Direktoratet for e-helse

Til	Nærings- og fiskeridepartementet
Dato	03.03.2016
Saksnr	15/188-5

Notat

Fra	Direktorat for e-helse
Saksbehandler	Mona Holsve Ofigsbø
Ansvarlig	Christine Bergland

Høringssvar om forslag til lov for gjennomføring av EUs forordning for elektronisk identifisering og tillitstjenester for elektronisk transaksjoner på det indre markedet

Direktorat for e-helse viser til høring på forslag om lov for gjennomføring av EU forordningen for eID og tillitstjenester (910/2014). Forordning 910/2014 ble vedtatt 23. juli 2014, basert på et forslag av Europakommisjonen av 4. juni 2012 (COM(2012) 238 final) og erstatter direktiv om e-signatur, direktiv 1999/93/EC. Forordningen trådte i kraft 17. september 2014 og gjelder direkte i EUs medlemsstater. Forutsatt at forordningen innlemmes i EØS-avtalen, må det gjennomføres i norsk rett med frist 1. juli 2016, jf. artikkel 52, med noen unntak.

Direktoratet stiller seg positive til forslag om lov for hvordan gjennomføre EUs forordning om eID og tillitstjenester. Dette er helt sentralt for å sikre at helseopplysninger kan utveksles over landegrensene og dermed være tilgjengelig for eksempel ved ytelse av helsehjelp i annet land enn bostedsland. Det er derfor viktig å ha en god og tydelig lov på dette som kan anvendes inn i fagmiljøene, samtidig som en tilhørende kravspesifikasjon bør utdype de tekniske kravene fra EU forordningen. Dette vil kunne bidra til en enklere forståelse av de nye reglene for en sektor som har ca 17000 virksomheter som benytter PKI i sitt daglige virke.

Helse- og omsorgsektoren anvender kvalifiserte sertifikater til signering av juridiske dokumenter som e-resept, sykemelding, legeerklæring, oppgjørsmeldinger og til autentisering mot kjernejournal. I tillegg benyttes virksomhetssertifikater til kryptering av helseopplysninger for å overføre helseopplysninger mellom virksomhetene. For eksempel signeres det ca.70 000-75 000 e-resepter per dag og i løpet av 2015 ble det utvekslet over 300 millioner krypterte elektroniske meldinger mellom virksomhetene i helse- og omsorgssektoren. I tillegg til anvendelse av PKI mellom aktørene i helse- og omsorgssektoren, tilbys det digitale e-helsetjenester mot innbyggerne gjennom pålogging mot helsenorge.no hvor det er ID-porten som håndterer autentiseringen.

Departementet har bl.a. særskilt bedt om innspill på:

- *vårt syn på at reglene ikke bør få anvendelse på lukkede systemer,*
- *om det er andre myndigheter enn Nkom som bør ha tilsynsoppgavene etter loven,*
- *om det er behov for å videreføre særhjemmel om esignatur i offentlig sektor,*
- *om det er behov for å beholde selvdeklarasjonsordningen.*

Direktoratet gir innspill på dette under de gjeldende kapitlene for temaene.

Direktorat for e- helse ble etablert 1. januar 2016 og skal sørge for nasjonal styring og koordinering på e- helsefeltet i samarbeid med alle aktørene i helse-Norge helse- og omsorgssektoren. Videre skal direktoratet realisere og forvalte digitale løsninger som forbedrer og forenkler helse-Norge. Direktoratet har derfor fokusert på innspill som gjelder hvordan forordningen vil påvirke bruk av eID og tillitstjenester for e- helse området i helse- og omsorgssektoren, i tillegg til det departementet har bedt særskilt innspill på.

Generelle kommentarer

For å kunne tilrettelegge for en vellykket gjennomføring av de krav som stilles i forordningen vil det være viktig å legge til grunn kompleksitet og erfaringer fra helse- og omsorgssektoren ved bruk av PKI. Direktoratet ønsker å bli involvert i prosessene videre fremover for å kunne sikre at overgang til de nye kravene håndteres og kommuniseres til sektor på en hensiktsmessig og god måte. Direktoratet ønsker videre å påpeke at høringsnotatet fremstår som vanskelig tilgjengelig. Konsekvensene ved gjennomføring av nye krav kommer ikke tydelig frem når det gjelder eventuelle endringer i ansvarsforholdene ved utstedelse av kvalifiserte sertifikater.

Helse- og omsorgssektoren har etablert nærmere 100 (L)RA-funksjoner [1] som vil måtte endre sine rutiner, prosedyrer og muligens systemer for å kunne utstede eID (digitale sertifikater) som følge av nye krav om ID-kontroll. Det vil være en fordel at dagens digitale sertifikater (med tre års levetid) fases ut på en kontrollert måte ved daglig drift og vedlikehold, slik at helsepersonell og IT-systemene ikke blir berørt på en uheldig måte. Sektoren består av systemer og tjenester med 24/7 opptidskrav og er derav sårbare for store infrastruktur endringer som PKI kan medføre. Det er viktig at innføring av nye krav ikke påfører vår sektor unødvendig ekstra kostnader eller går utover pasientsikkerheten.

