KITH
INFORMASJONSTEKNOLOGI
FOR HELSE OG VELFERD

Prosjektrapport – Forprosjekt

for PKI i helseforetakene

Versjon 1.0
Dato: 11.05.2006

KITH Rapport 06/06
ISBN 82-7846-2844-4

KITH-rapport

TITTEL

Prosjektraport – Forprosjekt for PKI i helseforetakene

Forfatter(e):

Bjarte Aksnes og Arnstein Vestad, KITH

Oppdragsgiver(e):

Nasjonal- IKT

KITH
INFORMASJONSTEKNOLOGI FOR HELSE OG VELFERD

Postadresse
Sukkerhuset
N-7489 Trondheim

Besøksaddresse
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:
82-7846-2844-4	11-05-2006			

Godkjent av:

Jacob Hygen, KITH

Rapportnr: 06/06

Sammendrag:

Denne rapporten er laget som et resultat av et forprosjekt for Nasjonal-IKT om PKI i helseforetakene. Kapittel 1 i rapporten oppsummerer de viktigste delene av rapporten og gir anbefalinger fra forprosjektet. Resten av rapporten gir utfyllende informasjon og bakgrunnsmateriale.

Innholdsfortegnelse

Innholdsfortegnelse 3

1. Oppsummering og anbefalinger 7

1.1. Behovet for PKI 7

1.2. Statusundersøkelse 8

1.3. SHDirs strategi for PKI-avtaler 9

1.4. Forslag fra forprosjektet til mulige løsninger og vedtak 10

1.5. Foreslått organisering og aktiviteter i PKI hovedprosjekt 11

1.6. Aktiviteter med rask oppstart i 2006 12

2. Bakgrunn og problemstilling for prosjektet 14

2.1. Bakgrunn for prosjektet 14

2.2. Problemstilling 14

3. Bakgrunnsinformasjon om PKI 17

3.1. Kort om PKI 17

3.2. Markedssituasjonen for PKI (pr. jan 2006) 19

3.3. Endringer som følge av at alle PKI-leverandører i markedet tilpasser seg Kravspesifikasjon for PKI i offentlig sektor 20

3.4. Sikkerhetsportalen 21

3.5. Finansieringsmodeller for PKI 22

3.6. Kostnader ved personlig PKI 23

4. Status for PKI i helseforetakene 26

4.1. Bruk av PKI på virksomhetsnivå 26

4.2. Bruk av PKI på personlig nivå 27

4.3. Bruk av PKI for kommunikasjon mot pasienter/pårørende 28

4.4. Bruk av PKI for Web Services 28

4.5. Bruk av dagens rammeavtale for PKI 28

4.6. Hindringer for PKI-utbredelse 29

4.7. Forventninger til framtidig PKI-løsning 30

5. Forslag til hovedprosjekt for PKI 31

5.1. Delmål 1: Å sikre fremdrift på PKI innføringen i spesialisthelsetjenesten 32

5.2. Delmål 2: Å sikre samordning av PKI i spesialisthelsetjenesten 32

5.3. Delmål 3: Å sikre konsistent nasjonal innføring 32

5.4. Framdriftstiltak 33

5.4.1. Oppfølging av PKI hovedprosjekt 33

5.4.2. Ny PKI-løsning for helsesektoren 34

5.4.3. Forberede løsning for personlig signatur i eResept 35

5.4.4. Følge opp innføring av HER 35

5.5. Samordningstiltak 36

5.5.1. Arbeidsgruppe for PKI i helseforetakene 36

5.5.2. Systemoversikt 36

5.5.3. Etablering av tekniske ekspertgrupper 37

5.5.4. Samordning med offentlig sikkerhetsportal 37

5.5.5. Vurdering av sikkerhetsnivå 37

5.6. Tiltak for å sikre konsistens 38

5.6.1. Informasjonsspredning 38

5.6.2. Dokumentere "best practice" for autentisering 38

5.6.3. Dokumentere "best practice" for personlig signatur 39

6. Vedlegg 1 – svar på statusundersøkelse 40

6.1. Helse Øst 40

6.1.1. Behov for PKI i helseforetaket 40

6.1.2. Dagens rammeavtale for PKI 42

6.1.3. Fremtidig PKI-løsning for helsesektoren 43

6.1.4. Annet 44

6.2. Helse Midt-Norge 44

6.2.1. Behov for PKI i helseforetaket 44

6.2.2. Dagens rammeavtale for PKI 47

6.2.3. Fremtidig PKI-løsning for helsesektoren 48

6.2.4. Annet 49

6.3. Helse Sør 50

6.3.1. Behov for PKI i helseforetaket 50

6.3.2. Dagens rammeavtale for PKI 51

6.3.3. Fremtidig PKI-løsning for helsesektoren 53

6.3.4. Annet 54

6.4. Helse Vest 55

6.4.1. Behov for PKI i helseforetaket 55

6.4.2. Dagens rammeavtale for PKI 56

6.4.3. Fremtidig PKI-løsning for helsesektoren 57

6.4.4. Annet..... 59

Referanseliste 60

1. Oppsummering og anbefalinger

1.1. Behovet for PKI

I foretaksmøter (og i protokollen fra disse) som ble avholdt i januar 2006 ble RHF-ene bedt om å arbeide med følgende knyttet til elektronisk samhandling:

- RHF Sør skal tilby sine samarbeidspartnere elektronisk epikrise i løpet av 2006, og legge til rette for mottak av elektroniske henvisninger i løpet av 2006/2007. Det skal legges til rette for standardisert infrastruktur og meldingsformat
- Helse Øst RHF + Helse Vest skal sikre at alle helseforetak kan tilby sine samarbeidspartnere elektronisk epikrise og kunne motta elektronisk henvisning i løpet av 2006.
- Helse Midt-Norge RHF skal sikre at alle helseforetak skal kunne motta elektronisk henvisning i løpet av 2006.
- Helse Nord RHF skal sikre at det stilles kompetanse til rådighet fra Nasjonalt senter for telemedisin for andre regionale helseforetak knyttet til implementering av elektronisk henvisning
- Alle RHF: Foretakene må planlegge og legge til rette for å etablere nødvendig infrastruktur for å kunne sende elektroniske resepter i tråd med de prosjektplaner som utarbeides i eResept-prosjektet, ledet av Sosial- og helsedirektoratet.

For å kunne tilby elektroniske epikriser og ta imot henvisninger på en standardisert måte må helseforetakene ta i bruk PKI med virksomhetssertifikater. Den samme løsningen vil også kunne benyttes for standardisert kommunikasjon av andre meldinger som fødselmelding, poliklinikkoppgjør (POLK), labsvar med mer.

Siden Norsk helsenett er å betrakte som et åpent nettverk der sensitiv informasjon ikke kan sendes i klartekst må alle sensitiv informasjon som sendes over nettet krypteres. *PKI-baserte løsninger vil være den eneste løsningen på dette som skalerer ift. det antall aktører som skal knyttes til nettet*. Uten PKI vil det være svært begrenset hva helsenettet kan benyttes til. Norsk Helsenett bør derfor ha en sentral rolle i det videre arbeidet med PKI. Spesielt i forhold til det å tilby virksomhetssertifikater bør Norsk Helsenett være sentral.

Personlige sertifikater har følgende hovedanvendelser i helseforetakene:

1. Det første anvendelsen er knyttet til **autentisering av enkeltpersoner til intern infrastruktur og tjenester/applikasjoner**. Her må lokale vurderinger av sikkerhetsbehov (risikovurderinger), arkitektur og kost/nytte avgjøre om og når man vil ta i bruk PKI for autentisering. Erfaringer fra St.Olavs og etter hvert Ahus vil gi nyttige innspill til andre HF som vurderer slike løsninger.
2. Den andre anvendelsen er knyttet til **personlig signering av dokumenter og meldinger**. Rikstrygdeverket har stilt dette som et krav ift. sykmelding og legeoppgjør, og det vil også være et krav for eResept. Innføring av PKI med personlige sertifikater vil derfor være nødvendig for å kunne sende slike meldinger.
3. Den tredje anvendelsen er knyttet til **personlig autentisering til eksterne tjenester**. Dette kan være tilgang til sentrale/regionale registre, publikumstjenester (pasientkommunikasjon) og lignende.

Oppsummert vil dette innebære følgende:

Virksomhetssertifikater må innføres i alle helseforetakene i løpet av 2006.

Innføring av personlige sertifikater for leger som skal sende eResept, sykmelding, legeoppgjør med mer må forberedes i løpet av 2007.

Innføring av personlige sertifikater for autentisering internt og eksternt må baseres på lokale vurderinger av aktuelle tjenester, sikkerhetsbehov og nytteverdi, samt sees i sammenheng med eResept.

Det største interessen for PKI i helseforetak er nå knyttet til autentisering og pålogging til systemer. Flere større helseforetak (St. Olav, Nye AHUS, Ullevål) er i ferd med å innføre eller planlegger å anskaffe PKI for sine ansatte. For autentisering og pålogging til systemer internt i helseforetakene kan det være tilstrekkelig med enklere og rimeligere løsninger enn nivå Høyt. Krav til sikkerhetsnivå for autentisering og pålogging til systemer må defineres konkret i forhold til situasjon og behov, ut fra en samlet risikovurdering hvor også andre elementer av informasjonssikkerhet må inngå.

1.2. Statusundersøkelse

Forprosjektet har gjennomført en statusundersøkelse og en workshop med deltagere fra alle regionene. I tillegg har vi samlet informasjon fra annet relevant arbeid. Hovedpunkter som er fremkommet er følgende (dette er nærmere beskrevet de påfølgende kapittel):

PKI på virksomhetsnivå er under utrulling i helseforetakene delvis som en konsekvens av pålegg ift. enkelte meldinger (fødselsmelding, POLK), og delvis som konsekvens av overgang til nye kommunikasjonsløsninger som baserer seg på bruk av ebXML rammeverket som benytter PKI. PKI på virksomhetsnivå benyttes pr. dato til kommunikasjon mellom helseforetak og primærleger og for innrapportering til nasjonale registre, og det er hovedsakelig virksomhetssertifikater anskaffet over

RTV's rammeavtale som benyttes. For andre typer meldinger er det identifisert få konkrete prosjekter iverksatt og det vil være en utfordring for foretakene å løfte eksisterende kommunikasjonsløsninger over på ny plattform i et samordnet løp.

For meldinger med *personlig signatur* er det oss bekjent per januar 2006 ingen HF/RHF som arbeider *aktivt* med å implementere dette. Den eneste aktuelle anvendelsen har til nå vært sykmelding til RTV, og uten eksterne pålegg har HF/RHF'ene ikke på egenhånd iverksatt aktiviteter for å implementere dette. eResept-prosjektet er ennå i en fase hvor det ikke er stilt konkrete krav for foretakene på PKI-området, men det forventes at løsningen vil kreve personlig signatur. Det er ikke kjent at HF-ene har iverksatt aktiviteter for å forberede slike løsninger.

For PKI til *autentisering* har til nå ett større foretak (St. Olavs Hospital HF) tatt dette i bruk i stor skala, mens Nye Ahus er i en planleggingsfase med sikte på å implementere dette i løpet av 2006. Å ta i bruk PKI på dette området krever en omfattende planlegging og tilpassing av lokal infrastruktur som til nå bare prosjekter som allerede har planer om omfattende endringer har gått inn på. Flere HF benytter likevel PKI til autentisering knyttet til pålogging for hjemmekontor og mobile løsninger. Dette er fortrinnsvis basert på lokale PKI-løsninger med lokal sertifikatutstedelse. Det er uklart om slike løsninger vil kunne benyttes for eksempel ift. eResept.

På nasjonalt plan er det etablert en felles offentlig sikkerhetsportal. Denne portalen er ment å skulle dekke offentlig sektors behov for tjenester innenfor autentisering og signatur. Til nå har prosjektet hatt fokus på å tilby tjenester for pålogging til websider, og prosjektet har derfor primært interesse ift. å legge til rette for publikumstjenester og kommunikasjon med pasienter og pårørende. Per januar 2006 ble det ikke identifisert at noen HF/RHF iverksatt aktiviteter på dette området.

1.3. SHDirs strategi for PKI-avtaler

Samtidig som prosjektdirektivet ble utarbeidet, gjennomførte SHDir en prosess rundt strategi for videre PKI-avtaler for helsesektoren. Helsesektorens avtale med Ergo utløper fra og med 1.6.2006 og helsevesenet står da uten sentral rammeavtale for PKI. Deltagere fra forprosjektet var involvert også i dette arbeidet. Hovedkonklusjonen fra dette arbeidet ble:

- Slik markedsutviklingen nå er på PKI-området, og i lys av sentrale tiltak for offentlig forvaltning, foreslås ikke en sentral rammeavtale for helsevesenet. I stedet utarbeides det en felles nasjonal kravspesifikasjon for PKI i helsesektoren, som bygger på, presiserer og supplerer Kravspesifikasjon for PKI i offentlig sektor og SEID-standardene.

- De enkelte brukersegmentene (f.eks. RHF-ene) kan velge å kjøre felles anbudsprosesser og etablere felles rammeavtaler med utgangspunkt i en sentral kravspesifikasjon.
- Planlagt anbudsprosess for PKI-tjenester til Nye AHUS utformes slik at det kan inngås en rammeavtale for helseforetakene (ansattsertifikater, og person høyt og virksomhetssertifikat).
- En felles kravspesifikasjon for PKI-tjenester til helsevesenet må sikre behov for samhandling og kontinuitet i løsninger, og presisere krav til støtte for lokal signering og kryptering for meldingsutveksling, grensesnitt mot lokale systemer, og evt. funksjonelle krav til PKI-tjenester.
- Legekontor og andre mindre helseaktører kan gjøre direkte kjøp av PKI i markedet med utgangspunkt i sentrale krav, og må forholde seg til de sertifikattilbydere som EPJ-leverandørene samarbeider med og som tilfredsstiller kravene.
- Det vurderes om Norsk Helsenett i fremtiden kan være utsteder eller videreformidler av virksomhetssertifikat til bruk for elektronisk kommunikasjon over Helsenettet.
- En felles kravspesifikasjon må forankres både i spesialisthelsetjenesten (gjennom Nasjonal IKT) og primærhelsetjenesten (ELIN-prosjektene), og må dekke kravene for eResept. Kravspesifikasjonen kan eventuelt forvaltes som en standard under samordnings- og standardiseringsprogrammet på KITH. Det langsikte målet bør kanskje være at FADs sentrale kravspesifikasjoner for PKI fullt ut ivaretar helsevesenets felles krav til PKI.

