



## PROSJEKTRAPPORT

# Sikkerhetsmodul i IKT-baserte pasientjenester

Nasjonalt senter for Telemedisin, Tromsø 15.02.01

[anders.lovold@telemet.no](mailto:anders.lovold@telemet.no)

### Forord

Denne rapporten er en del av NST's system for interndokumentasjon av prosjekter, og supplerer samtidig regnskaps- og sluttrapport til NIN (Nasjonalt Informasjonsnettverk).

Målgruppen forutsettes å ha noe kjennskap til sikkerhetsutfordringer i helsevesenet. Selv om en del spesiell terminologi knyttet til PKI (Public Key Infrastructure) er forklart underveis, egner ikke rapporten seg som en introduksjon til emnet.

### Sammendrag

Et av satsningsområdene ved [Nasjonalt senter for telemedisin](#), "Den nye pasientrollen", har fokusert mye på muligheter som ligger i nettbaserte tjenester for og med pasienter. Mange av disse tjenestene innebærer elektronisk kommunikasjon mellom såkalt "sikker sone" i helsevesenet, og pasienter på deres hjemmedatamaskiner. Erfaringene fra flere piloter, prosjekt og søknader tilsier imidlertid at slike opplegg krever datasikkerhet på et helt annet nivå enn hva helsevesenet hittil har tilgang til.

Dette prosjektet har derfor hatt som målsetning å utrede og utvikle en generell teknisk og organisatorisk løsning som sikrer dataintegritet og konfidensialitet for helsefremmende publikums- og pasienttjenester på Internett. Det var videre definerte mål at løsningen skulle basere seg på PKI-standarder (Public Key Infrastructure), samvirke med helsevesenets øvrige sikkerhetsløsninger, og kunne få godkjenning av Datatilsynet.

Resultatelementene er hentet fra flere prosesser som er koordinert opp mot målsetningene. De fleste er knyttet til pasienters behov og forutsetninger for datasikkerhet, og rapporten drøfter hvordan ulike typer tjenester fordrer PKI i ulik grad. Videre gir resultatet grunnlag for drøfting av hvordan pasienter skal få nødvendig tilgang til og kunnskap om PKI-løsninger mot helsetjenester. Et eget nettsted knyttet til datasikkerhet er opprettet under [www.telemet.no](http://www.telemet.no)

Hovedtyngden av den teknologiske utredningen er gjennomført i samarbeid med [Nordnorsk HelseNett](#) (NH). Denne utredningen har fokusert på ulike valgalternativ og utfordringer som er knyttet til implementering av PKI, og konkluderer hvorfor en åpen, hierarkisk tillitsstruktur med felles standarder vil være det mest naturlige valget.

Avslutningsvis kommenteres også arbeidet med nasjonal standardisering og innføring av PKI i det offentlige generelt. Her påpekes det at framdrift arbeidet med å tilgjengeliggjøre offentlige tjenester elektronisk krever at noen har en helhetlig oversikt over PKI, samt ansvar og kapasitet til aktiv formidling.

## Innholdsfortegnelse

<b>1</b>	<b>INNLEDNING .....</b>	<b>1</b>
1.1	BAKGRUNN .....	1
1.2	UTFORDRING OG HOVEDMÅL .....	1
1.3	ORGANISERING OG RAMMER .....	1
<b>2</b>	<b>BESKRIVELSE AV RELEVANT PKI-TEKNOLOGI.....</b>	<b>2</b>
2.1	DIGITALT SERTIFIKAT OG SERTIFISERINGSAUTORITET (CA) .....	2
2.2	TILLITSSTRUKTUR.....	2
2.3	SERTIFIKATTYPER .....	3
2.4	SERTIFIKATPROFILER .....	3
<b>3</b>	<b>PASIENTERS BEHOV OG FORUTSETNINGER.....</b>	<b>4</b>
3.1	GENERELL INFORMASJON FRA HELSEVESENET TIL HELSESØKENDE.....	4
3.2	FRA PASIENTER TIL HELSEVESENET.....	5
3.3	FRA HELSEVESENET TIL IDENTIFISERTE PASIENTER.....	5
3.4	MELLOM PASIENTER OG HELSEVESEN - BEHANDLING.....	5
3.5	MELLOM ALLE AKTØRENE .....	6
3.6	PKI FOR PASIENTER ELLER FOR HELSEVESENET .....	6
<b>4</b>	<b>GJENNOMFØRING OG RESULTAT .....</b>	<b>7</b>
4.1	STANDARDISERING/KOORDINERING I NORGE.....	7
4.2	IMPLEMENTERING AV PKI: VIKTIGE VALG .....	7
4.2.1	<i>Vurdering av tillitsstruktur .....</i>	<i>7</i>
4.2.2	<i>Vurdering av sertifikattype og profiler .....</i>	<i>8</i>
4.3	ERFARING FRA PRODUKTER .....	9
4.4	RISIKOANALYSE AV NH.....	10
4.5	ETABLERING AV KATALOGTJENESTER.....	10
4.6	PILOT MED SIKKER KOMMUNIKASJON INNENFOR HELSEVESENET.....	11
4.7	PILOT MED SIKKER KOMMUNIKASJON MELLOM PASIENT OG HELSEVESEN.....	11
4.7.1	<i>Eksem-prosjektet.....</i>	<i>11</i>
4.8	INFORMASJON TIL PASIENTER OG HELSESØKENDE.....	12
<b>5</b>	<b>KONKLUSJON OG AVSLUTTENDE KOMMENTARER.....</b>	<b>13</b>
5.1	IMPLEMENTERING AV PKI I NH.....	13
5.2	PKI FOR PASIENTER .....	14
5.3	PKI I DET OFFENTLIGE .....	15



## 1 Innledning

### 1.1 Bakgrunn

Utgangspunktet for prosjektet var det fokus Nasjonalt senter for telemedisin (NST) hadde på psykoedukative tjenester over nett. Målet var å tilby pasienter med psykiatriske diagnoser nettbasert oppfølging gjennom kunnskapsformidling, veiledning og selvhjelpsgrupper. Dette innebar i praksis elektronisk kommunikasjon mellom såkalt "sikker sone" i helsevesenet, og pasienter på deres hjemmedatamaskiner. Erfaringene fra flere piloter, prosjekt og søknader tilsa imidlertid at slike opplegg ville kreve datasikkerhet på et helt annet nivå enn hva helsevesenet har tilgang til.

Våren 2000 omdefinerte derfor NST en større søknad til NIN ([Norsk Informasjonsnettverk](#)) til kun å omfatte en generell sikkerhetsmodul for pasientrettede tjenester, basert på PKI, (Public Key Infrastructure). Dette prosjektet knyttet seg tett til NH's ([Nordnorsk HelseNett](#)) planlagte implementering av PKI, som i utgangspunktet var avgrenset til kun å inkludere helseinstitusjoner tilknyttet deres nett.

### 1.2 Utfordring og hovedmål

Prosjektets hovedmål var å utrede og utvikle en generell teknisk og organisatorisk løsning som sikrer dataintegritet og konfidensialitet for helsefremmende publikums- og pasient-tjenester på Internett.

Det var videre klart et definert mål at løsningen skulle basere seg på definerte PKI-standarder, samvirke med helsevesenet øvrige sikkerhetsløsninger, og kunne få godkjenning av datatilsynet. Under forutsetning av en slik godkjenning var det også åpnet for et pilotforsøk med pasientrettede tjenester.

### 1.3 Organisering og rammer

Formell prosjektoppstart var 20. juli 2000, mens alle kostnadsgenererende aktiviteter ble avsluttet 22. desember 2000. Forskningsrådet gjennom programmet NIN har med sitt bidrag på 580 000,- dekket nesten halvparten av kostnadene.

