

# **Anbefalinger og standarder for PKI i helsesektoren**

**Versjon 1.1**

**Dato: 14.10.2004**

**KITH Rapport 13/04**

**ISBN 82-7846-230-5**

# KITH-rapport



## TITTEL

**Anbefalinger og standarder for PKI i helsesektoren**

Forfatter(e): Arnstein Vestad

Oppdragsgiver(e)

SSP

Postadresse  
**Sukkerhuset  
N-7489 Trondheim**

Besøksadresse  
**Sverresgt 15**

Telefon  
**+47 - 73 59 86 00**

Telefaks  
**+47 - 73 59 86 11**

e-post  
[firmapost@kith.no](mailto:firmapost@kith.no)

Foretaksnummer  
**959 925 496**

ISBN	Dato	Antall sider	Kvalitetssikret av
82-7846-228-3		17	Bjarte Aksnes

Gradering

Godkjent av:

Rapportnr:

11/04

Sammendrag

Rapporten oppsummerer anbefalinger og standarder for bruk av PKI i helsesektoren. Rapporten har tatt utgangspunkt i tidligere arbeid, bl.a. forprosjekt for PKI, arbeidet med rammeavtale for PKI i helsesektoren inngått av Trygdeetaten i 2002 samt erfaringer i ettertid, og gir veiledning og anbefalinger for valg av standarder og implementering av pki-løsninger i helsesektoren.

# Innholdsfortegnelse

<b>Innholdsfortegnelse .....</b>	<b>3</b>
<b>1. Tekniske standarder for PKI .....</b>	<b>5</b>
1.1. Personlige sertifikater og virksomhetssertifikater .....	6
1.2. Kvalifiserte sertifikater og signaturer .....	6
1.3. Rammeverk for meldingsutveksling.....	7
<b>2. Formater .....</b>	<b>9</b>
2.1. Sertifikatformat .....	9
2.1.1. Personlige sertifikater .....	9
2.1.2. Virksomhetssertifikat.....	10
2.2. XMLDsig.....	10
2.3. S/MIME.....	11
2.4. Anbefalinger for signaturformat.....	12
<b>3. PKI-tjenester .....</b>	<b>13</b>
3.1. Krav til utstedere av kvalifiserte sertifikater .....	13
3.2. Krav til utstedere av virksomhetssertifikater.....	13
3.3. Katalogtjenester .....	14
3.4. Sperretjenester .....	14
<b>4. Sikker bruk av PKI.....</b>	<b>15</b>
4.1. Kvalifiserte sertifikater og signaturer .....	15

4.2.	Anbefalinger for implementering av PKI i fagsystemer .....	15
4.3.	Presentasjon før framvisning.....	16
4.4.	Symmetrisk kryptering.....	16
<b>5.</b>	<b>Tekniske krav til samtrafikk.....</b>	<b>17</b>
5.1.	Tilgang til sertifikater.....	18
5.2.	Tilgang til sperreinformasjon.....	18
5.3.	Kryssertifisering, brosertifisering og annet.....	19
5.4.	Felles signatur- og krypteringsformater.....	19
5.5.	Felles sertifikat-format .....	20
5.6.	Nøkkelbærere.....	20
	<b>Referanseliste .....</b>	<b>21</b>

# 1. Tekniske standarder for PKI

**Dette dokumentet beskriver ulike standarder og anbefalinger for bruk av PKI i helsesektoren. Det vil gis en oversikt over de mest aktuelle standardene og hvordan disse egner seg for signering, kryptering og andre sikkerhetsmekanismer. Dokumentet forutsetter en grunnleggende forståelse av PKI og digitale signaturer. Målgruppen er ansvarlige for anskaffelse av IT-løsninger som skal benytte PKI, samt leverandører av slike løsninger.**

Under og i forkant av utarbeidelsen av rammeavtalen for PKI i helsesektoren (v. RTV) (Se referanser) ble det gjort et arbeid for å identifisere de viktigste standarder, formater og protokoller for PKI med formål å inkludere disse i kravspesifikasjonen. Dette dokumentet vil ta utgangspunkt i standardene som rammeavtalen henviser til, samt senere erfaringer og utvikling på området.

Kapittel 1 beskriver grunnleggende begreper som personlige sertifikater og virksomhetssertifikater, samt gir en overordnet beskrivelse av bruken av sikkerhetsmekanismer i rammeverk for meldingsutveksling i helsesektoren.

