

 Norm for informasjonssikkerhet www.normen.no	Utgitt med støtte av:  HelseDirektoratet
<h1>Sikkerhets- og samhandlingsarkitektur</h1>	Støttedokument Faktaark nr 20 Versjon: 2.1 Dato: 15.12.2010

Målgruppe Dette faktaarket er spesielt relevant for:	<input checked="" type="checkbox"/> Leverandør <input checked="" type="checkbox"/> IKT-ansvarlig <input type="checkbox"/> Forsker <input type="checkbox"/> Prosjektleder	<input checked="" type="checkbox"/> Sikkerhetsleder/ sikkerhetskoordinator <input type="checkbox"/> Virksomhetens leder/ledelse <input type="checkbox"/> Forskningsansvarlig	<input type="checkbox"/> Medarbeider/ansatt <input type="checkbox"/> Databehandler <input type="checkbox"/> Personvernombud
Ansvar	IKT-ansvarlig er ansvarlig for å etablere en tilfredsstillende sikkerhets- og samhandlingsarkitektur		
Gjennomføring	Benyttes ved innføring av nye IKT-systemer eller endringer i eksisterende systemer		
Formål	<ul style="list-style-type: none"> • Standardisere virksomhetens sikkerhetsfunksjoner • Etablere tilfredsstillende sikkerhet ved elektronisk samhandling med andre aktører i helse- og sosialsektoren 		
Omfang	Alle tekniske løsninger som benyttes til behandling av helse- og personopplysninger. For mindre virksomheter bør leverandørene og Norsk Helsenett sørge for en tilfredsstillende sikkerhetsarkitektur.		
Hjemmel	Personopplysningsforskriften § 2-7		
Referanser	<ul style="list-style-type: none"> • Veiledning for innføring av ebXML og PKI i helseforetak (www.kith.no) • Veileder for fjernaksess for vedlikehold og oppdateringer mellom leverandør og helsevirksomhet • Veileder i informasjonssikkerhet ved tilknytning mellom kommuner, fylkeskommuner og helsenettet 		

Faktaarket har to hoveddeler:

1. Sikkerhetsarkitektur for en tjeneste
2. Meldingsflyt ved anvendelse av ebXML og PKI på virksomhetsnivå

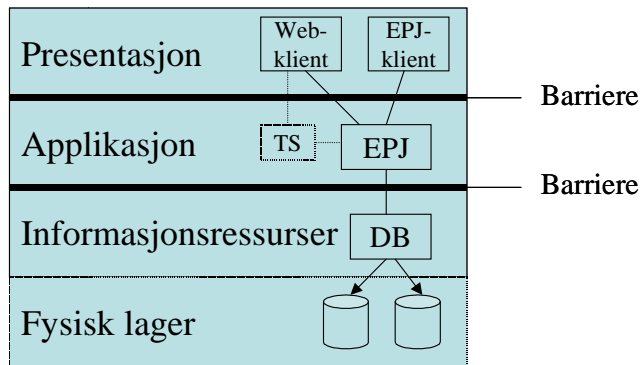
1. Sikkerhetsarkitektur for en tjeneste

Tabellen under illustrerer hvordan sikkerhetsarkitekturen kan beskrives i en lagdelt modell for hver enkelt tjeneste. Denne bør benyttes for å illustrere hvordan ulike tjenester og applikasjoner er bygd opp med tilhørende sikkerhetsmekanismer. Tabellen kan benyttes på tjenester innen egen virksomhet og for tjenester over Norsk Helsenett.

Lag	Eksempler på sikkerhetsmekanismer
Presentasjon (klient/arbeidsstasjon)	<ul style="list-style-type: none"> – Nettverksautentisering – Kryptering – Nettverkskontroll – Klientautentisering – Terminalløsninger
Applikasjon/ forretningslogikk	<ul style="list-style-type: none"> – Hendelsesregistrering i applikasjonen – Applikasjonsautentisering (for eksempel EPJ) og tilgangsstyring – Validering av felt og data
Informasjonsressurser (database)	<ul style="list-style-type: none"> – Transaksjonslogg og systemlogg – Låsemekanismer (read-only) – Tilgangsstyring til databasen – Integritetskontroll
Fysiske komponenter	<ul style="list-style-type: none"> – Redundans i teknologi – Fysisk sikring

