

Veiledning for innføring av ebXML og PKI i helseforetak

Versjon 1.1

Dato: 9.06.2010

KITH Rapport 12/05

ISBN 82-7846-256-9

KITH-rapport				
TITTEL				
Veiledning for innføring av ebXML og PKI i helseforetak				
Forfatter(e): Arnstein Vestad				
Oppdragsgiver(e):				Postadresse Sukkerhuset N-7489 Trondheim
Standardiserings- og samordningsprogrammet				Besøksadresse Sverresgt 15 Telefon +47 - 73 59 86 00 Telefaks +47 - 73 59 86 11 e-post firmapost@kith.no Foretaksnummer 959 925 496
ISBN:	Dato:	Antall sider:	Kvalitetssikret av:	Gradering:
82-7846-256-9	9.6.2010	23	Bjarte Aksnes	Åpen
Godkjent av:				
Jacob Hygen				
Rapportnr: KITH R 12/05				
Sammendrag:				
<p>Rapporten gir veiledning om hvordan helseforetakene skal gå til verks for å innføre PKI-løsninger og ebXML rammeverk for utveksling av meldinger. Det anbefales bl.a. å gå i gang med å flytte eksisterende kommunikasjon over fra X.400 til ebXML-rammeverket, samt å implementere PKI-løsninger basert på virksomhets sertifikater.</p> <p>Rapporten beskriver hvordan ebXML-rammeverket for meldingsutveksling kan tas i bruk av helseforetakene, og konkretiserer hvilke aktiviteter som må gjennomføres for å gå over til denne løsningen.</p>				

Innhold

Innhold	3
1. Bakgrunn	4
1.1. Start med virksomhets sertifikat for meldingsutveksling	4
1.2. Anvendelse av ebXML og PKI på virksomhetsnivå	5
1.3. Anvendelse av ebXML og PKI med personlig signatur	7
1.4. Hovedgevinster ved ebXML og PKI	9
2. Aktuelle parter og ansvar.....	12
2.1. Virksomheten som innfører rammeverket.....	12
2.2. Leverandør av kommunikasjonsmodul.....	13
2.3. Leverandør av journalsystem/fagsystem.....	13
2.4. PKI-leverandør	13
2.5. Norsk Helsenett.....	14
3. Endringer hos foretakene.....	15
3.1. Endringer i kommunikasjonsløsningen.....	16
3.2. Anskaffelse av PKI	17
4. Teknologisk bakgrunn	19
Kort om ebXML-rammeverket	19
4.1. Kort om PKI-løsningen	21
4.1.1. Sertifikat-typer.....	21
5. Referanseliste	23

1. Bakgrunn

Innføringen av ebXML rammeverk og PKI kommer som et resultat av en rekke faktorer, både endringer i rammebetingelser og nye tekniske løsninger. Bl.a. er Norsk helsenett etablert som felles kommunikasjonsnett for sektoren, og trygd/helse-postkassen, som har fungert som infrastruktur for meldingsutveksling i en årrekke, fases ut. Nasjonal IKT (styringsgruppe for de regionale helseforetakenes IKT-strategisamarbeid) har anbefalt at de regionale helseforetakene følger opp med en tempoplan for raskest mulig overgang for HF-ene fra trygd/helse-postkassen til bruk av SMTP-postkasse i Norsk Helsenett.

ebXML er en internasjonal standard for å håndtere utveksling av informasjon mellom virksomheter, og beskriver bl.a. mekanismer for sikkerhet og trygg og pålitelig meldingsutveksling. PKI er teknologi for å beskytte informasjon mot endringer og innsyn vha. kryptering og digitale signaturer.

Dette dokumentet er ment som en veiledning for foretakene som skal ta i bruk ebXML og PKI-løsningen, enten for å flytte eksisterende meldingskommunikasjon over på den nye plattformen, eller for å implementere nye meldinger som forutsetter denne plattformen. Målgruppen for veiledningen er prosjektansvarlige i foretakene og teknisk personell der samt andre interesserte. Veiledningen skal gi råd om hvordan man går fram for å implementere den nye plattformen. Den tekniske implementeringen er beskrevet i andre rapporter, særlig KITH-rapporten R-25/02 - "Rammeverk for meldingsutveksling". Informasjon om PKI-løsningen finnes også i rapport fra arbeidsgruppe for strategi for PKI-utrulling i helseforetak, oktober 2004 (se referanser).

1.1. Start med virksomhetssertifikat for meldingsutveksling

I forbindelse med innføringen av elektronisk sykmelding til Rikstrygdeverket, har RTV inngått rammeavtale om PKI-løsninger for helsesektoren. Rammeavtalen omfatter tjenester knyttet til virksomhetssertifikater og personlige sertifikater. I forslag til utrullingsplan for PKI i helseforetakene presentert for Nasjonal IKT anbefales det å fokusere det på *innføring av virksomhetssertifikater i*

helseforetakene i samband med innføringen av rammeverket for ebXML. Innføring av denne grunnleggende infrastrukturen reduserer behovet for endringer i interne fagsystemer og behovet for å rulle ut personlig signatur-løsninger til et stort antall ansatte, samtidig som de grunnleggende sikkerhetsbehovene dekkes for en lang rekke løsninger.