Kapittel 2 beskriver aktuelle formater for sertifikater og digitale signaturer.

Kapittel 3 beskriver krav knyttet til PKI-tjenesten, som krav til utstedere, krav til protokoller for kommunikasjon mot TTP-tjenesten osv.

Kapittel 4 skisserer aktuelle krav knyttet til bruken av PKI-tjenster, bl.a. krav knyttet til hvordan PKI-tjenesten skal benyttes av brukeren i ulike fagapplikasjoner osv.

Til slutt gis en referanse-liste for aktuell standarder og bakgrunnsdokumenter som dette dokumentet refererer til eller bygger på.

## 1.1. Personlige sertifikater og virksomhetssertifikater

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

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

I hvilke tilfeller det er ønskelig å benytte personlige sertifikater evt. virksomhetssertifikater avhenger av en rekke ulike faktorer og blir en avveining mellom juridiske faktorer, tekniske muligheter, brukervennlighet og annet. Signatur med en personlig signatur på en meldings sikrer entydig at meldingen er godkjent og stammer fra en enkeltperson. Særlig for meldinger som er knyttet til spesielle autorisasjoner vil dette være viktig, som resept og sykmelding. For andre typer meldinger, som timebestillinger vil dette være av mindre betydning. Også disse meldingene må ha et minimumsnivå av sikkerhet men løsningene behøver ikke i samme grad å være knyttet til enkeltperson via en ikke-benektelsesfunksjon.

## 1.2. Kvalifiserte sertifikater og signaturer

Kvalifiserte sertifikater er sertifikater utstedt etter en sertifikatpolicy som er i tråd med lov om elektronisk signatur og av en utsteder som er registrert av Post- og teletilsynet. Lovverket (og EU-direktivet det bygger på) stiller krav til utstedere av kvalifiserte sertifikater, bl.a. om ansvar for at opplysninger i sertifikatet er korrekt, krav til prosedyrer, økonomisk soliditet osv.

En fordel med kvalifiserte sertifikater er at de etablerer sikkerhetsnivå som er omforent og presumptivt relativt lett å kommunisere til sluttbrukere. Ved å velge et sikkerhetsnivå for sertifikatene som bygger på det aktuelle lovverket får man også de offentlige tilsynsordningene ”med på kjøpet”. I tillegg skaper man et minimumsnivå med en akseptabel sikkerhet rundt utstedelse og produksjon av sertifikatene slik at behovet for individuell vurdering av de aktuelle sertifikatpolicyene reduseres.

Kvalifiserte signaturer defineres i loven som avanserte elektroniske signaturer påført med et kvalifisert sertifikat og ved hjelp av et sikkert signaturframstillingssystem. Sikre signaturframstillingssystemer er godkjente enheter, f.eks. smartkort eller annet, som benyttes for å sikre den private nøkkelen.

### 1.3. Rammeverk for meldingsutveksling

Rammeverk for meldingsutveksling er beskrevet i KITH-rapport R-25/02 Rammeverk for meldingsutveksling (versjon 0.90). Der beskrives et rammeverk for utveksling av meldinger som omfatter innpakking, overføring over ulike protokoller (som SMTP og HTTP), signering og kryptering.

Rammeverket støtter sikkerhetsmekanismer på flere nivå:

- Applikasjonsnivå: En konkret melding kan ha støtte for signering, kryptering osv., dette avhenger av meldingsformatet. For XML-meldinger er det foreløpig XML-Dsig som beskrives senere som er aktuelt. I tillegg vil en melding som inneholder sensitiv informasjon ha behov for kryptering. Det anbefales primært at dette utføres vha. kryptering av meldingen iht. S/MIME og innpakking som MIME-objekt av typen "application/pkcs7".
- Konvoluttnivå: Selve rammeverket inneholder også støtte for signatur-funksjonalitet via XML-Dsig – denne signaturen vil omfatte payload (meldingen) og XML-elementene i konvolutten, for å sikre dennes integritet. Signaturen vil være på virksomhetsnivå
- Nettverksnivå / transportnivå: Ved overføring over http kan sikkerhetsprotokoller som SSL/TLS benyttes, evt. ulike løsninger for kryptering på nettverksnivå (VPN o.l.).