Direktoratet støtter departementets vurdering om at en ny lov vil være mer ryddig enn å revidere e-signaturloven. Samtidig er det viktig at forslag til ny lov om gjennomføring av EU forordningen for eID og tillitstjenester bør inneholde alle artiklene fra forordningen med tilhørende krav. Kravene bør gjengis i lov, forskrift eller en kravspesifikasjon der det er mest hensiktsmessig. Begrunnelsen for dette er behov for forenkling og tilgjengeliggjøring ved implementering av reglene i IT-systemene så vel som forvaltningsrutiner. Det betyr at det med stor sannsynlighet vil være behov for en ny kravspesifikasjon for PKI. En ny kravspesifikasjon bør også gjelde kommuner og private aktører som yter helsehjelp for å gjøre kravene like innad i helse- og omsorgssektoren. Videre er det nødvendig å se på behovet for *rammeverket for autentisering og uavviselighet i elektronisk kommunikasjon i og med offentlig sektor*. Spesielt vil dette gjelde for å harmonisere EU-forordningens sikkerhetsnivåer med de som er nedfelt i dagens rammeverk.

Kommentarer til Kap. 6.2 om avgrensningen mot lukkede systemer mv

Departementet ber om innspill på forslaget om at reglene ikke får anvendelse på lukkede systemer i henhold til nasjonal lovgivning eller avtale mellom en avgrenset krets av personer, iht. artikkel 2 og som utdypet i fortalen pkt. 21. Det vil være behov for å definere grenseoppgangen mellom lukkede og åpne systemer og vurdere hvilken betydning dette kan ha for en sektor som benytter seg av sertifikater til signering og kryptering mellom virksomheter i helsenettet. Dersom helsenettet blir definert som et lukket system vil dette kunne gi uheldig konsekvenser opp mot annet lovverk hvor det stilles krav til å bruke

[1] https://ehelse.no/Documents/Nasjonale%20prosjekter/NSI_Samordning_1.0.pdf

kvalifiserte sertifikater eller høyt sikkerhetsnivå (eksempler på dette kan være signere e-resept, autentisering på kjernejournal, kryptering av henvisning).

Kommentarer til kap. 7 Elektronisk identifisering

Artikkel 6, når det gjelder forordningens bestemmelser om elektronisk identifisering for notifiserte («notified») eID-løsninger («electronic identification scheme») og at offentlige myndigheter plikter å anerkjenne andre lands notifiserte elektroniske identitetsbevis («electronic identification means») er det behov for å se nærmere på ansvarsforholdet mellom offentlig myndighet og PKI-leverandørene. Helse- og omsorgssektoren benytter seg i dag av Buypass og Commfides. Begge er registrerte tilbydere av kvalifiserte sertifikater etter selvdeklarasjonsordningen. Dersom det blir endringer i ansvarsforholdet er det behov for å se nærmere på hvilken betydning dette vil ha for helse- og omsorgssektoren, se vedlegg 1.

Artikkel 7 og 9, det er beskrevet at anerkjennelsesplikten gjelder kun for offentlig sektor, men at identitetsbevisene mot privat sektor kan det stilles vilkår og betingelser for tilgang til valideringstjenesten jf. artikkel 7 bokstav f, annet ledd og fortalen pkt. 17, tredje punktum. Helse- og omsorgssektoren har mange private aktører og kommuner som yter helsehjelp, disse vil ha behov for tilgang til valideringstjenester.

Artikkel 12, direktoratet støtter forslaget om at det ved notifisering er det behov for å etablere en knytning mellom sikkerhetsnivåene ihht. nasjonalt rammeverk for de notifiserte eID-løsninger og eIDAS' sikkerhetsnivåer. Det vil videre være behov for å nedfelle eIDAS' sikkerhetsnivå i norsk lovverk eller kravspesifikasjon.

Kommentar til kap. 8.2.2.4 Er det behov for å videreføre særhjemmel om esignatur i offentlig sektor?

Departementet ber særskilt om innspill på om det er behov for å videreføre særhjemmel om esignatur i offentlig sektor. Direktoratet vurderer det dit hen at det ikke vil være behov for å videreføre særhjemmel i en ny lov. Forskriftshjemmelen i forvaltningsloven burde være tilstrekkelig for å stille krav til sertifikater og signaturer som kan brukes ved kommunikasjon med og i forvaltningen. Det er imidlertid viktig at eForvaltningsforskriften og kravspesifikasjonen for PKI i offentlig sektor ses i sammenheng med den nye forordningen og at alle krav som stilles i Norge er i henhold til forordningens formål, se vedlegg 1.

Kommentarer til kap. 8.3 Tilsynsorganets oppgave

Departementet foreslår på denne bakgrunn at Nasjonal kommunikasjonsmyndighet (Nkom) oppnevnes som tilsynsorgan etter den nye loven. Departementet ber imidlertid også høringsinstansene om innspill på om det er andre myndigheter enn Nkom som bør ha tilsynsoppgavene etter loven.