SHDir's arbeide konkluderte også med at Nasjonal IKT bør gjennomføre et hovedprosjekt for PKI som beskrevet i denne rapporten.

1.4. Forslag fra forprosjektet til mulige løsninger og vedtak

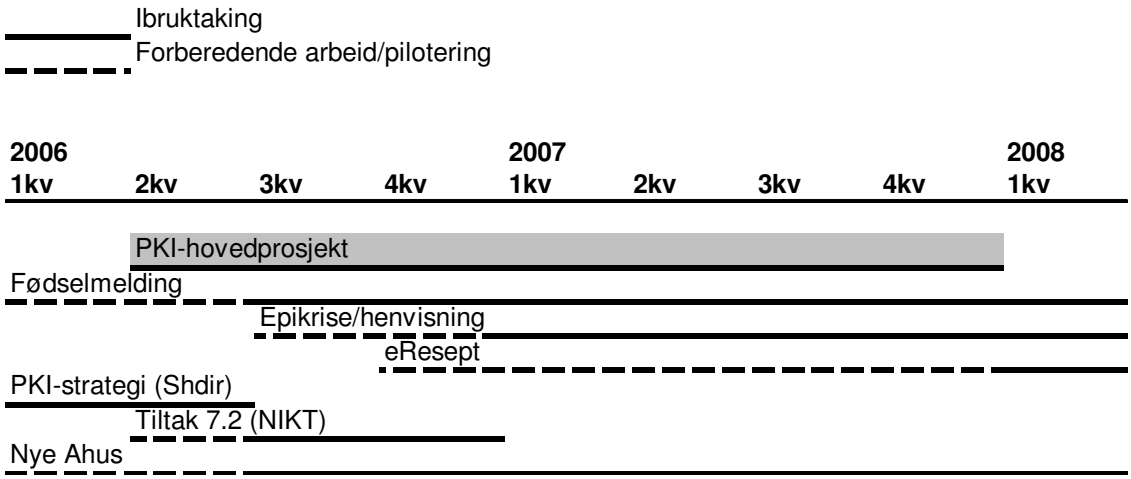
Med bakgrunn i disse utfordringene og med utgangspunkt i de nevnte igangsatte aktivitetene, samt flere andre aktiviteter er det et klart behov for samordning, erfaringsutveksling og oppfølging for å sikre at løsningene er konsistente og gjenbrukbare. For å sikre dette foreslås det at Nasjonal-IKT igangsetter et hovedprosjekt med følgende mulige hovedmål:

Å sikre samordning, fremdrift og konsistent nasjonal innføring av PKI i spesialisthelsetjenesten gjennom et nasjonalt samarbeid for oppfølging, erfaringsnettverk og kunnskapsformidling mellom øvrige tiltak.

Forprosjektet foreslår at mulige resultatmål som nås innen 2007 kan være:

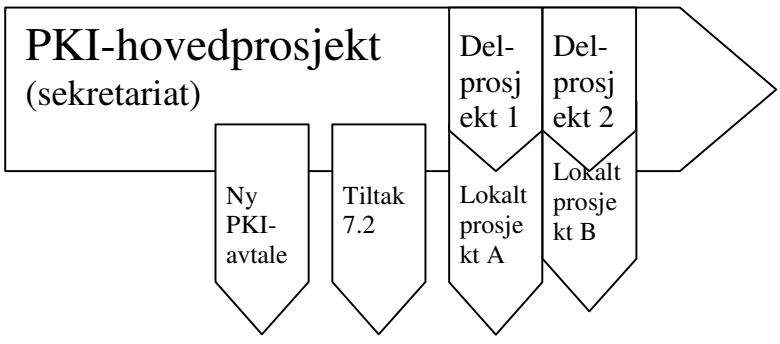
- Alle helseforetakene skal ha tatt i bruk virksomhetssertifikater for meldingskommunikasjon innen 1.8.2006
- I løpet av første halvår 2006 skal det for hver av EPJ-leverandørene være igangsatt minst ett prosjekt for å forberede signering av meldinger med personlig signatur i eResept.
- I løpet av 2007 skal alle regioner ha testet ut og klargjort løsning for signering av eResept med personlig signatur i egen infrastruktur.
- Minst 2 større helseforetak skal i løpet av 2007 ha innført autentisering ved hjelp av PKI for store grupper av ansatte.

- Innføre PKI-baserte løsninger for identitetshåndtering og autentisering i utvalgte anvendelser som publikumstjenester, mobile løsninger og tjenester for informasjonsdeling.



1.5. Foreslått organisering og aktiviteter i PKI-hovedprosjekt

Figuren viser forholdet mellom hovedprosjektet, nasjonale aktiviteter og ulike innføringsprosjekter (eksemplifisert ved lokalt prosjekt A, B). Innenfor hovedprosjektet vil det også være delprosjekter som skal bistå de lokale prosjektene.



Sentrale aktiviteter for prosjektet vil være:

1. Felles aksept av behov for PKI
2. Samarbeid med nye Ahus om løsninger for autentisering som kan spres i sektoren
3. Delta i arbeide med PKI-strategi for helsevesenet (denne aktiviteten er allerede igangsatt).
4. Forberede implementering av eResept i HF-ene
5. Oppfølging av implementeringen av virksomhetssertifikater

I forhold til alle disse aktivitetene må det kjøres lokale/regionale innføringsprosjekt med en tett og ***forpliktende*** kontakt med PKI-hovedprosjektet. Hovedprosjekt for PKI skal følge opp det enkelte prosjekt med rådgivning og samordningsaktiviteter for å sikre at PKI tas i bruk og integreres på en kostnadseffektiv, hensiktsmessig og mest mulig ensartet måte i de ulike foretakene.

Det må også opprettes et sekretariat (inkludert prosjektledelse) og en PKI-prosjektgruppe med deltagere fra HF-ene som m.a. vil ivareta følgende:

- kontakt/rådgivning ift. regionale/lokale prosjekter med behov for PKI-løsninger
- spre informasjon om aktuelle strategier og løsninger
- utarbeide dokumentasjon (m.a. ”best practice”)
- kontakt/oppfølging av andre relevante prosjekt som HER-mottaksprosjekt, offentlig sikkerhetsportal, Tiltak 7.2. med mer
- eventuelt opprette tekniske prosjektgrupper
- arrangere prosjektmøter og ev. workshops
- gjennomføre utredninger og gi anbefalinger

1.6. Aktiviteter med rask oppstart i 2006

Det er i forrige avsnitt og videre i kapittel 5 mer detaljert beskrevet en rekke tiltak vi mener er nødvendig for å oppnå prosjektets overordnede målsetninger i løpet av 2-3 år. Vi vil i dette kapitlet spesielt trekke frem noen tiltak som vi mener er et *minimum* og som må iverksettes umiddelbart for å ikke tape tid og unngå dobbeltarbeid ved å henge seg på prosesser som allerede er i gang. Dette er følgende tiltak:

Videreføre arbeidsgruppen for PKI

I forprosjektet ble det samlet en gruppe med god innsikt i PKI-området. Vi anbefaler at denne gruppen videreføres slik at RHF/HF-ene har en gruppe med kompetanse og innsikt i PKI som kan benyttes som ressursgruppe for lokale og nasjonale PKI-aktiviteter. Det bør også etableres et sekretariat i tilknytninug til gruppen.

Samarbeid med Nye-Ahus om rammeavtale og implementering av løsninger

Ahus er i gang med å inngå en rammeavtale for PKI som kan benyttes av alle HF/RHF. Dette arbeidet krever involvering fra andre for å sikre at avtalen er kjent og kan benyttes av andre HF. Det vil og være viktig å ta del i de erfaringer som Ahus gjør når de skal ta i bruk løsningene. Deler av arbeidsgruppen beskrevet under forrige punkt kan ivareta dette.

Vurdering av HF-enes interne behov

I regi av arbeidsgruppen bør det utarbeides et beslutningsgrunnlag for enklere å kunne avgjøre gevinster og ulemper ved innføring av PKI. Det bør pekes på ulike interne behov for PKI med anbefalinger om når eventuell innføring bør vurderes.

Samarbeid med tiltak 7.2 for etablering av sikkerhetspolicy

NIKT har igangsatt tiltak 7.2 som skal utarbeide en sikkerhetspolicy for HF-ene. Dette innebærer også en policy for PKI. Gruppen forutsetter at "PKI-prosjektet" deltar under utarbeidingen av PKI-policyen og denne aktivitetene må derfor gå parallelt med tiltak 7.2, og må starte før sommeren 2006.

2. Bakgrunn og problemstilling for prosjektet

Dette kapittelet gir bakgrunnen for at det ble startet et PKI-forprosjekt, samt peker på noen av de problemstillinger som et hovedprosjekt må ta fatt i.

2.1. Bakgrunn for prosjektet

Styringsgruppen for Nasjonalt helsenett besluttet i møte 22. januar 2004 å etablere en PKI-gruppe. Denne gruppen utarbeidet en utrullingsplan for PKI i helseforetakene som ble behandlet i Nasjonal IKT Styringsgruppemøte 05. november 2004. Vedtaket innbefattet at Nasjonal IKT sluttet seg til den foreslåtte strategien for utrulling av PKI i helseforetakene og forslaget til organisering av et utrullingsprosjekt som et nytt tiltak under Nasjonal IKT.

PKI-arbeidet i spesialisthelsetjenesten har til nå vært preget av manglende koordinering og styring. Enkelte aktiviteter er iverksatt som følge av offentlige pålegg (fødselsmelding), andre aktiviteter med bakgrunn i interne behov (autentisering). For personlig signatur har manglende pålegg og sviktende økonomiske incentiver hindret aksept og bruk av PKI. Med bakgrunn i dagens status er det behov for et prosjekt for å sikre oppfølging, erfaringsnettverk og kunnskapsformidling mellom prosjekter som tar i bruk PKI i spesialisthelsetjenesten.

Det ble derfor i Desember 2005/Januar 2006 gjennomført et forprosjekt for å utarbeide et prosjektdirektiv. Arbeidet ble gjennomført med prosjektledelse fra KITH AS, og det ble avholdt en workshop med representanter fra helseregionene for å beskrive aktiviteter og omfang av hovedprosjektet. Prosjektet utarbeidet et prosjektdirektiv for et hovedprosjekt, samt denne prosjektrapporten.

2.2. Problemstilling

I rapporten ”Nasjonal strategi for elektronisk pasientjournal” fra SHdir anbefales meldingsutveksling som hovedstrategi for informasjonsutveksling i helse- og omsorgstjenesten. Strategien sier også at det

bør stilles krav til bruk av standard formater og "transportkonvolutt" (ebXML-rammeverk) for meldingsutveksling over Norsk Helsenett. Denne strategien innebærer at alle helsevirksomheter som skal utveksle helseinformasjon elektronisk må ta i bruk PKI-løsninger, som et minimum med bruk av virksomhetssertifikater.

Innføring av eResept vil trolig kreve at alle foreskrivere har mulighet for digital signering med personlig signatur, slik det også kreves for sykmelding. Slike løsninger må ha et minimums sikkerhetsnivå og være basert på standarder. Det blir derfor viktig å samordne og koordinere ulike aktiviteter som skal forberede innføringen av eResept i HF og ha en tett dialog med eResept-prosjektet om hvilke krav som vil stilles.

Nye Ahus har planer om å innføre en PKI-løsning for alle sine ansatte i det nye sykehuset. Dette vil trolig bli den hittil største PKI installasjonen, i tillegg til St. Olavs, innen helsesektoren. Det blir derfor svært viktig at sektoren kan dra nytte av disse prosjektene ved å gjøre det mulig å gjenbruke avtaler, løsninger og erfaringer fra disse prosjektene. Det bør også sikres at løsningene som velges er i tråd med nasjonale anbefalinger på området.

Nasjonal IKT har planlagt Tiltak 7.2 – som har som mål å utarbeide et overordnet styringssystem for informasjonssikkerhet for de regionale helseforetakene/helseforetakene og Norsk Helsenett AS. Styringssystemet skal ta utgangspunkt i bransjenormen for informasjonssikkerhet og de eksisterende styringssystem. I dette prosjektet skal det også utarbeides retningslinjer for bruk av PKI. Prosjektet har planer om å samarbeide med "PKI-hovedprosjektet" om denne leveransen. Tiltak 12 på systemarkitektur vil også ha flere grenseflater mot dette prosjektet.

RTV's rammeavtale for PKI, som til nå har vært benyttet for sertifikater på virksomhetsnivå og for personlige signaturer, løper ut i januar 2007, og SHdir har initiert en prosess for å utarbeide strategi for hvordan helsevesenet skal forholde seg til utviklingen i markedet for PKI-tjenester. Gruppen skal drøfte mål og ambisjonsnivå for koordinering av PKI-arbeidet i helsesektoren og vurdere alternative strategier i forhold til dette. Mens den eksisterende løsningen primært var lagt til rette for fastlegene, må helseforetakene sikre at deres behov ivaretas i en ny ordning. En tett involvering av helseforetakene i dette arbeidet vil derfor være nødvendig. Arbeidsgruppen vil legge frem forslag til strategi i mars i 2006.

Styringsgruppen for Norsk helsenett besluttet i møte 22. januar 2004 å etablere en PKI-gruppe. Denne gruppen utarbeidet en utrullingsplan for PKI i helseforetakene som ble behandlet i Nasjonal IKT Styringsgruppemøte 05. november 2004. Vedtaket innbefattet at Nasjonal IKT sluttet seg til den

foreslåtte strategien for utrulling av PKI i helseforetakene og forslaget til organisering av et utrullingsprosjekt som et nytt tiltak under Nasjonal IKT.

