Felles teknisk løsning for regionalt eide nasjonale kvalitetsregistre

Sluttrapport for gjennomføring av Proof of concept

NIKT Tiltak 28.1

Dokumentnavn:
Vedl 6b SluttRapportFellesTekniskLøsningNasjonaleKvalitetsregistrePOC.doc

Revisjonshistorikk			
Dato	Versjon	Forfatter	Beskrivelse
02.06.2009	0.9	Prosjektgruppen	Til godkjenning

Innholdsfortegnelse

1 Sammendrag

Dette dokumentet har som formål å bidra til å etablere en felles teknisk plattform for medisinske kvalitetsregistre. Arbeidsformen har vært praktisk utprøving av utvalgte løsningskonsepter (*Proof of concept*).

Prosjektet er gjennomført på oppdrag fra *Nasjonal IKT* som en videreføring av arbeidet i rapporten *Felles teknisk løsning for regionalt eide nasjonale kvalitetsregistre*[4]. I arbeidet har det også blitt lagt vekt på føringer i dokumentet *Tjenesteorientert arkitektur i spesialisthelsetjenesten – Styringsdokument fra Nasjonal IKT*[10] for å sikre at løsningen også vil fungere i framover i tid samtidig som det må kunne leveres løsninger på kort sikt bygd på dagens arkitektur.

Utviklingen innenfor området har til nå gjerne hatt sitt utspring i ulike medisinske fagmiljø der behovet for å bedre kvaliteten på behandling har vært viktig. Tekniske løsninger for å ta vare på medisinske parametre har gjerne blitt utviklet i tilknytning til enkeltprosjekter uten noen form for overordnet koordinering. Totalt sett fører dette til tekniske løsninger som er kostnadsdrivende med tanke på utvikling, vedlikehold og drift.

Basert på erfaringer med utvikling av teknisk løsning for *Nasjonalt register for ryggkirurgi* (Helse Nord), *Nyfødtmedisinsk kvalitetsregister* (Rikshospitalet) og *MRS – Medisinsk Registreringssystem* (Helse Midt-Norge), ser vi at en felles teknisk løsning er mulig i svært mange tilfeller. Spesielt gjelder dette hvis systemet bygges opp modulært etter en tjenesteorientert modell. På den måten kan en ivareta både målet om integrering med EPJ på lang sikt og datainnsamling av strukturerte medisinske data på kort sikt. Etablering av et standardisert tjenestegrensesnitt for kvalitetsregistre som kan benyttes ved videreutvikling av dagens løsninger og gjenbrukes ved integrering mot EPJ er en betingelse for dette.

Siden etablering av tjenestebusser ikke er kommet veldig langt verken regionalt eller nasjonalt, må en videreutvikling av felles teknisk løsning for kvalitetsregistre skje koordinert med det arbeidet som pågår rundt arkitektur i regi av *Nasjonal IKT*. Arbeidet med prosjektet som her presenteres har imidlertid vist at det er mulig å realisere en tjenesteorientert løsning på tross av at tjenestebuss ikke er endelig implementert. Det skjer på den måten at tjenester som forventes å finnes i en endelig tjenestebuss leveres som en del av systemet.

En forutsetning for dette er at det er mulig å etablere det vi har kalt for *Tjenestetransport* via helsenettet samtidig som det finnes en velfungerende infrastruktur for håndtering av PKI sertifikater. Dette er de samme krav som stilles med dagens meldingsorienterte løsninger.

Prosjektet har for øvrig vist at MRS og OpenQReg kan installeres og kjøres som en *Sentral fagapplikasjon* tilgjengelig i *helsenettet*. Videre så kan MRS kjøres som en *Lokal fagapplikasjon* med mulighet for integrering mot andre lokale fagsystemer innen foretaket eller sentrale tjenester i *helsenettet*. MRS kan også integreres med en *Pseudonymiseringstjeneste* for pseudonymisering av personinformasjon ved overføring til et *Nasjonalt helseregister*.

Opprinnelig var intensjonen i dette prosjektet å teste ut alle løsningskonseptene i helsenettet mellom Helse Nord, Helse Vest og Helse Midt-Norge. Kommunikasjon over helsenettet på tvers av regioner derimot, viste seg å være en utfordring for dette prosjektet. Tilsvarende erfaringer fra Nasjonalt Kvalitetsregister for Ryggkirurgi underbygger dette. Testing ble derfor foretatt internt i Helse Midt-Norge i et simulert miljø for noen av løsningskonseptene. Det er imidlertid et ønske fra dette prosjektet å kunne gjennomføre en fullskala test i helsenettet når nødvendige ressurser i helseforetakene og helsenettet stilles til rådighet.

2 Innledning

Det finnes i dag nærmere 20 nasjonale kvalitetsregistre Norge. De fleste av disse registrene er isolerte løsninger som ikke har tatt hensyn til hva som finnes av liknende IT-systemer i helsevesenet. Dette har flere uheldige konsekvenser:

- Hvert kvalitetsregister må implementere hver sin tekniske løsning.
- Kompliserende for IT-drift ved at antall ulike IT-løsninger øker.
- Vanskelig å sammenstille data på tvers av registre og helseforetak.
- Kostnadsdrivende ved utvikling, vedlikehold og drift.

I rapporten *Felles teknisk løsning for regionalt eide nasjonale kvalitetsregistre*[4] slås det fast at innregistrering til kvalitetsregister bør foregå som en integrert del av *Elektronisk Pasientjournal* (EPJ) og som del av den ordinære dokumentasjonsprosessen: ”*Det langsiktige målet synes ennå å være langt unna, og for regionalt eide nasjonale kvalitetsregistre er det nå et sterkt behov for å ha en felles modell for tekniske løsninger. Dette betyr at tekniske løsninger må utformes for å dekke registrenes behov på kort til mellomlang sikt. Den tekniske modellen må også være fleksibel nok til at det langsiktige målbildet kan realiseres når dette blir mulig teknisk og økonomisk.*”

På bakgrunn av dette fikk HEMIT i oppdrag av Fagdirektørforum/Nasjonal IKT å kjøre prosjektet *Felles teknisk løsning for regionalt eide nasjonale kvalitetsregistre* for å utrede forslag til felles tekniske løsninger. Prosjektet skulle med utgangspunkt i eksisterende løsninger se på gjenstående tekniske utfordringer.

Prosjektet ble delt i to faser. En *Prosjekteringsfase* som resulterte i et *Prosjekteringsdokument*[1]. Dette dannet basis for en *Gjennomføringsfase* som er beskrevet i dette dokumentet.

Prosjektgruppa for *Gjennomføringsfasen* har bestått av de samme deltagerne som under *Prosjekteringsfasen*:

Are Edvardsen - Helse Nord IKT
Bernt Olav Økland – Helse Vest IKT
Jan Helge Wergeland – Helse Sør-Øst
Per Haug (leder) - HEMIT
Ronny Thomassen - Helse Nord IKT
Rudi Bech – HEMIT

I forbindelse med utarbeidelse av dette dokumentet har hele gruppa hatt et innledende fysisk møte og ukentlige telefonmøter underveis. Alle dokumenter og relevant informasjon har blitt lagt ut på et eget arbeidsområde fortløpende (Ekstranett – Helse Midt-Norge).

I dette dokumentet er betegnelsen ”dette prosjektet” eller bare ”prosjektet” bruk i forbindelse med omtale av oppdraget *Prosjektoppdrag/-plan Nasjonalt samarbeid Proof of concept - felles teknisk løsning*[2]. Med betegnelsen ”denne løsningen”, ”løsningen” eller ”MRS PoC”, menes det som er utviklet som en del av samme oppdraget.

Kildekode eller mer inngående teknisk beskrivelse enn det som gis i dette dokumentet kan utveksles etter nærmere avtale.

3 Oppdrag/mandat fra Fagdirektørforum/NIKT/HM RHF

Oppdraget til denne prosjektgruppa ble gitt av Helse Midt RHF/HEMIT i form av et prosjektplan/oppdragsdokument[2] der det er gitt føringer for prosjektet i forhold til mål, økonomi og rapportering. Et sammendrag av viktige målsettinger er gitt i her.

3.1 Overordnede mål

Følgende hovedmålsetning ble formulert i oppdraget:

- Implementere et kvalitetsregister.
- Teste ut tekniske mekanismer.
- Involvere alle helseregioner i arbeidet for å utnytte og bygge kompetanse.
- Videreutvikle teknisk og funksjonelt målbilde med tanke på:
    - Pseudonymisering
    - Personvern
    - Sikkerhet
- Sammenligne *Medisinsk registreringssystem*(MRS) fra Helse Midt-Norge IT(HEMIT) og OpenQReg fra Uppsala Clinical Research Center(UCR) som begge er systemer for strukturert registrering av medisinske parametre.

3.2 Effektmål

Hovedresultatet av utprøvingsprosjektet vil være en dokumentert, testet plattform for kvalitetsregistre, samt oversikt over hva som må utvikles videre for å realisere teknisk løsning.

3.3 Resultatmål

Følgende resultater er forventet i oppdraget:

1. MRS installert på *helseregister.no* som *Sentral fagapplikasjon*.
2. MRS installert i Helse Vest som *Lokal fagapplikasjon*.
3. Løsning med tiltrodd pseudonym forvalter testet ut.
4. Kommunikasjon og meldingsutveksling satt opp mellom *Lokal fagapplikasjon* og *Nasjonalt helseregister.* Heri inngår også uttesting av en installasjon i Helse Midt-Norge.
5. Oppslag mot *Interregionalt register for enheter i spesialisthelsetjenesten*(IR-RESH).
6. Integrasjon mellom et fagsystem i Helse Vest og *Lokal fagapplikasjon*.
7. En dokumentert sammenligning av MRS fra HEMIT og OpenQReg fra UCR.