Direktoratet viser til vurderingene av Difi som tilsynsmyndighet. Vi støtter deres vurdering om uheldig dobbeltrolle ved at Difi skal føre tilsyn samtidig som de har ansvar for forhandlinger med eID-leverandørene i ID-porten. Samtidig anbefaler vi å gjøre en vurdering av de andre tilsynsmyndighetene som nasjonal sikkerhetsmyndighet og Datatilsynet i tillegg til Nkom, før det gjøres en endelig beslutning på hvilken tilsynsmyndighet som bør ha en slik rolle i fremtiden.

Kommentarer til kap. 9 bør selvdeklarasjonsordningen beholdes?

Departementet ber om innspill på behovet for at hjemmelen til å etablere frivillige sertifiserings-, godkjennings- eller selvdeklarasjonsordninger for sertifikatutstedere beholdes inntil vurderingen av behovet for å beholde Kravspesifikasjon for PKI i offentlig sektor er gjennomført.

Da helse- og omsorgssektoren har anskaffet og etablert PKI – løsninger fra sertifikatutstedere som Buypass og Commfides er det behov for å beholde selvdeklarasjonsordningen inntil videre. Dersom dette blir endret er det behov til å se på konsekvenser dette har for helse- og omsorgssektoren, se vedlegg 1og ytterligere kommentarer for dette under kap. 7 om artikkel 6.

Helse- og omsorgssektorens regelverk

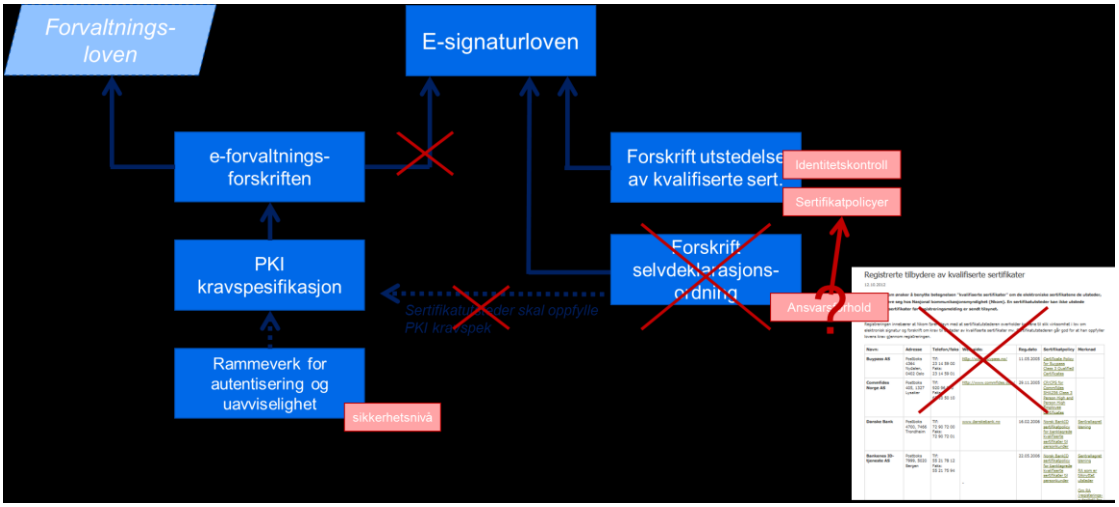
De tillitstjenestene som benyttes i vår sektor per i dag er autentisering, signering og kryptering. Disse er hjemlet i lovverk knyttet til bruksområdene og det er behov for å vurdere om dette er lovverk som blir berørt av den nye EU forordningen. Gjeldende lovverk er:

- Signering av resepter er hjemlet i forskrift om behandling av helseopplysninger i nasjonal database for elektroniske resepter (Reseptformidlerforskriften)
- Autentisering mot kjernejournal er hjemlet i forskrift om nasjonal kjernejournal (kjernejournalforskriften)

I tillegg til gjeldende lovverk i helse- og omsorgsektoren er det utarbeidet Norm for informasjonssikkerhet i helse og omsorgstjenesten (Normen). Det er et omforent sett av krav til informasjonssikkerhet basert på lovverket som vil bli påvirket etter nye reglene i EU forordningen.

Vedlegg 1 Mulige endringer i norsk lovverk og kravspesifikasjon

Figuren illustrerer hvordan mulig endringer av hjemmelsgrunnlag kan påvirke ansvarsforhold for helse- og omsorgssektoren. Vår sektor har pr. i dag ikke etablert egne PKI for utstedelse av kvalifiserte sertifikater, men benytter seg av kommersielle PKI-leverandører som Buypass og Commfides.



Fra figur:

1. Dersom e-forvaltningsforskriften ikke hjemles videre i e-signaturloven vil det være behov for å se nærmere på hvordan kravene fra PKI kravspesifikasjonen vil bli ivaretatt.
2. Dersom selvdeklarasjonsordningen fjernes, slik som foreslått, vil det medføre behov for å se nærmere på hvilke konsekvenser dette vil ha for helse- og omsorgssektoren. Videre må man vurdere betydningen av dette med hensyn til ansvarsforholdet mellom offentlig myndighet og PKI-leverandørene.