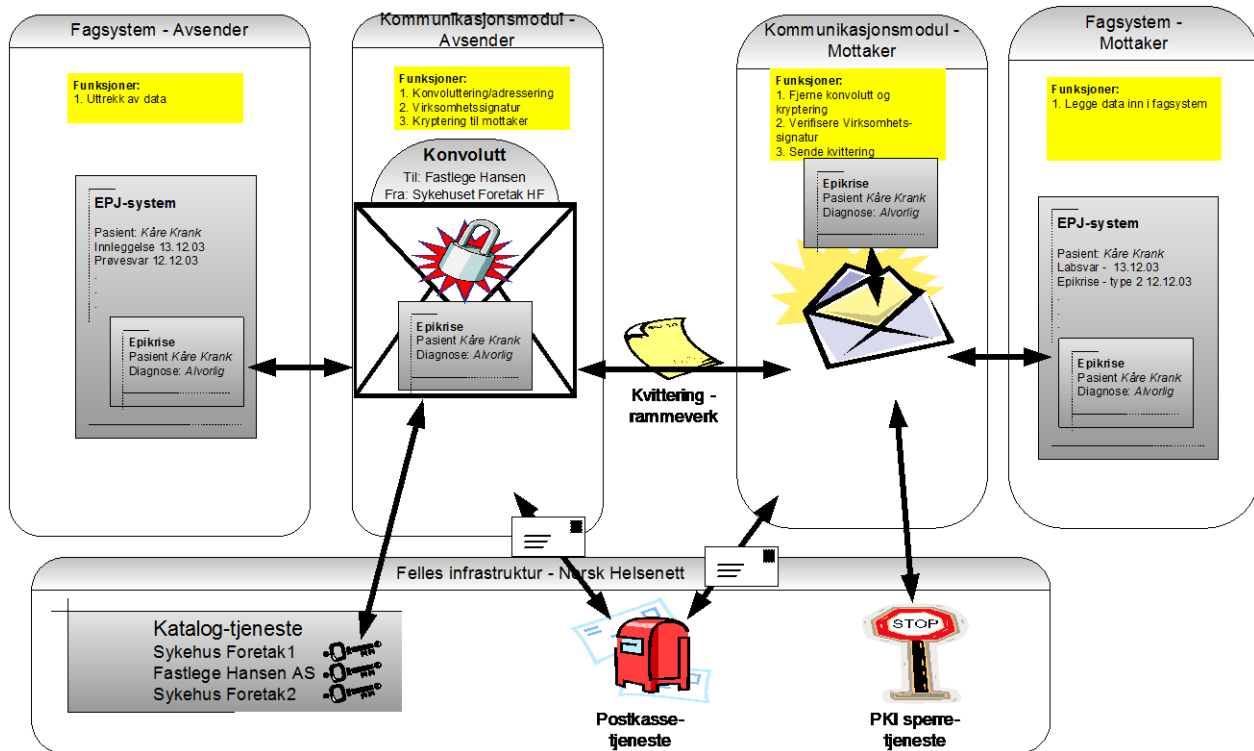
For det meste av meldingsutvekslingen mellom aktører i helsevesenet, som f.eks. henvisning og epikrise, rekvisisjoner og svar, vil bruk av virksomhetssertifikat for signering av en melding (på konvoluttnivå) gi tilstrekkelig og ønsket sikring av meldingen i forbindelse med kommunikasjon. Dokumentasjonskravet forutsettes ivaretatt i EPJ, og det skal fremgå av meldingen hvem som har signert. For sykmelding og legeoppgjør stilles det krav om signering med personlig sertifikat, og tilsvarende krav vil bli aktuelt for e-resept.

Dette innebærer at foretakene i første omgang bør fokusere på å *innføre virksomhetssertifikater for å sikre kommunikasjon mellom de kommunikasjonspartene man kommuniserer med*, som primærleger, laboratorier og andre foretak. Det er ikke nødvendig å rulle ut personlige sertifikater til alle ansatte for å dra nytte av sikkerhetsgevinsten og forenklet administrasjon knyttet til PKI for meldingsutveksling.

1.2. Anvendelse av ebXML og PKI på virksomhetsnivå

Bruken av ebXML kan illustreres med et eksempel. I dette tilfellet ser vi på meldingsflyten knyttet til en epikrise som sendes fra et helseforetak til en fastlege. Denne meldingen benytter kun signatur og kryptering på virksomhetsnivå, samt ebXML-rammeverket for overføring.

1. Data til epikrisen trekkes ut av lokalt fagsystem, i eksemplet EPJ
2. Informasjonen overføres til lokal kommunikasjonsmodul
3. Lokal kommunikasjonsmodul finner adresseinformasjon for meldingen og legger meldingen i konvolutt-melding.
4. Lokal kommunikasjonsmodul signerer konvolutt på virksomhetsnivå.
5. Lokal kommunikasjonsmodul henter offentlig nøkkel til mottaker fra katalogtjeneste i Norsk Helsenett – og krypterer vedleggene til mottaker
6. Lokal kommunikasjonsmodul overfører meldingen til SMTP/POP – postkasse, for eksempel i Norsk Helsenett



Figur 1 - Meldingsflyt ved anvendelse av ebXML og PKI på virksomhetsnivå

7. Mottakers kommunikasjonsmodul henter konvolutt-melding i postkasse i Norsk Helsenett
8. Mottakers kommunikasjonsmodul dekrypterer konvolutt-meldingen .
9. Mottakers kommunikasjonsmodul verifiserer virksomhetssignatur på konvolutten ved å kontrollere mot PKI-tjenestens sperretjeneste.
10. Mottakers kommunikasjonsmodul sender rammeverks-kvittering for å bekrefte at meldingen er mottatt av kommunikasjonsmodulen.
11. Lokal kommunikasjonsmodul mottar kvittering på at meldingen er mottatt av mottakers kommunikasjonsmodul. Hvis kvittering ikke er mottatt innen gitte tidsrammer, sendes meldingen på nytt.
12. Mottakers kommunikasjonsmodul overfører den utpakkede epikrisen til fastlegens journalsystem

Prosessene beskrevet ovenfor innebærer at avsendersystemet (hos det enkelte helseforetak) må tilpasses. Ved innføring av ebXML og virksomhetssertifikat gjelder dette først og fremst tilpasning i kommunikasjonssystem/meldingssystem. Nødvendige endringer er beskrevet i kapittel 3.