3.4 Fremdriftsplan

Følgende milepæler ble satt:

1. Prosjektplan for fiktivt kvalitetsregister er utarbeidet.
2. Beslutning om videreføring.
3. Fiktivt kvalitetsregister er implementert.

4 Realisering

I oppstarten av prosjektet ble følgende faser definert:

Fase	***Hovedaktivitet***
Prosjektstart	Etablering av prosjektgruppe
Prosjekteringsfasen	Planlegging og ansvarsfordeling
Gjennomføringsfasen	Implementering av tekniske løsninger
Avslutning	Sluttrapport ferdigstilt

Gruppen ble satt opp med én eller flere utviklere fra alle fire regionale helseforetak. Ved prosjektstart besto denne av én person fra Helse Sør-Øst (Rikshospitalet) og Helse Vest IKT samt to personer fra både HEMIT(Helse Midt-Norge IT) og Helse Nord IKT. Alle disse deltok aktivt fra *Prosjekteringsfasen* til avslutning. Utover selve oppdraget har dette vært med på å skape bedre kontakt mellom ulike tekniske miljø innen de regionale helseforetakene, samt at det har bidratt aktivt inn mot andre, utenforliggende prosjekter som eksempelvis deltagelse i *Nasjonalt helseregister prosjekt*[3] og etablering av nasjonalt sørvismiljø for kvalitetsregistre.

Selve *Gjennomføringsfasen* for prosjektet ble påbegynt umiddelbart etter *Prosjekteringsfasen*. Underveis har det kommet opp en del synspunkter som medfører endringer i forutsetninger satt i *Prosjekteringsfasen*. Den viktigste endringen er føringer gitt av *Tjenesteorientert arkitektur i spesialisthelsetjenesten*[10] som er et styringsdokument. Vi hadde opprinnelig lagt opp til en infrastruktur mellom foretak basert på meldingsutveksling. I arkitekturdokumentet er det tjenesteorientering som foretrekkes framfor meldingsorientering. Dette er omhandlet nærmere i eget kapittel.

4.1 Resultatmål

Forventede resultatmål er gitt i oppdraget under kapittel 3.3 og oppnådde resultatmål er gitt i mer detalj under kapittel 4.3. Endringer i forhold til forutsetninger gitt i oppdraget er kommentert og begrunnet. Selve utprøvingen ble i hovedsak basert på en installasjon av MRS både som *Lokal fagapplikasjon*, *Sentral fagapplikasjon* og *Nasjonalt helseregister* som en trelags arkitektur beskrevet i *Systemdokumentasjon MRS 2.0*[8]. Det fiktive kvalitetsregisteret ble definert som en *DataSettType* i MRS med tilhørende presentasjonsskjema og lastet i alle installerte instanser av *MRS PoC* for å få et koordinert testmiljø.

4.2 Endringer og utfordringer underveis

I *Gjennomføringsfasen* ble det gjort noen endringer som avviker fra de forutsetninger som ble gitt i prosjektplanen. Noe av dette er naturlige tilpassinger, mens andre baserer seg på utfordringer utenfor prosjektets kontroll. Selv om dette i stor grad er udramatiske endringer, så har noe av dette medvirket til en viss forsinkelse av *Gjennomføringsfasen*.

4.2.1 Meldingsorientering kontra tjenesteorientering

I et av resultatmålene i *Prosjektoppdraget* heter det: ”Kommunikasjon og meldingsutveksling satt opp mellom lokale innregistreringer og nasjonalt register”.

I forbindelse med utarbeidelsen av *Prosjekteringsdokumentet*[1] så vi for oss at overføring av data mellom *Lokal fagapplikasjon*, *Nasjonalt helseregister* og *Pseudonymiseringstjeneste* skulle foregå som meldinger. Hovedargumentet for dette var at vi da kunne benytte oss av allerede eksisterende infrastruktur samtidig som prosjektgruppen hadde kompetanse på

området bl.a. gjennom Helse Sør-Øst sine erfaringer fra *Norsk Nyfødtmedisinsk Kvalitetsregister.*

Etter hvert som vi jobbet oss inn i problemstillingene ble det fire forhold som endret vår oppfatning rundt dette:

1. Vanskelig tilgang på ressurser med dybdekompetanse på konfigurering og oppsett av meldingstjenere innen foretakene.
2. Føringer om tjenesteorienterting gitt i dokumentet *Tjenesteorientert arkitektur i spesialisthelsetjenesten*[10]: "*I den nye arkitekturen utøves samhandling ved hjelp av tjenester (tjenesteorientering), ikke oversendelse av informasjon (meldingsorientering)*"
3. MRS, som ble brukt som utgangspunkt for gjennomføringen av dette prosjektet, er designet med en 3-lags fysisk arkitektur og har derfor allerede et webtjenestelag.
4. Ved å definere et tydelig tjenestelag for kvalitetsregistre blir det faktisk lettere å integrere mot eksisterende meldingsservere innen foretaket. Løsningen letter dermed også muligheten for å implementere en meldingsorientert arkitektur der dette er ønskelig.

Summen av dette ble at vi fant det formålstjenlig både med tanke på gevinst for framtiden og med tanke på fremdrift å gjennomføre prosjektet basert på en tjenesteorientert arkitektur i stedet for en meldingsorientert arkitektur.

4.2.2 Interregional samhandling

Etablering av tekniske løsninger for medisinske kvalitetsregistre som skal ha nasjonal dekning krever at informasjon må kunne flyttes mellom juridiske enheter (HF) og regionale helseforetak. Slik utveksling av informasjon skal skje over helsenettet. Gjennomføringsfasen av dette prosjektet har vist at dette kan by på utfordringer. Det kan synes som om strukturen innenfor hver region er noen lunde homogen, og at kommunikasjon over helsenettet stort sett fungerer godt mellom de ulike juridiske enhetene innenfor regionen. Kommunikasjon over helsenettet på tvers av regioner derimot, viste seg å være en utfordring for dette prosjektet. Tilsvarende erfaringer fra *Nasjonalt Kvalitetsregister for Ryggkirurgi* underbygger dette.

Det kan synes som om mye av de tekniske problemene er knyttet til ruting av trafikk fra HF/RHF ut på det interregionale helsenettet, eller mangel på sådan. Erfaringer med etablering av interregionale/nasjonale tekniske løsninger viser at det alltid er problematisk å etablere nødvendig kommunikasjon over helsenettet. Når det opptrer feilsituasjoner vil dette involvere minst tre parter: avsender, NHN(Norsk helsenett) som nettleverandør og mottaker av informasjon. Dette gjør feilretting mer komplisert og tidkrevende.

4.3 Beskrivelse av løsningen

Utprøvingen baserer seg på en installasjon av *MRS PoC* både som *Lokal fagapplikasjon* og *Sentral fagapplikasjon* samt *Nasjonalt helseregister*. Disse tekniske løsningskonseptene er beskrevet nærmere i *Nasjonalt helseregister prosjekt – Teknisk gruppe – Hoveddokument Løsningskonsepter*[3].

I forbindelse med prosjektet ble det laget et fiktivt register basert på et eksisterende papirbasert kvalitetsregister (*Intensivregisteret*). Dette ble gjort for å illustrere mest mulig konkrete problemstillinger. Gyldigheten av denne implementasjonen i prosjektet er ikke vurdert av noe medisinsk fagmiljø. En slik definisjon består av fire XML dokumenter:

1. Datasetttype – registerets parametre
2. Valideringsregler – lovelige grenseverdier og sammenheng mellom registerets parametre.
3. Skjema – skjermbasert registreringsskjema.
4. Kontrollskript – ECMA-script for klientbasert validering og kontroll.

Sammen med en binær distribusjon av *MRS PoC* utgjør disse XML dokumentene *Lokal fagapplikasjon*, *Sentral fagapplikasjon* og *Nasjonalt helseregister*.

Som en del av prosjektet ble det også utviklet prototyp på en *Pseudonymiseringstjeneste* som kan plasseres hos en tiltrodd tredjepart mellom *Lokal fagapplikasjon*, *Sentral fagapplikasjon* og *Nasjonalt helseregister*. Prosjektet fikk etter avtale med Folkehelseinstituttet tilgang til kildekode som benyttes i *Reseptregisteret* ved pseudonymisering. Selve koden har ikke blitt benyttet her, men vil være høyst aktuell hvis prototypen skal realiseres som en virkelig tjeneste.

I forbindelse med utprøvingen ble det fra kildekodesystemet for MRS "branchet" ut en egen versjon til *MRS Development* basert på *MRS Main* versjon 2.0.20.* med navn *KvalitetsregisterPOC*. Det ble så utviklet en prototyp på et nytt tjenestelag tilpasset løsningen. I det gamle tjenestelaget var det ikke tatt hensyn til at data kan bli registrert i ulike databaser før de skal samles i en felles database. Det betyr bl.a. at det nå måtte benyttes Globally Unique Identifier (GUID) som nøkler på datasett i stedet for rene løpenummer.

For å binde de ulike tjenestene i løsningen sammen under utprøvingen ble det utviklet det vi har valgt å kalle for *Integrasjonspunkter*. I *Prosjekteringsdokumentet*[1] så vi for oss disse integrasjonspunktene skulle være meldingsorienterte. Etter hvert som prosjektet skred fram og føringene i dokumentet *Tjenesteorientert arkitektur i spesialisthelsetjenesten*[10] ble tydeligere, så ble også vår løsning mer tjenesteorientert. Det betyr at *Lokal fagapplikasjon, Pseudonymiseringstjenesten* og *Nasjonalt register* eksponerer tjenester som konsumeres av *Integrasjonspunktene*. I denne sammenheng forstår vi *Integrasjonspunktene* som selvstendige applikasjoner som kun har som formål å knytte de nevnte tjenestene sammen.