Statusundersøkelsen tyder på at PKI-arbeidet i spesialisthelsetjenesten til nå har vært preget av manglende koordinering og styring. Enkelte aktiviteter er iverksatt som følge av offentlige pålegg (f.eks. fødselsmelding), andre aktiviteter med bakgrunn i interne behov (for eksempel ift. autentisering). For personlig signatur har manglende pålegg og mangel på økonomiske incentiver hindret aksept og bruk av PKI.

3. Bakgrunnsinformasjon om PKI

Dette kapittelet oppsummerer dagens markedssituasjon for PKI, mulighetene som ligger i etableringen av en felles offentlig sikkerhetsportal og gir en oversikt over kostnader og finanseringsmodeller knyttet til PKI.

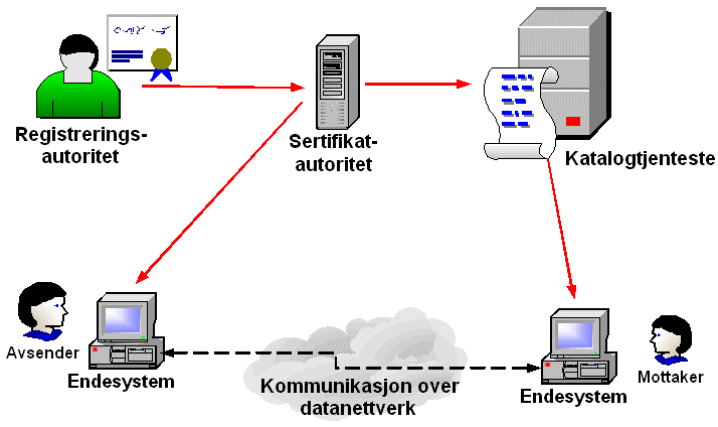
3.1. Kort om PKI

PKI står for Public Key Infrastructure og er en løsning for blant annet elektronisk signatur og elektronisk legitimasjon. PKI benyttes for å kunne kommunisere på en sikker måte over usikre nett slik som Internett. Det benyttes offentlige og private nøkler som er ervervet og delt gjennom en tiltrodd tredjepart.

Innenfor helsevesenet finnes det flere behov for sikker elektronisk kommunikasjon. Gjennom rikstrygdeverket (RTV) ble det derfor i 2003 etablert en rammeavtale for PKI-tjenester i helsesektoren med tanke på kommunikasjon av elektroniske meldinger.

Avtalen som forvaltes av RTV er utarbeidet for å sikre en trygg infrastruktur for elektronisk kommunikasjon i helseektoren, og som kan gjøre det mulig å kommunisere på tvers av helseforetak, virksomheter og enkeltaktører på en sikker måte.

PKI er en infrastruktur som består av flere ulike deler. Et generelt system for PKI består gjerne av følgende deler (se figuren):



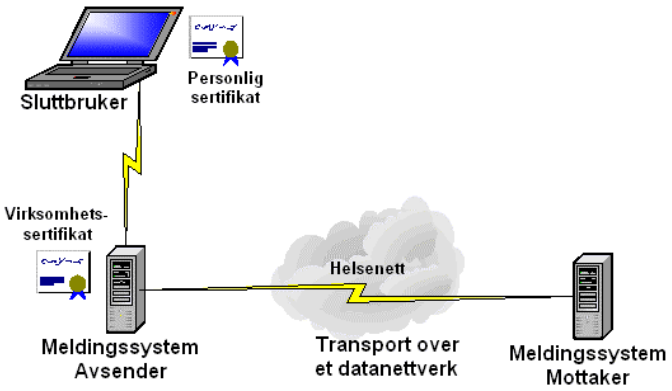
1) En sertifiseringsautoritet (SA) som utsteder og verifiserer digitale sertifikater
2) En registreringsautoritet (RA) som verifiserer opplysninger som skal inngå i et sertifikat før det utstedes
3) Katalogtjenester som tilgjengeliggjør sertifikatene
4) Endesystemer som gjør bruk av sertifikatene for ulike sikkerhetstjenester (f.eks. kryptering, autentisering, ikke-benekting/signering)

For helsevesenet er to hovedtyper av sertifikater som er aktuelle: personlige sertifikater og virksomhetssertifikater.

Personlige sertifikater er som navnet tilsier knyttet til deg som person og benyttes av den enkelte for å signere digitalt, legitimere deg overfor nett-tjenester osv. Personlige sertifikater kreves når et er du som person som skal signere noe elektronisk.
Virksomhetssertifikater knyttes til virksomhet, og er primært tenkt brukt til å sikre kommunikasjon inn og ut av en virksomhet, særlig ift. elektroniske meldinger. Virksomhetssertifikatet installeres typisk på en server, f.eks. i en kommunikasjonsløsning i et sykehus eller på et legekontor, og benyttes til å signere og kryptere/dekryptere elektroniske meldinger som kommer inn.

En viktig del av et PKI-system er å sikre at sertifikater er gyldige. Sertifikater må derfor fornyes med jevne mellomrom (eksempelvis hvert 2. år). Dette gjelder både for virksomhets- og personlige sertifikat, og om sertifikatet er på et smartkort eller det ligger på en PC/server.

Det må også finnes rutiner for å kunne trekke tilbake (revokere) sertifikater når det er behov for det.



3.2. Markedssituasjonen for PKI (pr. jan 2006)

Markedet for PKI-tjenester i Norge er under stadig utvikling, og det er vanskelig å spå hvordan markedet vil fortone seg framover. Noen viktige hendelser den siste tiden er særlig etableringen av en felles sikkerhetsportal for offentlige tjenester og en felles kravspesifikasjon for PKI i offentlig sektor.

Med BBS's oppkjøp av ZebSign som m.a. utsteder sertifikater for Norsk Tipping, kontrollerer BBS de to største leverandørene av PKI-sertifikater: BankID og ZebSign. ZebSign-sertifikatene benyttes i dagens rammeavtale for helsesektoren, men med Ergo som leverandør.

Ergo har signalisert at den utrullingstakten som har funnet sted under dagens rammeavtale ikke har vært tilstrekkelig til å gi en lønnsom avtale for dem. Særlig den manglende utrullingen av personlige sertifikater til helseforetakene har medført at avtalen ikke har levd opp til forventningene verken fra leverandør eller brukersiden. Ut fra disse signalene er det naturlig å anta at det vil være vanskelig å inngå en ny rammeavtale som ikke gir forpliktelser på avrop.

At PKI-aktører kan knytte seg til den offentlige sikkerhetsportalen og dermed gi sine brukere tilgang til et etter hvert forhåpentligvis bredt sett med offentlige tjenester kan bidra til å øke aktiviteten på PKI-området og gjøre det mer attraktivt å lansere PKI-tjenester, men dette blir en antakelse.

Sertifikater utstedes med ulike sikkerhetsnivå og baserer seg på ulike tekniske løsninger. Noen andre sentrale aktører på PKI-markedet nasjonalt er:

- BankID: Utsteder sertifikater til bruk for pålogging til nettsteder og elektronisk signatur. Tilbyr tjenester for det samme, basert på en nett-tjeneste, dvs. at bl.a. signatur forutsettes å skje via web-grensesnitt.
- Sertifikater på nivå Person-Standard fra sikkerhetsportalen: BBS, leverandør av sikkerhetsportalen, skal også levere sertifikater av nivå Person-Standard. Dette er software-sertifikater den enkelte bruker kan laste ned i sin nettleser, basert på å autentisere seg selv med en pin-kode fra selvangivelsen eller lignende.

Internasjonalt er det en rekke aktører som utsteder PKI-sertifikater og tilbyr PKI-tjenester. Deres tilbud er varierte, alt fra salg av sertifikater til komplette pakker for PKI-håndtering i en virksomhet. En hovedutfordring med internasjonale aktører er at de sjelden har de nødvendige lokale forutsetningene for å fylle krav til bl.a. personlig oppmøte ved utstedelse osv., krav som stilles til utstedelse av sertifikater på nivå Person-Høyt. Men også for lavere nivåer vil det være utfordringer knyttet til å opprettholde et sikkerhetsnivå som vil være akseptabelt for kommunikasjon av sensitive opplysninger.

3.3. Endringer som følge av at alle PKI-leverandører i markedet tilpasser seg Kravspesifikasjon for PKI i offentlig sektor

Rikstrygdeverkets rammeavtale med Ergo for levering av PKI-sertifikater til helsesektoren utløper 15. januar 2007. Alle utstedere av sertifikater i markedet tilpasser seg nå Fornyingsdepartementets sentrale kravspesifikasjon for PKI fra 1.6.06. Selv om det dreier seg om små justeringer i sertifikatprofil, får det uansett konsekvenser for de PKI-løsningene som hittil er implementert på legekontor. Det skjer også endringer i grensesnitt mot applikasjoner og smartkort.

Det er inngått endringsavtale mellom RTV og Ergo, som bl.a. innebærer at

- Alle sertifikater som er utstedt før 1.6.2006 vil fortsatt være gyldige ut levetiden på 2 år, men Ergo vil fra 15.1.07 stoppe support på integrasjonsverktøyet EnablePKI som har vært benyttet av systemleverandørene for etablering av løsninger for signering av sykmelding og kryptering av elektronisk konvolutt (ebXML).
- Ergos forpliktelser for levering av nye sertifikater etter 1.6.06 bortfaller.
- Det vil ikke bli utstedt softwaresertifikater på nivå person høyt etter 1.6.06. Slike sertifikater er i dag i bruk på mange legekontor.

Konsekvensene av endringene er at

- Fra 1.6.06 må alle nye brukere av PKI (legekontor og andre) og tidligere brukere som har sertifikater som må fornyes, ha tilpasset sine lokale systemer (EPJ- og meldingssystemer) til ny sertifikatprofil og nye integrasjonsgrensesnitt. Dette er et utviklingsarbeid som må gjøres av legekontorenes systemleverandører.
- Fra 15. januar 2007 må alle de som har tatt i bruk PKI med "gammel" sertifikatprofil og integrasjonsprogrammet EnablePKI ha lagt om systemene sine til ny sertifikatprofil og nye grensesnitt (gjelder så godt som alle legekontor som benytter PKI).

Samtidig skjer det en utvikling i PKI-markedet. Det finnes markedsløsninger for sertifikater som tilfredsstiller krav til personsertifikater nivå høyt i Fornyingsdepartementets Kravspesifikasjon for PKI i offentlig forvaltning, og med mer åpent grensesnitt mot lokale systemer, lengre levetid (3 år), samt forenklede bestillings- og vedlikeholdsrutiner i forhold til eksisterende rammeavtale.

Rikstrygdeverket vil tilpasse sine systemer for å støtte nye godkjente PKI-løsninger i det norske markedet senest fra 1.6.06. I en overgangsperiode, så lenge gamle sertifikater er gyldige, må Rikstrygdeverket støtte både gamle og nye PKI-løsninger som tilfredsstiller kravene.

3.4. Sikkerhetsportalen

Sikkerhetsportalen er en tjeneste som skal brukes av offentlige brukersteder for å sikre felles tjenester som autentisering og "single sign-on" mellom brukerstedene. Etter hvert vil tjenesten også støtte for eksempel signering og arkivering av dokumenter.

Sikkerhetsportalen er ment som et kostnadseffektivt alternativ til at de ulike offentlige etatene selv utvikler og drifter nødvendige sikkerhetstjenester for bl.a. autentisering. Portalen baserer seg på å videreformidle identitetsinformasjon fra eksisterende PKI-leverandører som allerede er etablert med brukermasser. Dette gjør at den enkelte etat ikke må bygge opp en egen brukerdatabase, sørge for sikker distribusjon av påloggingsmekanismer, lage sikre mekanismer for å håndtere glemte passord, og andre slike funksjoner som er nødvendig for en sikker brukerhåndtering. For borgeren/brukeren av tjenestene vil det også oppleves som bedre at alle offentlige etater har et felles grensesnitt for pålogging.

Integrasjon av flere sentrale PKI-leverandører i portalen skal gjøre det mulig å verifisere en brukers elektroniske signatur eller identitet/pålogging uten at den enkelte etat/kommune må etablere avtaler med flere PKI-leverandører og integrere deres løsninger i sin egen tjeneste. Brukeren vil i utgangspunktet kun forholde seg til PKI-leverandøren ved anskaffelse av sin PKI-tjeneste. Ved bruk av tjenester som Min Side vil påloggingsfunksjonaliteten håndteres av sikkerhetsportalen.

Sikkerhetsportalen skal på sikt tilby et vidt spekter av PKI-relaterte tjenester, men er foreløpig begrenset til autentisering til et nettsted. Løsninger for signatur er under utvikling, men det er uklart hvorvidt disse vil dekke helsesektorens behov for funksjonalitet knyttet til signatur. Hovedfokuset for sikkerhetsportalen har vært autentisering for pålogging til et nettsted.. Den samme teknologien er ennå ikke tilpasset behovene knyttet til autentisering internt i virksomheter, særlig pålogging til operativsystem og lokale applikasjoner.

Sikkerhetsportalen dekker i dag ikke helsevesenets krav til PKI for sikring av elektronisk meldingsutveksling, med lokal signering og kryptering internt før meldingen sendes ut fra virksomheten. Ved slik bruk er det kun tilgang til katalogtjenester for validering av sertifikater som kan være aktuelle tjenester fra Sikkerhetsportalen. Både signatur i fagsystemer og mekanismer for autentisering og pålogging til systemer må fungere i et lokalt sikkert miljø, med garantert tilgjengelighet. Det er også usikkert om forretningsmodellen for Sikkerhetsportalen er et egnet konsept for å håndtere store volumer av meldinger mellom profesjonelle aktører internt helsetjenesten.

Hvordan sikkerhetsportalen skal tilby tjenester for elektronisk signatur, virksomhetssertifikater osv. er ennå uklart.