Steg 1 – uttrekk av data medfører at lokalt system må tilpasses for å trekke ut nødvendig informasjon som skal inngå i meldingen. Dersom nødvendig uttrekk av meldingen allerede er implementert i journalssystem/fagsystem (f.eks. tidligere Edifact-melding) vil dette kunne redusere behovet for tilpasninger i fagsystem.

Steg 3 og 4 – nødvendig tilpassing av kommunikasjonsmodul, er beskrevet i kapittel 3.1. Steg 5 og 6 - nødvendig PKI-funksjonalitet, er beskrevet i kapittel 3.2.

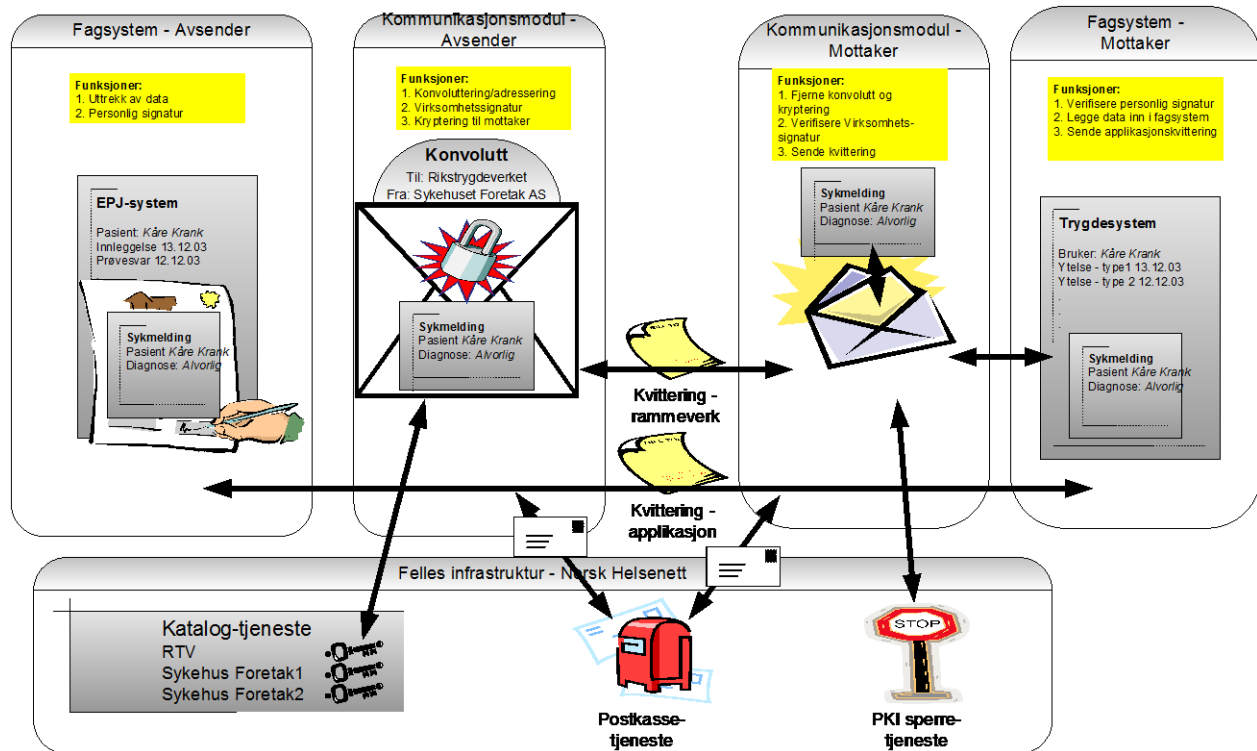
Meldingskommunikasjonen kan også innbefatte bruk av applikasjonskvittering.

Applikasjonskvitteringen er en kvittering som går fra applikasjon til applikasjon, og som kan gi noe mer detaljert informasjon om behandlingen av meldingen etter at den er ankommet mottakers fagsystem. Bruk av denne illustreres i det neste eksemplet sammen med personlig signatur, men avhenger ikke av dette.

1.3. Anvendelse av ebXML og PKI med personlig signatur

ebXML-rammeverket og PKI vil også benyttes i sammenheng med personlige signaturer (hvor helsepersonellet er utstyrt med smartkort eller andre former for personlig PKI-løsning). Per i dag er det bare for sykmelding og elektronisk legeoppgjør med RTV hvor det kreves slik personlig signatur. Innføring av elektronisk sykmelding er et eksempel på en melding som benytter seg av flere viktige komponenter og funksjoner i rammeverket, bla. kryptering og signering, både personlig og på virksomhetsnivå, kvitteringsmeldinger på transportnivå samt applikasjonskvittering.