I et praktisk eksempel vil tjenestene for *Lokal fagapplikasjon* kun finnes tilgjengelig innenfor hvert enkelt foretak, mens *Pseudonymiseringstjenesten* og *Nasjonalt helseregister* er nasjonale tjenester som kan befinne seg i helsenettet.

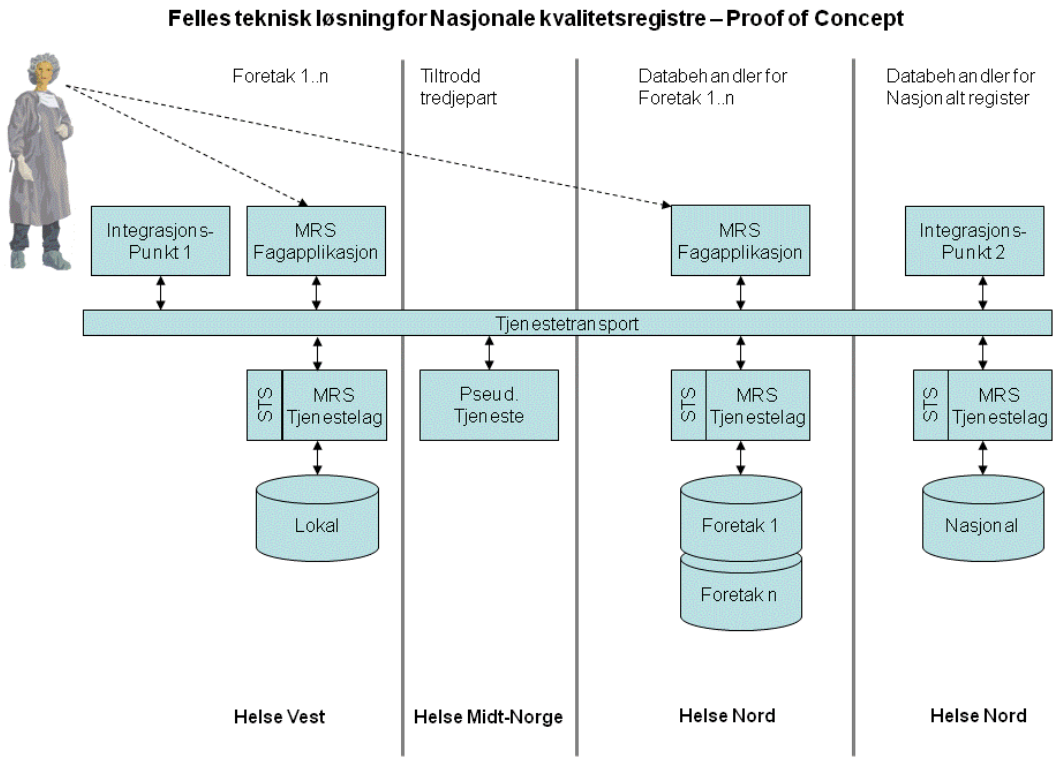
Det er viktig å være oppmerksom på at de tjenestene vi ser for oss også kan konsumeres av meldingstjenere (som BizTalk) slik at en tradisjonell meldingsorientert infrastruktur godt kan bygges på toppen av løsningen hvis det er ønskelig.

Et annet viktig området er sikkerhet. Det gamle tjenestelaget var konstruert for trafikk internt i helseforetaket og tilfredsstilte derfor ikke de krav som forventes når helsenettet skal benyttes som transport. Helsenettet er å betrakte som et usikkert nett sett fra helseforetakene. Sikkerhet i denne sammenhengen er omfattet av 4 områder:

1. *Mutual Authentication* – både sender og mottaker må entydig identifiseres.
2. *Authorization* – brukeren som benytter servicen må ha en rolle i MRS for å få tilgang til nødvendig funksjonalitet.
3. *Integrity* – digital signering av overføringer slik at innholdet ikke kan endres underveis.
4. *Confidetiality* – sesitive opplysninger skal kunne krypteres slik at ingen kan se på innholdet underveis.

Med bakgrunn i dokumentet *Tjenesteorientert arkitektur i spesialisthelsetjenesten*[10], så ble tjenestelaget implementert basert på føderert sikkerhet i stedet for nasjonal brukerdatabase. Implementasjonen ble gjort ved å benytte rammeverket i *Windows Communication Foundation* (WCF) slik det er implementert under .NET 3.5 Service Pack 1.

Normalt ved implementering av føderert sikkerhet vil *Security Token Service*(STS) være en fellestjeneste innen foretaket. Den er da gjerne koblet mot tilsvarende tjeneste hos partnere som *trustes*. Her ble den implementert som en tjeneste bare med tanke på dette prosjektet. Prinsippene er de samme slik at muligheten for å koble mot en fellestjeneste er fullt mulig senere. Her kan det være interessant å vurdere produkter som allerede finnes tilgjengelig i markedet som *PingFederate*® fra *PingIdentity*® (http://www.pingidentity.com/).



Figur 1 - Prinsippskisse for felles teknisk løsning for regionalt eide nasjonale kvalitetsregistre – Proof of concept.

Integrasjonspunkt 1 henter først et SAML-token fra *Security Token Service*(STS) og data fra *MRS tjenestelag* som så overføres til *MRS tjenestelag* i *Nasjonalt helseregister*. I samme operasjon overfører *Integrasjonspunkt 1* fødselnummer/saksnummer til *Pseudonymiseringstjeneste*.

Integrasjonspunkt 2 henter SAML-token fra STS og overfører pseudonym/saksnummer fra *Pseudonymiseringstjeneste* til *MRS Tjenestelag* i *Nasjonalt helseregister*.

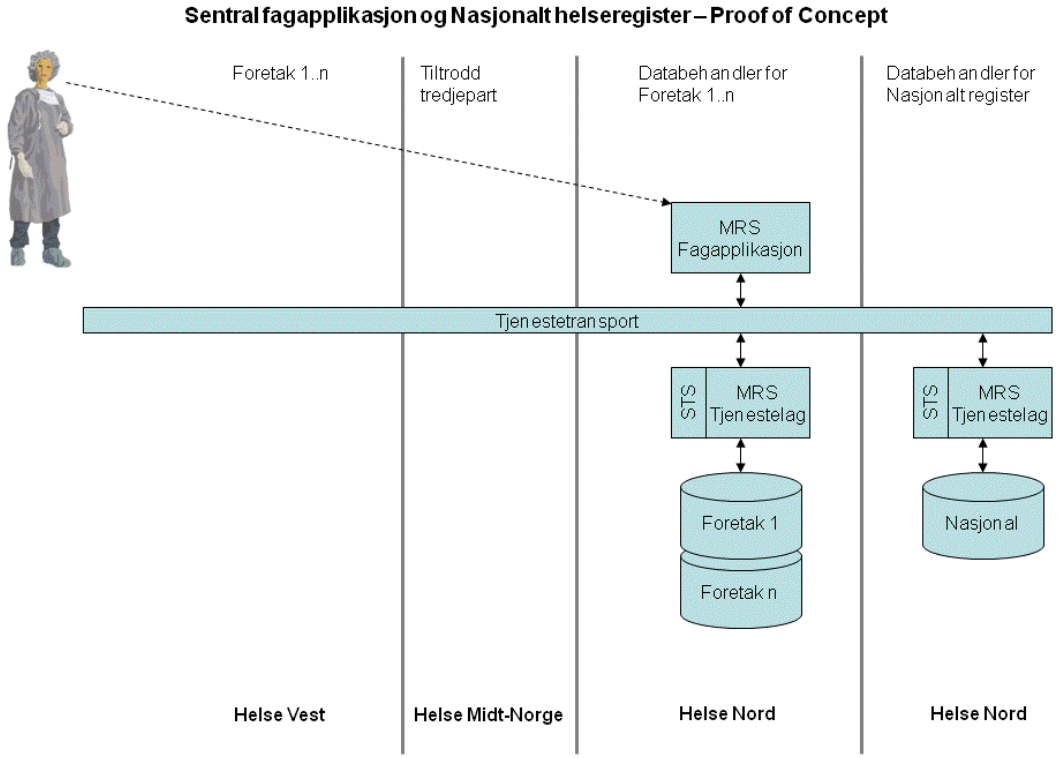
Ved rett konfigurasjon og ved bruk av sertifikater kan alle fire punktene for sikkerhet dekkes opp gjennom løsningen.

1. *Mutual Authentication* - ligger i sertifikat og selve SAML tokenet.
2. *Authorization* – ligger som Claims(assertions) i SAML tokenet (XACML).
3. *Integrity* - gjennom signering med PKI sertifikat.
4. *Confidetiality* - gjennom kryptering med PKI sertifikat.

4.3.1 Sentralt register

Et sentralt register i denne sammenheng er det vi oppfatter som *Sentral fagapplikasjon*. Denne ble realisert som en installasjon av *MRS PoC* på server i Helse Nord eksponert via SSL på helsenettet med adresse: https://helseregister.no/intensivregister/. Løsningen ble installert med egen bruker- og pasientdatabase uten noen kobling mot andre registre.

Denne installasjonen av *MRS PoC* inneholder også *MRS* Tjenestelag som representerer *Nasjonalt helseregister* ved kommunikasjon mellom lokalt og sentralt register som beskrevet i eget kapittel.



Figur 2 - Sentral fagapplikasjon med Nasjonalt helseregister installert i Helse Nord

4.3.2 Lokalt register

Et lokalt register i denne sammenheng er det vi oppfatter som *Lokal fagapplikasjon*[3].