Ift. bruk av hhv. virksomhetssertifikater eller personlige sertifikater anbefales det generelt at personlige sertifikater benyttes til signering av meldinger (på applikasjonsnivå) når dette er påkrevd av anvendelsen (f.eks. sykmelding eller resept). For kryptering anbefales det generelt at virksomhetssertifikater benyttes for å sikre at meldinger kan mottas hos en helsevirksomhet uten å være avhengig av tilstedeværelse av enkeltpersoner som kan dekryptere meldingen.

På konvoluttnivå anbefales det generelt at det kun benyttes virksomhetssertifikater, særlig fordi konvolutten skal behandles utelukkende automatisk og ikke bør være avhengig av brukerinteraksjon i forbindelse med dekryptering og signering.

For utdypende informasjon om de ulike standardene henvises til etterfølgende kapitler samt referanselisten. For implementasjonsdetaljer henvises til R-25/02 Rammeverk for meldingsutveksling (versjon 0.90).

## 2. Formater

**Bruk av PKI for sikker kommunikasjon forutsetter en rekke standardiserte formater, bl.a. for sertifikatet og for representasjon av signaturen. De ulike formatene kan ha ulike fordeler og ulemper, f.eks. hvorvidt signaturformatet støtter både signatur og kryptering, hvorvidt sertifikatet skal identifisere personer eller virksomheter osv.**

For sertifikater skiller vi i hovedsak mellom virksomhetssertifikater og personsertifikater, avhengig av hva som skal identifiseres av sertifikatet. Anbefalte standarder for personsertifikat baserer seg på ETSI-standarder utarbeidet ihht. EU-direktivet om kvalifisert signatur. For signatur anbefales to hovedformat, hhv. XML-Dsig og S/MIME.

### 2.1. Sertifikatformat

Det skilles i hovedsak mellom to typer sertifikater – personlige sertifikater og virksomhetssertifikater.

Nøkkellengden som benyttes i sertifikatet er avgjørende for sikkerheten. Etter hvert som beregningskraften i IT-systemer øker vil også behovet for større nøkler øke. Pr. dags dato anbefales en minimums nøkkellengde på 1024 bits. Dette anses som tilstrekkelig for anvendelser med

Ulike anbefalinger er gitt for antall nøkkelpar i sertifikater. Det finnes gode argumenter for å benytte 3 nøkkelpar, et for signatur, et for autentisering og et for kryptering. Etablert praksis tilsier likevel bruk av 2 nøkkelpar, hvor sertifikat for autentisering og kryptering kombineres. Hvis sertifikatet skal benyttes for personlige signaturer som stiller krav til ikke-benektning skal et nøkkelpar dedikeres til dette formålet (Key-usage = non-repudiation)

#### 2.1.1. Personlige sertifikater

Sertifikater for elektroniske signaturer bør følge de europeiske standardene for kvalifiserte sertifikater. Dette sikrer overensstemmelse m. lov om elektroniske signaturer og dermed at sertifikatet kan benyttes

til å generere en kvalifisert signatur. Gjeldende standard for kvalifiserte sertifikater er ETSI TS 101 862 v 1.2.1 ” Qualified Certificate Profile”. Denne standarden er en utvidelse av en IETF RFC for kvalifiserte sertifikater som igjen bygger på RFC 2459 som er den gjeldende standard for internett-sertifikater basert på x.509 v. 3. Sertifikatet skal dermed være kompatibelt m. alle typiske applikasjoner som sikker e-post, web-sertifikater o.l.

Sertifikatet må inneholde en entydig identifikator som identifiserer innehaver av sertifikatet. En slik identifikator kan være fødselsnummer, helsepersonellnummer, HER-id (id fra Helse Enhetsregisteret) eller annet løpenummer. Normalt sett er det ikke ønskelig å la sertifikatet inneholde fødselsnummer. Siden det i en del tilfeller vil være nødvendig å knytte sertifikatet til fødselsnummer må sertifikatutsteder bevare en kobling mellom den unike id'en i sertifikatet og fødselsnummer og kunne tilby denne til autoriserte brukere.