Prosjektet er organisert under satsningsområdet "Den nye pasientrollen" ved NST. Dette områdets målsetning er å bidra til at myndigheter, helsevesen, pasientorganisasjoner og kommersielle aktører har beslutningsrelevant kunnskap for utvikling av helsefremmende IKT-baserte pasient- og publikumstjenester. Mer utfyllende informasjon om NST finnes på: <http://www.telemet.no>

Flere andre prosjekt og aktiviteter ved NST er også koordinert opp mot dette sikkerhetsprosjektet. En referansegruppe bestående av sikkerhetsansvarlige fra NST, NH og Regionssykehuset i Tromsø (RiTø) har fulgt prosjektet siden oppstart, og vil fortsette sin virksomhet som felles sikkerhetsgruppe også ut over prosjektperioden.

## 2 Beskrivelse av relevant PKI-teknologi

PKI kan forklares fra en rekke ulike perspektiv, og gode definisjoner finnes hos [Globalsign](#) og [RSA](#). Vi vil i denne rapporten bruke betegnelsen på en struktur av digitale signaturer med offentlige og private nøkkelsystem. Nøklene er elektroniske, og de opptrer i par, hvorav den ene er offentlig kjent, mens den andre er privat og hemmelig. Strukturens hensikt er å håndtere nøkler og sertifikater slik at elektroniske transaksjoner kan utføres med tillit mellom aktørene.

Gjennom PKI-teknologi kan en rekke utfordringer med elektronisk kommunikasjon i og til helsevesenet tilnærmes. Funksjoner som signering, autentisering og kryptering kan garantere meldingens innhold, avsender og mottager, samt sikre at kun autoriserte får tilgang til ulike informasjonstjenester i nettet.

Kjernen i PKI kan sies å være det digitale sertifikatet og sertifiseringsautoriteten, men innhold og strukturer rundt disse kan variere betydelig, og innebærer mange valg under implementeringen. Kapittel 2 beskriver og belyser noen av de sentrale valgalternativene.

### 2.1 Digitalt sertifikat og sertifiseringsautoritet (CA)

Et digitalt sertifikat er en datastruktur som inneholder en representasjon av en identitet og tilhørende offentlige nøkkel. Sertifikater kan lagres som filer på harddisk eller diskett, eller legges på fysiske lagringsenheter (for eksempel smartkort).

En person kan ha flere sertifikater, hvor hvert sertifikat kan ha forskjellig bruksområde. Det vanlige er at alle sertifikat låses ned i én fil eller på en lagringsenhet (smartkort). Tilgangen til sertifikatet reguleres av et passord, og som regel åpnes alle nøkler med samme passord. Eventuelt kan passordet erstattes med tilgangssystemer basert på biometri, feks. fingeravtrykk.

Sertifiseringsautoritet (eng. akronym: CA) er den som utsteder et sertifikat ved å knytte nøkler til en person/identitet og bekrefter at innholdet i sertifikatet er riktig. Dette gjøres ved at CA signerer sertifikat med sin private nøkkel, og dermed binder et nøkkelpar til en gitt identitet.

### 2.2 Tillitsstruktur

En type eksempel på tillitstruktur er om en bedrifts egen CA er ansvarlig for å utstede sertifikater til alle ansatte. Gjennom tillit til én enhet, bedriftens CA, har dermed de ansatte også implisitt tillit til hverandres sertifikater.

Motsatt av at alle har tillit til en enhet, er at ingen gitt enhet har tillit. Det mest kjente eksemplet er PGP. Her tas avgjørelsen om tillit hos brukeren istedenfor hos CA. Adams/Lloyd [i s. 88] viser til noen elementære tillitsmodeller:

#### HIERARKI

Øverst i et hierarki er en rot-CA som alle stoler på. Under denne finnes eventuelt et eller flere lag av underliggende CAer med sine brukere nederst. Rot-CA er alles start eller slutt punkt for sertifikat verifisering, og hver enhet i hierarkiet har en kopi av rot-CAens offentlige nøkkel.

I et **distribuert hierarki** distribueres tillit mellom to eller flere CAer. En slik arkitektur kan bli resultatet når flere virksomheter har egen PKI, og disse strukturene ikke springer ut fra samme rot-CA. Prosessen med å sammenkople rot-CAer kalles kryss-sertifisering.

I kombinasjon med begge Hierarki-formene kan også en del av oppgavene til en CA settes bort

til en RA (Registration Authority – registreringsautoritet). En RA registrerer brukere og bekrefter fysisk deres identitet, men vil aldri signere sertifikater.

#### WEBMODELL

Her er den offentlige nøkkelen til et antall CA lagt inn i standard nettlesere. Disse nøklene gir et sett av CA'er som nettleseren vil stole på automatisk. Dette gjøres ved at leverandører av nettlesere har sin egen rot-nøkkel, som de sertifiserer CA'er som er inkludert i nettleseren.

#### USER-CENTRIC TRUST – MODELL

I denne modellen er hver bruker direkte og totalt ansvarlig for å bestemme hvilke sertifikater som de skal stole på, og hvilke de skal avvise. Det mest kjente eksempel på denne modellen er PGP. Her fungerer brukere som CA ved å signere offentlige nøkler til andre og ved å ha sin egen offentlige nøkkel sertifisert av andre.

## 2.3 Sertifikattyper

Det fins flere ulike typer sertifikat; X.509, SPKI, PGP, SET og attributtsertifikater. Selv om de likner hverandre, har de likevel forskjellig format og kan ikke brukes på tvers. SET og attributtsertifikater er laget for andre formål enn vårt behov, og er derfor uaktuell. PGP mangler tilbakekallingslister, mens SPKI er definert av en arbeidsgruppe fra IETF<sup>1</sup> som nå er avsluttet uten kjent produktstøtte.

Vi står dermed igjen med **X.509**, som finnes i tre forskjellig versjoner. Både den originale X.509v1, definert i 1988, og versjon 2 hadde få muligheter til attributtutvidelser. Versjon 3 har derimot både obligatoriske felt som må fylles ut, felter som normalt er med, og helt valgfrie felt. Algoritmeidentifikasjon, serienummer og den offentlige nøkkelen er eksempler på obligatoriske felter. Eksempler på elementer som normalt legges til, er Certificate Policiesutvidelsene og informasjon om bruksområde.[i og ii]

## 2.4 Sertifikatprofiler

I tillegg til forskjellige versjoner av sertifikatet, kan også hver versjon brukes på forskjellige måter. Et eksempel på dette er tidligere nevnte SET, som er en utgave av X.509v3 laget spesielt for sikker E-handel.

En slik tilpasning av en versjon av en standard kalles en profil. Profiler kan defineres av nasjonale eller internasjonale standardiseringsorganisasjoner, av leverandørene selv, eller av store kunder – for eksempel offentlig sektor i Norge. Eksempel på leverandørprofil fins hos Entrust. De har laget en profil, og publisert denne. Mange leverandører følger disse spesifikasjonene. Slike produkter kalles Entrust-Ready produkter. Telenor har eksempelvis valgt å legge seg opp til profilen definert av Entrust.

En annen standard (på en profil) er laget av SEIS (Secured Electronic Information in Society). SEIS krever tre nøkkelpar / sertifikater for hver sertifikatnehaver[iii]. Det svenske firmaet ID2 bruker SEIS, og skal ha implementert støtte for tre nøkkelpar/sertifikater i sine produkter. Postens profil er basert på denne standarden og bruker programvare fra ID2 [iv, s8 og v, s3].