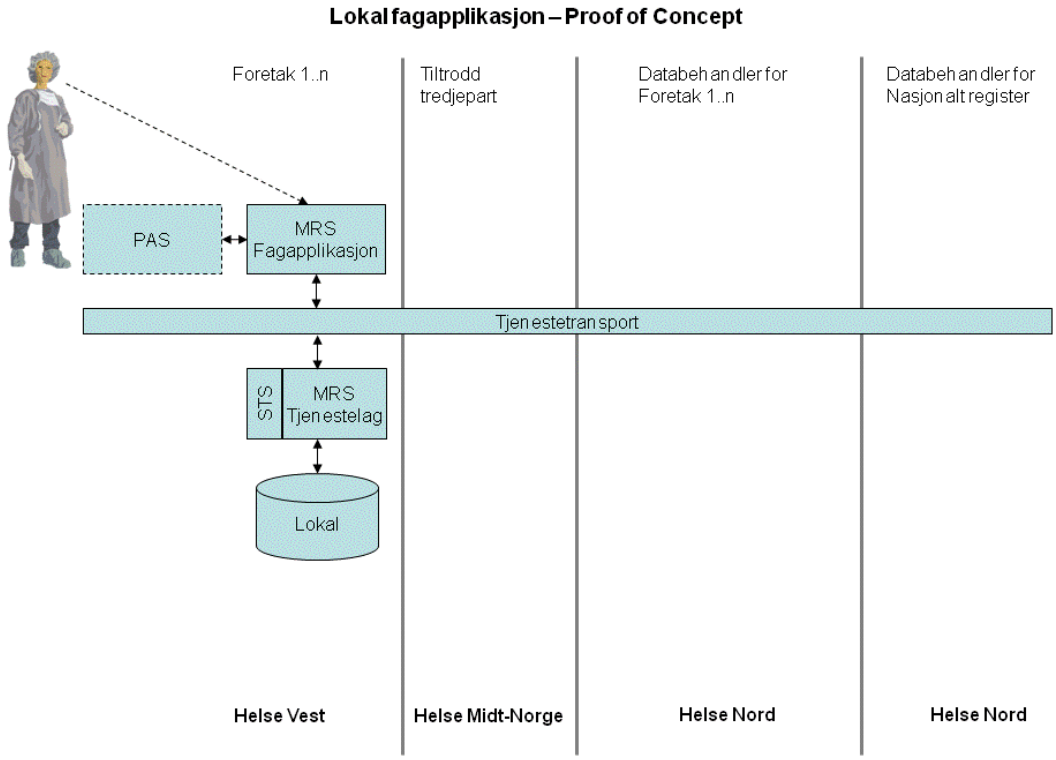
I Helse Vest er *MRS PoC* installert som en helt frittstående løsning som kan nås internt i foretaket på adressen http://bgo-app98.ihelse.net/Intensivregister/. Den er ikke integrert med PAS/EPJ eller Active Directory. Installasjonen er fordelt over 3 ulike servere.

- Database server, Microsoft SQL Server 2005,
- Applikasjons servere Microsoft Internet Information Services (IIS) 6.0
- Rapport server Microsoft SQL Server 2005: Reporting Services.

Ved valg av denne serverstrukturen kan Helse Vest IKT sine standard servertjenester benyttes og man unngår dermed investeringskostnader til dedikerte servere..

MRS PoC installasjonen er eksponert både på port 80(http) og port 443 (https).

Planlagt kobling mot lokal PAS i Helse Vest er beskrevet i eget kapittel.



Figur 3 Lokal fagapplikasjon installert i Helse Vest

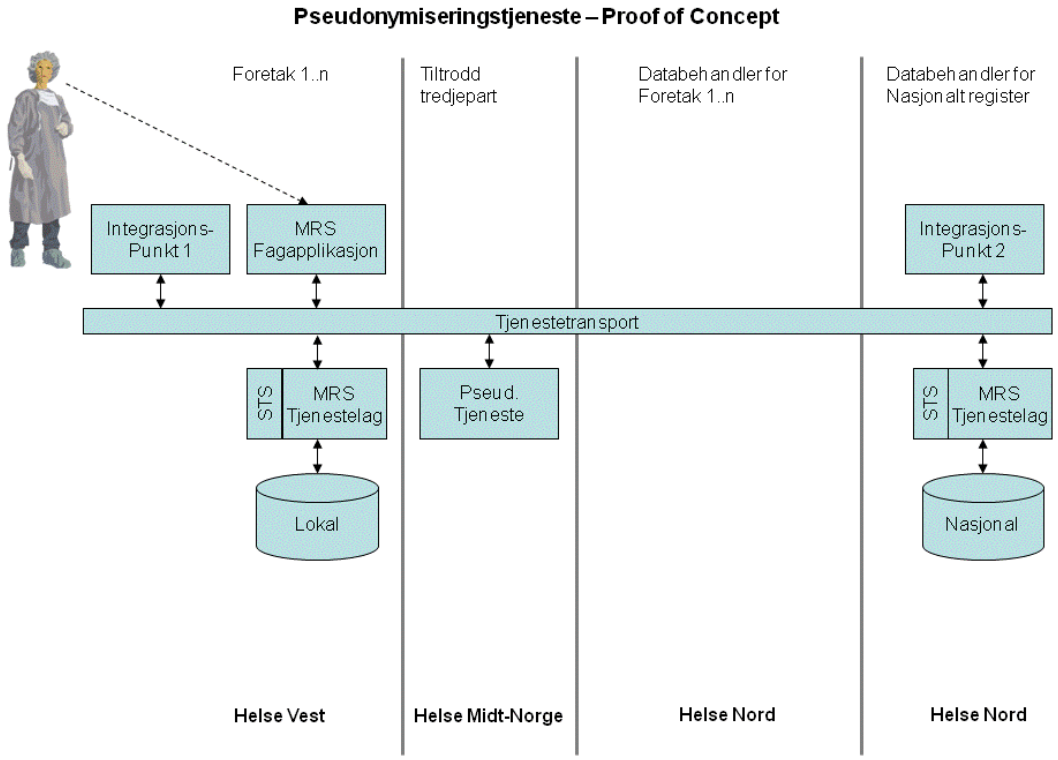
4.3.3 Tiltrodd Pseudonym Forvalter (TPF)

Pseudonyme registre er registre der en persons identitet er erstattet med et pseudonym. Det betyr at opplysningene i registeret ikke kan knyttes til en bestemt person. Opplysningene er allikevel entydige på en slik måte at når det kommer til nye opplysninger om vedkommende i registeret, så blir disse knyttet til samme pseudonym. Opplysningene om et pseudonym kan derfor spores over tid, noe som er viktig for et kvalitetsregister.

For at dette skal foregå på en sikker måte i forhold til personvernet og helseregisterloven skal det benyttes en *Tiltrodd pseudonymforvalter* (TPF). TPF kjenner koblingen mellom personens identitet og pseudonymet, uten at TPF samtidig har tilgang til helseopplysninger om personen.

Funksjonen som utføres av TPF kan en tenke seg som en tjeneste i helsenettet. Tjenesten kan brukes både ved selve pseudonymiseringen av det nasjonale registeret og ved kobling av opplysninger fra flere registre i forbindelse med forskning.

Løsningen ble utviklet spesielt for dette prosjektet med de tjenester som var tilstrekkelig for å kunne gjennomføre *Proof of concept.*



Figur 4 Pseudonymisering som tjeneste i helsenettet

4.3.4 Kommunikasjon mellom lokalt og sentralt register

Kommunikasjon mellom *Lokalt fagsystem* og *Nasjonalt helseregister* foregår over *helsenettet*. *Helsenettet* er fra helseforetakene sin side å betrakte som et usikkert nett og derfor må all trafikk krypteres. I alle figurer i dette dokumentet er begrepet *Tjenestetransport* å betrakte som noe som skjer via helsenettet.

Sikringen må skje minimum ved bruk av SSL mellom alle aktører. Videre så må det benyttes PKI-sertifikater for å sikre at *Autentisering* og *Authorization* foregår på en sikker måte. For å sikre *Integrity* og *Confidetiality* bør det også benyttes PKI-sertifikater.

4.3.5 Bruk av *IR-RESH*

IR-RESH (*InterRegionalt Register for Enheter i SpesialistHelsetjenesten*) er en database som inneholder organisasjonskartet for spesialisthelsetjenesten. Databasen er komplett med beskrivelser av hva de ulike helseforetakene og deres underenheter er, og hvilke tjenester de yter.

- Sentralt skal data brukes ved innrapportering og kvalitetssikring av aktivitets- og kvalitetsdata til statsforvaltningen.
- Lokalt ved RHF og HF skal data benyttes til blant annet styring på områder som kvalitet, organisering, aktivitet og økonomi.

IR-RESH har tidligere vært ivaretatt som et prosjekt i regi av Nasjonal IKT, men driftes nå av Norsk Helsenett på vegne av sektoren. Norsk Helsenett har systemeierskap og driftsansvar, mens RHF-ene har ansvaret for informasjon og forvaltningen av denne. Norsk pasientregister er gitt ansvar for drift og implementering av *Register for Enheter i SpesialistHelsetjenesten* (RESH). RESH vil bygge på registrering i *IR-RESH*.

Tekniske løsninger for medisinske kvalitetsregistre bygd på *MRS PoC* kan ta i bruk *IR-RESH* koder gjennom integrasjon mot de tjenester som er eksponert på NHN. Da dette ikke ble ansett som vesentlig for gjennomføringen, ble det ikke etablert teknisk integrasjon eller oppslag mot *IR-RESH* for *MRS PoC*.

IR-RESH brukes per mai 2009 blant annet som del av brukeradministrasjonen på portalen *helseregister.no*. som er en ressurs eksponert på helsenettet for nasjonale helseregistre og forskningsstudier der blant annet den sentrale delen av fiktivt register (*Intensivregisteret*) i dette prosjektet er installert.

4.3.6 Integrasjon mellom lokalt register og fagsystem

For å sikre størst mulig fleksibilitet i systemet er MRS modularisert opp ved hjelp av såkalte providere. En provider er som navnet sier en tilbyder av en eller annen tjeneste eller funksjon i systemet.