## 2.1.2. Virksomhets sertifikat

For virksomhets sertifikater er det ikke etablert profiler tilsvarende for personlige sertifikater. Det er likevel flere krav som bør stilles:

- Hovedformat for sertifikatet er RFC 2459.
- NOU 2001:10 – Uten penn og blekk – Vedlegg 2 gir anbefalinger for sertifikatprofil for virksomhets sertifikater ift. innhold i sertifikatfeltene
- Virksomheter skal identifiseres iht. organisasjonsnummer i Enhetsregisteret. Hvis det skal benyttes annen form for id-nummer må dette være entydig og klart definert, samt at eierskap, organisering og ansvar knyttet til sertifikatet er klart.

## 2.2. XMLDsig

XML-Dsig er en standard for å representere digitale signaturer vha. XML. XML-Dsig er fleksibelt og kan benyttes til å signere hele eller deler av et XML-dokument samt andre typer data som kan refereres vha. en URI.

Det er tre hovedtyper XML-signatur:

- Enveloped: XML-signaturen er inkludert i XML-dokumentet. XML-signaturen er et underelement i dokumentet.
- Enveloping: XML-signaturen omfavner dokumentet. Det som signeres er underelementer i XML-signaturen.
- Detached: Signaturen refererer til et eksternt dataobjekt vha. en URI.

Signering vha. XML-Dsig innebærer følgende steg:

1. Avgjøre hvilke elementer/ressurser som skal signeres
2. Beregne "digest" (hash-verdi) for ressursene
3. Legge URI, evt. transforms, digest-metode og resultat inn i et <Reference>-element, og samle alle <Reference>-element i et <SignedInfo>-element.
4. Beregne digest for <SignedInfo>-elementet og signere dette, resultatet legges inn i et <SignatureValue>-element.
5. Evt. nøkkelinformasjon kan legges inn i et <KeyInfo>-element.
6. Alle elementene legges så inn i et <Signature>-element.

Endring av en meldingsstandard for å kunne tilby XML-dsig innebærer å endre schema-definisjonen til å inkludere et XML-Dsig-element, en endring som innebærer minimale konsekvenser, og både framtidige og eksisterende meldinger vil kunne tilpasses. Pr. dags dato er sykmelding og resept allerede tilpasset slik signatur. Primært vil dette innebære å benytte "enveloped signature" m. en transform av typen "http://www.w3.org/2000/09/xmldsig#enveloped-signature" - som sikrer at hele meldingen minus selve signatur-elementet tas med i signaturberegningen.

## 2.3. S/MIME

S/MIME er i utgangspunktet en standard utviklet for uveksling av sikker e-post, og støtter kryptering og signering av e-post-meldinger. S/MIME baserer seg på en samling av IETF-standarder, særlig:

- S/MIME Version 3 Message Specification (RFC 2633)
- Cryptographic Message Syntax (RFC 3369)

- S/MIME Version 3 Certificate Handling (RFC 2632)

I tillegg avhenger S/MIME av MIME-standarden.

S/MIME har relativt stor utbredelse, og en rekke meldingsapplikasjoner, f.eks. epostlesere som Microsoft Outlook, støtter standarden. I tillegg eksisterer det en rekke programmeringspakker som kan benyttes ved utvikling av applikasjoner som skal benytte standarden.

## 2.4. Anbefalinger for signaturformat

Både XML-Dsig og S/MIME vil ha anvendelser innen helsesektoren.. En viktig fordel med S/MIME er at formatet støtter både signering og kryptering. Det eksisterer en standard for kryptering av XML-meldinger og representasjon av den krypterte informasjonen i XML – XML-encryption, men denne er foreløpig relativt lite utbredt. Når meldingsutvekslingen har behov for kryptering anbefales det derfor at S/MIME (som anbefalt i ENV 13608-2) anvendes, også om meldingen benytter seg av signatur i form av XML-dsig i selve meldingen. Rammeverk for meldingskommunikasjon som beskrevet overfor benytter ENV 13608-2 som innpakking av meldingen for kryptering.

For meldinger som har behov for personlig elektronisk signatur med høy grad av tillit, som sykmelding, resept o.l., bør meldingene tilpasses til å støtte XML-Dsig. Meldingen bør fortrinnsvis benytte enveloped-signature over hele meldingen med mindre særskilte behov tilsier at signatur kun over enkeltelementer i meldingen er nødvendig.