1. Data trekkes ut av lokalt fagsystem, EPJ
2. Sykmelding signeres med personlig signatur (Generelt kan melding signeres med personlig sertifikat eller virksomhetssertifikat. Dette steget er ikke nødvendig for journalmeldinger som epikrise, henvisning, rekvisisjoner og svar hvis meldingsmeldingen sikres med ebXML-rammeverk som omtalt under pkt. 4-7, med mindre det er stilt særskilte krav til slik signatur.)
3. Melding overføres til lokal kommunikasjonsmodul



Figur 2 - Informasjonsflyt ved bruk av ebXML og PKI med personlig signatur

4. Lokal kommunikasjonsmodul finner adresseinformasjon for meldingen og legger meldingen i konvolutt-melding.
5. Lokal kommunikasjonsmodul signerer konvolutt på virksomhetsnivå.
6. Lokal kommunikasjonsmodul henter offentlig nøkkel til mottaker fra katalogtjeneste i Norsk Helsenett – og krypterer konvolutten til mottaker
7. Lokal kommunikasjonsmodul overfører meldingen til SMTP/POP – postkasse for eksempel i Norsk Helsenett
8. Mottakers kommunikasjonsmodul henter konvolutt-melding i postkasse i Norsk Helsenett
9. Mottakers kommunikasjonsmodul dekrypterer konvolutt-meldingen .
10. Mottakers kommunikasjonsmodul verifiserer virksomhetssignatur på konvolutten ved å kontrollere mot PKI-tjenestens sperre-tjeneste.
11. Mottakers kommunikasjonsmodul sender rammeverks-kvittering for å bekrefte at meldingen er mottatt av kommunikasjonsmodulen.

12. Lokal kommunikasjonsmodul mottar kvittering på at meldingen er mottatt av mottakers kommunikasjonsmodul. Hvis kvittering ikke er mottatt innen gitte tidsrammer, sendes meldingen på nytt.
13. Mottakers kommunikasjonsmodul overfører den utpakkede sykmeldingen til RTV's fagsystem
14. Mottakers (RTV's) fagsystem verifiserer den personlige signaturen på sykmeldingen. Ut fra dette er det mulig å fastslå korrekt identitet for å kontrollere at sykmeldingen er sendt av en autorisert lege, bl.a. ved å slå opp sertifikateters fødselsnummer.
15. Mottakers fagsystem sender applikasjonskvittering for å bekrefte at meldingen er mottatt av fagsystemet (sendes også som melding over ebXML-rammeverket). Applikasjonskvittering er ikke del av ebXML-rammeverket, men implementeres for meldinger der det er ønskelig med kvittering som kommer helt inn i fagsystemet.
16. Lokalt fagsystem (EPJ) mottar applikasjonskvittering på at meldingen er mottatt av mottakers fagsystem, retter eventuelle feil som kvitteringen beskriver og sender eventuelt på nytt.

1.4.Hovedgevinster ved ebXML og PKI

EbXML-rammeverket og PKI-løsningen er valgt som helsevesenets standard og som plattform for fremtidige løsninger for elektronisk meldingsutveksling. ebXML-rammeverket benytter seg av en åpen standard for meldingsutveksling, ” ebXML Messaging Service specification (ebMS)”, som igjen er en utvidelse av den ledende standarden for Web-services, SOAP. ebXML utvider SOAP-standardens med tjenester for sikkerhet og pålitelighet som er nødvendige for å utveksle meldinger på en trygg måte. ebXML er også ISO-standard, ISO 15000.

ebXML er et omfattende rammeverk, og så langt er det kun deler av standarden som innføres. Det er derfor kun delene som omfatter meldingsutveksling (konvolutten) som skal benyttes når ulike virksomheter, det være seg foretak eller etater, skal utveksle standardiserte meldinger.

I tillegg til bruk av ebXML-rammeverk benyttes PKI, evt, kun med virksomhetssertifikat, som sikkerhetsmekanisme for å beskytte meldingene som sendes over helsenettet. Dette innebærer at alle virksomheter som skal utveksle informasjon må anskaffe et virksomhetssertifikat for å identifisere seg selv, og som benyttes for å kryptere og signere meldingene som utveksles.

I dag er flere ulike metoder for meldingsutveksling i bruk, over SMTP e-post, over X.400 postkasse osv. Bruk av ebXML og PKI vil sammen gi en mer effektiv meldingsutveksling ved å gi:

- **Standardisert plattform for meldingsutveksling:** Ved å standardisere på ebXML som rammeverk vil helsesektoren ha en enhetlig omforent måte å utveksle meldinger på, og en plattform som støtter de krav til sikkerhet og pålitelighet som sektoren stiller. Samme løsning kan benyttes for å håndtere alle typer meldinger og vedleggsformater på en ensartet måte.
- **Forenkling:** Rammeverket forenkler sending av ulike typer vedlegg. Rammeverket vil bidra til god og effektiv utnyttelse av katalogtjenester, og forenkler mange-til-mange kommunikasjon ved at f.eks. informasjon om sertifikater, rekvirenter og meldingskommunikasjon kan hentes fra katalogene i stedet for å settes opp lokalt hos hver enkelt aktør.

Når løsning for rammeverket og PKI er innført, vil dette kunne gjenbrukes på nye framtidige meldinger. Rammeverket og PKI-løsningen vil da ligge som en sikker basis infrastruktur for meldingsutveksling og nye meldinger kan innføres på toppen av infrastrukturen med minimale modifikasjoner.

- **Bedre sikkerhet og tillit:** Bruk av PKI vil generelt gi bedret informasjonssikkerhet ved utveksling av elektroniske meldinger. Bruk av PKI vil også føre til mindre muligheter for svindel eller misbruk fordi de elektroniske meldingene må signeres med et elektronisk sertifikat tilhørende enten helsepersonell eller en helseinstitusjon.
- **Integritet:** Rammeverket og PKI fører til at meldingen kommer frem til mottakeren i samme form som den sendes. Det er imidlertid opp til fagsystemet som tar i mot meldingen, hvordan den vises forbrukeren.
- **Beskyttelse mot innsyn:** Ved bruk av PKI (gjelder både virksomhets sertifikat og personlig sertifikat) vil man kunne overføre meldinger kryptert uten på forhånd å avtale hvilke nøkler man skal bruke. Krypteringsnøklerne vil være tilgjengelig i en åpen katalog.
- **Trygghet for at meldingen kommer frem til mottaker:** ebXML-rammeverket støtter funksjoner for å automatisk sende meldinger på nytt med mindre man ha fått kvittering for at meldingen er mottat, evt. varsle dersom meldingen ikke kommer frem til mottaker.