3.5. Finansieringsmodeller for PKI

Ved innføring av PKI-løsninger er det kostnader knyttet til selve innføringen og til driften/bruken av løsningen.

Etableringskostnader knytter seg til:

- Anskaffelse av sertifikater til brukergruppen
- Tilpassing av egne tjenester til bruk av PKI
- Utstedelse og utlevering av sertifikater/smartkort
- Opplæring av brukere

Driftskostnader knytter seg til:

- Drift av tjenester for sertifikatvalidering og katalogtjenester
- Eventuelle transaksjonskostnader ved bruk av PKI-tjenester, som f.eks autentisering og signering
- Brukerstøtte
- Re-utstedelse av tapte sertifikater/kort

Leverandører av PKI-tjenester har basert seg på ulike modeller for å dekke sin del disse kostnadene. Rammeavtalen for PKI i helsesektoren har basert seg på at den enkelte kjøper av sertifikat betaler fast pris for sertifikatet, og har fri bruk av dette i ettertid. Andre PKI-tjenester i markedet baserer seg på en transaksjonsprising der det betales for bruk av sertifikatet.

Bruken kan betales av sertifikatinnehaver eller mottaker.

Selv om selve kostnaden knyttet til PKI kan knyttet til enten anskaffelse eller bruk, må ikke dette ha sammenheng med hvem som ”betaler” for tjenesten. En løsning hvor bruk av sertifikatene er fri forutsetter ikke at sertifikatinnehaver må betale for PKI-løsningen, og en løsning hvor det betales pr. transaksjon/bruk forutsetter ikke at nødvendigvis bruker eller sertifikatmottaker må betale for den enkelte transaksjon.

Ulike anvendelser av PKI vil ha ulik effekt av de ulike betalingsmodellene. Ved høy bruk vil det være lønnsomt med frikjøp av sertifikater (engangskostnad), men sett ift. den enkelte anvendelse vil dette

variere. For anvendelser med lavt bruk vil det være rimeligere å betale for et lite antall transaksjoner. Anvendelser med hyppig bruk vil tjene på en modell med frikjøp. En ulempen med transaksjonsprising er uoversiktlighet ift. den totale kostnaden knyttet til den enkelte tjeneste. En tjeneste som blir uventet populær kan medføre at tjenesten må nedlegges pga. manglende finansiering.

En fast pris for PKI-løsningen medfører at den som betaler for løsningen løper risikoen knyttet til investeringen og hvorvidt denne vil lønne seg. Med transaksjonsprising kan noe av denne risikoen flyttes over på PKI-leverandøren. Hvis risikoen knyttet til gevinstrealiseringen er høy vil dette kunne være fornuftig, da leverandøren kan fordele sin risiko over flere kunder. Hvis risikoen knyttet til gevinstrealiseringen er mindre vil forutsigbarheten ved en fastpris være av større betydning. For sektoren samlet vil en felles satsning på PKI da gjøre det mer økonomisk å basere seg på en fastprismodell.

For PKI anvendt til pålogging på interne systemer vil antallet transaksjoner komme opp i så høye tall at transaksjonsprisen må bli meget lav for at dette skal lønne seg. Det kan også være tekniske utfordringer knyttet til å legge funksjoner for telling/transaksjonsprising inn i virksomhetskritiske påloggingssystemer, særlig hvis dette forutsetter kommunikasjon mot en sentral part utenfor det enkelte foretak. St.Olavs eksempel med sertifikater av samme type som utstedt under RTV's rammeavtale, men anskaffet fra en annen leverandør understreker muligheten for reduserte priser når det garanteres et visst omfang på anskaffelsen.

3.6. Kostnader ved personlig PKI

Arbeidsgruppen som utarbeidet forslag til utrullingsplan for PKI i helseforetakene i 2004 vurderte to ulike alternativer for kostnader knyttet til personlig PKI:

1) Personlige sertifikater anskaffes til en begrenset brukergruppe, i første omgang leger, som har behov for å signere sykmeldinger og elektroniske resepter.
2) Personlige sertifikater, basert på rammeavtalen, til alle ansatte, som felles løsning for pålogging og autentisering, og for ekstern kommunikasjon.

Forutsetninger for kostnadsanslagene:

- eksempel for sykehus med 2500 ansatte, hvorav 300 leger/andre med behov for personlig signatur (12 %)
- det antas at helseforetak oppnår 30 % rabatt på innkjøp av sertifikater over rammeavtalen med Ergo
- integrasjonskostnadene er ikke anslått, men det antas at begge alternativene krever samme integrasjon i fagsystem og kommunikasjonsløsning

	Alternativ 1: begrenset brukergruppe	**Alternativ 2: kvalifisert sertifikat til alle ansatte**
Initialkostnader:		
kjøp av personsertifikat (smartkort)	300*399 = 119.700	2500*399 = 997.500
smartkortlesere til alle terminaler (antatt 500)	500x170 = 85.000	500*170 = 85.000
Integrasjon i fagsystem	felles	felles
Integrasjon i kommunikasjonsløsning	felles	felles
Enkel brukerveiledning	30.000	30.000
Utrulling/installasjon	½ årsverk (2 t x 500)	1 årsverk
Sum initialkostnader (utenom integrasjon)	**234.700**	**1.112.500**
Driftskostnader:		
- fornyelse av sertifikater	150*399: ca. 60.000	1250*399: ca. 500.000
- erstatning av tapte kort/sertifikater	(300*399)*0,12/2= ca. 6.000	ca. 50.000

For alternativ 1:

Dersom foretaket i tillegg trenger en intern løsning for tilgang til systemer (f.eks. single sign-on) vil foretaket i tillegg har kostnader til intern sertifikatkatalog og sertifikatutstedelse, og eventuelle tilleggsmoduler i PKI-systemet som må installeres på klienter.

For mange virksomheter kan det bli nødvendig å oppgradere maskinparken. Hvis foretaket har oppgradert maskinpark med bare Windows XP, vil jobben være mindre.

En del av disse kostnadene er knyttet til hardware-kostnader, særlig til utstedelse av smartkort. Priser for anskaffelse av dette avhenger i stor grad av volum.

4. Status for PKI i helseforetakene

Som en del av forarbeidet for utarbeidelsen av prosjektdirektivet ble det gjennomført en statusundersøkelse av bruk av PKI-løsninger i helseforetakene. Undersøkelsen ble gjennomført i desember 2005/januar 2006 og resultatene baserer seg på utfylte spørreskjema som er besvart av hhv.:

- Helse Sør
- Helse Midt
- Helse Øst v. AHUS
- Helse Vest (Helse Vest IKT på vegne av Helse Vest)

Det er også tatt hensyn til kommentarer framkommet på workshop gjennomført av forprosjektet 12. januar 2006.

Statusrapporten må anses som delvis dekkende, da deltagerne har rapportert at de pga. kort tidsfrist ikke har kunnet gjøre mer omfattende undersøkelser i egen virksomhet, særlig omkring framtidige planer og ift. behov for ny PKI-løsning.

4.1. Bruk av PKI på virksomhetsnivå

PKI på virksomhetsnivå er på full fart inn i helseforetakene delvis som en konsekvens av pålegg ift. enkelte meldinger (fødselsmelding, POLK), og delvis som konsekvens av etablering/utskifting av kommunikasjonsløsninger og innføring av nye meldinger hvor det er naturlig å basere seg på ny sikkerhetsløsning. PKI på virksomhetsnivå benyttes til kommunikasjon mellom helseforetak og primærleger og for innrapportering av elektroniske meldinger, og det er virksomhetssertifikater anskaffet over RTV's rammeavtale som benyttes.

- Nye Ahus planlegger å benytte virksomhetssertifikat(er) i forbindelse med meldinger til andre helseforetak, offentlige myndigheter, primærhelsetjenesten
- Alle helseforetakene i Helse Sør skal benytte virksomhetssertifikater til utveksling av fødselsmeldinger og svangerskapsavbrudd.
- I Helse Midt er det iverksatt pilotprosjekt på henvisninger og som benytter PKI. Fødselsmeldinger er søkt utsatt, men vil starte ila 1. halvår 2006. POLK kommer.

- I Helse Vest skal sertifikater fra rammeavtalen for PKI benyttes til POLK og fødselsmelding, tidsplan sommeren 2006.

4.2. Bruk av PKI på personlig nivå

PKI på personlig nivå har tre hovedanvendelser i helseforetakene:

- Signering av meldinger med krav om personlig signatur
- Autentisering og pålogging internt i foretaket
- Pålogging fra eksterne nett (hjemmekontor og lignende)

Ingen av disse anvendelsene kan sies å ha "tatt av" ennå, men tallmessig ligger anvendelsen av PKI for autentisering og pålogging internt et godt stykke foran, i all hovedsak pga. St. Olavs innføring av dette for alle ansatte i det nye sykehuset. St. Olavs løsning baserer seg på sertifikater av samme type som utstedes under RTV's rammeavtale, men som er anskaffet av en annen leverandør.

St. Olavs løsning bruker PKI på et multi-funksjons smartkort, som brukes for autentisering og pålogging til Windows og Citrix, samt for visuell identifikasjon og identifisering ved RFID. PKI-løsningen brukes for pålogging og for etablering av kryptert kanal for VPN, men er også forberedt for signering og kryptering. Helse Midt har for øvrig kun overordnede planer om at PKI for personlige signaturer må tas i bruk.

I Helse Øst planlegger Nye Ahus å benytte personlige sertifikater for eResept og sykemelding på nivå Person-Høyt. Nye Ahus planlegger å benytte PKI til pålogging/autentisering av brukere mot applikasjoner. For å unngå å håndtere flere typer personlige sertifikater vil man benytte samme sertifikatutsteder som for signering, men ikke samme nivå på sertifikatet for alle brukere. Foretakets systemer vil spore alle aktiviteter knyttet til bruk i forbindelse med pålogging. Kun brukere som skal signere vil få Personnivå Høyt.

Det benyttes ikke personlige sertifikater i Helse Sør. I forbindelse med etableringen av ny basis plattform i regionen, vil man se på funksjonaliteten PKI kan gi som autentiseringsnøkkel. Det er ikke utført arbeider i regionen for å anskaffe teknologien. Sykehuset Buskerud har påbegynt en offentlig anskaffelse, men leverandør er ikke blitt valgt, fordi anskaffelsen er stanset.

Helse Vest IKT leverer i dag "fjernaksess" løsning basert på personlig PKI og Smartkort. Dette er mulig å benytte i alle foretak i Helse Vest, men mest utbredt i Helse Berge og Helse Vest IKT selv. Dette basert på sertifikater utstedt av Helse Vest IKT. Helse Vest har ellers ikke planer om å benytte PKI for personlig signatur.

4.3. Bruk av PKI for kommunikasjon mot pasienter/pårørende

Ingen av helseforetakene har konkrete planer for bruk av PKI i kommunikasjon mot pasienter og pårørende.

I Helse Øst anser Nye AHUS dette for å være et nasjonalt prosjekt, og ikke et foretaksspesifikt prosjekt. Man vil forholde seg til felles løsninger innenfor Helse Øst og den nasjonale sikkerhetsportalen.

Helse Sør sin strategi på PKI satsning sammenfaller med de overordnede føringer som er gitt. Det er ingen konkrete gjennomføringsplaner på benytte PKI til kommunikasjon mot pasienter/pårørende men det er besluttet å innlemme benyttelse av PKI ved utvikling av nye tjenester der denne formene for sikkerhet er påkrevd.

Helse Midt avventer utviklingen på området.

4.4. Bruk av PKI for Web Services

Ingen av helseforetakene signaliserer konkrete planer for bruk av PKI for Web-services, flere vil vurdere dette der det er nødvendig.

Helse Øst knytter dette særlig til å tilby web-tjenester til f.eks. primærlegene, hvor det vil være naturlig å benytte PKI til sikring av slike web services. Man forutsetter da at brukerne benytter nasjonale felles løsninger tilsvarende RTV avtalen.

For Helse Midt knyttes dette opp mot sentralt arkitekturarbeid i helseregionen.

Det foreligger muligheter for slike anvendelser i de sertifikater som utstedes av Helse Vest IKT, men det foreligger ingen konkrete planer om bruksområder.

4.5. Bruk av dagens rammeavtale for PKI

Dagens rammeavtale for PKI har primært lagt til rette for bruk av PKI for elektronisk signatur på sykmeldingsmeldingen til RTV. Avtalen er ellers benyttet av apotekene for kommunikasjon mot RTV. Tall fra leverandøren, innhentet i november 2005 er:

- 750 apotek (virksomhetssertifikat)
- 500 legekontor (virksomhetssertifikat)
- 1500 leger (personlig sertifikat)

De personlige sertifikatene er utstedt til fastleger som sender sykmelding.

De fleste foretakene benytter eller har konkrete planer om å benytte dagens rammeavtale for PKI for anskaffelse av virksomhetssertifikater. Dette knyttes særlig til behovet for å implementere pålagte meldinger som fødselsmelding.

Ingen foretak har planer om å benytte rammeavtalen for anskaffelse av personlige sertifikater. Dette begrunnes til dels i at avtalen er i ferd med å løpe ut og videre at den anses som dyr.

4.6. Hindringer for PKI-utbredelse

For PKI på virksomhetsnivå trekkes det fram få hindre for utbredelse av PKI. Etter hvert som foretakene etablerer løsninger for meldingskommunikasjon over ebXML-rammeverket er selve PKI-bruken uproblematisk. Utfordringen knytter seg mer til den enkelte anvendelse, kost/nytte for denne osv., og ikke til PKI.

Flere trekker fram manglende informasjon og kunnskap som et viktig hinder for utbredelse av PKI-løsninger. Ute blant foretakene er man lite kjent med PKI og funksjonene dette kan tilby, eller Rammeavtalen for PKI.