## 3. PKI-tjenester

**En komplett PKI-tjeneste omfatter flere ulike deltjenester, som sertifikatutstedelse og tilgjengeliggjøring i en katalog, tilby sperretjenester osv.**

**En rekke tjenester i helsenettet vil være avhengig av sikkerheten og tilgjengeligheten til disse tjenestene og det er derfor nødvendig å stille klare krav til utsteder av sertifikatene, bl.a. til hvilke tjenester som skal tilbys.**

### 3.1. Krav til utstedere av kvalifiserte sertifikater

Utstedere av kvalifiserte sertifikater skal følge kravene i i ETSI TS 101 456 "Policy requirements for certification authorities issuing qualified certificates". Dokumentet stiller krav bl.a. til utstederens prosedyrer for identitetskontroll, utstedelsen av sertifikatene, fysisk sikkerhet, informasjonssikkerhet og beredskapshåndtering.

Utstederen må sikre at personopplysninger som legges inn i sertifikatet er kontrollert opp mot offentlig register. For ID gjelder dette fødselsnummer og navn. Hvis sertifikatet skal inneholde annen informasjon, f.eks. knyttet til autorisasjoner osv. må utstederen verifisere disse opp mot autorativ kilde.

Siden flere brukersteder/mottakere av signaturer har behov for å identifisere brukere på bakgrunn av fødselsnummer og sertifikatet normalt ikke vil inneholde fødselsnummer, må utstederen tilby grensesnitt for verifikasjon av fødselsnummer. Denne tjenesten må kreve autentisering før bruk, slik at bare autoriserte brukere har tilgang til å koble sertifikat og fødselsnummer.

Utsteder må ha rutiner som sikrer at kvalifiserte sertifikater kun utstedes til personer som har vist fysisk legitimasjon til en kontrollinstans i løpet av utstedelsesprosessen.

### 3.2. Krav til utstedere av virksomhetssertifikater

Utstedelsesprosessen må ha rutiner som sikrer at kun personer med autorisasjon får tilgang til sertifikatet. Dette kan f.eks. innebære at sertifikatet sendes rekommandert til noen med myndighet til å signere på vegne av virksomheten. Sikkerhetsnivået rundt utstedelsen av sertifikatene bør ellers være på linje m. kravene til kvalifiserte sertifikater.

Private nøkler kan lagres som software-nøkkel. Utsteder bør kunne overføre og tilby nøklene i PKCS #12-format.

### **3.3. Katalogtjenester**

Katalog for sertifikater bør være tilgjengelig som LDAP v.3.

Katalogtjenesten bør ha mulighet for å legge inn adgangsbegrensninger for enkelte typer informasjon.

### **3.4. Sperretjenester**

Ulike faktorer kan medføre behov for sperring av sertifikater, f.eks. tap av privat nøkkel, tap av rettigheter knyttet til sertifikatet osv. Et brukersted som skal autentisere brukere vha. av sertifikater har derfor behov for å kontrollere sperre-informasjonen om sertifikatet. Pr. i dag er det to hovedløsninger for kontroll av revokeringsinformasjon: CLR (Certificate revocation list) eller sperreliste og OCSP (Online certificate status protocol) – online-tjeneste for sertifikatstatus.

Ved revokering må informasjon gjøres tilgjengelig i tilbaketrekkingsliste uten ugrunnet opphold. Sertifikatets `crldistributionPoint`-attributt skal peke til tilbaketrekkingslisten. CRL bør være i henhold til RFC 2459.

Ved revokering bør informasjon også gjøres tilgjengelig vha. en OCSP-tjeneste som definert i RFC 2560. Sertifikatets `AuthorityInfoAccess`-felt skal peke til OCSP-tjenesten.

## **4. Sikker bruk av PKI**

**Sikkerheten i PKI-løsningene forutsetter at bruken av løsningen foregår på en sikker måte. Særlig er det viktig at den private nøkkelen oppbevares sikkert, ved bruk av løsninger for kvalifisert signatur endog på en måte som sikrer at ikke brukeren selv kan ha tilgang til nøkkelen direkte. Sikker bruk av PKI innebærer også at brukergrensesnittet i applikasjoner som benytter PKI er brukervennlige og bistår brukeren i å utnytte signatur og kryptering på en sikker måte.**

### **4.1. Kvalifiserte sertifikater og signaturer**

Sertifikater for bruk til personlig signatur av meldinger bør være kvalifiserte. Dette sikrer at informasjonen i sertifikatet er kvalitetssikret av en uavhengig tredjepart med strenge krav til kvalitet og rutiner. Sertifikatene vil dermed kunne benyttes til å kommunisere mot andre parter også utenfor egen virksomhet.