Bruken av nøkkelpar er spesielt sentralt i en profil. I helsevesenet og offentlig forvaltning kan det eksempelvis være ønskelig med separate nøkkelpar for signering og kryptering. Slik kan en saksbehandlers krypterte informasjon gjenopprettes gjennom en sikkerhets kopi av krypteringsnøkkel oppbevart av arbeidsgiver. Signaturnøkkelen har ingen tilsvarende sikkerhets kopi, og signaturens validitet må dermed ikke samtidig kompromitteres. Dette støttes av både Entrust og SEIS, mens nøkkelbruken for autentisering er ulik

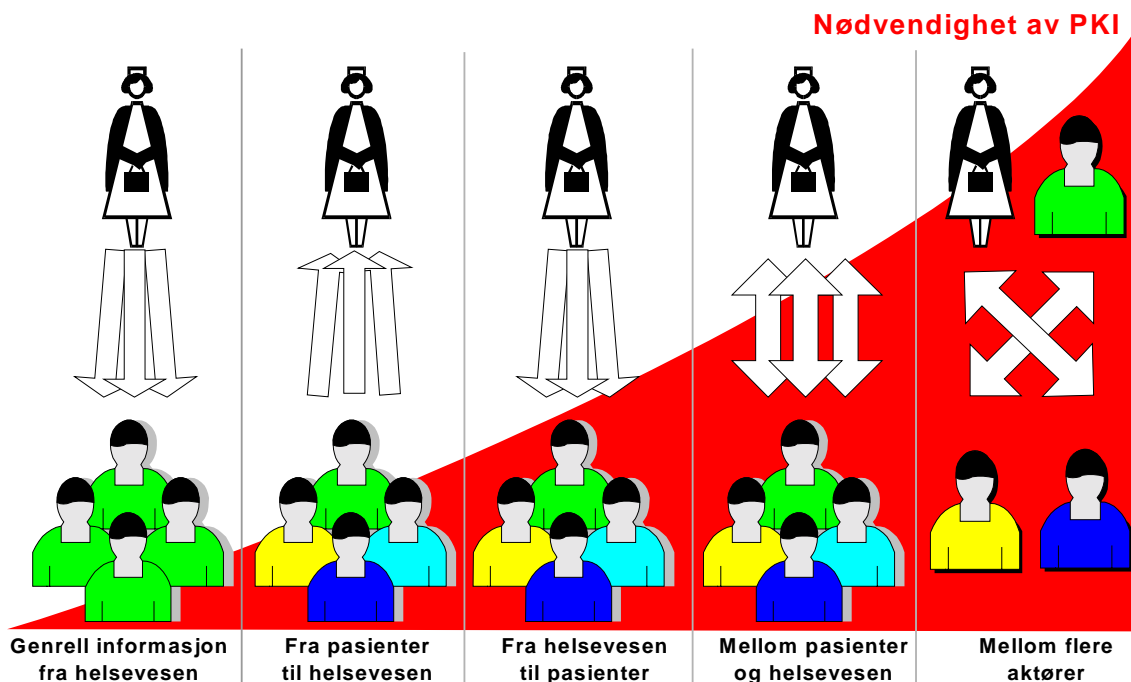
---

<sup>1</sup> Internet Engineering Task Force.

### 3 Pasienters behov og forutsetninger

En sikkerhetsstruktur som også inkluderer pasienter, må selvsagt ta utgangspunkt i deres behov og forutsetninger. Det er imidlertid metodisk vanskelig å etablere denne kunnskapen uten at løsningene først er realisert. Denne oppsummeringen er derfor basert på andre studier [vi, vii] og prosjekter som er koordinert opp mot sikkerhetsmodul-prosjektet (se hovedkapittel 4.7 og 4.8), samtidig som utviklingstrender for de nærmeste årene er analysert.

Figuren nedenfor forsøker å illustrere nødvendigheten av PKI. Inndelingene er koblet til de påfølgende underkapitler.



Figur 1

#### 3.1 Generell informasjon fra helsevesenet til helsesøkende

Pasienters enkleste informasjonsbehov er generell informasjon tilsvarende hva som normalt ligger på en helseinstitusjons "hjemmeside". Eksempel kan være informasjon om organisasjonsform, hvilke type helsetjenester som er tilgjengelig, og hvordan pasienter kan få tilgang til disse. Dette er vanligvis ikke personsensitivt, og derfor et behov som kan dekkes av andre sikkerhetsløsninger enn PKI.

Det er også et klart behov for helseinstitusjoner å legge ut konkret helseinformasjon på nettet, gjerne knyttet til rådgivning for konkrete diagnoser. I tillegg kommer opplysninger om ledig kapasitet og ventetid for ulike typer behandling. Dette er et felt der det forventes en betydelig økning i forbindelse med innføringen av fritt sykehusvalg.

Når informasjonen dreier fra generell informasjon om åpningstider og lignende mot helserådgivning og ventelister, øker samtidig pasientenes behov for å verifisere at informasjonen virkelig kommer fra helseinstitusjonen. En slik verifisering vil bli forenklet med PKI, men krever ikke nødvendigvis en fullt utbygd infrastruktur for å være funksjonell.

### 3.2 Fra pasienter til helsevesenet

Med kommunikasjon fra pasienten til helsevesenet, tenker vi oss pasienter som eksempelvis sender anmodninger om konsultasjonstimer eller egenrapporteringer av sin tilstand. Når det åpnes for slik kommunikasjon over nettet, kan man imidlertid ikke kontrollere hva pasienter faktisk vil oversende. Kravene til kryptering vil være relativt høye, siden man ikke kan sikre seg mot at personer sender informasjon som av helsevesenet vil bli oppfattet som sensitive.

Det er også sannsynlig at vi framover får et økende behov for overføring av måleinformasjon fra kroppsbårne sensorer, for eksempel i forbindelse med satsing på smarthusteknologi som skisseres i den statlige tiltaksplanen for 2001-2003 fra SHD [viii] Denne informasjonen - fra f.eks. hjerte og EEG sensorer - kan være både kritisk og sensitiv, og krever en god sikkerhetsstruktur for å unngå feilsendinger og misforståelser i alarmsituasjoner.

Selv om disse skisserte bruksområdene vil kreve kryptering og en viss sikkerhetsinfrastruktur, vurderers likevel behovet for PKI som moderat her. Årsaken er at helsevesenet i de fleste tilfellene kan utsette verifisering av autentisiteten av meldingene til et senere møte med pasienten. Først når helsevesenet sender informasjon tilbake til en person som er autentisert over nettet (3.3 og 3.4) vil PKI være en forutsetning for ordinær drift i stor skala.

### 3.3 Fra helsevesenet til identifiserte pasienter

Vi kan tenke oss flere tilfeller der det er ønskelig å sende informasjon elektronisk fra helsevesen til pasient. Dette er typisk tilfeller der det i dag brukes brev. Eksempler kan være prøvesvar, innkalling til timer og utskrift av journalnotater. Fordelen med å gjøre dette elektronisk, er blant annet de sparte administrasjonsutgiftene og tidsaspektet.

Ved en utbygd PKI-løsning, vil man kunne sørge for at tilgang og innsyn er i tråd med bestemmelsene i den nye Pasientrettighetsloven [ix] og lov om personopplysninger [x]. Man kan også sikre seg at pasienten mottar den informasjonen som sendes.

Siden helsevesenet står ansvarlig for at ikke sensitive personopplysninger leveres ut til uvedkommende, vil behovet for PKI være betydelig større her enn når pasienter sender opplysninger til helsevesenet.

### 3.4 Mellom pasienter og helsevesen - Behandling

De fleste tjenester for kontakt mellom helsevesen og pasienter forutsetter at informasjonsflyten kan gå begge veier. Vi har allerede sett flere forsøk på "nettbasert behandling", både fra psykologer, allmennpraktiserende leger og helseinstitusjoner. De fleste er basert på oppfølging og dialog på ordinær mail eller websider, og forsøkene har til felles at verken Datatilsyn, Helsetilsyn eller andre kontrollorgan har gitt noen umiddelbar approbasjon.

