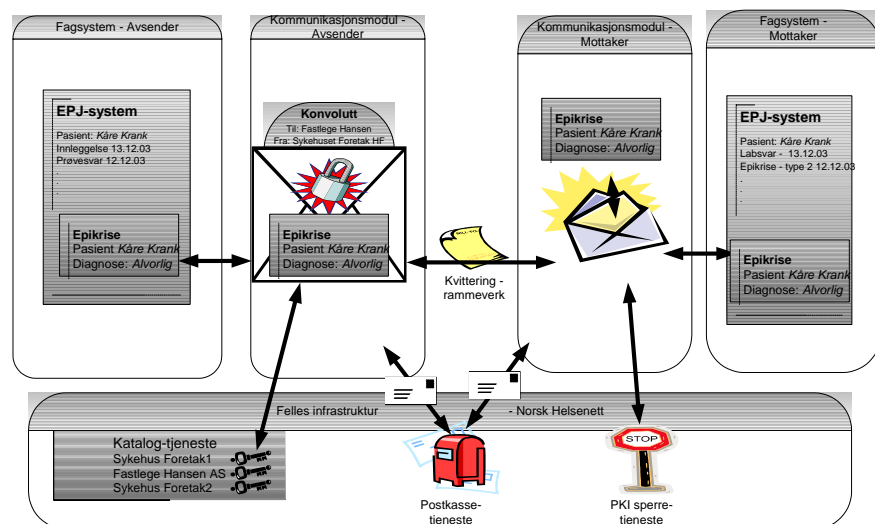


Sikker og standardisert elektronisk kommunikasjon i helse- og sosialsektoren

Bruk av ebXML og PKI for informasjonsutveksling

Helsesektoren har standardisert på ebXML som rammeverk for utveksling av elektroniske meldinger. Dette innebærer at visse deler av standarden ebXML (konvolutt) skal benyttes når ulike virksomheter, det være seg foretak eller etater, skal utveksle standardiserte meldinger. ebXML-rammeverket omfatter kort fortalt en felles konvolutt for innpakning av elektroniske meldinger samt prosesser for kvittering, pålitelighet i meldingsoverføringen og sikkerhet.

I tillegg til bruk av ebXML-rammeverk benyttes PKI 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.



Hvorfor ebXML og PKI

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, rekvisiter 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. Krypteringsnøkklene 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 mottatt, 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.

Start med virksomhets sertifikater

For det meste av meldingsutvekslingen mellom aktører i helsevesenet, som f.eks. henvisning og epikrise, rekvisisjoner og svar, vil bruk av virksomhets sertifikat 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 virksomhets sertifikater 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.

Kort om ebXML rammeverket og PKI

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).

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-benektning (innholdet knyttes bindende til avsender, som regel i forbindelse med personlig elektronisk signatur)

Rikstrykdeverket inngikk i januar 2003 en rammeavtale med Ergo Ephorma AS om PKI-tjenester for bruk i helsevesenet. Rammeavtalene tar utgangspunkt både i Rikstrykdeverkets behov for sikring av elektronisk sykmelding til trykdeetaten, 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.

Hva innebærer dette

Overgangen til ebXML-rammeverk og PKI 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 helsenett 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.

Mer informasjon

Ytterligere informasjon om innføring av ebXML rammeverk og PKI kan finnes i KITH-rapport R 12/05, "Veiledning for innføring av ebXML og PKI i helseforetak".

"Implementering av PKI i norsk helsevesen - Forslag til utrullingsplan for helseforetakene" er tilgjengelig fra Sosial- og Helsedirektoratets hjemmesider: <http://www.shdir.no/samspill>