Kvalifiserte signaturer vil ihht. lov om elektroniske signaturer sidestilles med papir-signaturer, noe som har fordeler i en del sammenhenger. Det anses likevel ennå (pr. juni 2004) for tidlig å stille krav om bruk av sikkert signaturframstillingssystem, bl.a. siden slike løsninger ennå ikke er i tilstrekkelig grad standardisert og utbredt i alle aktuelle brukermiljø.

### **4.2. Anbefalinger for implementering av PKI i fagsystemer**

CWA 14170 – "Security Requirements for Signature Creation Applications" gir krav og anbefalinger knyttet til implementasjon av PKI og signering i applikasjoner og vil kunne ha anvendelse på bl.a. fagsystemer som EPJ.

### **4.3. Presentasjon før framvisning**

Ved signering er det et naturlig krav at bruker skal ha full oversikt over hva som signeres. Dette forutsetter at brukeren gis en entydig representasjon av innholdet som skal signeres og at brukeren har mulighet til å få en fullstendig oversikt over hva som signeres. Dokumentet som signeres bør ikke inneholde skjulte felter eller aktiv kode som kan gjøre endringer i dokumentet.

### **4.4. Symmetrisk kryptering**

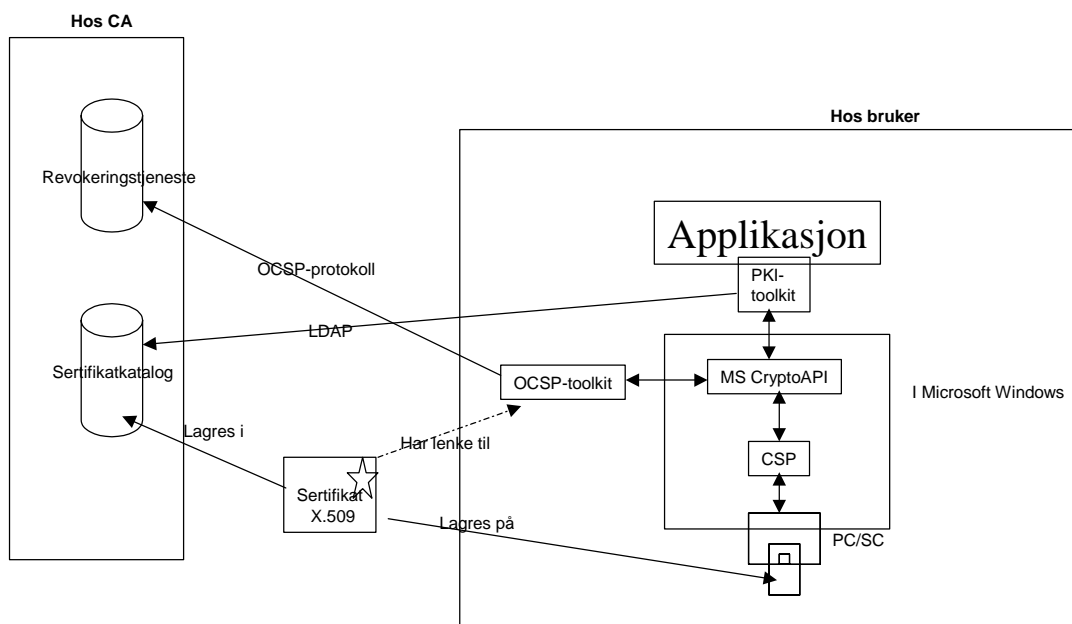
Datatilsynet stiller krav til at sensitive personopplysninger skal krypteres når disse overføres over eksterne datanett. For tiden stilles det krav om at krypteringsstyrken skal tilsvare DES128, dvs. kryptering med DES-algoritmen kombinert m. en effektiv symmetrisk nøkkellengde på 112 bits.

