntax – RFC3986.
15. Extensible Markup Language (XML), www.w3.org/XML
16. Web Services Business Process Execution Language Version 2.0.
17. Web Services Policy 1.5 – Primer, W3C Working Group Note 12 November 2007.
18. Standards for XML and Web Services Security.
19. Department of Defense, "Trusted Computer Security Evaluation Criteria," *DoD 5200.28-STD*, 1985.
20. Access Control, Principles and Practice, (1994).
21. Role-Based Access Controls, (1992).
22. SAML V2 Executive Overview, (2005).
23. Enabling SAML for Dynamic Identity Federation Management (2009)
24. Supporting Attribute-Based Access Control with Ontologies(2006)
25. eXtensible Access Control Markup Language (XACML) Version 3.0 (2013)
26. An XACML-Based Privacy-Centered Access Control System(2005)
27. The NIST Definition of Cloud Computing(2011)
28. Comparing Public Cloud Providers(2010).
29. IKT strategi og handlingsplan HSØ(2012).
30. God vilje dårlig verktøy - Paulsen, Grimsmo(2008).
31. Elektronisk samhandling i helse- og omsorgssektoren, Hygen, Heimly, Landsem(2009).
32. Tjenesteorientert arkitektur i spesialisthelsetjenesten(2008).
33. A Dynamic, Context-Aware Security Infrastructure for Distributed Healthcare Applications(2004).
34. Context-Aware Access Control for Clinical Information Systems(2012).

35. EPJ-systemer og tilgang på tvers(2009).
36. Identitets- og tilgangsstyring Forprosjekt for Helse Sør-Øst. Versjon 0.7 (2013).
37. HL-7 www.hl7.org
38. Computer-Supported Cooperative Work in Tele Home Care - Jinlun Liu(2012).
39. XML Schema Primer. [Online] http://www.w3.org/TR/xmlschema-0/
40. XSPA [Online] http://saml.xml.org/wiki/cross-enterprise-security-and-privacy-authorization-xspa
41. Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of Security Assertion Markup Language (SAML) for Healthcare v1.0
42. Role Based Access Control (RBAC) Healthcare Permission Catalog (2010).
43. American Society for Testing and Materials (ASTM) ASTM E1986-98(2005) Standard Guide for Information Access Privileges to Health Information. [Online] http://www.astm.org/DATABASE.CART/HISTORICAL/E1986-98R05.htm
44. Integrating the Healthcare Enterprise (IHE), IT Infrastructure Technical Framework, vol. 1 (ITI TF-1, kapittel 10) (2012).
45. Health Information Exchange, Enabling Document Sharing Using IHE Profiles (2012).
46. 46 - A security architecture for interconnection health information systems (2004).
47. On the usage of SAML delegate assertions in an healthcare scenario with federated communities (2010).
48. Understanding PKI (2002).
49. SAPHIRE, intelligent healthcare monitoring based on semantic interoperability platform.
50. Design Science In Information Systems Research (2011)
51. Kravspesifikasjon for PKI i offentlig sektor (2010)
52. Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor (2008)
53. Kerberos Explained (2000)
54. Brukerdokumentasjon Beslutningsstyrt tilgang DIPS
55. Veien frem til samarbeid og samhandling i praksis, Anders Grimsmo