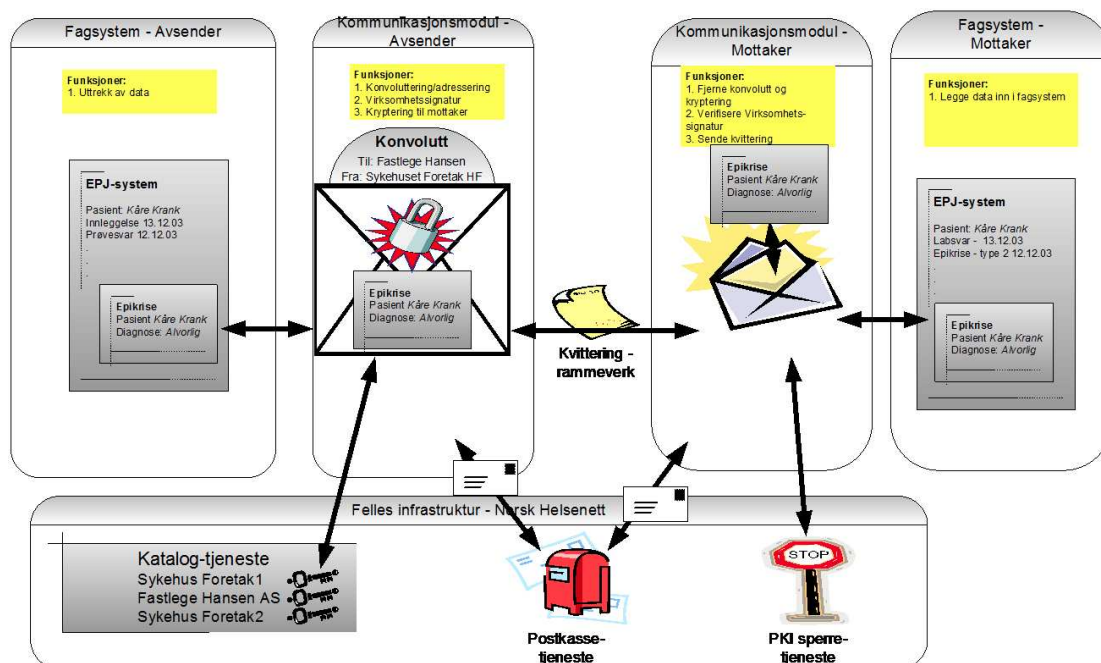
Eksempel:

Figuren under illustrerer sikkerhetsarkitekturen for en EPJ-løsning. Presentasjonslaget viser frem den aktuelle informasjonen ved hjelp av en webklient (nettleser) eller en egen EPJ-klient. Klienten kommuniserer med en applikasjon (EPJ). Det er også mulig å benytte en terminalserverløsning (TS), som i realiteten betyr at all databehandling skjer i applikasjonslaget. Kommunikasjonen mellom presentasjon og applikasjon kan om nødvendig krypteres. I datanettverket kan det være sikkerhetsbarrierer. Selve applikasjonen (EPJ) kommuniserer med databasen (DB) som holder kontroll på alle dataelementene som er lagret i et fysisk lager. Det fysiske lageret kan være fordelt på ulike lagringssystemer eller servere.



2. Meldingsflyt ved anvendelse av ebXML og PKI på virksomhetsnivå

Bruken av ebXML illustreres nedenfor. I eksemplet vises meldingsflyten av 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 konvoluttmelding.

4. Lokal kommunikasjonsmodul signerer konvolutt på virksomhetsnivå.
5. Lokal kommunikasjonsmodul henter offentlig nøkkel til mottaker fra katalogtjeneste i Norsk Helsenett – og krypterer konvolutt til mottaker
6. Lokal kommunikasjonsmodul overfører meldingen til SMTP/POP-postkasse, for eksempel i Norsk Helsenett
7. Mottakers kommunikasjonsmodul henter konvoluttmelding i postkasse i Norsk Helsenett
8. Mottakers kommunikasjonsmodul dekrypterer konvoluttmeldingen
9. Mottakers kommunikasjonsmodul verifiserer virksomhetssignatur på konvolutt ved å kontrollere mot PKI-tjenestens sperretjeneste
10. Mottakers kommunikasjonsmodul sender rammeverkskvittering 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, sende meldingen på nytt
12. Mottakers kommunikasjonsmodul overfører den utpakkede epikrisen til fastlegens journalsystem