Manglende eller ikke tilpasset infrastruktur i helseforetakene for å kunne utnytte PKI-tjenester trekkes fram, både ift. personlige sertifikater og virksomhetssertifikater. For virksomhetssertifikater er dette i ferd med å endre seg, men manglende katalogtjeneste (HER) trekkes fram som en problemstilling.

For personlige sertifikater trekker flere fram kostnader som en sentral hindring for PKI-utbredelse. Rammeavtalen for PKI anses generelt som dyr, og dette gjelder generelt for løsninger for PKI på høyt nivå.

Helse Øst trekker fram muligheten for å støtte fysisk adgangskontroll og pålogging som behov som ikke er dekket direkte i dagens rammeavtale for PKI.

4.7. Forventninger til framtidig PKI-løsning

Helse Øst, Helse Sør og Helse Vest ønsker at en PKI-løsning i framtiden må kunne tilby tjenester som helseforetakene kan dra nytte av direkte, som at sertifikatene må kunne benyttes for fysisk tilgangskontroll, pålogging/autentisering i tillegg til signering på et høyt sikkerhetsnivå.

Fra Helse Sør påpekes det at løsningene bør være differensierte, slik at foretaket kan velge tjenester etter behov og ambisjonsnivå, alt fra kun til intern pålogging, kun fysisk tilgangskontroll eller et fullt tjenestespekter. Tjeneste bør dekke et vidt spekter som pålogging, e-post, kryptering, signering, kryssertifisering. Tjenesten bør også settes i sammenheng med registreringsoppgaver som helsepersonellet utfører i dag, bl.a. registrering i fm uthenting av blod fra blodbanken.

Fra Sør trekkes det også fram at sertifikatene bør kunne fungere på tvers av virksomheter, slik at man har kun et sertifikat å forholde seg til. Det bør også være mulig med flere sertifikater på samme kort.

Helse Vest påpeker at de samme sertifikatene bør kunne gjenbrukes i alle aktuelle løsninger med PKI-behov. Det bør være sertifikater på personlig nivå og på virksomhetsnivå som kun identifiserer person, og rolle og funksjoner bør knyttes til identiteten via katalogtjenester. Sikkerhetskrav til løsningen må framkomme i en risikovurdering ift. de krav og konsekvenser som ligger til grunn.

Ift. kostnader og finansieringsmodell påpekes det fra Helse Vest at dette bør gjenspeile kostnader med drift og forvalting av en tjeneste. Helse Sør ønsker at dagens betalingsmodell, dvs. pr. sertifikat, beholdes. Helse Midt mener at finansieringen bør knyttes til tilhørende tjeneste.

Helse Midt påpeker at helsesektorens PKI-løsninger må samstemmes med nasjonale løsninger for PKI. Fra Helse Vest pekes det på ”Kravspesifikasjon for PKI i offentlig sektor” som virkemiddel for dette.

5. Forslag til hovedprosjekt for PKI

Arbeidsgruppen foreslår at det igangsettes et hovedprosjekt for innføring av PKI i helseforetakene. Følgende er innspill til et prosjektdirektiv for et PKI-hovedprosjekt med 2 års varighet.

Prosjektet bør ha følgende hovedmål:

Å sikre samordning, fremdrift og konsistent nasjonal innføring av PKI i spesialisthelsetjenesten gjennom et nasjonalt samarbeid for oppfølging, erfaringsnettverk og kunnskapsformidling mellom øvrige tiltak.

Prosjektet skal bidra til at følgende resultatmål nås innen utgangen av 2007.

- Alle helseforetakene skal ha tatt i bruk virksomhetssertifikater for meldingskommunikasjon innen 1.8.2006
- I løpet av første halvår 2006 må det for hver av EPJ-leverandørene være igangsatt minst ett prosjekt for å forberede signering av meldinger med personlig signatur i eResept.
- I løpet av 2007 må alle regioner ha testet ut og klargjort løsning for signering av eResept med personlig signatur i egen infrastruktur.
- Minst 2 større helseforetak har i løpet av 2007 innført autentisering ved hjelp av PKI for store grupper av ansatte.
- Innføre PKI-baserte løsninger for identitetshåndtering og autentisering i utvalgte anvendelser som publikumstjenester, mobile løsninger og tjenester for informasjonsdeling.

De regionale helseforetakene må forplikte seg til å iverksette nødvendige tiltak for å oppnå disse målene. PKI-hovedprosjektet skal legge til rette for at ulike regionale/lokale innføringsprosjekter kan nå disse målene.

PKI-hovedprosjektet har følgende delmål:

5.1. Delmål 1: Å sikre fremdrift på PKI innføringen i spesialisthelsetjenesten

For å sikre fremdrift må RHF/HF-ene forplikte seg til å gjennomføre en del tiltak i forhold til PKI, dette innebærer m.a. å tilrettelegge for å ta i bruk virksomhetssertifikater på eksisterende og nye meldinger, etablere løsning for bruk av personlige sertifikater og forberede og teste ut løsning for signering av meldinger med personlig signatur (spesielt eResept og sykmelding).

Innføringen av PKI-basert autentisering på St.Olavs og Ahus skal tjene som eksempel for andre som ønsker å innføre tilsvarende løsninger.

Det bør også igangsettes aktiviteter i helseforetakene for å innføre PKI-baserte løsninger for identitetshåndtering og autentisering i utvalgte anvendelser som publikumstjenester, mobile løsninger og tjenester for informasjonsdeling.

5.2. Delmål 2: Å sikre samordning av PKI i spesialisthelsetjenesten

Prosjektet vil ha ansvar for organisering av erfaringsnettverk og kunnskapsformidling mellom de ulike tiltakene/prosjektene som gjennomføres, samt ansvar for utarbeiding av generell informasjon/veiledninger. Aktuelle tiltak for å oppnå dette vil være å opprette en felles ressursgruppe med sentrale aktører i HF/RHF-ene, samt ekspertgrupper på utvalgte områder. Andre oppgaver vil være å utarbeide informasjonsmateriell, avholde arbeidsmøter og gi veiledning.

5.3. Delmål 3: Å sikre konsistent nasjonal innføring

Aktuelle tiltak for å oppnå dette vil være å spre informasjon om aktuelle anbefalinger, standarder og avtaler, samt samle inn og spre erfaringer fra de som er langt fremme (for eksempel St. Olavs og etter hvert nye Ahus).

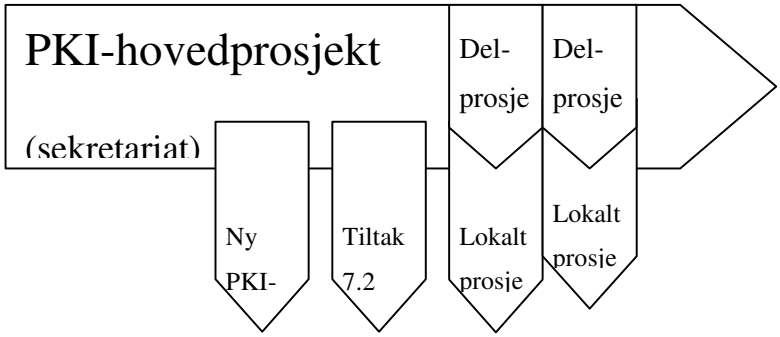
Prosjektet bør være en pådriver og deltager i arbeid for å etablere en løsning som erstatter "RTV-løsningen". Prosjektet må i samarbeid med RTV og SHdir utrede hvordan en fremtidig løsning for levering av PKI-sertifikater (med høyt sikkerhetsnivå) til helsevesenet bør organiseres. Dersom man velger å kjøre et ny anbudsforespørsel for helsevesenet bør dette kjøres som et eget løp, og det må også avklares hvem som skal være ansvarlig (SHdir, RTV, Nasjonal-IKT, Norsk Helsenett).

For å nå disse målene har arbeidsgruppen utarbeidet en rekke tiltak for å sikre framdrift, samordning og konsistens i innføringen av PKI-løsninger.

5.4. Framdriftstiltak

Framdriftstiltakene skal bidra til å få etablere løsninger på ulike områder som sikker meldingsutveksling, autentisering, hjemmekontor og mobile løsninger og for personlig signatur. Målsetningen er at prosjektene skal fungere som gode eksempler for andre prosjekter på samme område, og de må derfor være knyttet til dokumentasjonsaktivitetene beskrevet under "Dokumentasjon av resultater".

5.4.1. Oppfølging av PKI hovedprosjekt



Figuren viser forholdet mellom hovedprosjektet, nasjonale aktiviteter og ulike innføringsprosjekter (eksemplifisert ved lokalt prosjekt A, B). Innenfor hovedprosjektet vil det også være delprosjekter som skal bistå de lokale prosjektene.

Hovedprosjekt for PKI skal følge opp det enkelte prosjekt med rådgivning og samordningsaktiviteter for å sikre at PKI tas i bruk og integreres på en kostnadseffektiv, hensiktsmessig og mest mulig ensartet måte i de ulike foretakene.

Sentrale aktiviteter for prosjektet vil være:

1. Felles aksept av behov for PKI
2. Samarbeid med nye Ahus om løsninger for autentisering som kan spres i sektoren
3. Delta i arbeide med PKI-strategi for helsevesenet (denne aktiviteten er allerede igangsatt).
4. Forberede implementering av eResept i HF-ene

5. Oppfølging av implementeringen av virksomhetssertifikater

I forhold til alle disse aktivitetene må det kjøres lokale/regionale innføringsprosjekt med en tett og ***forpliktende*** kontakt med PKI-hovedprosjektet.

Det må også opprettes et sekretariat (inkludert prosjektledelse) og en PKI-prosjektgruppe med deltagere fra HF-ene som m.a. vil ivareta følgende:

- kontakt/rådgivning ift. regionale/lokale prosjekter med behov for PKI-løsninger
- spre informasjon om aktuelle strategier og løsninger
- utarbeide dokumentasjon (m.a. "best practice")
- kontakt/oppfølging av andre relevante prosjekt som HER-mottaksprosjekt, offentlig sikkerhetsportal, Tiltak 7.2. med mer
- eventuelt opprette tekniske prosjektgrupper
- arrangere prosjektmøter og ev. workshops
- gjennomføre utredninger og gi anbefalinger

Følgende hovedområder bør være dekket av ulike innføringsprosjekter:

1. Innføring av løsning for virksomhetssignatur
    - Rammeverk for meldingskommunikasjon (ebXML) og PKI på virksomhetsnivå for kommunikasjon mellom helseforetak og primærhelsetjenesten
2. Innføring av løsning for autentisering
    - Aktiviteten må samarbeide med og støtte opp under innføringen av løsning for PKI-basert autentisering ved et helseforetak (Nye Ahus)
    - Det må arbeides for at en avtale som inngås av Ahus/Helse Øst også kan benyttes av andre regioner og helseforetak som ønsker å ta i bruk PKI for autentisering
3. Innføring av løsning for personlig signatur (nærmere beskrevet under 5.4.3)
    - Aktiviteten skal støtte opp under innføring av løsning for personlig signatur på e-meldinger ved et helseforetak.
    - Aktiviteten må ses i sammenheng med innføring av eResept fra 2007, og innføre en løsning som kan benyttes for både eResept og sykmelding til RTV.

5.4.2. Ny PKI-løsning for helsesektoren

Med bakgrunn i behovet for ny PKI-løsning for helsesektoren når RTV's rammeavtale løper ut tidlig i 2007, bør RHF/HF'ene være en pådriver og deltager i arbeidet med ny løsning.

Hovedansvaret for aktiviteten vil ligge hos ShDir, men helseforetakene må delta aktivt i planlegging og strategivalg som leder opp til en videre prosess.

Det forutsettes at ShDir tar initiativ til en arbeidsgruppe mellom SHdir (inkl. eReseptprosjektet), RTV og Nasjonal IKT for å utrede strategi for videre arbeid med og utrulling av PKI i helsevesenet. Helseforetakene må stille med tilstrekkelig ressurser til å delta aktivt i denne prosessen.

- Løsningen må ta høyde for behov fra eResept og ift. sykmelding
- Løsningen må fokusere på behov og utfordringer knyttet til integrasjon i helseforetakenes infrastruktur
- Komme fram til egnede måter å integrere PKI i helseforetakenes fagsystemer
- Avklare den mest optimale anskaffelsesstrategien for PKI til foretakene

Omfanget av aktiviteten vil i stor grad avhenge av hvilken strategi som velges for ny PKI-løsning, og ressursinnsatsen må tilpasses deretter. Et anskaffelsesløp må organiseres som et separat prosjekt hvor RHF/HF må være prosjektdeltagere.

5.4.3. Forberede løsning for personlig signatur i eResept

For hver av EPJ-leverandørene skal det igangsettes minst ett prosjekt for å forberede signering av meldinger med personlig signatur i eResept. Prosjektene skal være forankret i et eller flere HF/RHF og utarbeide og dokumentere en løsning for hvordan eReseptmeldingene (og evt. sykmelding) kan signeres med personlig signatur i foretakets pasientjournalsystem.

Det enkelte HF/RHF må i samarbeid med sin EPJ-leverandør kartlegge behov og utarbeide krav til signaturløsningens utforming, krav til teknisk integrasjon og eventuelle forutsetninger/ krav til PKI-løsningen.

Hovedprosjekt for PKI skal følge opp det enkelte prosjekt med rådgivning og samordningsaktiviteter for å sikre at løsningen integreres på en hensiktsmessig og mest mulig ensartet måte i de ulike foretakene.

Hovedprosjektet for PKI skal

- Gjennomføre et arbeidsmøte med eResept-prosjektet for å diskutere løsningsmodeller for personlig signatur i eResept-prosjektet.
- Følge opp det enkelte lokale prosjekt
- Arrangere workshop el. for samordning på tvers av prosjektene

5.4.4. Følge opp innføring av HER

Aktiviteten skal sikre at HER kan benyttes på en effektiv måte for å støtte opp under helseforetakenes behov ift. PKI. Dette kan være hvordan sertifikater skal legges inn i og tilgjengeliggjøres via HER.

Det skal gjennomføres et arbeidsmøte med HER-mottaksprosjektet for å etablere metoder for å integrere PKI og sertifikater i HER-tjenesten.