I tillegg til risikoen for kompromittering ved at andre får tilgang til behandlingsinformasjon, er også konsekvensene ved tilsiktet eller tilfeldig endring av ordlyd og meningsinnhold i meldinger stor. Hvem har ansvaret dersom meldingen fra legen mottas som "ta 200 Dispril og ring tilbake i morgen"?

Ved ulike former for behandling over nett har pasienter behov for alle sikkerhetsfunksjoner i en PKI-løsning. Infrastrukturen må kunne gi høy dataintegritet helt ut til pasienter, og vil sammen med autentisering og kryptering, kunne garantere avsender, mottager og meldingens innhold. Av juridiske hensyn må også funksjonen "ikke-benektning" støttes. Vi tror kreftene bak denne typen nettbasert behandling er så sterk at det i fremtiden vil komme flere nye tjenesteforsøk. Det er imidlertid tvilsomt om ordinær drift i stor skala kan gjennomføres før PKI er på plass.

### 3.5 Mellom alle aktørene

De siste årene har vi i økende grad sett at pasienter delvis behandler seg selv, gjerne i selvhjelpsgrupper, med eller uten deltagelse fra helsearbeidere. Flere slike grupper bruker også Internet som møtepunkt, enten i dedikerte grupper, eller i åpne diskusjonsfora. Det ser ut til å være en økende aksept fra helsevesenet om at dette har en gunstig mestrings- og helseeffekt, og at det er i helsevesenets interesse at slike grupper eksisterer selv når helsepersonell ikke er direkte relatert til selve behandlingen [xi].

Ved deltagelse i slike grupper er anonymitet viktig for mange av de helsesøkende. De fleste velger derfor også ulike "nicknames" i diskusjonsgrupper, selv om elektroniske spor ofte kan peke direkte tilbake til den reelle identiteten.

Dersom helsevesenet selv skal kunne etablere eller anbefale nettbaserte selvhjelpsgrupper må det derfor sette høye krav til sikkerhet. Både verifisering/autentisering av nettstedet, og prosessen med anonymisering eller pseudonymisering av pasienter må sikres. Når helsepersonell er veiledere i slike løsninger må også disse autentiseres og autoriseres gjennom samme teknologi som finnes innenfor helsevesenet.

Det er vanskelig å tenke seg sikkerhetsløsninger for storskala drift som tilfredsstillende disse kravene uten bruk av PKI.

### 3.6 PKI for pasienter eller for helsevesenet

Det er ingen automatikk i at en PKI-løsning som er godt egnet for helsevesenet, også skal være egnet for pasienter. De viktigste forskjellene ligger i at man internt i helsevesenet kan forutsette en betydelig større grad av homogenitet både i brukergruppe, kunnskapsnivå, maskinvare og lokalitet.

Forskjellene kan oppsummeres i disse punktene:

- **Maskinuavhengighet:** En kan ikke stille krav om ensretting i valg av hardware og software. Mens man internt i helsevesenet kan forutsette valg av hardware (for eksempel Intel-kompatibel prosessor) og software (for eksempel et spesielt operativsystem eller en bestemt nettleser), vil dette ovenfor pasienter være uforenlig med lik tilgang til alle.
- **Brukervennlighet:** Sett i forhold til pasienter er faktisk helsearbeidere en forholdsvis homogen gruppe. Helsearbeidere har i all hovedsak høyere utdanning, de er i alderen 20-65 år, de har i liten grad alvorlige funksjonshemninger etc. Hvis man skal utforme en PKI-løsning med tanke på pasienter, stilles det derfor større krav til enkelhet og brukervennlighet enn hvis den kun er tenkt benyttet innenfor helsevesenet.
- **Vedlikehold:** En løsning bør kreve minimalt eller ingen support på pasientenes datamaskiner, da dette vil være svært kostnadskrevende på maskiner som ikke er fysisk samlokalisert.

## 4 Gjennomføring og Resultat

Under dette hovedkapitlet beskrives en del av aktivitetene som prosjektet har generert, og kort om hvilke resultater disse har gitt knyttet til hovedmålene. Overskifter og inndelinger er relatert til delaktivitetene.

### 4.1 Standardisering/koordinering i Norge

En vesentlig del av prosjektideen var at pasienter også skulle få ta del i de løsninger som etter hvert blir innført innenfor det offentlige. Det var derfor viktig å holde seg innenfor standarder og strukturer som det offentlige i Norge valgte, slik at verken NH eller pasienter skulle ende opp med proprietære løsninger som ikke samvirket med de øvrige.

Informasjon tilgjengeliggjort gjennom [Forvaltningsnettsamarbeidet](#) har her vært sentral, og har sammen med leverandører og ulike konferanser dannet et rimelig godt forståelsesgrunnlag. Drøftingene med Fjeldheim (RTV) og Kvaase (SHD), hvor helsevesenets behov og forutsetninger har vært i fokus, har også vært av uvurderlig nytte.

Det samlede informasjonsgrunnlaget gav likevel ikke entydige svar på en del av våre valg i løsningsutviklingen. Eksempler er usikkerheter knyttet til hvilke typer sertifikat som bør innføres, hvordan og hvilke nøkler som skal brukes, samt hvordan CP (Certificate Profile) skal implementeres. Spesielt vanskelig var det å avklare detaljer rundt kryssertifiseringen mellom ulike TTP'er i Norge, og dette viktige grunnlaget manglet helt ved vår siste milepælsfrist for igangsetting av brukersøk. Ved utgangen av januar 2001 klarer fortsatt ikke vår valgte TTP leverandør å fremstille en komplett løsning som fullt understøtter kryssertifiserte sertifikater.

Kompleksiteten i arbeidet med koordinering og standardisering avspeiler seg også i at *"Utvalget for utredning av digital signatur i offentlig forvaltning"* heller ikke ble ferdig med sin innstilling som planlagt i høst.

### 4.2 Implementering av PKI: viktige valg

Som nevnt i kapittel 2 er det en rekke sentrale valg som danner grunnlaget for en PKI-løsning. Dette kapitlet beskriver vår analyse og tilnærming til disse utfordringene, før noen av erfaringene fra gjennomgåtte produkter kort oppsummeres.

#### 4.2.1 Vurdering av tillitsstruktur

##### **HIERARKI - LUKKET**

I utgangspunktet ønsket NH å lansere en egen CA for alle brukere innenfor helsenettet. Produktet RSA Keon ble derfor tidlig valgt som basis i en pilot med lukket PKI og hierarkisk tillitsstruktur. Fordelen ved at alle har tillit til en enkelt enhet er at forklaring ovenfor brukere blir lettere. Dersom en bruker har et sertifikat utstedt av NH, og oppslag viser at det ikke er trukket tilbake, har det ubetinget tillit. Videre slipper man kryssertifisering

Det ble ikke vurdert som nødvendig at NH selv kontrollerte legitimasjon til brukere som ønsker sertifisering. Dette kunne for eksempel delegeres slik at hvert sykehus ble RA (autoritet som registrerer brukere) for NH.

Ulempen med en slik lukket løsning er at den bare fungerer for personer/enheter innenfor helsenettet. Pasienter, helsearbeidere og ansatte i andre offentlige etater utenfor helsenettet vil bli avskåret fra sikret kommunikasjon. Dette gjorde at andre modeller måtte vurderes.

## HIERARKI - ÅPENT

Ved en åpen løsning kan rot-CA tjenesten kjøpes fra ekstern leverandør, som dermed blir en Tiltrodd Tredjepart (TTP). Vi har primært gjort vurderinger med Posten SDS som TTP. TTPen kan enten levere komplett CA funksjonalitet, eller deler av den. Ved levering av deler er det naturlig at NH påtar seg rollen som RA for sluttbrukere, eller eventuelt at RA-funksjonen organiseres ved de enkelte helseinstitusjonene. Delegering vil gi forsterket skalerbarhet og mindre driftskostnader med det høye antallet sluttbrukere og geografisk spredning i NH.