## 5. Tekniske krav til samtrafikk

**Samtrafikk skal sikre at PKI-tjenester fra ulike leverandører kan samvirke. Dette innebærer bl.a. at brukere skal kunne benytte sertifikater fra ulike leverandører og at ulike applikasjoner med pki-funksjonalitet kan utveksle informasjon.**

Samtrafikk er ønskelig av økonomiske og praktiske grunner, men reiser en rekke utfordringer både av teknisk, økonomisk og organisatorisk art. Dette dokumentet oppsummerer helsevesenets valg av tekniske løsninger for å sikre interoperabilitet mellom PKI-løsninger levert av ulike leverandører og mellom IT-løsninger med PKI-funksjonalitet levert av ulike leverandører.

Figuren nedenfor gir en oversikt over noen av de grensesnitt, protokoller og formater som er standardiserte og kan bidra til samtrafikk mellom ulike leverandører av PKI-tjenester.



**Figur – Protokoller og formater for samtrafikk**

## 5.1. Tilgang til sertifikater

Tilgang til sertifikater er primært nødvendig når en avsender skal kryptere informasjon til en mottaker og ikke allerede har lagret sertifikatet i lokalt lager. I mange typiske bruksscenarioer overføres avsenders sertifikat sammen med den signerte informasjonen eller når brukeren autentiserer seg mot en tjeneste. I tilfeller hvor dette ikke er tilfelle legges sertifikater i en PKI-leverandørs sertifikatkatalog.

For elektronisk samhandling innen helsesektoren er HER-registeret tenkt som sentral katalogtjeneste for informasjon om enheter som kan kommunisere. HER-registeret bør derfor ha informasjon som peker til en enhets sertifikat, enten i form av selve sertifikatet eller en lenke til PKI-leverandørens sertifikat-katalog.

Det eksisterer ulike løsninger for å sikre at brukere fra ulike sertifikat-leverandører kan få tilgang til sertifikater utstedt av andre leverandører. Enkelte løsninger innebærer at hver enkelt leverandør pålegges å videreformidle informasjon fra andre leverandører, for eksempel alle leverandører innen en rammeavtale. Andre løsninger innebærer bruk av metakataloger som aggregerer informasjon fra de ulike leverandørenes katalog-tjenester. Innen helsesektoren kan HER være en slik løsning.

Alle katalog-løsninger bør baseres på LDAP.

## 5.2. Tilgang til sperreinformasjon

For å verifisere en mottatt signatur må mottaker kontrollere at sertifikatet knyttet til signaturen er gyldig, noe som normalt foregår ved å slå opp i en sperre-liste (CRL) eller ved å sjekke sertifikatets status via en online-tjeneste (OCSP)

En sentral utfordring ift. løsninger hvor en leverandør ”går god” for sertifikatene fra en annen leverandør er håndtering av tillit. Siden helsesektoren har valgt å basere sertifikater på lov om elektronisk signatur og kvalifiserte sertifikater, kan denne problemstillingen reduseres noe. De kan da være tenkelig å pålegge de ulike leverandørene å videreformidle oppslag og sperrefunksjoner for andre utstedere av kvalifiserte sertifikater, uten at leverandøren påtar seg et videre ansvar for sertifikatet. Brukerstedet vil likevel ha den sikkerheten som ligger i at det verifiserte sertifikatet er kvalifisert. Dette betyr at man reduserer samtrafikkproblemet for sertifikatverifikasjon til en teknisk løsning for å gå mot en framfor flere leverandører, samtidig som hver enkelt leverandør har ansvar for innhold i sine egne sertifikater.

En slik løsning forutsetter likevel at de ulike leverandørene har tilgjengelig sperreinformasjon som kan integreres i hverandres løsninger, noe som forutsetter standardisert og åpen tilgang, enten gjennom sperreliste eller status-tjeneste.

Aktuelle protokoller for sperretjenester er sperrelister CRL ihht. RFC 3280, evt. online statuskontroll ihht. OCSP (RFC 2560).

### **5.3. Kryssertifisering, brosertifisering og annet**

Kryssertifisering innebærer at ulike PKI-leverandører gjensidig signerer hverandres sertifikater. Dette sikrer at brukere i ulike sertifikat-domener kan stole på sertifikater fra andre utstedere.

Kryssertifisering er en omfattende prosess, som bl.a. innebærer å avklare at de ulike utstederne har sammenfallende sertifikatpolicyer, avklaring av juridiske, avtalemessige og økonomiske rammer osv. Prosessen har derfor vist seg vanskelig å gjennomføre i mange sammenhenger, også pga. manglende incentiver fra leverandørsiden.