5.5. Samordningstiltak

5.5.1. Arbeidsgruppe for PKI i helseforetakene

Det må etableres en prosjektgruppe for å sikre informasjonsspredning og koordinering mellom aktivitetene som gjennomføres i det enkelte HF/RHF. Arbeidsgruppen vil ha jevnlige møter i prosjektperioden og gjennomgå status og resultater fra de enkelte aktivitetene i hovedprosjektet og prosjektene som er forankret i det enkelte helseforetak. Arbeidsgruppen skal også kunne delta med rådgivning inn mot enkeltprosjekter som kjøres i RHF/HF.

Arbeidsgruppen bør ta utgangspunkt i arbeidsgruppen for forprosjektet, men bør også bestå av prosjektledere for de enkelte aktivitetene. Arbeidsgruppen må ha et sekretariat med ansvar for å kalle inn til samordningsmøter og som vil ha hovedansvar for å utarbeide dokumentasjon som skal utarbeides av prosjektet.

I tillegg til koordineringsansvaret vil arbeidsgruppen ha ansvar for å gjennomføre samordningsaktiviteter og utarbeide dokumentasjon som beskrevet i aktivitetene nedenfor på områdene (mer utfyllende beskrevet under 3.3 Tiltak for å sikre konsistens):

- Vurdering av sikkerhetsnivå
- Dokumentere ”best practice” for personlig signatur
- Dokumentere ”best practice” for autentisering
- Samordning med offentlig sikkerhetsportal

5.5.2. Systemoversikt

For å sikre samordning og erfaringsutveksling er det behov for en samlet oversikt over systemer og kommunikasjonsløsninger i helsesektoren. En slik oversikt vil gjøre det enkelt å finne frem til andre som erfaringer fra implementering av tilsvarende løsninger. En oversikt over aktører og meldinger som disse kan utveksle på spesialisthelsetjenesten er utviklet av ELIN-prosjektet og Norsk Helsenett. Denne oversikten bør videreutvikles av Norsk Helsenett i samarbeid med prosjektet slik at man for det enkelte helseforetak kan få oversikt over:

- Meldingsmotor
- EPJ-system og versjon
- Meldinger og versjon
- Status for de enkelte meldinger
- Kontaktpersoner

5.5.3. Etablering av tekniske ekspertgrupper

Det bør etter behov opprettes tekniske ekspertgrupper på spesielle områder. Arbeidsgruppen bør initiere slike ekspertgrupper etter behov på områder som krever erfaringsutveksling og teknisk kompetanse.

Et eksempel på en slik ekspertgruppe kan være knyttet til integrasjon av PKI-løsning mot Microsoft Windows-plattformen, Active Directory-baserte løsninger osv.

HF'ene må avsette ressurser som kan delta i ekspertgruppene.

5.5.4. Samordning med offentlig sikkerhetsportal

Arbeidsgruppen må innlede en dialog med forvaltningsorganisasjonen for den offentlige sikkerhetsportalen med sikte på å avklare:

- Hvilke av sikkerhetsportalens tjenester som er aktuelle å benytte for helseforetakene
- Hvordan evt. sikkerhetsportalens tjenester, nåværende og framtidige, kan tilpasses for å nyttiggjøres for helseforetakene.
- Hvordan helseforetakene kan delta i videre arbeid rundt sikkerhetsportalen

Arbeidet må konkludere med hvordan helseforetakene kan nyttiggjøre seg tjenestene fra sikkerhetsportalen, og i hvilken grad helseforetakene skal bidra i det videre arbeidet med sikkerhetsportalen.

5.5.5. Vurdering av sikkerhetsnivå

Det skal gjennomføres en vurdering av sikkerhetsnivå for ulike anvendelser med behov for PKI. Vurderingen skal avklare hvilke sikkerhetskrav som skal stilles til ulike anvendelser i helsesektoren

som meldingsutveksling, autentisering/pålogging, hjemmekontorløsninger osv. Vurderingen bør ta utgangspunkt i sikkerhetsnivåene i "Kravspesifikasjon for PKI i offentlig sektor".

Aktiviteten skal komme fram til en samordnet vurdering av sikkerhetskravene for løsninger som har behov for PKI. Vurderingene skal være forankret i helseforetakene.

5.6. Tiltak for å sikre konsistens

5.6.1. Informasjonsspredning

Det skal gjennomføres aktiviteter for å sikre informasjonsspredning mellom tiltak og prosjekter.

- Avholde workshop om PKI
- Spre informasjonsmateriell om PKI
- Informasjon på web

5.6.2. Dokumentere "best practice" for autentisering

Det må utvikles en "best practice"/veiledning for hvordan PKI kan benyttes for autentisering i helseforetak. Resultatet bør dokumentere framgangsmåte for å implementere en slik løsning, og dokumentere effekt og nytteverdi av dette.

- Krav til sertifikater
- Krav til infrastruktur på klientsiden
    - Smartkort og lesere
    - Teknisk plattform, operativsystem
    - Funksjonalitet via Terminalserver-løsninger
- Krav til infrastruktur på server-siden
    - Katalogtjenester
    - Domenestruktur
- Funksjonalitet
- Kost/nytte

Arbeidet vil kreve innsats fra St. Olavs hospital og Nye Ahus.

5.6.3. Dokumentere ”best practice” for personlig signatur

Det må utvikles en ”best practice”/veiledning for hvordan PKI kan benyttes for å implementere løsinger med personlig signatur i helseforetak. Resultatet bør dokumentere hvordan det enkelte helseforetak må gå fram for å etablere en løsning med personlig signatur og nødvendige krav til arkitektur og infrastruktur for å etablere løsningen. Løsningen som beskrives må ta høyde for krav som stilles fra RTV ift. sykmelding og fra ShDir ift. eResept. Beskrivelsen må omfatte de journalsystemene som benyttes i helseregionene, Dips, IMX, Doculive.

Det må dokumenteres:

- Krav til infrastruktur på klientsiden
- Krav til integrasjon mot fagsystem

Arbeidet vil kreve innsats fra lokale prosjekter som skal innføre personlig signatur.

6. Vedlegg 1 – svar på statusundersøkelse

I dette vedlegget er svarene som kom inn fra helseregionene på status på utbredelse av PKI. Svarene er oppsummert i kapittel 4 - Status for PKI i helseforetakene.

Det ble mottatt svar fra 4 av regionene, Helse Sør, Helse Midt, Helse Øst v. AHUS, Helse Vest.

Undersøkelsen stilte spørsmål innen 3 hovedområder, behov for PKI i helseforetaket, dagens rammeavtale for PKI og framtidig løsning for PKI i helsesektoren.

6.1. Helse Øst

6.1.1. Behov for PKI i helseforetaket

PKI kan benyttes på ulike måter i helseforetakene, ift. signatur og kryptering ved meldingsutveksling både på personlig nivå, virksomhetsnivå osv. Mange benytter seg av sertifikater utstedt under RTV's rammeavtale for PKI, mens andre utsteder og håndterer lokale sertifikattjenester. Denne hoveddelen søker å kartlegge behovet for PKI-løsninger.

Benytter eller har helseforetaket planer om å benytte PKI til personlig signatur på elektroniske meldinger (sykmelding/legeerklæring)? Hvordan og til hva?
Ja. Nye Ahus planlegger å benytte dette for eResept og sykemelding. Personnivå Høyt.
Benytter eller har helseforetaket planer om å benytte PKI til sikring av meldingsutveksling på virksomhetsnivå (POLK, elektronisk fødselsmelding, andre meldinger?) Hvordan og til hva? Hvem utsteder sertifikatene?
Ja. Nye Ahus planlegger å benytte virksomhetssertifikat(er) i forbindelse med meldinger til andre helseforetak, offentlige myndigheter, primærhelsetjenesten

Benytter eller har helseforetaket planer om å benytte PKI til autentisering/pålogging internt i foretaket? Hvordan og til hva? Hvem utsteder sertifikatene?
Ja. Nye Ahus planlegger å benytte PKI til pålogging/autentisering av brukere mot applikasjoner. For å unngå å håndtere flere typer personlige sertifikater vil man benytte samme sertifikatutsteder som for signering, men ikke samme nivå på sertifikatet for alle brukere. Foretakets systemer vil spore alle aktiviteter knyttet til bruk i forbindelse med pålogging. Kun brukere som skal signere vil få Personnivå Høyt.
Benytter eller har helseforetaket planer om å benytte PKI til kommunikasjon mot pasienter/pårørende? Hvordan og til hva?
Nei. Dette anser vi å være et nasjonalt prosjekt, og ikke er foretaksspesifikt prosjekt. Vi antar at vi må forholde oss til felles løsninger innenfor Helse Øst og den nasjonale sikkerhetsportalen.
Benytter eller har helseforetaket planer om å benytte PKI til sikring av Web Services eller lignende infrastrukturtjenester? Hvordan og til hva?
Ja. Dersom vi kommer til å tilby web-tjenester til f.eks. primærlegene, vil det være naturlig å benytte PKI til sikring av slike web services. Forutsetter da at brukerne benytter nasjonale felles løsninger tilsvarende RTV avtalen.
Benytter eller har helseforetaket planer om å benytte PKI for andre formål? Angi i tilfelle hvilke og hvordan?
Pt. ikke, men det kan være aktuelt å benytte PKI for kryptering av personlige meldinger (epost). Foreløpig er det ikke identifisert behov for dette.
Benytter eller har helseforetaket planer om å benytte andre mekanismer for sterk autentisering (for eksempel engangspassord, "passordkalkulator"? Angi i tilfelle hvilke og hvordan?
Det kan være aktuelt å benytte andre mekanismer i forbindelse med reautentisering av brukere som midlertidig forlater sin arbeidsstasjon (fingeravtrykk f.eks.)
Benytter eller har helseforetaket planer om å benytte rammeavtalen for PKI i helsesektoren, utsteder helseforetaket sertifikater selv eller benyttes annen leverandør av PKI-tjenster?
Nei. Denne rammeavtalen går ut i 2006, og vi vil ikke starte utrulling før i 2007. Nye Ahus arbeider

med å lage en felles spesifikasjon for Helse Øst.

6.1.2. Dagens rammeavtale for PKI

Rikstrygdeverket har inngått en rammeavtale for PKI på vegne av helsesektoren. Denne delen fokuserer på bruk og effekt av denne.

Hvor godt er helseforetaket kjent med dagens rammeavtale for PKI i helse- og sosialsektoren (inngått av Rikstrygdeverket)?
Delvis kunnskap. Vår forutsetning er at denne avtalen går ut i 2006.
Har dere anskaffet virksomhetssertifikat under avtalen? I tilfelle ja, hvor mange?
Nye Ahus har ikke det. Vi kjenner ikke til hva Ahus har gjort.
Har dere anskaffet personlige sertifikat under avtalen? I tilfelle ja, hvor mange?
Nei
Er helseforetaket fornøyd med PKI-tjenestene som leveres over dagens rammeavtale, evt. Hva kunne vært forbedret eller mangler?
N/A
Er helseforetaket fornøyd med betingelsene knyttet til dagens rammeavtale, evt. hva kunne vært forbedret eller mangler?
N/A
Hva vurderer du/dere som de viktigste hindringene for bruk av PKI på virksomhetsnivå for helseforetaket i dag?
Kompetanse. Samt teknisk infrastruktur i foretaket for å understøtte bruken av dette.
Hva vurderer du/dere som de viktigste hindringene for bruk av PKI på personlig nivå for helseforetaket i dag?
Pris på sertifikat. Kostnader for utstedelse. Felles kort for fysisk adgang og pålogging

6.1.3. Fremtidig PKI-løsning for helsesektoren

Denne delen fokuserer på behov og modell for PKI-løsning for helsesektoren i framtiden.

Hva slags tjenester bør inngå i en PKI-tjeneste etter helseforetakets mening?
Personlige sertifikater for signering (og som kan benyttes i forbindelse med kryptering og pålogging/autentisering) Personlige sertifikater som kan benyttes kun for pålogging/autentisering (antas å være billigere enn de første både i anskaffelse og drift) Virksomhetssertifikater for
Hva slags typer PKI-sertifikater bør benyttes i helsesektoren (f.eks. sikkerhetsnivå, virksomhetsnivå, personlig, ansatt/rolle osv)?
Hva slags typer PKI-sertifikater har eller vil ditt/deres helseforetak ha behov for i framtiden?
Hvordan ser helseforetaket for seg å benytte PKI-løsninger på lengre sikt (5-årsperspektiv)?
Hvilke sikkerhetskrav bør stilles til PKI-sertifikater i helsesektoren (for eksempel ift. utstedelse av sertifikater, kontroll av legitimasjon, lagring av nøkkel (smartkort/software) osv.)
Hva slags tjenester bør PKI-tjenester støtte? (pålogging, e-post, signering, kryptering, annet? Hva bør prioriteres?)
Bør det stilles spesielle krav til innhold og format for PKI-sertifikater i helsesektoren?
Ønsker helseforetaket å koble PKI og sertifikattjenester med andre lokale tjenester, for

eksempel lokal kortutstedelse, fysisk adgangskontroll osv.?
Hvordan bør en PKI-løsning for helsesektoren forvaltes? Hvem bør eie og hvem bør drifte en PKI-løsning for helsesektoren? Hvorfor?
Hvordan bør PKI-løsninger i helsesektoren finansieres? (Noen modeller er betaling pr. transaksjon/bruk (signering/kryptering/validering) eller betaling pr. sertifikat og fri bruk av dette (frikjøp), andre modeller?) Hvilke finansieringsalternativ bør vurderes/velges?
Hvordan bør bruk av PKI-løsninger samordnes mellom helseforetakene? Hva må koordineres? Hvilke tiltak bør iversettes for å sikre koordingering?
Hvordan bør helsesektorens PKI-løsninger forholde seg til nasjonale løsninger for PKI (for eksempel sikkerhetsportal, kravspesifikasjon for PKI i offentlig sektor)?