En åpen løsning gir to umiddelbare fordeler. Helsepersonell med sertifikater utstedt av helsenettet vil lett samhandle med personer som ikke er sertifisert i NH. Dette gjelder både personer med sertifikater fra Posten og personer med sertifikater som er kryssertifisert med Posten. Man oppnår på den måten et distribuert hierarki hvor kryssertifisering skjer ved at CA'ene godkjenner hverandre.

En ekstern rot-CA vil også overta en betydelig del av dokumentasjonsansvaret. Blant annet CP (CertificatePolicy) og CPS (Certification Practice Statement), som definerer sikkerhetsnivå og implementasjon, må oppdateres regelmessig. Gjennom å lokalisere dette omfattende og viktige arbeidet til f.eks. Posten, oppnås klare stordriftsfordeler.

## WEB-MODELL

I web-modellen er mange CA'er forhåndsgodkjent av nettleser. For eksempel ligger det i Windows 2000 ca. 140 forskjellige offentlige nøkler. Sertifikatene fra disse utstederne kan prosesseres uten videre. En klar ulempe er at valget av nettleser ofte baseres på helt andre faktorer enn sikkerhet, og grunnlaget for nettleserprodusentenes forhåndsgodkjenning av CA-leverandører er heller ikke entydig.

Dette innebærer problemer med å skille mellom ulike sikkerhetsnivå på sertifikat utstedt av samme eller ulike CA'er. Eksempelvis vil et gratis sertifikat fra Thawte mottatt uten legitimering ha samme forhåndsgodkjenning i nettleseren som sertifikat verifisert gjennom legitimering hos offisiell notar.

Videre er det begrenset mulighet for tilbaketrekking av en forhåndsgodkjent CA, og dermed de nøklene som denne har utstedt. Sikkerhetsbrudd ved en rot-CA gir dermed svært uoversiktlige konsekvenser, og krever mye innsats fra brukerne for å sikre kontinuerlig tillit.

## USER-CENTRIC MODELL

User-centric modellen mangler fullstendig en CA, og krever dermed enda mer innsats fra brukeren for å sjekke tillit. Her skal man ikke bare sjekke sertifikater, men også sertifisere andre. En helsearbeiders sertifikat kan kun verifiseres ved at det er sertifisert av en annen helsearbeider man har tillit til. Det finnes ingen mulighet for revokering.

### 4.2.2 Vurdering av sertifikattype og profiler

Alle CA'er og PKI leverandører vi kjenner til, har implementert X.509v3 sertifikater, primært på smartkort som loven anbefaler [xii], noe som også er helt samstemt med vår analyse.

Valget av profil var imidlertid mer usikkert. Som nevnt i kap 2.4 bestemmer profilen blant annet hvordan nøkler brukes, og PKI-utvalget skisserer bruk av tre nøkkelpar, tilsvarende SEIS standarden. De tre nøkkelparene brukes her hhv. til kryptering, signering og ikke benektning.

I arbeidet med å avklare profilspørsmål oppdaget vi at Posten SDS og RSA begge hevder å følge SEIS-standard, men har likevel kun to nøkkelpar, og bruker *krypteringsnøkkelen* til

autentisering. Den andre standardprofilen, definert av Entrust, brukes blant annet av Telenor. Deres profil bruker *signeringsnøkkelen* til autentisering.

Utfordringene med profilvalg er nært knyttet til valg av rot-CA/TTP, dersom åpent hierarki velges. Det er derfor ikke gjort definitive avklaringer på profilvalg og nøkkelbruk i prosjektperioden. Det er tilsvarende heller ikke endelige vurderinger på om det er gunstig med ekstra nøkkelpar/sertifikater for hver av de ulike rollene som en person kan ha i ulike sammenhenger

### 4.3 Erfaring fra produkter

Vi har i prosjektperioden gått dypere inn i flere produkter, og erfaringene fra disse gjennomgangene er delvis bygd inn i ovenstående kapittel. Nedenfor følger likevel en kort oppsummering av erfaringer og funksjoner.

#### THAWTE

Thawte er gjennom sin forhåndsgodkjenning i nettlesere basert på en Web-modell. Samtidig er tjenesten også User-centric ettersom det er brukere som går god for hverandre. Brukere som har fått status som ”notar” verifiserer en annen brukers identitet gjennom legitimering. Thawte utsteder deretter et sertifikat med personens navn. Thawte tilbyr videre sertifikater for servere, og kan på den måten tilfredsstillende behovet for sikker autentisering av informasjonstjenester.

Sertifikatene fra Thawte er i utgangspunktet myke, d.v.s. de fås som en fil som legges på diskett/harddisk. Gjennom samarbeidspartnere kan sertifikatet og privat nøkkel eventuelt også legges på et token. Dette token plugges direkte inn i USB-porten istedenfor bruk av smartkort og smartkortleser [xiii]. Dette er en løsning som er spesielt interessant for storskala bruk av pasienter. De vil i tilfelle unngå dyre smartkortlesere, og fremdeles få et portabelt sertifikat.

Imidlertid er ikke den blandete tillitsstrukturen i prinsippet tilstrekkelig for helseformål, og vil måtte innebære klare begrensninger dersom brukt i pasientsammenheng.

#### MICROSOFT

Windows 2000 advanced server har innebygd CA-funksjonalitet. Win2000 har også gjennomgående god støtte for digitale signaturer og smartkort i tilhørende applikasjoner. Så langt vi kan vurdere er disse også greit dokumentert, og fungerer i de sammenhengene vi har testet.

Dessverre er disse funksjonene i stor grad avhengig av Microsoft-produkter i den øvrige nettstrukturen og på klienter. Dette innebærer en ensretting av programvare i helsevesenet som må vurderes nøye i en sikkerhetsanalyse, og samtidig kan gi begrensninger i videreutviklingen av åpne standarder.

#### POSTEN SDS

SDS er en TTP-leverandør, og tilbyr sertifikater på smartkort og tilbakekallingslister for sertifikatene. De ønsker imidlertid ikke å ha RA-funksjonen, slik at et samarbeid med Posten innebærer en annen organisering av denne funksjonen for våre brukere.

Løsningen for sikker E-post som var tilgjengelig ved prosjektoppstart, kan de for tiden ikke levere. Dette skyldes problemer med en programvaremodul, som nå søkes erstattet gjennom samarbeid med en ekstern part. Posten SDS kan imidlertid fortsatt levere RA-programvare fra den svenske leverandøren ID2 Technologies.

## RSA

RSA's PKI-løsning kan enten brukes lukket innenfor en bedrift, eller i kombinasjon med en CA leverandør som Posten. Det kan utstedes sertifikater også for servere og applikasjoner, og løsningen inneholder langt flere moduler enn behandlet i dette prosjektet. Blant annet finnes "Single Sign On" som er nyttig blant helsevesenets mange datasystemer.

De mange modulene utgjør imidlertid en kompleks pakke, og RSA klarte ikke å levere en fungerende PKI-løsning innenfor prosjektets rammer. Vi vurderer en av årsakene til å være manglende kompetanse i Norge.

Vi vurderer at en kombinasjon av Postens løsning og RSA skal kunne gi den ønskede tillitsstruktur hvor NH er RA, mens CA-funksjonen kjøpes fra Posten SDS. I desember ble det også avtalt med Posten og RSA at dette skulle utprøves. Dette har blitt midlertidig stanset ettersom Posten ikke kunne levere de nødvendige sertifikater.

