Datatilsynet

Fornyings- og administrasjonsdepartementet
Postboks 8004 Dep

0030 OSLO

Deres referanse	Vår referanse (bes oppgitt ved svar)	Dato
200700605-KDB	07/00401-2 /AÅR	14. mai 2007

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

Datatilsynet viser til høringsbrevet av 12. mars 2007 vedrørende forslag til strategi for bruk av eID og e-signatur i offentlig sektor.

Generelt er Datatilsynet fornøyd med at befolkningen, via den aktuelle strategien, vil komme nærmere en mulighet for sikker elektronisk kommunikasjon med det offentlige.

I forhold til rammeverket for autentisering og uavviselighet

Det bør kun bes om identitet der informasjon om identitet er klart nødvendig. Når dette er klarlagt vil det være enklest for brukeren at det benyttes en løsning med tilstrekkelig sikkerhet. Usikkerhet om hvilket sikkerhetsnivå som bør brukes, kan i seg selv representere en fare mht. nødvendig trygghet. Datatilsynet vil derfor anbefale at det etableres færrest mulig sikkerhetsnivåer, for eksempel kun sikkerhetsnivå 4.

Kravene for forholdet mellom sikkerhetsnivå 3 og sikkerhetsnivå 4 er etter Datatilsynets mening ikke hensiktsmessig utformet, dette på grunn av at Datatilsynet generelt mener at bruk av sikkerhetsnivå 3 vil åpne for uklarheter og tolkningsrom.

I forhold til strategiens hoveddokument

Datatilsynet mener at å etablere kun nasjonalt ID-kort som primær strategi for å realisere eID på sikkerhetsnivå 4 ikke er et personvernmessig optimalt valg. Datatilsynet anser det som en personvernmessig fordel at det etableres en valgfrihet og at det finnes flere tilbud for sikkerhetsnivå 4. Det er en personvernmessig fordel at brukerne selv kan velge sin leverandør som tilbyr sikkerhetsnivå 4, altså også en markedsbasert distribusjon. En løsning med kun en tilbyder av sikkerhetsnivå 4 til bruk mot offentlig sektor vil skape en sentralisert ordning som erfaringsmessig ikke vil gi optimalt personvern. Brukerne vil da ikke kunne forlate en

Postadresse:	Kontoradresse:	Telefon:	Telefaks:	Org.nr:	Hjemmeside:
Postboks 8177 Dep 0034 OSLO	Tollbugt 3	22 39 69 00	22 42 23 50	974 761 467	www.datatilsynet.no

leverandør denne er misfornøyd med, for eksempel om brukeren er misfornøyd med leverandørens håndtering av personopplysninger.

Datatilsynet har ingen spesielle kommentarer til offentlig utstedelse av virksomhetssertifikater som beskrevet i høringsdokumentet kapittel 5.

Datatilsynet har innvendinger til strategien som er skissert for samtrafikknav. Datatilsynet har i flere år og ved mange anledninger påpekt sin bekymring for bruk av tiltrodd digitalt arkiv. Det foreligger ikke tilstrekkelige beskrivelser for hvordan dette tiltrodde digitale arkivet skal fungere. Datatilsynet ser flere personvernmessige problemer med et slikt arkiv og nevner stikkord som behandlingsansvar, innsyn, formål, sletting. Et digitalt arkiv (innsynsarkiv) kan, slik Datatilsynet ser det, ikke tilbys som en sentral grunnleggende tjeneste.

Når det gjelder samtrafikknavets oppgave som formidler av identitet, berører dette sentrale personvernmessige prinsipper. Det å stå som pålogget, er noe helt annet enn å identifisere seg når identifisering er nødvendig. Datatilsynet mener at det er dårlig personvern å stå som innlogget (identifisert) når behov for dette ikke er tilstede. En økt (en borgers besøk på et nettsted) kan, bestå i å både hente frem spesifikk informasjon på identitet, men også hente generell informasjon hvor identitet ikke er nødvendig. Datatilsynet mener at det generelt må legges vekt på å ivareta muligheten for å kunne opptre anonymt for de som ønsker det. Det er samtidig viktig at bruker settes i stand til å forstå når vedkommende opptrer med identitet.

Datatilsynet har ingen spesielle kommentarer til hvordan det skisserte tidsløpet i kapittel 2 passer inn i egne planer. Generelt kan det nevnes at det er avgjørende at hver enkelt behandlingsansvarlig selv har kontroll med de personopplysninger de er behandlingsansvarlige for, og at eksternt tidspress ikke får den behandlingsansvarlige til å miste denne kontrollen.

I forhold til foretningsmodeller (kapittel 7)

Datatilsynet har tatt til etterretning at det er åpnet for at de enkelte aktører i tillegg vil kunne ha egne avtaler med underleverandører og at disse ikke er synliggjort i forretningsmodellene. Ellers har Datatilsynet ikke spesielle kommentarer med tanke på en sentral forretningsmodell i forhold til en desentralisert forretningsmodell, slik disse modellene er beskrevet i rapporten. Sentral forretningsmodell betyr i henhold til rapporten ikke-økonomiske avtaler mellom samtrafikknav og brukersted. Desentralisert forretningsmodell betyr i henhold til rapporten økonomiske avtaler mellom samtrafikknav og brukersted.

Datatilsynet er imidlertid skeptisk til at det opprettes et faktisk monopol via et felles samtrafikknav for sluttbrukernes kommunikasjon med offentlig sektor. Slik sentralisering og faktisk monopol vil kunne ble en kritisk sentralisering av kommunikasjon av personopplysninger. Det fremkommer av strategidokumentet at offentlige virksomheter ikke vil ha et eget behov for å etablere egne løsninger når det etableres et samtrafikknav. En slik modell vil måtte medføre en restriktiv holdning til enhver logging av aktivitet for å unngå at navet vil oppleves som et sentralt overvåkingsinstrument. I strategien er innsynsarkivet nevnt. Fra tidligere arbeid med sikkerhetsportalen har det vært nevnt omfattende logging av den

enkelte borgers aktivitet. Datatilsynet forutsetter at ansvarlige for samtrafikknavet unngår logging av aktivitet og sentrale arkiver, hvilket vil styrke tilsynets aversjon mot løsningen.

Med hilsen

Georg Apenes
direktør

Atle Årnes
senioringeniør