I en overgangsfase kan det være ønskelig å overføre EDIFACT-meldinger over rammeverket som erstatning for kommunikasjon over x.400 og Trygd-Helsepostkassen som fases ut. Det vil si at meldingen kan beholdes som før, men pakkes inn i en annen konvolutt (ebXML) enn i X.400.

Rammeverket kan også utnyttes i forbindelse med statistikk for meldingsutveksling, ved at konvolutten inneholder informasjon om type melding, som kan telles uten at meldingsinnhold gjøres kjent.

ELIN-prosjektet har stilt krav om bruk av ebXML-rammeverk for leverandører som deltar i prosjektet.

Helsedepartementet har med hjemmel i forskrift stilt krav om at fødselsmelding til Medisinsk fødselsregister skal benytte ebXML-rammeverk. Løsningen vil også bli benyttet for fødselsmelding til Skattedirektoratet. Implementering i fødsesystemer og kommunikasjonsprogramvare er i gang hos leverandørene.

Rikstrygdeverket har stilt krav om ny POLK-melding basert på ebXML-rammeverk i løpet av 2005.

2. Aktuelle parter og ansvar

Flere aktører vil være involvert i ulik grad ved innføring av ebXML-rammeverket og PKI-løsningen. Hovedansvaret vil ligge hos virksomheten som innfører løsningen, og denne må fungere som bestiller ift. leverandører og ift. nødvendige endringer i egne systemer.

2.1. Virksomheten som innfører rammeverket

Virksomheten som innfører rammeverket vil ha hovedansvar for innføringsprosessen, og må bestille de nødvendige endringer og produkter fra sine leverandører. Innføring av rammeverket vil typisk skje i forbindelse med innføring av en ny elektronisk melding som krever rammeverket, for eksempel elektronisk sykemelding eller fødselsmelding. Nødvendige steg vil bl.a. være:

1. **Valg av melding(er) som skal implementeres over rammeverket:** De fleste foretak vil allerede ha rutiner eller prosesser de gjennomfører når nye elektroniske meldinger skal innføres. Dette kan være mer generelle rutiner rundt konfigurasjonkontroll, risikovurdering osv., men også mer konkrete vurderinger rundt de aktuelle fagsystemer som berøres, kommunikasjonsmoduler som må tilpasses osv. Valg av melding kan også komme som eksternt krav, f.eks. krav om elektronisk overføring av fødselsmelding.
2. **Tilpassing av avgiver-system:** Systemet som skal avgi data som inngår i meldingen må tilpasses, evt. må det utvikles/tilpasses løsninger for å hente ut nødvendig data fra systemet. Hvis meldingen er implementert i avgiver-systemet tidligere, for eksempel i form av EDIFACT-melding over X.400 vil dette kunne redusere behovet for endringer.
3. **Anskaffelse av PKI-løsning:** Hvis virksomheten ikke allerede besitter nødvendig virksomhetssertifikat må dette anskaffes.
4. **Modifisering av kommunikasjonsløsning:** Nødvendige endringer i kommunikasjonsløsning for å støtte ebXML-rammeverket og PKI-funksjonaliteten må bestilles fra leverandør (evt. egenutvikles), jf. pkt. 2.2 nedenfor.

5. **Konfigurering, test og drift:** Når de nødvendige komponenter er anskaffet eller tilpasset, må løsningen konfigureres, bl.a. settes opp mot nødvendige kommunikasjonsparter og testmeldinger utveksles før løsningen settes i drift.

2.2. Leverandør av kommunikasjonsmodul

Hvis det benyttes en ekstern leverandør av kommunikasjonsmodul må denne implementere støtte for ebXML-funksjonaliteten i sitt system. ebXML-standarden slik den benyttes i helsesektoren beskrives nærmere i KITH-rapporten R-25/02 - ”Rammeverk for meldingsutveksling”.

Leverandøren må også implementere nødvendig funksjonalitet for å håndtere signatur/verifikasjon og kryptering/dekryptering av innholdet i konvolutten. Dette vil også innebære oppslag mot nødvendige sperretjenester for å validere sertifikatene som er benyttet, dvs. kontrollere at disse ikke er sperret eller svartelistet.

2.3. Leverandør av journalsystem/fagsystem

Leverandør av journalsystem/fagsystem vil i liten grad påvirkes av innføring av ebXML-rammeverk (med mindre leverandøren også er ansvarlig for kommunikasjonsmodulen). Som for andre meldinger vil fagsystemet være ansvarlig for å generere meldingen som skal overføres, evt. påføre en personlig signatur hvis meldingen krever dette (f.eks. sykmelding). Det kan være behov for tilpasning av mappingtabeller som følge av overgang til bruk av ebXML, men annet meldingsinnhold vil normalt være uendret.

Grensesnitt mellom applikasjon og kommunikasjonsmodul vil avhenge av valgt løsning hos det enkelte foretak.

2.4. PKI-leverandør

PKI-leverandøren, per april 2005 Ergo Ephorma, har inngått en rammeavtale med Rikstrygdeverket om å levere sertifikater, programvare og konsulent tjenester. Priser og betingelser for PKI-tjenesten er tilgjengelig fra deres web-sider – <http://pki.ergo.no/>

2.5. Norsk Helsenett

Norsk Helsenett leverer grunnleggende infrastruktur for sikker kommunikasjon i helsesektoren. Når meldinger skal kommuniseres basert på ebXML-rammeverk og PKI-løsning er dette særlig tilgang til PKI-leverandørens katalogtjeneste og sperretjeneste, samt å tilby en SMTP/POP-basert postkassetjeneste for overføring av meldingene.