Pasientprovideren håndterer alt som har med selve pasienten å gjøre. Dette gjør at en kan trekke all pasientinformasjon ut av selve systemet, og få en fullstendig avidentifisert database. Det eneste som ligger igjen i databasen til MRS er en kobling mellom den interne pasientid'en i MRS og pasient'iden i det eksterne pasientsystemet.

Men pga at MRS skal kunne fungere frittstående, er det også utviklet en egen intern pasientdatabase i systemet. Denne er kryptert, og håndteres av systemet ellers som om den skulle vært en ekstern database.

MRS PoC er installert med intern pasientdatabase både for *Lokal fagapplikasjon* og *Nasjonalt helseregister*. Opprinnelig var tanken at det som en del av dette prosjektet skulle utvikles en

Pasientprovider mot PAS-systemet i Helse Vest. Imidlertid ble det også behov for en *Pasientprovider* for *Nasjonalt helseregister* og derfor ble den utviklet i stedet. Det var for å kunne verifisere gjennom brukergrensesnittet i *MRS PoC* at data faktisk blir overført pseudonymisert til *Nasjonalt helseregister*.

4.4 Test av løsningen

Den opprinnelige planen var å teste løsningen ved å installere QAppLocal(*Lokal fagapplikasjon*) i Helse Vest, QAppCentral(*Nasjonalt helseregister*) i Helse Nord og QAppTtp(*Pseudonymiseringstjeneste*) i Helse Midt-Norge. Grunnet brannmurproblematikk så har det ikke vært mulig for de aktuelle serverne i de ulike regionene å snakke sammen. Løsningen og samspillet mellom de ulike delene er følgelig testet ved hjelp av tre servere hos HEMIT. Kapittel 4.4.1 beskriver hvordan disse maskinene var satt opp, men dette kan ikke regnes som systemkrav da det for eksempel er mulig å sette opp løsningen uten Windows Vista.

4.4.1 Testoppsett

- Server 1 (lokalt register)
  - Basisprogramvare
    - Windows Server 2003 R2
    - Microsoft .Net Framework 2.0 SP2
    - Microsoft .Net Framework 3.5 SP1
    - IIS6
    - IE8
  - MQR deler
    - MqrFederationServices.MqrStsHost (QAppLocalSts)
    - MrsPocQAppTtp.IntegrationPoint.QappLocalToQAppTtp (IP1)
    - ServiceHost (QAppLocalService)
    - Intensivregister (QAppLocal)
  - Sertifikater (X509)
    - Local Computer
      - Personal
        - Server1.domain
      - Trusted Root Certification Authorities
        - CN = hemit.no Software Development CA
      - Trusted People
        - Server1.domain
        - Server3.domain
    -
- Server 2
  - Basisprogramvare
    - Windows Server 2003 R2
    - Microsoft .Net Framework 2.0 SP2
    - Microsoft .Net Framework 3.5 SP1
    - Microsoft SQL Server 2005 (9.0.4035) (Instans 1)
    - Microsoft SQL Server 2008 (10.0.1600) (Instans 2)
  - MQR deler
    - MqrIntensivCentral (Instans 1)
    - MqrIntensivLocal (Instans 1)
    - MrsPocQAppTtpUsingHeritage (Instans 2)
- Server 3 (sentralt register)
  - Basisprogramvare
    - Windows Vista w/SP1
    - Microsoft .Net Framework 2.0 SP2
    - Microsoft .Net Framework 3.5 SP1
    - IIS7
    - IE8
  - MQR deler
    - MqrFederationServices.MqrStsHost

        - MrsPocQAppTtp.IntegrationPoint.QappCentralQAppTtp (IP2)
        - ServiceHost (QAppCentralService)
        - MrsPocQAppTtp.ServiceHost (TtpService)
        - Intensivregister
    - Sertifikater (X509)
        - Local Computer
            - Personal
                - Server3.domain
            - Trusted Root Certification Authorities
                - CN = hemit.no Software Development CA
            - Trusted People
                - Server1.domain
                - Server3.domain

4.4.2 Beskrivelse av MQR deler

Her vil det bli gitt en kort presentasjon av de ulike delkomponenetene som er brukt i forbindelse med testingen. Server1.domain og Server3.domain må byttes ut med FQDN for de serverne dette skal testes på. Testingen er utført med kode som er kompilert i DEBUG-modus og sjekket inn per 25.05.2009 07:00. Det er forløpig ikke laget installasjonspakker for alle delene.

4.4.2.1 MqrFederationServices.MqrStsHost

Denne tjenester fungerer som en *Security Token Service* (STS) som autentifiserer brukerne og utsteder *tokens*. Et *token* har en bestemt gyldighetsperiode (10 timer i dette oppsettet), og kan i prinsippet gjenbrukes innenfor denne perioden. Slik testene er satt opp så vil ikke disse bli gjenbrukt. Tjenesten bruker samme database som Intensivregisteret på den aktuelle serveren. Det er mulig å anvende både integrert sikkerhet og brukernavn/passord i forbindelse med autentifisering, men det er kun brukernavn/passord som er testet. Disse blir verifisert mot brukerne som er registrert i MQR-databasen til registeret. Det ble opprettet en bruker i QAppCentral og en i QAppLocal i forbindelse med testingen.

4.4.2.2 ServiceHost

ServiceHost eksponerer blant annet MqrDataService som håndterer uthenting og lagring av DataSetMetaene. Autentifisering håndteres med WS-Federation og tjenesten konfigureres til å stole både sertifikatene som er utstedt for Server 1 og Server 3. Autorisasjon er ikke håndtert forløpig, men det skal i framtiden håndteres ved at *Claims* signert av den aktuelle STS sjekkes. Det kan i den sammenheng bli aktuelt å ta i bruk *Home Federation* på en slik måte at et token utstedt av QAppLocalSts brukes til å autentifisere brukeren mot QAppCentralSts som igjen bruker dette til å utstede et nytt token som gir brukeren tilpassede Claims som kan brukes mot QAppCentralService. Ferdigstilling og testing av disse mekanismene bør være en sentral del når test av *MRS PoC* i helsenettet skal fullføres.

4.4.2.3 Intensivregister

Intensivregisteret er en installasjon av MQR laget i forbindelse med prosjektet som viser et enkelt skjema tilsvarende papirskjemaet NIR bruker i dag. Ved installasjon av Intensivregister som QAppLocal settes det opp til å bruke MQR sin interne pasientdatabase. Ved installasjon av registeret som QAppCentral settes det opp til å bruke en alternativ implementasjon for å håndtere pasienter som gjør det mulig å søke fram og presentere pseudonyme pasienter i QAppCentral. Dette gjøres ved å legge til følgende i provider.config for QAppCentral:

```
<component id="pasientProvider"
      service="Hemit.MRS.BusinessLayer.ProviderInterfaces.IPasientPro
      vider, Hemit.MRS.ProviderInterfaces"
      type="Hemit.MRS.BusinessLayer.DefaultProviders.ExternalIdPatien
      tProvider, Hemit.MRS.DefaultProviders"
```

```
        lifestyle="transient"
/>
```

Eksisterende konfigurasjon for pasientProvider må så fjernes fra den sammen filen. *ExternalIdPatientProvider* er utviklet I forbindelse med prosjektet og demonstrerer hvordan MQR kan konfigureres til å håndtere pasienter på ulike måter. Kodemessig tilsvarer denne provideren en integrasjon mot et lokalt PAS, men i dette tilfellet gjøres oppslagene fortsatt mot MQR-databasen.

4.4.2.4 MrsPocQAppTtp.ServiceHost (TtpService)

Denne tjenesten tar i mot et sett med identiteter med assosierte saksnummer og oversetter identitene til en annen type identitet. Hvordan identitetene skal oversettes styres av hvordan kontraktene er satt opp, men i prosjektet så finnes det bare en *Contract* og en måte å oversette identiteter på og det er fra fødselsnummer til pseudonymer. Pseudonymene lages som GUID'er. Dersom samme fødselsnummer blir oversendt flere ganger så vil det uansett bare bli opprettet ett pseudonym.

Løsningen ble opprinnelig laget med tanke på meldingsutveksling, men overgang til tjenesteorientering gjør at datamodellen og tjenestegrensesnittet bør revideres litt. Nå vil en innkommende melding (`IdentityTransformationRequest`) alltid føre til at det lages en utgående melding (`TransformedIdentities`) som må hentes ut av QAppCentral . Det vil trolig være mer hensiktsmessig å gjøre det mulig å slå opp pseudonym ved hjelp av saksnummer.

Sikkerheten er nå slik at tjenesten stoler på alle tokens utstedt av tiltrodde STS'er, men for framtiden må dette løses slik at sertifikatene til de aktuelle STS'ene assosieres med kontraktene. Da vil en bruker som har fått utstedt et token fra "sin" STS kun få lov til å sende/hente meldinger relatert til "sin" kontrakt. Sjekking av Claims i forhold til dette kan abstraheres ut fra selve tjenesten ved å innføre en egen STS for TtpService som utsteder Claims tilpasset tjenesten. Dette bør løses når test av *MRS PoC* i helsenettet skal fullføres.

4.4.2.5 MrsPocQAppTtp.IntegrationPoint.QappLocalToQAppTtp (IP1)

Integrasjonspunkt 1 (heretter kalt IP1) bruker WS-federation mot QAppLocalSts for å skaffe et *token* som brukes ved tilkobling til QAppLocalService, QAppCentralService og MrsPocQAppTtp.ServiceHost. IP1 henter ut en liste over nøklene til alle *DataSetMeta*'ene som finnes i QappLocalService. Disse nøklene brukes igjen til å hente ut hver *DataSetMeta* og tilhørende pasientopplysninger. DataSetMetaene lagres til QAppCentral via QAppCentralService. Fødselsnummer og nøkkel (DataSetMetaGuid) overføres til TtpService.