## 4.4 Risikoanalyse<sup>2</sup> av NH

En risikoanalyse beskriver hvilke risikosituasjoner som kan forekomme, sannsynligheten for at de skal oppstå, og hvilke sannsynlige konsekvenser som vil kunne følge av dem. Dette er viktig dokumentasjon til Datatilsynet og helsenettets kunder, og selvsagt nødvendig grunnlag for implementering av PKI.

Analysen som er utarbeidet for NH inkluderer også tilhørende tiltak, og omfatter faktorer som brann, strømstans, dokumentasjon og kompetanse. Risikovurderingen er inndelt i egne matriser for eksterne og interne parametere. Her vises sannsynlighet kontra konsekvensklassifisering, som støtte i vurderingen av hvilke sikkerhetstiltak som må iverksettes for å forhindre uønskete situasjoner.

Akseptabel risiko er klargjort etter definerte kriterier, og disse vil også ligge i bunnen for videre vurdering av PKI-løsninger. Ettersom endelige valg av PKI-løsning ikke ble gjennomført i prosjektperioden, er imidlertid ikke analysen konkret rettet mot produkter. Prosessen med konsekvensvurdering av ulike modellvalg vil derfor fortsette ut over prosjektperioden.

## 4.5 Etablering av katalogtjenester

Et annet viktig grunnlag for en sikkerhets-infrastruktur med digitale nøkler er katalogtjenester. Disse muliggjør sertifikatoppslag, og er dessuten en viktig påbygning rettet mot autorisasjon i tjenestutevksling. Gjennom oppslag i katalogtjenesten skal det f.eks. være mulig å verifisere at en person har gyldig (lege)lisens, og er autorisert til transaksjonen hun har signert elektronisk.

En katalog kan sammenlignes med en svært strukturert database, hvor informasjonselementer kan gjøres tilgjengelig på tvers av institusjoner gjennom definerte oppslag. utfordringen er at alle de ulike institusjonene i f.eks. et helsenettverk har ulike og heterogene nettstrukturer, med enda mer kompliserte og proprietære datastrukturer. Det er også komplisert å sikre transporten av kataloginformasjon gjennom ulike brannmurer og sikkerhetsløsninger.

Anders Baardsgard ved NH har, etter et betydelig forarbeide relatert til analyse og forslag av minimumsstandarder, innledet et samarbeid med flere av de store sykehusene i Nord-Norge. Selv om arbeidet ikke er helt fullført, er allerede tjenesteforsøk med katalogtjenester nå tilgjengelig gjennom helsenettet. Også denne prosessen fortsetter ut over prosjektperioden.

---

<sup>2</sup> Dokumentet er kun tilgjengelig for styret, ansatte, kunder og leverandører i NH, samt DT

## 4.6 Pilot med sikker kommunikasjon innenfor helsevesenet

Ettersom PKI i dag har meget begrenset utbredelse også innenfor helsevesenet var det naturlig å prioritere dette området før vi passerte grensen ut til pasienter. Prosjektet avgrenset seg til sikker E-post, og engasjerte seg i utredningen av krav, ønsker og utfordringer. Flere ulike helseinstitusjoner og etater er rådført, før vi valgte å fokusere på et prosjekt mellom et legekontor og to lokalisasjoner av hjemmetjenesten i en bydel.

Ingen av disse hadde i utgangspunktet ekstern nettilknytning, eller tilgang til mail. Rundt årsskiftet var det imidlertid planlagt tilkobling til hhv NH og kommunens felles dataanlegg, men løsningene ville utformes slik at det ikke ville bli tilgang til å utveksle sensitiv informasjon om felles pasienter. NST's forslag om implementering av PKI-basert sikker mail ble derfor godt mottatt av aktørene.

Etter den innledende behovs- og risikoanalysen var konklusjonen at Datatilsynet måtte gjøre den endelige vurderingen av sikkerhet. Det omfattende arbeidet med dokumentasjon av nettstruktur, utstyr, rutiner mv, ble ledet av Siri Uldal ved NST, med bidrag fra både NH og kommunen. Det er også utarbeidet prosedyrer for m.a. egenkontroll, konfigurasjonsendring, beredskapsplaner, avviksbehandling, dokumentetsikkerhet, dataoverføring, adgangs- og tilgangskontroll. Søknaden er ved avslutning av denne rapporten fortsatt under behandling.

## 4.7 Pilot med sikker kommunikasjon mellom pasient og helsevesen

Prosjektplanen åpnet for en konkret pilot med kommunikasjon mellom sikker sone innenfor helsevesenet, og ut til pasienter på deres egen PC. Selve pilotgruppen var også tidlig definert, og pilotprosjektet forberedt oppstartet oktober 2000 med behandler og pasienter knyttet til psykiatri.

I sonderingene før oppstart ble det imidlertid avklart at Datatilsynet ikke ønsket å motta søknader om konsesjon eller dispensasjon etter september 2000. Dette skyldtes ikrafttredelse av nytt lovverk Januar 2001[x], og hadde sammenheng med Datatilsynets behandlingstid. Samtidig viste risikoanalysen at i en pilotgruppe knyttet til psykiatri ville konsekvensen av sikkerhetsbrudd være stor. Det ble derfor vurdert som uaktuelt å starte brukersøk uten Datatilsynets bifall. Prosjektet havnet slik i en "bakevje" mellom nytt og gammelt lovverk, hvor brukersøk burde avvendes til nye lover var gjeldene.

### 4.7.1 Eksem-prosjektet

For å erstatte resultatelementer som forsvant sammen med brukersøket, engasjerte prosjektets sikkerhetsgruppe seg i stedet i et annet prosjekt med betydelig mindre konsekvens av sikkerhetsbrudd; "Eksem-prosjektet". I dette prosjektet fikk 5 eksempasienter elektronisk veiledning av spesialsykepleier, basert på innsendt tekst og bildemateriale. Applikasjonen "DORIS" som dette prosjektet baserte seg på, hadde innebygd kryptering med bruk av private nøkler på inntil 448-bits over Blowfish algoritmen.

Gjennom blant annet "Eksem-prosjektet" framkom en rekke krav til brukergrensesnitt, hardware og software for pasienter, og forståelse om hvordan dette avviker fra helsevesenets forutsetninger for bruk av PKI. I tillegg til momenter beskrevet i kap.3, framkom også entydig risikoen ved at pasienters datautstyr står utenfor sikre soner, og har liten beskyttelse mot virus eller innbrudd. Utstyret brukes dessuten primært til oppgaver langt utenfor helsesammenheng, og ofte har andre brukere i en familie eller bedrift tilgang til lagrede data. Videre var det store variasjoner i utstyrets alder, type, pris, programvare, tilkoblingsmuligheter og andre parametere.

Det var også en viss variasjon i kunnskap om hvordan ivareta sin egen sikkerhet, men generelt var det moderat engasjement for å sikre at informasjon ikke kom på avveie. Dette bekreftet klart vårt inntrykk av at PKI-Løsninger må bli enkle, ukompliserte, samt kreve minimalt av utstyr, installasjon og brukerstøtte på hver enkelt klient. I tillegg må løsningen være billig i anskaffelse og ha så lave transaksjonskostnader at den faktisk blir brukt.

Erfaringene fortalte også at helsevesenet og allmennbefolkningen må ha tilgang til samme standarder, slik at ikke hver enkelt helsetilbyder selv må implementere ekstraordinære og halvproprietære løsninger for pasientrettet kommunikasjon. En kroniker med relasjoner til flere nivå og etater innenfor helsevesenet vil ellers risikere å måtte ha mange ulike typer sikkerhetsløsninger, hvorav noen av disse nok vil være på kanten av forskrifter og regelverk, eller interferere med hverandre.