3. Endringer hos foretakene

En innføring av rammeverk for ebXML og PKI vil innebære behov for tilpasninger og endringer, særlig i den enkelte virksomhets meldingshåndteringssystem. Hvis man bare tar i bruk virksomhetssertifikat for meldingsutvekslingen i første omgang, vil omleggingen være begrenset i forhold til eksisterende meldinger.

En innføring av denne løsningen vil særlig innebære:

- Forberedelser og tilpasning til konkrete anvendelser
 - PKI-løsningen må tas i bruk på konkrete meldinger, enten nye eller eksisterende. Både avsender og mottaker da må tilpasse sine systemer for anvendelsen. Siden X.400-løsningene (trygd-helsepostkasse) er under utfasing, vil det være hensiktsmessig å se overgang til ny kommunikasjonsløsning i Norsk helsenet i sammenheng med dette.
- Innføring av ebXML-rammeverket
 - Helseforetakene må etablere ebXML-rammeverket i egne meldingssystemer, inkl. kvitteringsmekanismer, funksjoner for pålitelig overføring osv. Dette vil typisk gjøres av leverandør av kommunikasjonsprogramvare.
- Etablering av mottaksløsninger for innkomne meldinger:
 - Innføring av løsninger for å verifisere signaturer på mottatte meldinger, kryptering og dekryptering. Dette håndteres typisk av funksjonene i ebXML-rammeverket i meldingssystemet. For hver part må det sannsynligvis legges inn sertifikat (fortrinnsvis fra katalogtjeneste)
 - Etablering av nødvendige mekanismer ift. oppslag i nødvendige katalogtjenester (sertifikatkatalog, HER-katalog) og kontroll av sertifikater mot sperretjenester.

I forbindelse med innføring av ebXML rammeverk og PKI vil det kunne være fornuftig å gjøre strategiske vurderinger rundt organisering av meldingsflyt og håndtering internt i foretaket. Dette kan innebære å vurdere:

- Hvorvidt det bør implementeres et sentralt meldingsmottak/meldingssystem for helseforetaket, evt. hos en felles regional databehandler/IT-driftsenhet.
- Hvorvidt man ønsker å ha ett eller flere virksomhetssertifikater pr. helseforetak. (flere sertifikater kan øke sporbarhet ift. bruken av sertifikatene internt i foretaket, særlig ift. sikkerhetsbrudd).

ebXML-rammeverket støtter bruk av samhandlingsavtaler (CPA) mellom kommunikasjonspartene (samhandlingsavtalene inneholder omforente parametere for kommunikasjonen, som f.eks. krav til hvor mange ganger meldingen skal re-sendes ved feil, hvorvidt det skal gis kvitteringer osv.).

Samhandlingsavtalene er tenkt å kunne genereres ut fra den enkelte parts samhandlingsprofil (CPP) – en profil som beskriver de tekniske egenskapene og ønskene til parten knyttet til kommunikasjonen. Samhandlingsavtaler er ikke nødvendig for å kommunisere vha. ebXML konvolutten (MS), men kan være en fordel ift. å konfigurere meldingssystemet på enklest mulig måte.

KITH-rapport R-25/02 - ”Rammeverk for meldingsutveksling” beskriver og standardiserer enkelte parametere som kan inngå i en samhandlingsavtale, evt. benyttes direkte ved konfigurasjon av kommunikasjonsmodulen. Noen parametre vil være felles for de fleste praktiske formål, men andre er forskjellige fra hver gang (adresser etc.).

3.1. Endringer i kommunikasjonsløsningen

Innføring av ebXML-rammeverk og PKI-løsningen vil innebære tilpasninger av helseforetakenes systemer for meldingsutveksling. Tilpasningene vil innebære å legge inn støtte for de deler av ebXML som benyttes i norsk helsesektor, som dokumentert i KITH-rapporten R-25/02 - ”Rammeverk for meldingsutveksling”. Dette omfatter bla. inn- og utpakking i konvolutten, overføring av meldingen over valgt kommunikasjonsprotokoll, feilhåndtering og håndtering av kvitteringer.

Systemet for meldingsutveksling må i tillegg ha funksjoner for kryptering og signering basert på virksomhetssertifikater. Rapporten over beskriver også hvordan dette implementeres. Når kommunikasjonsmodulen er tilpasset og installert hos foretaket, må denne kunne nå nødvendige infrastruktur-tjenester i Norsk Helsenett. Kommunikasjonsmodulen må kunne sende og hente meldinger i SMTP/POP-postkasse i Norsk Helsenett. Kommunikasjonsmodulen må kunne slå opp i PKI-leverandørens sertifikat-kataloger og sperretjeneste, og etter hvert også felles katalogtjenester som etableres i Norsk Helsenett, som HER-katalogen (Helsetjenestens Enhetsregister) for

adresseinformasjon. Bruk av HER i sammenheng med rammeverket vil kunne lette administrasjonen av kommunikasjonsparter, fremhenting av adresseinformasjon og PKI-informasjon betraktelig. HER er ikke en forutsetning for å gå over til ebXML-rammeverket, denne informasjonen kan også håndteres på tradisjonelt vis, med bl.a. lokale rekvisitregister, interne kataloger o.l.

Grensesnittet mellom avsendende og mottakende applikasjon og de respektive kommunikasjonsmoduler vil avhenge av flere faktorer, bl.a. valgte leverandører og løsninger og intern IT-arkitektur.