6.1.4. Annet

Andre kommentarer fra helseforetaket?

6.2. Helse Midt-Norge

6.2.1. Behov for PKI i helseforetaket

PKI kan benyttes på ulike måter i helseforetakene, ift. signatur og kryptering ved meldingsutveksling både på personlig nivå, virksomhetsnivå osv. Mange benytter seg av sertifikater utstedt under RTV's

rammeavtale for PKI, mens andre utsteder og håndterer lokale sertifikattjenester. Denne hoveddelen søker å kartlegge behovet for PKI-løsninger.

Benytter eller har helseforetaket planer om å benytte PKI til personlig signatur på elektroniske meldinger (sykmelding/legeerklæring)? Hvordan og til hva?
Har kun overordnede planer om at dette må tas i bruk
Benytter eller har helseforetaket planer om å benytte PKI til sikring av meldingsutveksling på virksomhetsnivå (POLK, elektronisk fødselsmelding, andre meldinger?) Hvordan og til hva? Hvem utsteder sertifikatene?
Har nettopp iverksatt pilotprosjekt på henvisninger og som benytter PKI. Deriga er ansvarlig for gjennomføring. Fødselsmeldinger er søkt utsatt, men vil starte ila 1. halvår 2006. POLK kommer Det er sertifikater fra ERGO som er ment brukt fremover.
Benytter eller har helseforetaket planer om å benytte PKI til autentisering/pålogging internt i foretaket? Hvordan og til hva? Hvem utsteder sertifikatene?
Nye st. Olavs Hospital har tatt dette i bruk : Telenor har etablert en PKI-løsning for Helsebygg Midt-Norge ifm. entreprisen for IKT infrastruktur. Løsningen omfatter personell ved St. Olavs hospital, DMF ved NTNU og HIST. Løsningen bruker PKI på et multi-funksjons smartkort, som brukes for autentisering og pålogging til Windows og Citrix, samt for visuell identifikasjon og identifisering ved RFID. PKI-løsningen brukes for pålogging og for etablering av kryptert kanal for VPN, men er også forberedt for signering og kryptering. PKI-sertifikatene følger ZebSigns Community Policy på samme måte som de sertifikatene som RTV anvender. Denne policyen er innmeldt til NPT som policy for kvalifiserte sertifikater. Opsjonsfeltene i sertifikatet inneholder de nødvendige parametere som skal til for at løsningen skal virke "sømløst" mot Windows og Citrix terminalservere. Ved å følge Community Member CP er sertifikatene også konforme med MODs krav til Person Høy og SEID fellesstandard. Det betyr at sertifikatene også kan benyttes i Sikkerhetsportalen ved Brønnøysund-registeret. Dette er avtalt med BBS. Sertifikatene skal derfor også være klargjort for eResept når dette kan brukes og for HER. Sertifikatene følger også KITHs anbefalinger for PKI i helsenett. Det tas forbehold om at løsninger som ikke ennå er ferdig etablert må testes og kvalitetssikres før man kan ta disse i bruk i operativt miljø. Sertifikater med Community CP inneholder ikke personnummer i sertifikatet. Personnummeret kan

hentes ved et oppslag i DSP-tjenesten hos ZebSign basert på sertifikatet.

Etter som Community CP følger Person Høy fra MOD og forskriftene for kvalifisert sertifikat etter norsk Lov om elektronisk signatur, som i sin tur bygger på EU-direktivet, ligger utfordringen i utstedelsen av sertifikater av slik høy kvalitet. Telenor har etablert en RA-løsning (registerings- og utstedelsesløsning) bestående av en sentra RA-server og lokale PCer - LRA-stasjoner - på St. Olavs hospital. Nøklene genereres "on-board" på kortet og sertifikatet utstedes og signeres av ZebSign CA etter kontroll av alle data, bl.a. at personen er oppført i DSP - det sentrale personregisteret - med det navn som oppgis. LRA-stasjonene betjenes av kvalifisert og sertifisert personell, som bl.a. kontrollerer søkerens legitimasjon (norsk pass, førerkort eller norsk bankkort) etter forskriftene i Lov om elektronisk signatur og Lov om folkeregistrering.

Dette betyr at det ikke er kritisk for løsningen om helsepersonellet har fødselsnummer i HPR, men at det er kritisk at fødselsnummeret (eller D-nummeret) finnes i DSP. Det er for øvrig ingen kontroll av at søkeren finnes i HPR. St. Olavs hospital går god for at søkeren er en gyldig søker, bl.a. ved kvittering fra overordnet på søknaden, og at nødvendige personopplysninger for ansatte overføres automatisk fra personalsystemet PRS.

Den utfordringen som vi har møtt er at helsepersonell ikke har fått tildelt D-nummer og derved finnes i DSP. Da kan ikke et kvalifisert PKI-sertifikat utstedes. Det kan skyldes ulike årsaker; lang saksbehandlingstid hos norske myndigheter eller at det ikke er søkt om D-nummer i det hele tatt.

Ønskelig(?) at SAFH kunne ta en aktiv rolle i også å fremme søknad om D-nummer for utenlandsk helsepersonell, da gjerne med dispensasjon fra Politidirektoratet eller gjennom forskriftsendring til Lov om folkeregistrering. Telenor har, sammen med St. Olavs hospital, hatt et møte med Skattedirektoratet med tanke på å oppnå en slik løsning, men søknaden om dette må komme fra SAFH eller SHDir.

Ved St. Olavs hospital har Telenor etablert en alternativ LRA-løsning som kan utstede sertifikater av type Person Standard etter MODs spesifikasjon for personell som ikke kan verifiseres i DSP. Lokalt stilles det da krav om legitimasjon ved kontrollerbart pass av tilforlatelig kvalitet. Det er stadig ingen forbindelse eller kontroll mot HPR.

Benytter eller har helseforetaket planer om å benytte PKI til kommunikasjon mot pasienter/pårørende? Hvordan og til hva?

Avventer

Benytter eller har helseforetaket planer om å benytte PKI til sikring av Web Services eller lignende infrastrukturtjenester? Hvordan og til hva?

Diskuteres i forhold til HEMITs arkitekturstrategi
Benytter eller har helseforetaket planer om å benytte PKI for andre formål? Angi i tilfelle hvilke og hvordan? labsvar,
Benytter eller har helseforetaket planer om å benytte andre mekanismer for sterk autentisering (for eksempel engangspassord, "passordkalkulator"? Angi i tilfelle hvilke og hvordan?
Benyttes i forbindelse med hjemmekontor
Benytter eller har helseforetaket planer om å benytte rammeavtalen for PKI i helsesektoren, utsteder helseforetaket sertifikater selv eller benyttes annen leverandør av PKI-tjenster?
Antar at rammeavtalen benytte for pilotprosjekt henvisninger. Se for øvrig egen ordning for St. Olavs Hospital

6.2.2. Dagens rammeavtale for PKI

Rikstrygdeverket har inngått en rammeavtale for PKI på vegne av helsesektoren. Denne delen fokuserer på bruk og effekt av denne.

Hvor godt er helseforetaket kjent med dagens rammeavtale for PKI i helse- og sosialsektoren (inngått av Rikstrygdeverket)?
Er kjent på RHF og HF, men kun på overordnet nivå
Har dere anskaffet virksomhetssertifikat under avtalen? I tilfelle ja, hvor mange?
Antar at dette er gjort i forbindelse med polk !. Ett stk.
Har dere anskaffet personlige sertifikat under avtalen? I tilfelle ja, hvor mange?
Nei
Er helseforetaket fornøyd med PKI-tjenestene som leveres over dagens rammeavtale, evt. Hva kunne vært forbedret eller mangler?
Vet ikke

Er helseforetaket fornøyd med betingelsene knyttet til dagens rammeavtale, evt. hva kunne vært forbedret eller mangler?
Dyr
Hva vurderer du/dere som de viktigste hindringene for bruk av PKI på virksomhetsnivå for helseforetaket i dag?
Manglende informasjon og forståelse
Hva vurderer du/dere som de viktigste hindringene for bruk av PKI på personlig nivå for helseforetaket i dag?
Som ovenfor. Ingen har spesifikke ønsker om å ta dette i bruk. Må komme som et direktiv

6.2.3. Fremtidig PKI-løsning for helsesektoren

Denne delen fokuserer på behov og modell for PKI-løsning for helsesektoren i framtiden.

Hva slags tjenester bør inngå i en PKI-tjeneste etter helseforetakets mening?
Alle hvor det kan dokumenteres behov
Hva slags typer PKI-sertifikater bør benyttes i helsesektoren (f.eks. sikkerhetsnivå, virksomhetsnivå, personlig, ansatt/rolle osv)?
-
Hva slags typer PKI-sertifikater har eller vil ditt/deres helseforetak ha behov for i framtiden?
-
Hvordan ser helseforetaket for seg å benytte PKI-løsninger på lengre sikt (5-årsperspektiv)?
-
Hvilke sikkerhetskrav bør stilles til PKI-sertifikater i helsesektoren (for eksempel ift. utstedelse av sertifikater, kontroll av legitimasjon, lagring av nøkkel (smartkort/software) osv.)
-

Hva slags tjenester bør PKI-tjenester støtte? (pålogging, e-post, signering, kryptering, annet? Hva bør prioriteres?)
-
Bør det stilles spesielle krav til innhold og format for PKI-sertifikater i helsesektoren?
Bør baseres på standard løsninger
Ønsker helseforetaket å koble PKI og sertifikattjenester med andre lokale tjenester, for eksempel lokal kortutstedelse, fysisk adgangskontroll osv.?
Ja
Hvordan bør en PKI-løsning for helsesektoren forvaltes? Hvem bør eie og hvem bør drifte en PKI-løsning for helsesektoren? Hvorfor?
-
Hvordan bør PKI-løsninger i helsesektoren finansieres? (Noen modeller er betaling pr. transaksjon/bruk (signering/kryptering/validering) eller betaling pr. sertifikat og fri bruk av dette (frikjøp), andre modeller?) Hvilke finansieringsalternativ bør vurderes/velges?
Må gjøres enkelt. Finansiering bør knyttes til tilhørende tjeneste
Hvordan bør bruk av PKI-løsninger samordnes mellom helseforetakene? Hva må koordineres? Hvilke tiltak bør iversettes for å sikre koordingering?
-
Hvordan bør helsesektorens PKI-løsninger forholde seg til nasjonale løsninger for PKI (for eksempel sikkerhetsportal, kravspesifikasjon for PKI i offentlig sektor)?
Må samstemmes

6.2.4. Annet

Andre kommentarer fra helseforetaket?

6.3. Helse Sør

6.3.1. Behov for PKI i helseforetaket

PKI kan benyttes på ulike måter i helseforetakene, ift. signatur og kryptering ved meldingsutveksling både på personlig nivå, virksomhetsnivå osv. Mange benytter seg av sertifikater utstedt under RTV's rammeavtale for PKI, mens andre utsteder og håndterer lokale sertifikattjenester. Denne hoveddelen søker å kartlegge behovet for PKI-løsninger.

Dette skjemaet er fylt ut på vegne av hele Helse Sør. Dersom svaret har foretaksspesifikke forskjeller er dette merket med foretakets navn i forkant av kommentarene.

Benytter eller har helseforetaket planer om å benytte PKI til personlig signatur på elektroniske meldinger (sykmelding/legeerklæring)? Hvordan og til hva?
Det benyttes ikke personlige sertifikater i Helse Sør.
Benytter eller har helseforetaket planer om å benytte PKI til sikring av meldingsutveksling på virksomhetsnivå (POLK, elektronisk fødselsmelding, andre meldinger?) Hvordan og til hva? Hvem utsteder sertifikatene?
Alle helseforetakene i Helse Sør skal benytte virksomhetssertifikater til utveksling av fødselsmeldinger og svangerskapsavbrudd. Regionen har søkt om dispensasjon fra å levere nevnte meldinger frem til 1/7-06. Alle helseforetakene i Helse Sør har fått utstedt virksomhetssertifikater fra Ergo group. Rikshospitalet-Radiumhospitalet HF leverer elektroniske fødselsmeldinger ved bruk av virksomhetssertifikater.
Benytter eller har helseforetaket planer om å benytte PKI til autentisering/pålogging internt i foretaket? Hvordan og til hva? Hvem utsteder sertifikatene?
I forbindelse med etableringen av ny basis plattform i regionen, vil vi se på funksjonaliteten PKI kan

gi som autentiseringsnøkkel. Det er ikke utført arbeider i regionen for å anskaffe teknologien. Sykehuset Buskerud har påbegynt en offentlig anskaffelse, men leverandør er ikke blitt valgt, fordi anskaffelsen er stanset.
Benytter eller har helseforetaket planer om å benytte PKI til kommunikasjon mot pasienter/pårørende? Hvordan og til hva?
Helse Sør sin strategi på PKI satsning sammenfaller med de overordnede føringer som er gitt. Det er ingen konkrete gjennomføringsplaner på benytte PKI til kommunikasjon mot pasienter/pårørende men det er besluttet å innlemme benyttelse av PKI ved utvikling av nye tjenester der denne formene for sikkerhet er påkrevd.
Benytter eller har helseforetaket planer om å benytte PKI til sikring av Web Services eller lignende infrastrukturtjenester? Hvordan og til hva?
Planen er å benytte PKI dersom krav til sikringen tilsier det.
Benytter eller har helseforetaket planer om å benytte PKI for andre formål? Angi i tilfelle hvilke og hvordan?
Den overordnede strategi fra Helse Sør vil være å benytte PKI for de formål som er påkrevet og hensiktsmessige. Planer for dette vil legges fortløpene for pågående og nye prosjekter og vil sammenfalle med de overordnede føringene fra eier om krav til bruk av både virksomhets- og personlige sertifikater.
Benytter eller har helseforetaket planer om å benytte andre mekanismer for sterk autentisering (for eksempel engangspassord, "passordkalkulator"? Angi i tilfelle hvilke og hvordan?
Det benyttes passordkalkulatorerer for ekstern pålogging til noen av helseforetakenes nettverk
Benytter eller har helseforetaket planer om å benytte rammeavtalen for PKI i helsesektoren, utsteder helseforetaket sertifikater selv eller benyttes annen leverandør av PKI-tjenster?
Helse Sør benytter rammeavtalen til Ergo

6.3.2. Dagens rammeavtale for PKI

Rikstrygdeverket har inngått en rammeavtale for PKI på vegne av helsesektoren. Denne delen fokuserer på bruk og effekt av denne.

