Til:
Fornyings- og administrasjonsdepartementet
Avdeling for IT-politikk
Postboks 8004 Dep
0030 Oslo

Deres ref.	Vår ref.	Dato
200700605-KDB		14.05.2007

Forslag til strategi for bruk av eID og e-signatur i offentlig sektor

Norsk Regnesentral (NR) er av den oppfatning at ***Strategi for bruk av eID og e-signatur i offentlig sektor*** kan være svært nyttig for å koordinere ulike initiativ innen stat og kommune. Spesielt bør strategien følges opp med nødvendige økonomiske midler, forskrifter og reguleringer for å gjennomføre hovedtrekkene i anbefalingene.

Rapporten er et grundig arbeid som gir et dekkende bilde av situasjonen per i dag og en del av de utfordringene man står overfor ved innføring av eID og e-signatur i offentlig tjenester. Det er tatt et viktig steg gjennom de anbefalte forretningsmodeller og estimerte økonomiske konsekvenser knyttet til offentlige investeringer. Disse er i det alt vesentlige riktige og vil bidra til effektivisering av offentlig sektor.

Vi er imidlertid av den oppfatning at det er enkelte viktige mangler ved definisjonene av Risikonivåer og Sikkerhetsnivåer. Videre er diskusjonen av personvernkonsekvensene av forslagene som fremmes mangelfull og vi er bekymret for at det kan bli enda mer uklart hvem som ansvaret for å gjøre den *reelle* vurderingen av om sikkerheten er tilfredsstillende i henhold til Personopplysningslovens §§ 13 og 14 i hvert enkelte tilfelle. Det er her viktig å understreke at vi ikke er motstandere av hovedmålet for utstedelse av offentlig eID og økt elektronisk kommunikasjon av personopplysninger. Det vi savner er en helhetlig analyse av de virkninger forslagene vil ha på personvern og sikkerhet i de tjenestene som berøres.

Når det gjelder personvern har det offentlige et helt spesielt ansvar, og samtidig en unik mulighet til å etablere gode løsninger. Dette er også understreket i St.meld.nr.17 (2006-2007) der *Tiltak 8.2, 8.3 og 8.4* er særdeles relevant i denne sammenheng. Behovet for en grundig og helhetlig analyse knyttet til strategien som fremlegges er spesielt, ettersom viktige elementer i det som foreslås er sentralisert på nasjonalt nivå. Dette blir en "de facto" løsning for mesteparten av offentlig sektor med de fordeler, ulemper og ikke minst *muligheter* dette bringer for å ivareta og styrke personvernet.

Vi ønsker å kommentere definisjonen av sikkerhetsnivåer; disse er ikke direkte relatert til begrepene "personopplysninger" og "sensitive personopplysninger" slik disse defineres i Personopplysningsloven. Dette bør gjøres slik at personopplysninger knyttes til **sikkerhetsnivå 3** og sensitive personopplysninger knyttes til **sikkerhetsnivå 4**.

Videre er definisjonen av selve risiko og sikkerhetsnivåene ikke entydige og klare nok slik de foreligger, men åpner for en lang rekke realiseringer med svært varierende sikkerhet. Dette gjelder spesielt for sikkerhetsnivå 3 som åpner for at dette skal kunne implementeres med andre mekanismer enn det som er spesifisert som "Person Standard" i Kravspesifikasjon for PKI i offentlig sektor. Dette bør ikke tillates for tilgang til personopplysninger.

Vi har spesielt å bemerke;

a) definisjonen av "sikkerhetsnivå 3 – utlevering til bruker" er mangelfull da denne lyder

"Samme krav som i 2, med tilleggskrav om en eller annen form for sikring av at rette vedkommende tar dette i bruk."

Denne definisjonen anses å være altfor åpen til å kunne etablere et enhetlig sikkerhetsnivå og det bør her kreves sporbarhet på utleveringen, minimum ved innsamling av signert kvittering på mottak.

b) definisjonen av "sikkerhetsnivå 3 – krav til offentlig godkjenning" *(Ingen krav)* er problematisk da dette i praksis vil medføre en utvanning av hva nivået innebærer i praksis.

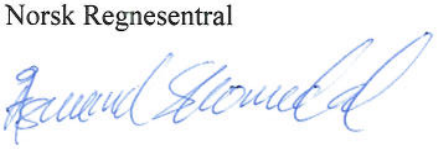
c) definisjonen av "sikkerhetsnivå 4 – krav til offentlig godkjenning" *("selvdeklarering")* er problematisk som eneste godkjenning eller tilsyn med løsninger for risikonivå 4, eksempelvis helseopplysninger.

Punkt b) og c) over vil i praksis medføre at det blir ført altfor lite tilsyn med at en eID på rett sikkerhetsnivå faktisk brukes i tilknytning til behandling av opplysninger på et gitt risikonivå. Etablering av en egen forskrift, eller utvidelser av e-signaturforskriften, som ivaretar godkjenning og kontroll med regelverket for offentlig sektor bør vurderes.

Vedrørende etablering av et offentlig samtrafikknav for eID og e-signatur; her har vi å bemerke at slike tjenester er både hensiktsmessige og effektive. Anbefalingene anses i det vesentlige å være riktige. Vi vil påpeke at når det offentlige tilrettelegger utstrakt elektronisk utveksling av personopplysninger vil det ha som logisk konsekvens at en gjør tilgjengelig elektroniske tjenester som ivaretar innsynsretten i henhold til Personopplysningslovens Kapittel III, spesielt §§ 18 og 19. Slike tjenester vil naturlig falle inn under det et samtrafikknav tilbyr.

Med vennlig hilsen

Norsk Regnesentral



Åsmund Skomedal

Forskningssjef