3.2. Anskaffelse av PKI

PKI-løsningen skal sikre at meldinger overføres på en sikker måte, dvs. at meldingene krypteres og signeres slik at uvedkommende ikke kan endre eller lese innholdet i meldingen. Å ta i bruk PKI på virksomhetsnivå innebærer to hovedtrinn:

- Helseforetaket må anskaffe seg et virksomhetssertifikat. Sertifikatene leveres per april 2005 av Ergo Ephorma, og kan bestilles fra web-siden <http://pki.ergo.no/>
- Helseforetaker må anskaffe/installere programvare for PKI-funksjonaliteten, dvs. signering, kryptering, verifikasjon av signatur osv. Dette kan være gjennom programpakker levert av PKI-leverandøren, gjennom funksjonalitet innebygd i valgt ebXML-programvare eller annen tilgjengelig programpakker for eksempel fra andre PKI-leverandører.

Det siste punktet må ses i sammenheng med de nødvendige endringer som må gjennomføres i kommunikasjonsmodulen for å implementere ebXML-rammeverket. I mange tilfeller vil eventuell software for å håndtere rammeverket også inneholde nødvendig PKI-funksjonalitet, hvis ikke må dette anskaffes separat.

ErgoEphorma tilbyr produktet enablePKI som er et PKI-toolkit utviklet i Java. Produktet gir i følge leverandøren tilgang til:

- Digital signering
- Kryptering/dekryptering
- Integritet

- Autentisering
- Generering av XML-meldinger basert på ebXML / XML-DSIG
- Bruk av smartkort og HSM for oppbevaring av private nøkler. Smartkort kan brukes i kombinasjon med softsertifikater.
- Fullstendig validering av sertifikater og gyldighet på signaturer
- Oppslag mot ulike katalog- og register- tjenester³ (LDAP, CRL, fødselsnummer, HelseEnhets-Register (HER), helsepersonell-nummer).

Funksjonaliteten for XML-meldinger og oppslag er opsjoner.

Tjenestene som tilbys under rammeavtalen for PKI er basert på åpne standarder, og funksjonalitet for å nå disse er i hovedsak tilgjengelig fra en rekke leverandører av programvarekomponenter. Bruk av enablePKI kan likevel lette integrasjonsarbeidet, siden produktet er spesialtilpasset PKI-leveransen fra leverandøren. Dette gjelder særlig funksjonalitet for oppslag mot katalogtjenester, og evt. funksjonalitet for å motta fødselsnummer knyttet til personlige sertifikater.

4. Teknologisk bakgrunn

Kort om ebXML-rammeverket

ebXML-rammeverket benytter seg av en åpen standard for meldingsutveksling, ” ebXML Messaging Service specification (ebMS)”, som igjen er en utvidelse av den ledende standarden for Web-services, SOAP. ebXML utvider SOAP-standarden med tjenester for sikkerhet og pålitelighet som er nødvendige for å utveksle meldinger på en trygg måte.

Rammeverket definerer både et meldingsformat (en konvolutt for andre meldinger), og tekniske prosesser for programvare som utveksler ebXML-meldinger (som funksjonalitet for å sende meldinger på nytt). Den delen som er tatt i bruk i helsevesenet er det laveste funksjonalitetsnivået, ebXML Messaging Service (meldingshåndtering).

Rammeverket omfatter en elektronisk konvolutt (transportkonvolutt) som signeres med virksomhetssertifikat, slik at avsenderorganisasjon identifiseres. Rammeverket m/virksomhetssertifikat sikrer i tillegg:

- entydig identifikasjon av kommunikasjonspartene (avsender og mottaker)
- overføring av kvitteringer på mottak av meldinger
- at meldingen faktisk kommer frem til rett mottaker (fortsetter å sende til meldingen kommer igjennom og kvittering mottatt)
- kryptering for å sikre integritet og konfidensialitet

Rammeverket forenkler sending av ulike typer vedlegg. Rammeverket vil bidra til god og effektiv utnyttelse av katalogtjenester, og forenkler mange-til-mange kommunikasjon ved at f.eks. informasjon om sertifikater, rekvirenter og meldingskommunikasjon kan hentes fra katalogene i stedet for å settes opp lokalt hos hver enkelt aktør.

Noen funksjoner/egenskaper som rammeverket støtter er bl.a:

- En konvolutt kan inneholde en eller flere meldinger (for eksempel flere laboratoriesvar) fra en og samme avsender til en mottaker. Et labsvar er i utgangspunktet én melding som inneholder

flere labsvar, men man kan sende flere meldinger av samme type (i prinsippet også forskjellige typer, men dette kan være mindre hensiktsmessig). For eksempel kan man sende 100 labsvar fordelt på 10 meldinger med 10 labsvar i hver, i én konvolutt.

- En konvolutt kan inneholde en melding med relaterte vedlegg (f.eks. en patologirekvisisjon og et relatert bilde). Det anbefales da at hvis man sender med tilknyttede vedlegg i tillegg til ”hovedmeldingen”, skal man kun sende én melding (+ tillegg) per konvolutt. Hvis man ønsker å kunne sende flere meldinger med tilhørende vedlegg i samme konvolutt må det finnes funksjonalitet i den enkelte meldingen som identifiserer korrekt relatert vedlegg.
- Avsender og mottakerinformasjon ligger i konvolutten (muliggjør statistikk, uten å åpne innhold). Man kan legge inn én eller flere ID’er per avsender/mottaker, f.eks. epostadresse og HER-ID.
- Konvolutten kan utveksles via flere ulike nettverksprotokoller. Konvolutten er en såkalt ”SOAP-message with attachments”, en XML/MIME-melding som i prinsippet kan overføres på alle tenkelige måter. I første omgang anvendes SMTP (mail-protokollen), men overgang/parallellkjøring med HTTPS kan være ønskelig, bl.a. for å slippe å kryptere de enkelte meldingene/vedleggene i en sending og i stedet bruke transportsikring over SSL/TLS.
- Meldinger som inneholder dokumenter skal ha global unik identifikator
- Når konvolutten brukes som en kvittering eller feilrapport må den inneholde identifikasjon av meldingsutvekslingen som den er et svar på. Denne funksjonen må ikke forveksles med applikasjonskvitteringen (AppRec).
- Konvolutten inneholder informasjon om når den er generert
- EDIFACT –meldinger kan overføres på samme måte som en XML-melding, eller hvilken som helst annen fil.
- Funksjon for kryptering m/virksomhets sertifikat. Ved SMTP og andre asynkrone overføringer (FTP, diskett...) skal man kryptere det enkelte vedlegg som skal legges inn i konvolutten (i praksis kryptering, så base64-koding, og så lagt inn som MIME-attachement). Ved bruk av HTTPS trenger man ikke dette, da man oppretter en kryptert tunnel mellom avsender og mottaker ved hjelp av virksomhets sertifikatene.