Hvor godt er helseforetaket kjent med dagens rammeavtale for PKI i helse- og sosialsektoren (inngått av Rikstrygdeverket)?
Avtalen er kjent i Helse Sør. Det sås tvil om RTVs rammeavtale er juridisk holdbar som avtale for det enkelte helseforetaket.
Har dere anskaffet virksomhetssertifikat under avtalen? I tilfelle ja, hvor mange?
Alle helseforetakene i Helse Sør har anskaffet virksomhetssertifikater gjennom denne avtalen.
Har dere anskaffet personlige sertifikat under avtalen? I tilfelle ja, hvor mange?
Foreløpig ikke (forbehold om manglende kartlegging)
Er helseforetaket fornøyd med PKI-tjenestene som leveres over dagens rammeavtale, evt. Hva kunne vært forbedret eller mangler?
Det har fremkommet generelle kommentarer til avtalen der kritikken spesielt har gått på kostbarheten ifbm.anskaffelse av personlige sertifikater. I tillegg er leverandøren blitt kritisert for ikke å kunne gi gode nok oversikter over avtalen samt produkt og kundeoversikter.
Er helseforetaket fornøyd med betingelsene knyttet til dagens rammeavtale, evt. hva kunne vært forbedret eller mangler?
Se punkt over.
Hva vurderer du/dere som de viktigste hindringene for bruk av PKI på virksomhetsnivå for helseforetaket i dag?
Det er få hindringer, men bruk og behov må samsvare. Per nå er det signalisert et behov for teknologien knyttet til meldingsutveksling.
Hva vurderer du/dere som de viktigste hindringene for bruk av PKI på personlig nivå fr helseforetaket i dag?
På anskaffelse av personlige sertifikater spiller de høye kostnadene en rolle. i tillegg til problemstillinger ifbm. infrastruktur,, administrasjon og opplæring.

6.3.3. Fremtidig PKI-løsning for helsesektoren

Denne delen fokuserer på behov og modell for PKI-løsning for helsesektoren i framtiden.

Hva slags tjenester bør inngå i en PKI-tjeneste etter helseforetakets mening?
Det bør eksistere et utvalg av tjenester som helseforetakene kan gjøre avrop mot. Alt fra avanserte løsninger (helintegrert bruk av kortet) til enkle løsninger (for eksempel kun tilgangskontroll).
Hva slags typer PKI-sertifikater bør benyttes i helsesektoren (f.eks. sikkerhetsnivå, virksomhetsnivå, personlig, ansatt/rolle osv)?
Det bør tilbys virksomhetssertifikater og person høy. Tjenesten må kunne tilbys til alle ansatte, men også være fleksibel med hensyn til at kun enkelte roller tildeles sertifikater.
Hva slags typer PKI-sertifikater har eller vil ditt/deres helseforetak ha behov for i framtiden?
Ikke kartlagt…
Hvordan ser helseforetaket for seg å benytte PKI-løsninger på lengre sikt (5-årsperspektiv)?
PKI vil benyttes i takt med behov som fremkommer og de føringer som er gitt som kommentert tidligere.
Hvilke sikkerhetskrav bør stilles til PKI-sertifikater i helsesektoren (for eksempel ift. utstedelse av sertifikater, kontroll av legitimasjon, lagring av nøkkel (smartkort/software) osv.)
Helseforetakene bør legge seg på et nivå som gjør det mulig å kryssertifisere sertifikatene med andre virksomheter slik at man kun må ha ett sertifikat å forholde seg til.
Hva slags tjenester bør PKI-tjenester støtte? (pålogging, e-post, signering, kryptering, annet? Hva bør prioriteres?)
Tjeneste bør dekke et vidt spekter som pålogging, e-post, kryptering, signering, kryssertifisering. Tjenesten bør også settes i sammenheng med registreringsoppgaver som helsepersonellet utfører i dag, bl.a. registrering i fm uthenting av blod fra blodbanken. (Her kan det være behov for en kartlegging).
Bør det stilles spesielle krav til innhold og format for PKI-sertifikater i helsesektoren?
Dette skal være utredet i tidligere prosjekt fra Shdir ang. for bruk at PKI i helsesektoren..

Ønsker helseforetaket å koble PKI og sertifikattjenester med andre lokale tjenester, for eksempel lokal kortutstedelse, fysisk adgangskontroll osv.?
Ja, med mulighet for trinnvis utrulling. Kort som anskaffes bør inneholde en kombinasjon av sertifikat, magnetstriper og antenne.
Hvordan bør en PKI-løsning for helsesektoren forvaltes? Hvem bør eie og hvem bør drifte en PKI-løsning for helsesektoren? Hvorfor?
Det bør eksistere en nasjonal CA med RA ute i helseforetakene.
Hvordan bør PKI-løsninger i helsesektoren finansieres? (Noen modeller er betaling pr. transaksjon/bruk (signering/kryptering/validering) eller betaling pr. sertifikat og fri bruk av dette (frikjøp), andre modeller?) Hvilke finansieringsalternativ bør vurderes/velges?
Betaling per sertifikat.
Hvordan bør bruk av PKI-løsninger samordnes mellom helseforetakene? Hva må koordineres? Hvilke tiltak bør iversettes for å sikre koordingering?
Bør eksistere mulighet for kryssertifisering og mulighet for flere sertifikater på ett kort.
Hvordan bør helsesektorens PKI-løsninger forholde seg til nasjonale løsninger for PKI (for eksempel sikkerhetsportal, kravspesifikasjon for PKI i offentlig sektor)?
Se tidligere besvarelse.

6.3.4. Annet

Andre kommentarer fra helseforetaket?

6.4. Helse Vest

6.4.1. Behov for PKI i helseforetaket

PKI kan benyttes på ulike måter i helseforetakene, ift. signatur og kryptering ved meldingsutveksling både på personlig nivå, virksomhetsnivå osv. Mange benytter seg av sertifikater utstedt under RTV's rammeavtale for PKI, mens andre utsteder og håndterer lokale sertifikattjenester. Denne hoveddelen søker å kartlegge behovet for PKI-løsninger.

Forord: Besvarelsene er besvart av Helse Vest IKT påvegne av alle de ulike Helseforatak i Helse Vest.

Benytter eller har helseforetaket planer om å benytte PKI til personlig signatur på elektroniske meldinger (sykmelding/legeerklæring)? Hvordan og til hva?
NEI
Benytter eller har helseforetaket planer om å benytte PKI til sikring av meldingsutveksling på virksomhetsnivå (POLK, elektronisk fødselsmelding, andre meldinger?) Hvordan og til hva? Hvem utsteder sertifikatene?
De skal benyttes organisasjonssertifikater fra ERGO til signering/krypteinrg av POLK og Fødselsmeldinger. (ebXML) tidsplan estimert til sommer 2006. I tillegg motar enkelte legekontor meldinger fra Helse Bergen via SMIME, dette er sertifikater som er utsedet av Helse Vest IKT selv.
Benytter eller har helseforetaket planer om å benytte PKI til autentisering/pålogging internt i foretaket? Hvordan og til hva? Hvem utsteder sertifikatene?
Helse Vest IKT leverer i dag "fjernaksess" løsnining basert på personlig PKI og Smartkort. Dette er mulig å benytte i alle foretak i Helse Vest, men mest utbredt i Helse Berge og Helse Vest IKT selv.
Benytter eller har helseforetaket planer om å benytte PKI til kommunikasjon mot pasienter/pårørende? Hvordan og til hva?
NEI
Benytter eller har helseforetaket planer om å benytte PKI til sikring av Web Services eller lignende infrastrukturtjenester? Hvordan og til hva?

Det foreligger muligheter for dette i de sertifikater som utsedes av Helse Vest IKT, men det foreligger pr.dd ingen konkrete planer om bruksområder.
Benytter eller har helseforetaket planer om å benytte PKI for andre formål? Angi i tilfelle hvilke og hvordan?
NEI
Benytter eller har helseforetaket planer om å benytte andre mekanismer for sterk autentisering (for eksempel engangspassord, "passordkalkulator"? Angi i tilfelle hvilke og hvordan?
NEI
Benytter eller har helseforetaket planer om å benytte rammeavtalen for PKI i helsesektoren, utsteder helseforetaket sertifikater selv eller benyttes annen leverandør av PKI-tjenster?
Ergo leverer organisasjonsertifikater mens Helse Vest IKT selv står for utstedelse av personsertifikater.

6.4.2. Dagens rammeavtale for PKI

Rikstrygdeverket har inngått en rammeavtale for PKI på vegne av helsesektoren. Denne delen fokuserer på bruk og effekt av denne.

Hvor godt er helseforetaket kjent med dagens rammeavtale for PKI i helse- og sosialsektoren (inngått av Rikstrygdeverket)?
Foretakene er lite kjent med både PKI og rammeavtalen med ergo. Helse Vest IKT derimot har god kjenskap til både PKI og rammeavtalen.
Har dere anskaffet virksomhetssertifikat under avtalen? I tilfelle ja, hvor mange?
Ja, et antall på 5, er stigende.
Har dere anskaffet personlige sertifikat under avtalen? I tilfelle ja, hvor mange?
Nei
Er helseforetaket fornøyd med PKI-tjenestene som leveres over dagens rammeavtale, evt. Hva

kunne vært forbedret eller mangler?
Anskaffelse og bruk er helt ok, men prisen for personlige sertifikater er urimelige iforhold til det det koster og forvalte/utsdede et personlig sertifikat. Samt at levetiden for et sertifikat er for kort.
Er helseforetaket fornøyd med betingelsene knyttet til dagens rammeavtale, evt. hva kunne vært forbedret eller mangler?
Sjekkes ifht andre notater NIBO
Hva vurderer du/dere som de viktigste hindringene for bruk av PKI på virksomhetsnivå for helseforetaket i dag?
Liten eller null gevinst og høy pris.
Hva vurderer du/dere som de viktigste hindringene for bruk av PKI på personlig nivå for helseforetaket i dag?
Uklare gevinster og meget høy anaskaffelse- og innføringskostnader.

6.4.3. Fremtidig PKI-løsning for helsesektoren

Denne delen fokuserer på behov og modell for PKI-løsning for helsesektoren i framtiden.

Hva slags tjenester bør inngå i en PKI-tjeneste etter helseforetakets mening?
Personlige sertifikater og er knyttet til personer og roller og leverandøravhenig, sertifiakter kan gjennbrukes i felere ulikeløsninger. Med felleskataloger osv…
Hva slags typer PKI-sertifikater bør benyttes i helsesektoren (f.eks. sikkerhetsnivå, virksomhetsnivå, personlig, ansatt/rolle osv)?
Det bør eksistere to sertifikater, et for virksomhet og et personlig. Funksjoner, roller og rettihgeter bør knyttes til sertfikat via sentrale katalog(er)/systemene.
Hva slags typer PKI-sertifikater har eller vil ditt/deres helseforetak ha behov for i framtiden?
Ser over!
Hvordan ser helseforetaket for seg å benytte PKI-løsninger på lengre sikt (5-årsperspektiv)?

I de tilfellene der det er veldig viktig å vite hvilken person / organisajson som en kommuniserer med. Eller det sannsyneligheten for at en kompromitering er høy.
Hvilke sikkerhetskrav bør stilles til PKI-sertifikater i helsesektoren (for eksempel ift. utstedelse av sertifikater, kontroll av legitimasjon, lagring av nøkkel (smartkort/software) osv.)
Sikkerhetskrav skal alltids fremkomme i en risikovurdering ifht. de krav og konsekvenser som ligger i grunn.
Hva slags tjenester bør PKI-tjenester støtte? (pålogging, e-post, signering, kryptering, annet? Hva bør prioriteres?) autentisering, signering og kryptering
Bør det stilles spesielle krav til innhold og format for PKI-sertifikater i helsesektoren?
En bør ikke gå utover fastsatte standarder
Ønsker helseforetaket å koble PKI og sertifikattjenester med andre lokale tjenester, for eksempel lokal kortutstedelse, fysisk adgangskontroll osv.?
JA
Hvordan bør en PKI-løsning for helsesektoren forvaltes? Hvem bør eie og hvem bør drifte en PKI-løsning for helsesektoren? Hvorfor?
Enher utsteder av PKI til offentligsektor (helsesektoren) bør ha løsninger for samhandling på tvers.
Hvordan bør PKI-løsninger i helsesektoren finansieres? (Noen modeller er betaling pr. transaksjon/bruk (signering/kryptering/validering) eller betaling pr. sertifikat og fri bruk av dette (frikjøp), andre modeller?) Hvilke finansieringsalternativ bør vurderes/velges?
Kostmodell bør gjenspeile kostnader med drift og forvalting av en tjeneste
Hvordan bør bruk av PKI-løsninger samordnes mellom helseforetakene? Hva må koordineres? Hvilke tiltak bør iversettes for å sikre koordingering?
Se tok pkt opp.
Hvordan bør helsesektorens PKI-løsninger forholde seg til nasjonale løsninger for PKI (for

eksempel sikkerhetsportal, kravspesifikasjon for PKI i offentlig sektor)?
Kravspesifikasjon for PKI i offentlig sektor

6.4.4. Annet

Andre kommentarer fra helseforetaket?
Mye bør drøftes

Referanseliste

Strategi for PKI-avtaler for helsevesenet - Forslag fra arbeidsgruppe - Utarbeidet av arbeidsgruppe ledet av ShDir, 6.3.2006

Kravspesifikasjon for PKI i offentlig sektor Versjon 1.02, januar 2005 – Vedlikeholdes av Fornyings- og administrasjonsdepartementet