## 4.8 Informasjon til pasienter og helsesøkende

En klar konklusjon fra ovenstående kapittel om pasienters forutsetninger og behov var at de mangler nødvendig kunnskap om sikkerhet. Pasienter har problemer med å vurdere hvilken sikkerhetsrisiko de ulike helsesrelaterte tjenestene i dag innebærer, og gjør lite for å beskytte spredning av informasjon om seg selv. Undersøkelser viser også at Internet blir en stadig mer brukt kanal for helseinformasjon, samtidig som det er kjent at denne informasjonen er av svært varierende kvalitet.

Innføring av PKI er som nevnt motivert av at pasienter skal kunne utveksle informasjon med helsearbeidere på en sikker måte. Vår meningsmåling utført høsten 2000 viser at en tredel av pasientene ønsker å kontakte legen per e-post, og hele 16 prosent kunne tenke seg å bytte lege for å få tilgang til Internett-baserte legetjenester. En slik informasjonsutveksling basert på PKI krever en betydelig økning i pasienters behov for sikkerhetskompetanse.

Koordinert med sikkerhetsmodul-prosjektet startet derfor "Den nye pasientrollen" ved *Nasjonalt senter for telemedisin* arbeidet med en informasjons-tjeneste som retter seg spesielt mot pasienter. Målet er et nettsted som popularisert beskriver hvordan de kan og bør forholde seg som konsumenter av helsetjenester på nettet. Nettstedet er inndelt etter de sikkerhetsproblemer som i dag eksisterer på Internett, og vil også inneholde diskusjonsfora knyttet til problemstillingen helse og IKT. Første utkast er tilgjengelig på [www.telemet.no/brukerinfo](http://www.telemet.no/brukerinfo), men arbeidet er relativt omfattende og påventes ikke ferdigstilt før sommer 2001.

Vi har gjennom møter og konferanser også startet arbeidet med å koble andre aktører opp mot denne aktiviteten, og Helsetilsynet har allerede respondert positivt på vår henvendelse om "standarder og retningslinjer i forbindelse med nettbaserte helsetjenester". På deres forespørsel har også vi gjennom Deede Gammon takket ja til å være norsk representant i Committee of experts on the impact of information technologies on health care – The Patient and Internet.



## 5 Konklusjon og avsluttende kommentarer

Selv om teknologien som sikrer konfidensialitet, integritet, autensitet og ikke-benekting ved elektronisk kommunikasjon har vært tilgjengelig i mer en 10 år, kan løsningene fortsatt betegnes som umodne. Løsningsimplementeringen krever dyptgående datafaglig kompetanse på tvers av operativsystem, og på både applikasjons- og systemnivå. Det fordres også utredninger og avklaringer basert på juridisk og organisasjonsfaglig kompetanse.

Dette prosjektet er i så måte en tilnærming mot bare avgrensede deler av problemkomplekset PKI utgjør. Hovedsakelig er det rettet mot **pasientrelaterte behov**, selv om prosjektet er koordinert mot flere tilgrensende prosesser. I konklusjonen er det derfor naturlig å fokusere på momenter direkte relevant til prosjektets hovedmål.

### 5.1 Implementering av PKI i NH

Fordi en del grunnleggende faktorer ikke lot seg entydning avklare i løpet av prosjektperioden, ønsker ikke NH å endelig konkludere rundt innføring av PKI innenfor helsenettet. Helseministerens nylig annonserte koordinering av helsenettene bidrar også til ønsket om å utsette avgjørelsen, slik at en fastlåst standard-diskusjon med andre sentrale aktører kan unngås.

Basert på erfaringene beskrevet i kapittel 4.2 er det likevel mulig å antyde NH's foreløpige standpunkt knyttet til PKI:

Utgangspunktet bør være et åpent hierarki med en ekstern rot-CA (TTP) representert i Forvaltningsnettsamarbeidet. RA-funksjoner tenkes koordinert av helsenettet, mens deler av utføringen kan delegeres til f.eks. større sykehus for økt skalerbarhet. Sertifikatprofilen (CP) bør være tilsvarende Forvaltningsnettets, slik at hele det offentlige Norge får like profiler. Helsevesenets behov for multiple nøkler til ulike tjenester bør eventuelt drøftes inkludert i denne profilen. Tilsvarende bør sikkerhetsnivå og andre spørsmål knyttet til sertifikatinnhold og nøkkelbruk bli entydig utredet og testet.

Under forutsetning av klart nok definerte standarder, vil valg av lokale sikkerhetsapplikasjoner gjøres av den enkelte RA eller helseinstitusjon. Lagringen av sertifikat for helsevesenet bør inntil videre begrenses til kun å være på smartkort, men kan senere utvides til andre fysiske lagringsmedia.

Ved en sammenslåing av helsenettene vil arbeidet med felles katalogtjenester måtte intensiveres. Kostnader forbundet med innføringen av PKI bør også utredes videre. Denne utredningen må inkludere kostnader forbundet med RA & CA -tjenester, hard & software, opplæring & supportsystem, samt prisstrukturen for disse tjenestene.

Blant fordelene med en slik åpen hierarkisk løsning er at helsenettene får redusert ansvar for dokumentasjon og kryssertifisering mellom CA'er. Sentralt i forhold til hovedmålsetningen i dette prosjektet er også at pasienter og andre utenfor helsenettet slik kan kommunisere sikkert over nettgrensene. Pasienter og helsearbeidere vil kunne få sertifikater fra samme CA, som samtidig er en uavhengig tredjepart – en "Trusted Third Part".

Åpningen av PKI-basert kommunikasjon innebærer likevel ikke at NH vil ta ansvar for eller direkte understøtte pasientrettede tjenester i sitt nett. Helsenettet skal primært fokusere på sikker kommunikasjon og samhandling mellom helsearbeidere. Avgrensede pilotforsøk tilsvarende dette vil imidlertid fortsatt regnes å gi nyttige erfaringer og innspill for NH.

## 5.2 PKI for pasienter

Prosjektets hovedmålsetning var å utrede og utvikle en generell teknisk og organisatorisk løsning som sikrer dataintegritet og -konfidensialitet for helsefremmende publikums- og pasienttjenester på Internett. I utgangspunktet var det to mulige veier for en realisering av dette; enten at helsevesenet inkluderer pasienter i sin lukkede løsning, eller at helsevesenet velger en åpen løsning basert på samme standarder som er tilgjengelig for pasienter.

Som forrige kapittel oppsummerer, er sistnevnte alternativ nå mest sannsynlig. Dette er for så vidt en god løsning for pasientene. Gjennom muligheten for at en ekstern *Tiltrodd TredjePart* kan garantere for sikre transaksjoner, vil deres rettsikkerhet og kontrollmulighet øke.

Den største utfordringen ved dette alternativet er at det foreløpig er uklart hvem som skal være registreringsautoritet (RA) for pasienter og helsesøkende. Det er naturlig og svært ønskelig at helsevesenet, f.eks. større sykehus, også kan organisere pasienters RA-tjenester. Apparatet må likevel skaleres for et stort antall helsearbeidere, samtidig som at pasientene tradisjonelt er innoom sykehuset på et eller annet tidspunkt. Dersom sykehus også kan levere ut personifiserte smartkort, vil samtidig utleveringsrutiner og opplæring kunne effektiviseres.