4.4.2.6 MrsPocQAppTtp.IntegrationPoint.QAppCentralQAppTtp (IP2)

Integrasjonspunkt 2 (heretter kalt IP2) bruker WS-federation mot QAppCentralSts for å skaffe et *token* som brukes ved tilkobling til QAppCentralService og TtpService. IP2 henter ut en liste over `TransformedIdentities` tilknyttet en ContractId. Hver av disse transformerte identitene består av et pseudonym og et saksnummer (DataSetMetaGuid). IP2 bruker disse opplysningene til å knytte pseudonymene til de tidligere mottatt DataSetMetaene. Når dette er gjort er det mulig å søke fram dataene som ble registrert i QAppLocal i QAppCentral ved hjelp av pseudonymene. Før IP2 har gjort denne koblingen så er det ikke mulig å søke fram mottatte DataSetMeta i webgrensesnittet, men det vil være mulig å lage rapportert som viser hvilke- og hvor mange DataSetMeta som mangler kobling til pasient.

4.4.3 Sertifikater

WS-Federation krever bruk av X509 sertifikater. Det har ikke blitt vurdert som hensiktsmessig å kjøpe sertifikater fra generelt aksepterte sertifikatutstedere i forbindelse med dette POC prosjektet. Slike sertifikater kan dessuten være et problem når man jobber innenfor Norsk Helsenett da disse sertifkatene typisk vil kreve at det gjøres CRL-oppslag mot Internett, og det er ikke gitt at servere i våre nett har tilgang til Internett. Det har derfor vært nødvendig å

bruke selvsignerte sertifikater for å teste løsningen. HEMIT har den sammenheng opprettet et selvsignert *Root Certification Authority* sertifikat som igjen er brukt til å signere sertifikatene som er brukt til de ulike serverne. Ved installering av løsningen må nødvendige sertifikater lages og installeres for at de ulike MQR delene skal klare å snakke sammen. På sikt bør slike sertifikater komme fra en CA etablert i Norsk Helsenett eller fra en sub-CA i de ulike regionene som igjen er godkjent av en felles CA i Norsk Helsenett. Dette er viktig for at sikkerheten skal bli tilstrekkelig god. Serversertifikater bør også være identifisert med riktige DNS-navn. Sertifikatet som skal brukes til å signere tokens på Server1.domain bør altså ha CN=Server1.domain. Det anses som viktig å kartlegge hvem som har ansvar for en slik infrastruktur i Norsk Helsenett og de ulike helseregionene for å kunne få satt opp løsningen riktig. Dersom infrastrukturen ikke er på plass så bør **Fase 2** ha som delmål å være pådriver for at denne infrastrukturen skal komme på plass.

For at sertifikater installert på en gitt maskin skal kunne brukes til signering av STS'ene så må brukeren som eksekverer STS'ene ha tilgang til det aktuelle sertifikatets private nøkkel. Alle webapplikasjoner i IIS er assosiert med en Application Pool (AppPool) og det er identiten til denne som må ha tilgang til de private nøklene. Som default er alle Application Pools satt opp til å kjøre som *Network Service*, men man må alltid validere at rett bruker har tilgang.

Sertifkatene som er brukt i denne testen ble opprettet med certmgr.exe på følgende vis:

1. Opprette rot sertifikat:

```
makecert -pe -n "CN=hemit.no Software Development CA" -ss Root -sr
LocalMachine -sv "HemitDevelopmentCA.pvk" -a sha1 -sky signature -r
"HemitDevelopmentCA.cer"
```

2. Legge til rotsertifikat til Trusted Root Certification Authorities

```
certmgr -add "HemitDevelopmentCA.cer" -s -r localmachine root
```

3. *Opprett serversertifikat (gjøres bade på Server 1 og Server 3)*

```
makecert -pe -n "CN=%COMPUTERNAME%.hemit.helsemn.no" -ss my -sr LocalMachine -
a sha1 -sky exchange -eku 1.3.6.1.5.5.7.3.1 -ir LocalMachine -sp "Microsoft
RSA SChannel Cryptographic Provider" -sy 12 -iv "HemitDevelopmentCA.pvk" -ic
"HemitDevelopmentCA.cer" "%COMPUTERNAME%.hemit.helsemn.no.cer"
```

4. Gi tilgang til privat nøkkel (**Obs**! Dette gir tilgang til alle nøkler)

```
cacls "%ALLUSERSPROFILE%\Application Data\Microsoft\Crypto\RSA\MachineKeys" /e
/g "NT AUTHORITY\NETWORK SERVICE":R /t /c
```

5. **I**nstaller og verifisert at sertifikatene er installert "riktig sted" i henhold til testoppsettet.

4.4.4 Testgjennomføring

Det ble opprettet en bruker i QAppCentral og en i QAppLocal. Begge brukerne ble gitt tilgang som pasientansvarlig for den eneste avdelingen som finnes i en standard MQR installasjon. Det ble verifisert at avdelingen hadde samme IR-RESH kode i begge registrene.

Etter konfigurasjon av testoppsettet ble det registrert fire pasienter i QAppLocal, og ett til fire skjema per pasient. Deretter ble IP1 kjørt uten å gi noen feilmelding. Manuell verfisering av innholdet i databasene bekreftet at IP1 hadde gjort det som var forventet. Så ble IP2 kjørt uten at det kom noen feilmeldinger. Testeren logget seg så på QAppCentral og søkte fram pasientene med søkestrengen "%". Alle pasientene kom fram i listen og ble presentert med deres pseudonymer i steden for navn. Ved å gå inn på hver av disse pasientene var det mulig å se at data var overført, og ved å klikke seg inn på hvert enkelt skjema kunne man også se at data samsvarte med det som ble registrert i QAppLocal.

4.5 Alternative tekniske løsninger

En grunnleggende egenskap for det tekniske rammeverket rundt medisinske kvalitetsregistre er at de er relevant og dekkende for kvalitetsregistrenes formål. Framtidige medisinske kvalitetsregistre vil ha store forskjeller i de krav som stilles til funksjonalitet i det tekniske rammeverket som skal brukes (e.g. krav om integrasjon mot fagsystemer, spesielle krav til sikkerhet, aktiv medvirkning fra pasienter, kobling mot andre registre etc.). Det vil derfor være formålstjenlig med et knippe av teknisk løsninger som samlet kan fylle kravene som stilles av framtidige medisinske kvalitetsregistre. Med dette som bakgrunn, ble denne gruppen bedt om å sammenligne MRS med OpenQReg som i likhet med MRS er en plattform for å bygge innregistreringsløsninger på. MRS er utviklet av HEMIT mens OpenQReg har vært i bruk for flere nasjonale medisinske kvalitetsregister i Sverige over mange år. OpenQReg er utviklet av Uppsala Centre of Research (UCR). Tabell x gir noen sammenligninger mellom MRS og OpenQReg, men er ikke uttømmende.

Egenskap	***MRS***	***OpenQreg***
Utviklingsmiljø		
Microsoft .NET v3.5 sp1	x	
Eclipse		x
C#	x	
Java		x
Maven		x
ASP.NET	x	
ECMA Script	x	x
JavaServer Pages (JSP)		x
Andre		
MS Test	x	
MS Team Foundation Server (bugtracking,source control, scrum)	x	
Subversion versjonshåndtering		x
FireBug		x
Driftsmiljø		
Windows Server	x	x
Unix/Linux server		x
IIS, v6, v7	x	x
Apache		x
Apache Tomcat		x
Microsoft SQL Server 2005, 2008	x	
MySQL v5.x		x
Registerplattform		
Metadata drevet/definert	x	x
Språkhåndtering, system	x	x
Språkhandtering, register		x
Støtte for utf8 (fra datalag til applag)	x	x
Distribusjon av system/driftsmeldinger	x	x
Log, brukeraktivitet som innlogging, les og skriv	x	x
Log, tilfredsstiller normen for informasjonssikkerhet		
Log, systemfeil	x	x
Log, missbruk		x
Registrering av data		
Klient Internet Explorer	x	x
Klient Firefox		x

Klient andre		
Hjelpefunksjonalitet (per felt)	x	x
Feltvalidering ved innregistrering	x	x
Kladd/mellomlagring av skjema	x	x
Ferdig/låsmarkering av skjema	x	x
Deaktivering/aktivering av data	x	x
Import av historiske data/importfunksjon		
Transport av data		
Direkte mellom applikasjon og lokal database	x	
Direkte mellom applikasjon og sentral database	x	x
Via meldingsbuss mellom applikasjon og lokal database	x	
Via meldingsbuss mellom lokal og sentral database	x	
Kryptert mellom bruker og applikasjon	x	x
Kryptert mellom applikasjon og lokal database	x	
Kryptert mellom lokal og sentral database	x	
Kryptert mellom applikasjon og sentral database	x	
Lagring av data		
Lokalt	x	
Sentralt	x	x
Lokalt og sentralt	x	
Rapportering av data		
Rapportering som mulig påbygg til hvert enkelt register	x	x
Innebygd rapporteringsfunksjonalitet		
Generiske/ferdigdefinerte univariate rapporter		
Integrasjon		
Kobling mot Folkeregister på NHN		
Kobling mot journal og andre fagsystemer	x	
Brukeradministrasjon/SSO på helseregister.no	x	x
kobling mot IR-RESH		
Eksponering av egne tjenester	x	
Brukerhåndtering		
Innlogging med brukernavn og passord	x	x
Krav til (sterke) passord		x
Innlogging med smartkort		x
Delegert brukerstyring via webapplikasjon	x	x
Tilgangsstyring til (enkelt)tjenester		x
Katalog AD	x	x
Katalog andre	x	x
SSO	x	
Brukerinnstillinger		
Endre kontaktinformasjon	x	x
Endre passord	x	x
Endre språk		x
Legge til lokale (sykehus/avdelingsspesifikke) ekstravariabler		x
Samme bruker kan tilhøre flere sykehus/avdelinger	x	x
Lisenser og rettigheter		
Proprietært/kommersielt produkt		

Åpen kildekode	x	x
Kildekode tilgjeng for alle	x	x
Annen type lisens		

Som en kort oppsummering vil MRS være egnet det er behov for lokal eller sentral innregistrering, eller en kombinasjon av dette. OpenQReg vil kun være egnet for sentral innregistrering. MRS er klargjort for integrasjon mot fagsystemer og en eventuell pseudonymforvalter. OpenQReg har ikke denne funksjonaliteten. MRS er bygd på informasjonsteknologi fra Microsoft, mens OpenQReg i større grad tar i bruk informasjonsteknologi basert på åpen kildekode og fri programvare.