Kryssertifisering innebærer primært at utstederne tar risiko og ansvar for hvem sluttbrukeren/sertifikatkontrolløren skal stole på. Dette reduserer kompleksiteten knyttet til tillitsvurderinger for den enkelte sluttbruker. I et lite og oversiktlig marked med få utstedere vil denne problemstillingen være mindre. Hvis alle aktuelle leverandører følger et minimumskrav til utstedelse osv, som kravene i lov om elektronisk signatur reduseres dette behovet ytterligere.

### **5.4. Felles signatur- og krypteringsformater**

Felles signatur- og krypteringsformat sikrer at applikasjoner kan utveksle informasjon som er sikret vha. PKI-løsningen på en standardisert måte. Det eksisterer ulike formater for å sikre dette, og disse formatene kan igjen støtte ulike valg bl.a. av krypterings- og signeringsalgoritmer. I hovedsak er det format som er aktuelle for digitale signaturer:

- XMLDsig – hvor signaturen representeres i XML
- S/MIME – basert på innpakking av signerte objekter i CMS-format – definert i PKCS #7

Valg av format og algoritmer ift. bruk av S/MIME er beskrevet i ENV-13608-2 – ”Secure data objects”.

Hvordan XMLDsig kan benyttes er beskrevet i KITH-rapport R-25/02 Rammeverk for meldingsutveksling i tillegg til XML-Dsig-dokumentet: "XML-Signature Syntax and Processing, RFC 3275".

## 5.5. Felles sertifikat-format

Standardisering av sertifikatformat og innhold er nødvendig for å sikre at ulike PKI-tilpassede applikasjoner og løsninger kan behandle sertifikatene og trekke ut nødvendig informasjon fra disse. Dette innebærer bl.a. at felt som beskriver identitet, hvor sperreinformasjon kan finnes osv. er standardiserte.

Hovedstandard for sertifikatformat basert på X.509 er Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 3280). Denne profilen benyttes både for person- og virksomhetssertifikater. For personlige sertifikater benyttes kvalifiserte sertifikater i tråd med lov om elektronisk signatur. For disse har IETF utviklet: Internet X.509 Public Key Infrastructure: Qualified Certificates Profile (RFC 3739). Denne er utvidet av ETSI til TS 101 862 - V1.2.1 - Qualified certificate profile – som p.t. ligger til grunn for rammeavtalen for PKI i helsesektoren.

## 5.6. Nøkkelbærere

Den private nøkkelen som er knyttet til sertifikatene må oppbevares på et betryggende vis slik at innehaver av sertifikatet har full kontroll med bruken av den private nøkkelen. Eksempler på dette er smartkort, USB-token, krypterte filer osv. For at en bruker skal kunne benytte sine sertifikater og nøkler i en løsning må denne løsningen være kompatibel med den plattform og systemløsning som brukeren befinner seg på. Dette krever ulike lag av standardisering – for smartkort innebærer dette standardisering av smartkort og leser, grensesnitt for smart-kortet, drivere osv. for at smart-kortet skal fungere i operativsystemet osv.

Eksisterende rammeavtale for PKI stiller ikke konkrete krav til disse løsningene. Det er definert to hovedbærere for privat nøkkel – softwarebasert og på smartkort.

Den mest aktuelle standarden for bruk av smartkort på PC-plattform er PC/SC. I tillegg bør krypto-funksjonalitet som minimum være tilgjengelig via MS CryptoAPI.

## Referanseliste

XML-Dsig: XML Digital signature: <http://www.w3.org/Signature/>

S/MIME – S/MIME Mail security: <http://www.ietf.org/html.charters/smime-charter.html>

Lov om elektronisk signatur: <http://www.lovdata.no/all/hl-20010615-081.html>

ETSI TS 101 862 v 1.2.1 ” Qualified Certificate Profile”

KITH-rapport R-25/02 Rammeverk for meldingsutveksling (versjon 0.90):

[http://www.kith.no/vedlegg/14491/R25-02-Rammeverk\\_meldingsutveksling.pdf](http://www.kith.no/vedlegg/14491/R25-02-Rammeverk_meldingsutveksling.pdf)

Rammeavtale for PKI i helsesektoren – se <http://pki.ergo.no/>