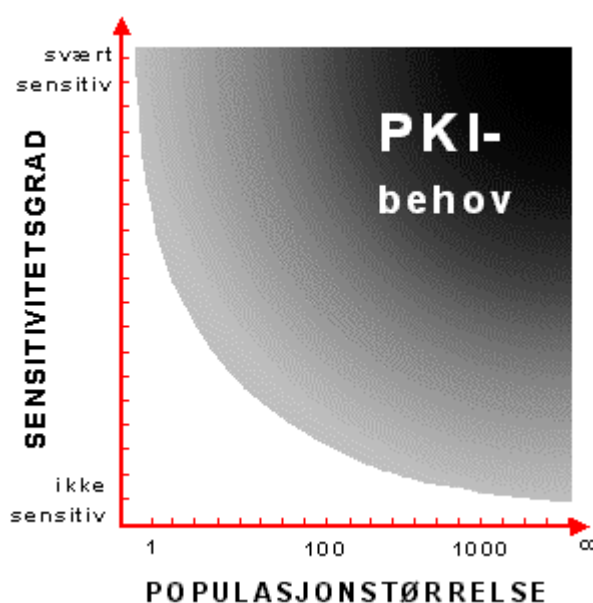
I tillegg til opplæringsspørsmålet er også pasienters tilgang til supportfunksjon viktig. Resultatene fra prosjektet viser at mange pasienter har et betydelig opplæringsbehov knyttet til ivaretagelse av sin egen sikkerhet, og PKI-funksjoner kan være en klar utfordring for disse gruppene. Det er ikke naturlig å tro at dagens helsevesen har kompetanse og kapasitet til å ivareta dette ansvaret alene. Det er heller ikke selvsagt at en kommersiell CA vil kunne prise slik support, eller selve transaksjonene slik at PKI vil få nødvendig utbredelse blant pasienter. Dette kan innebære at helsevesenets innføring av PKI faktisk vil **begrense** mulighet for elektronisk kommunikasjon med pasienter.

Med utgangspunkt i kapittel 3's beskrivelse av pasientrelaterte behov, og mulige konsekvenser skissert i kapittel 4.7 er dette svært ugunstig. Spissformulert har helsevesenet behov for at utviklingen med informerte og "selvhjulpne" pasienter fortsetter. Dette er nødvendig om vi skal beholde dagens nivå av tilgjengelighet, kontinuitet og faglig utførelse i helsevesenet, uten betydelig ressursøkning. Pasienter og allmennbefolkning trenger derfor en sikkerhetsinfrastruktur som er absolutt koordinert med helsevesenets.

Som figuren til høyre illustrerer, finnes det likevel pasientrelaterte tjenester hvor sikkerhetsbehovet kan realiseres på andre måter enn full PKI. Vår mening er at meldinger med relativt høy grad av sensitivitet kan overføres med annen kryptering, dersom dette skjer i et klart avgrenset omfang. Tilsvarende kan helseaktører kommunisere med mange pasienter, dersom sensitiviteten avgrenses til kun å omfatte timebestilling og lignende.

Flere ulike teknologier som også er nevnt i denne rapporten kan understøtte slik kommunikasjon. Imidlertid må dette regnes som ikke fullgode løsninger, og inntill videre vil vi ikke anbefale slike til annet enn i forskningssammenheng.

Pasienttjenester i rutinedrift av det offentlige helsevesen må etter vår mening bygges på Public Key Infrastructure.



### 5.3 PKI i det offentlige

Nettbaserte pasient og publikumstjenester er et viktig element på veien mot mer effektive og tilgjengelige offentlige tjenester. Dette fordrer igjen at sikker elektronisk kommunikasjon fungerer på tvers av forvaltningsnivå, sektorer og geografiske grenser. Vi ser likevel at det gjenstår betydelig arbeide og noe tid før Norge har entydige standarder knyttet til bruk av digitale sertifikat i en infrastruktur.

Utfordringene er både teknisk relatert, f.eks. knyttet til kompatibilitet mellom ulike produkter og leverandører, men også av mer organisatorisk karakter. Blant annet kreves koordinering mellom en rekke ulike informasjonskilder og aktører. For vår egen satsning har det eksempelvis vært aktuelt å innlede dialog med departementer eller underetater som SHD, RTV, AAD, Datatilsyn, Justervesen, Helsetilsyn, og FO/-Sikkerhetstjenesten. I tillegg kommer dialogen med leverandører og produsenter, sluttbrukere og enheter innenfor nettverket, samt pasientgrupper og organisasjoner.

Dersom hver enkelt organisasjon som vurderer PKI løsninger selv må koordinere mot en slik heterogen aktørmengde og komplekse problemstillinger, vil dette alene stoppe initiativet. Framdrift i det offentliges PKI-implementering krever at noen har en endelig oversikt, samt ansvar og kapasitet for å formidle den. Teknisk dokumentasjon og juridisk språk må omformuleres til konkrete anbefalinger, og ”kokebokoppskrifter” må tilbys til offentlige tjenester som skal tilgjengeliggjøres.

Det er derfor svært betryggende at se at det offentlige absolutt er på banen, gjennom f.eks. Forvaltningsnettsamarbeidet og PKI-utvalget. Vår primære bekymring er imidlertid knyttet til om det offentlige investerer tilstrekkelig med ressurser for å realisere praktisk fungerende funksjoner også for pasienter og publikum. Vår neste bekymring er konsekvensen av at etterspørselen kan presse fram proprietære Ad-Hoc-løsninger for å dekke et umiddelbart behov.

Framover finner vi det derfor helt legitimt å gjenåpne diskusjonen rundt statlig innføring av elektroniske personkort, slik som f.eks. Finland og noen andre land har påbegynt.

---

## REFERANSER

- i Adams, C., Lloyd, S *Understanding public-Key Infrastructure*, Indianapolis, USA, Macmillan Technical Publishing, 1999
- ii *Elektroniske ID-kort* [on-line]. JB consult 3. oktober 2000. Tilgjengelig fra: [www.statskonsult.no/prosjekt/pki/rapporter/elektronisk%ID.pdf](http://www.statskonsult.no/prosjekt/pki/rapporter/elektronisk%ID.pdf) [Aksessert 3/10-2000]
- iii Client Software and Digital Certificates from Posten [on-line] Tilgjengelig fra: [http://peid.sds.no/english/clients\\_eid\\_overview.htm](http://peid.sds.no/english/clients_eid_overview.htm) [Aksessert 09.11.2000]
- iv Posten SDS: Vedlegg 2 til rammeavtale, Tiltrodde tredjepartstjenester og løsninger for digital signatur og meldingskryptering 11/1 –1999, rev 7/5 -1999
- v Overview of multismart Toolkit from Posten SDS [on-line] Tilgjengelig fra: <http://peid.sds.no/english/multismart-toolkit.htm> [Aksessert 09.11.2000]
- vi Gammon D, Rosenvinge J: "[\*Er Internett til hjelp for personer med alvorlige psykiske lidelser?\*](#)", Tidsskr Nor Lægeforen. Tidsskr Nor Lægeforen 2000; 120: 1890-2
- vii Kummervold, P.E., Gammon, D., Johnson, J.A., Hasvold, T., & Rosenvinge, J.H. (in press). *Social support in a wired world - use of mental health discussion forums in Norway*. Nordic Journal of Psychiatry.
- viii Statlig tiltaksplan 2001-2003: Elektronisk samhandling i helse- og sosialsektoren [online] <http://odin.dep.no/shd/norsk/publ/handlingsplaner/030011-120002/index-dok000-b-n-a.html>
- ix Lov om pasientrettigheter (pasientrettighetsloven) <http://www.lovdatab.no/all/nl-19990702-063.html>
- x Lov om behandling av personopplysninger (personopplysningsloven) <http://www.lovdatab.no/all/nl-20000414-031.html>
- xi NORGES OFFENTLIGE UTREDNINGER NOU 1998: 18 "Det er bruk for alle" [online] <http://odin.dep.no/shd/norsk/publ/utredninger/NOU/030005-020018/index-dok000-b-n-a.html>
- xii Forslag til lov om elektronisk signatur. Prop.nr.82. 1999-2000
- xiii iKey 2000 Overview [on-line]. Rainbow Technologies. 6/12-2000. Tilgjengelig fra: <http://www.rainbow.com/ikey2000/index.html> [Aksessert 26/1-2001]