4.1. Kort om PKI-løsningen

PKI står for Public Key Infrastructure og omfatter infrastruktur og tjenester for sikring av informasjonsutveksling og tilgang til systemer:

- elektronisk signering av dokumenter
- autentisering (sikker identifisering) av kommunikasjonsparter eller brukere av systemer
- sikring av integritet og konfidensialitet ved overføring/utveksling av informasjon (kryptering)
- Ikke-benekting (innholdet knyttes bindende til avsender, som regel i forbindelse med personlig elektronisk signatur)

Rikstrygdeverket inngikk i januar 2003 en rammeavtale med Ergo Ephorma AS om PKI-tjenester for bruk i helsevesenet. Rammeavtalene tar utgangspunkt både i Rikstrygdeverkets behov for sikring av elektronisk sykmelding til trygdeetaten, og andre behov for sikker meldingsutveksling mellom ulike aktører i helsevesenet omtalt i en forprosjektrapport fra januar 2002 . Dette er anvendelsesområder hvor det er stort behov for koordinering av PKI-løsninger i helsevesenet. Den inngåtte rammeavtalen gir en standardisert løsning med et sikkerhetsnivå som gjør det mulig å benytte samme PKI for mange ulike formål på tvers av regioner.

For nærmere informasjon om bruk av PKI i helsesektoren, se rapport fra arbeidsgruppe for strategi for PKI-utrulling i helseforetak, oktober 2004, samt KITH-rapport R13/04 - ”Anbefalinger og standarder for PKI i helsesektoren”.

4.1.1. Sertifikat-typer

Rammeavtalen for PKI i helsevesenet omfatter to typer sertifikater, personsertifikater og virksomhetssertifikater.

Virksomhetssertifikater er sertifikater som skal sikre kommunikasjonen til og fra virksomheter og virksomhetsenheter. Disse sertifikatene inneholder derfor ikke personinformasjon, men identifiserer virksomheter og virksomhetsenheter. Hensikten med virksomhetssertifikater er å få en entydig og sikker kopling mellom en virksomhet og dennes offentlige nøkkel. Virksomhetssertifikater bør inneholde informasjon om virksomhetens navn og organisasjonsnummer hentet fra Enhetsregisteret.

I en del tilfeller er det behov for å knytte signaturer og informasjon til et konkret individ, noe som forutsetter personsertifikater. Et personsertifikat identifiserer en enkeltperson, normalt vha. en unik ID som personnummer eller annet løpenummer. Personsertifikatet forutsetter at det kun er denne personen som har tilgang til den private nøkkelen og kan benytte denne til å signere eller dekryptere informasjon.

På de fleste områdene for standard meldingsutveksling mellom virksomheter i helsevesenet, som f.eks. henvisning og epikrise, rekvisisjoner og svar, kan bruk av virksomhetssertifikater gi tilstrekkelig sikring. Bruk av virksomhetssertifikat kan håndteres på ”konvolutt-nivå”, forutsatt at brukersystemene har nødvendige rutiner for å rute meldingene til riktig bruker innenfor virksomheten.

Bruk av virksomhetssertifikater vil bidra til at kommunikasjonspartene ikke trenger å utveksle krypteringsnøkler på forhånd og at sikkerheten rundt nøkkelhåndtering bedres betraktelig i forhold til dagens rutiner.

Muligheten for å påføre enkeltmeldinger personlig signatur åpner muligheten for elektronisk sending av meldinger og e-post med høye krav til sikkerhet. F.eks. gjelder det på områder der det er viktig med sikker identifisering av en individuell avsender av informasjon, og der avsenderen står personlig ansvarlig.

5. Referanseliste

Helsesektorens PKI-løsning:

Websidene til leverandøren gir mulighet til å bestille sertifikater, samt lese kravspesifikasjon for løsningen og avtaler: <https://pki.ergo.no/>

Rammeverk for meldingsutveksling i helsesektoren:

Beskrivelse av rammeverket er tilgjengelig fra KITH's hjemmesider: KITH-rapport R-25/02 "Rammeverk for meldingsutveksling".

<http://www.kith.no/>

ebXML-standard

Dokumentene som beskriver selve ebXML-standard er tilgjengelig fra OASIS på siden:

<http://www.ebxml.org/>

Implementering av PKI i norsk helsevesen - Forslag til utrullingsplan for helseforetakene

Tilgjengelig fra Sosial- og Helsedirektoratets hjemmesider: <http://www.shdir.no/index.db2?id=14468>

PKI-anbefalinger:

Rapporten "Anbefalinger og standarder for PKI i helsesektoren" (KITH-rapport R13/04) er tilgjengelig fra KITH's hjemmesider: <http://www.kith.no/>