Tabellen gjelder for plattformene som register blir bygd på. Når spesifikke register implementeres kan det bety endringer i tabellen over, blant annet basert på faglige, tekniske og juridiske krav som gjelder for et gitt register. Punktet **Log, tilfredsstiller normen for informasjonssikkerhet** er ikke evaluert for noen av plattformene, men vil kunne være gjenstand for en gjennomgang i en seinere fase av dette prosjektet, men vil uansett være relevant i en risikovurdering for implementering av spesifikke register.

5 Anbefalinger og videre arbeid

Under arbeidet med prosjektet har det kommet opp en del nye ideer og problemstillinger som vi mener det bør kikkes nærmere på.

5.1 Definering av fellestjenester for kvalitetsregistre

Hensikten med et tjenestelag er å identifisere autonome tjenester som så kan gjenbrukes av flere aktører.

Vi kan tenke oss at hvis vi definerer tjenester spesifikt for kvalitetsregistre, så kan et eksisterende journalsystem utvides til å tilby registrering av data som så lagres og vedlikeholdes via disse tjenestene. Selve tjenesten kan være en fellestjeneste på helsenettet eller i foretaket.
.
Det bør derfor settes av midler for å kunne definere et slikt lag for kvalitetsregistre hvor relevante aktører inviteres til å bidra. En slik aktivitet bør ha en forankring inn mot *Nasjonal IKT*.

5.2 Føderert sikkerhet

Føderert sikkerhet er et alternativ når det gjelder å tilby sikre webtjenester i helse og sosialsektoren som beskrevet i *Referansearkitektur for web services sikkerhet i helse- og sosialsektoren*[12]. Den primære gevinsten ved føderering ligger i en løs kobling mellom autentisering og forretningslogikk. I dette prosjektet har vi basert oss på å implementere nødvendige tjenester selv (*Security Token Service*), men ofte vil det være mer hensiktsmessig med en sentral STS tjeneste innenfor foretakene etter hvert som flere og flere løsninger trenger en slik.

Hvis vi i en overgangsfase ønsker å etablere en egen STS slik som vi har gjort her, bør en sjekke ut mulige verktøy for å gjøre dette mest mulig hensiktsmessig som for eksempel:

- PingFederate® fra PingIdentity® (http://www.pingidentity.com/).
- Microsoft Code Name ”Geneva” (http://www.microsoft.com/forefront/geneva/en/us/).
- Shibboleth (http://shibboleth.internet2.edu/).

5.3 Identity and Access Management (IAM)

På sikt bør IAM(*Identity and Access Management*) løsninger rundt om i foretakene tilby *Secure Token Service*(STS) type funksjonalitet.

Det forhindrer ikke at vi kan starte med å implementere STS selv for så seinere ta i bruk sentraliserte tjenester. Et grunnleggende vilkår for det er selvfølgelig at en bestemmer seg for å bruke standardisert funksjonalitet ved utvikling av tjenestene som SAML 2.0/XACML og tydelig dokumentert hvilke claims(assertions) som kreves av token som leveres til tjenesten.

5.4 Videreføre samarbeid mellom regionene og Norsk helsenett

Det er viktig med en fortsatt koordinering når det gjelder felles tekniske løsninger for kvalitetsregistre. I dette prosjektet har vi opplevd en positiv effekt av at regionene jobber sammen om felles problemstillinger.

Det er viktig at *Norsk* Helsenett som binder oss sammen rent nettverksmessig også deltar aktivt når det gjelder definering og tilrettelegging for nasjonale tjenester for hele helse-Norge. For at løsningen her skal kunne fungere via helsenettet er det bl.a. essensielt at det finnes en enkel og entydig infrastruktur for PKI-sertifikater.

Det er også viktig å koble inn NIKT sitt fagforum for arkitektur slik at de til enhver tid kan verifisere og sikre at løsningene utvikles i tråd med krav til NIKT sin arkitektur.

Følgende framtidige tiltak kan derfor være relevant å vurdere:

1. Tverregionale prosjekter bør ha tilknyttet ressursperson i NHN
2. Det bør finnes føringer for interregional kommunikasjon over helsenettet som i større grad forplikter HF/RHF til mer enhetlig og lik struktur og regulering med hensyn til kommunikasjon mellom nasjonal teknisk infrastruktur, som for eksempel medisinske kvalitetsregistre.
3. NHN bør oppfordres til å utgi en mal som beskriver hvordan foretak skal koble seg til helsenettet for å oppnå interregional samhandling.
4. Stimulere til økt bruk av nasjonale fellestjenester, som for eksempel oppslag mot folkeregister-katalogen.

5.5 Norm for informasjonssikkerhet i helsesektoren

Dette prosjektet har tatt i bruk det som finnes av standarder for sikkerhet definert i *WCF*. Imidlertid er det ikke foretatt noen analyse av hvor sikker løsningen faktisk er.

Det bør derfor foretas en risikovurdering i forhold til *Norm for informasjonssikkerhet i helsesektoren*[13].

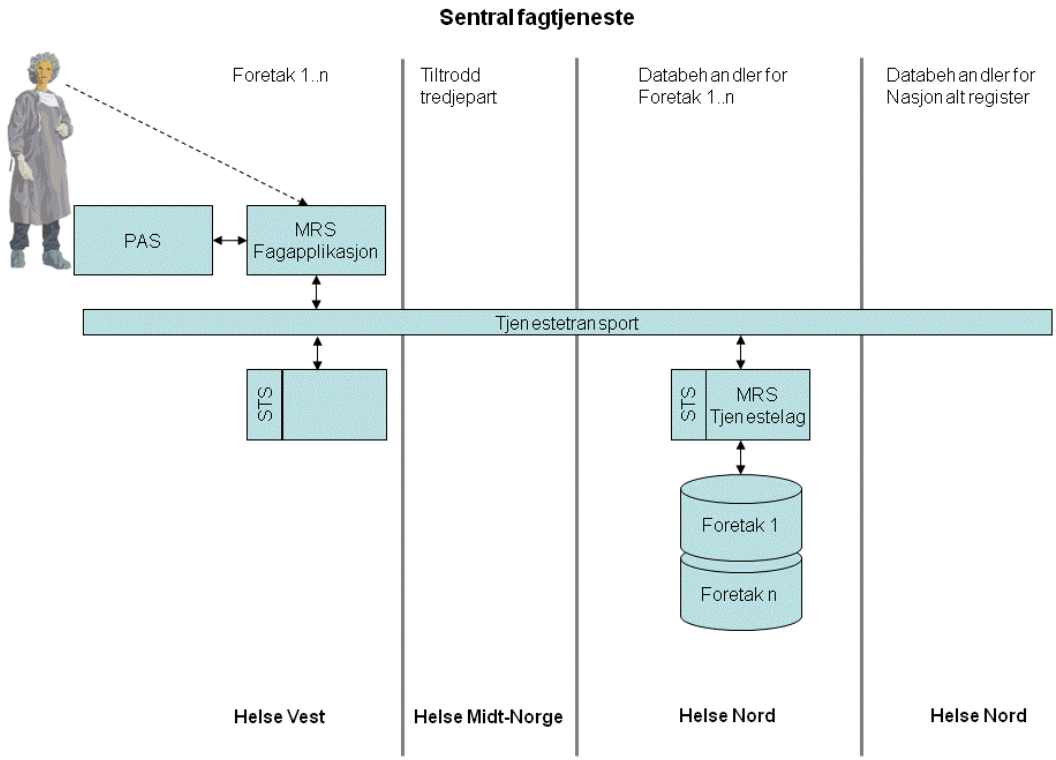
5.6 Fullføre test av *MRS Poc* i helsenettet

Opprinnelig var intensjonen i dette prosjektet å teste ut alle løsningskonseptene i helsenettet mellom Helse Nord, Helse Vest og Helse Midt-Norge. Kommunikasjon over helsenettet på tvers av regioner derimot, viste seg å være en utfordring for dette prosjektet. Tilsvarende erfaringer fra Nasjonalt Kvalitetsregister for Ryggkirurgi underbygger dette. Testing ble derfor foretatt internt i Helse Midt-Norge et simulert miljø for noen av løsningskonseptene. Det er imidlertid et ønske fra dette prosjektet å kunne gjennomføre en fullskala test i helsenettet når nødvendige ressurser i helseforetakene og helsenettet stilles til rådighet.

5.7 Sentral fagtjeneste

I forbindelse med arbeidet med dette prosjektet og en sterkere forståelse av betydningen av et vel definert tjenestelag kom det opp et nytt løsningskonsept som heller ikke er behandlet i *Nasjonalt helseregister prosjekt*[3] som vi har valgt å kalle *Sentral fagtjeneste*.

Denne løsningen representerer en krysning mellom løsningskonseptene *Lokal fagapplikasjon* og *Sentral fagapplikasjon*. Denne løsningen har både sentral lagring kombinert med kobling mot lokale fagsystemer.



Figur 5 Nytt løsningskonsept vi har kalt *Sentral fagtjeneste*

6 Konklusjon

Basert på erfaringer med utvikling av teknisk løsning for *Nasjonalt register for ryggkirurgi* (Helse Nord), *Nyfødtmedisinsk kvalitetsregister* (Rikshospitalet) og *MRS – Medisinsk Registreringssystem* (Helse Midt-Norge), ser vi at en felles teknisk løsning er mulig i svært mange tilfeller. Spesielt gjelder dette hvis systemet bygges opp modulært etter en tjenesteorientert modell. På den måten kan en ivareta både målet om integrering med EPJ på lang sikt og datainnsamling av strukturerte medisinske data på kort sikt. Etablering av et standardisert tjenestegrensesnitt for kvalitetsregistre som kan benyttes ved videreutvikling av dagens løsninger og gjenbrukes ved integrering mot EPJ er en betingelse for dette.

Siden etablering av tjenestebusser ikke er kommet veldig langt verken regionalt eller nasjonalt, må en videreutvikling av felles teknisk løsning for kvalitetsregistre skje koordinert med det arbeidet som pågår rundt arkitektur i regi av *Nasjonal IKT*. Arbeidet med prosjektet som her presenteres har imidlertid vist at det er mulig å realisere en tjenesteorientert løsning

på tross av at tjenestebuss ikke er endelig implementert. Det skjer på den måten at tjenester som forventes å finnes i en endelig tjenestebuss leveres som en del av systemet.

En forutsetning for dette er at det er mulig å etablere det vi har kalt for *Tjenestetransport* via helsenettet samtidig som det finnes en velfungerende infrastruktur for håndtering av PKI sertifikater. Dette er de samme krav som stilles med dagens meldingsorienterte løsninger.

Med utgangspunkt i prosjektets resultatmål kan vi trekke noen videre konklusjoner.

6.1 MRS installert på helseregister.no som *Sentral fagapplikasjon*.

MRS PoC ble installert på helseregister.no som en *Sentral* fagapplikasjon og kan kjøres via helsenettet på https://helseregister.no/intensivregister/.

Installasjonen er en standard MRS installasjon med XML-skjema for *Intensivregisteret* installert. Det har egen pasient- og brukerdatabase. Applikasjonen kjører via en sikker forbindelse (SSL).

Installasjonen fungerer som forventet og for kvalitetsregistre som har definerte sine parametre og har en fastlagt skjemalayout og som ikke krever kobling mot lokal PAS eller folkeregister kan løsning leveres så raskt som skjema kan defineres.

6.2 MRS installert i Helse Vest som *Lokal fagapplikasjon*.

MRS PoC ble installert i Helse Vest som en *Lokal fagapplikasjon* og kan kjøres internt i foretaket på http://bgo-app98.ihelse.net/Intensivregister/.

Installasjonen er en standard MRS installasjon med XML-skjema for Intensivregistreret installert. Det har egen pasient- og brukerdatabase. Applikasjonen kjører via en sikker forbindelse (SSL).

Installasjonen fungerer som forventet og for kvalitetsregistre som har definerte sine parametre og har en fastlagt skjemalayout og som ikke krever kobling mot lokal PAS eller folkeregister kan løsning leveres så raskt som skjema kan defineres.

6.3 Løsning med tiltrodd pseudonym forvalter testet ut.

Her har vi slått sammen to resultatmål:

1. Løsning med tiltrodd pseudonym forvalter testet ut.
2. Kommunikasjon og meldingsutveksling satt opp mellom *Lokal fagapplikasjon* og *Nasjonalt helseregister.* Heri inngår også uttesting av en installasjon i Helse Midt-Norge.

På grunn av problemer med å få satt opp testservere innenfor regionene og kommunikasjon mellom disse via helsenettet er denne testen så langt kun utført innenfor Helse Midt-Norge sitt nettverk. Selve testen er beskrevet i eget kapittel og det ble ikke avdekt strukturelle problemer med selve løsningen.

Løsningen kan uttestes på samme måte i helsenettet, men hvis den skal sette i drift i helsenettet så er det viktig å ha en skikkelig infrastruktur for bruk av PKI-sertifikater på plass. Utover det stilles det ikke andre krav enn pålitelighet og kapasitet samt tilgang til nødvendige ressurser i foretakene og hos NHN. Sikkerhet er her tenkt innebygget i selve applikasjonen siden det ikke finnes standardiserte fellestjenester for dette i dag.

For å kunne levere en produksjonsklar versjon basert på *MRS PoC* så må det påregnes ytterligere analyse, videreutvikling, uttesting og stabilisering av løsningen. Det gjelder ikke minst vurdering av sikkerhet basert på *Norm for informasjonssikkerhet i helsesektoren*[13].

6.4 Oppslag mot *IR-RESH*

Dette resultatmålet ble ikke utført som en del av dette prosjektet, men her finnes det erfaringer fra før i Helse Nord for portalen helseregister.no. *IR-RESH* (*InterRegionalt Register for Enheter i SpesialistHelsetjenesten*) er der brukt som del av brukeradministrasjonen.

I MRS sin organisasjonstruktur registreres det *IR-RESH* koder allerede i dag, men automatisk oppslag er ikke på plass. Det er planlagt en slik kobling, men når den er ferdig for utgivelse er ikke fastlagt. Man forventer ikke større problemer med å få til dette.

6.5 Integrasjon med fagsystem i Helse Vest fra *Lokal fagapplikasjon*.

Dette resultatmålet ble ikke utført som opprinnelig forutsatt i dette prosjektet.

Det ble imidlertid behov for en integrasjon mellom *MRS PoC* og *Nasjonalt helseregister* og derfor ble den utviklet i stedet. Det ble gjort for å kunne verifisere gjennom brukergrensesnittet i *MRS PoC* at data faktisk blir overført pseudonymisert til *Nasjonalt helseregister* fra *Lokal fagapplikasjon*.

Det er uansett planlagt en kobling mellom webtjeneste for folkeregisteret i Helse Vest og MRS som skal utgis seinest ved utgangen av 2009 (det bør her også vurderes om funksjonaliteten skal utnytte sentral tjeneste i helsenettet i stedet for lokal tjeneste i Helse Vest).

6.6 En dokumentert sammenligning av MRS og OpenQReg

Det ble utført en sammenligning av MRS og OpenQReg for utvalgte egenskaper for disse to registerplattformene. Bakgrunnen for denne sammenligningen er antagelsen av at ulike registre vil ha ulike behov med hensyn til tekniske løsninger, og at det dermed bør kunne tilbys et utvalg løsninger som sammen kan dekke dette behovet.

I denne sammenstillingen vil MRS være egnet det er behov for lokal eller sentral innregistrering, eller en kombinasjon av dette. OpenQReg vil kun være egnet for sentral innregistrering. MRS er klargjort for integrasjon mot fagsystemer og en eventuell pseudonymforvalter. OpenQReg har ikke denne funksjonaliteten. MRS er bygd på informasjonsteknologi fra Microsoft, mens OpenQReg i større grad tar i bruk informasjonsteknologi basert på åpen kildekode og fri programvare.

7 Ordliste

Parameter	Variabler for strukturert lagring av kliniske data for en pasient.	
TTP	Tiltrodd TredjePart.	
TPF	Tiltrodd PseudonymForvalter.	
POC	Proof-of-Concept. Sansynliggjøre brukbarheten av et løsningskonsept basert på praktisk uttesting av utvalgte problemstillinger.	
NIKT	Nasjonal IKT.	
IR-RESH	InterRegionalt Register For Enheter i SpesialistHelsetjenesten.	
HEMIT	Helse Midt-Norge IT.	
UCR	Uppsala Clinical Research Center.	
OpenQReg	Open source system for strukturert registrering av medisinske parametre utviklet ved UCR.	
MRS	Medisinsk RegistreringsSystem - strukturert registrering av medisinske parametre utviklet ved HEMIT.	
IPLOS	Individbasert PLeie- og OmorgsStatistikk.	
PAS	PasientAdministrativt System.	
AD	Active Directory.	
.NET	Microsoft utviklingsplattform.	
KITH	Kompetansesenter for IkT i Helse- og sosialsektoren.	
SKDE	Senter for Klinisk Dokumentasjon og Evaluering.	
MQR	Medical Qualty Registery.	
NHN	Norsk HelseNett.	
STS	Security Token Service.	
IAM	Identity and Access Management.	
PKI	Public Key Infrastructure.	

8 Referanser

1. Felles teknisk løsning for nasjonale kvalitetsregistre - Prosjekteringsdokument for gjennomføring av POC - NIKT Tiltak 28.1 (januar 2009)
2. Prosjektoppdrag/-plan Nasjonalt samarbeid Proof of concept - felles teknisk løsning (september 2008)
3. Nasjonalt helseregister prosjekt – Teknisk gruppe – Hoveddokument Løsningskonsepter (april 2009)
4. Felles teknisk løsning for regionalt eide nasjonale kvalitetsregistre (mai 2008) Prosjektrapport
   Funksjonell og teknisk modell
5. Håndbok for medisinske kvalitetsregistre – SKDE 2008 (september 2008)
6. Koordinerte løsninger for kvalitetsregistre - KITH-rapport 38/03 (februar 2004)
7. Pseudonyme Helseregistre – Rundskriv I-8/2005 – Det kongelige helse- og omsorgsdepartement (juni 2005)
8. Systemdokumentasjon MRS 2.0
9. Drifts- og installasjonsveiledning MRS 2.0
10. Tjenesteorientert arkitektur i spesialisthelsetjenesten – Styringsdokument fra Nasjonal IKT (oktober 2008)
11. Forprosjekt kvalitetsregister – Sluttrapport for Helse Sør-Øst RHF (mars 2009).
12. Referansearkitektur for web services sikkerhet i helse- og sosialsektoren - KITH rapport nr. 07/09 (Status: Til kommentering april 2009)
13. Norm for informasjonssikkerhet i helsesektoren (2006)