Statskonsult

Vår dato	Vår referanse
29.11.02	2002/875-1
Deres dato	Deres referanse
21.10.2002	2001/5605 KDB

Saksbehandler
Anne Karen Bonnevie Seip

Nærings- og handelsdepartementet
Postboks 8014
0030 Oslo

Att.: Katarina de Brisis

Høring - grunnlagsdokument for utarbeidelse av nasjonal strategi for informasjonssikkerhet

Statskonsult mener at det utsendte grunnlaget er bra for utarbeidelse av en kommende nasjonal strategi. Vi har noen forslag og kommentarer som vi håper kan være bidrag til det videre arbeidet.

Til kap 3, Utviklingstrekk og forhold som påvirker IT-sikkerhet

I tillegg til det som står i grunnlagsdokumentets kapittel 3, er det etter vår mening et viktig trekk i utviklingen at vi har fått et økende antall ulike lover og forskrifter i den senere tid som direkte og indirekte regulerer informasjonssikkerhet. Vi synes dette kommer for lite frem i grunnlagsdokumentet, både i beskrivelsen av utviklingstrekkene i kapittel 3 og i forslagene til strategier og tiltak i kapitlene 6, 7 og 8.

Til punkt 3.4 kunne man sagt noe mer om dette. Teksten nedenfor er ikke forsøkt tilpasset den kortfattede teksten man ellers finner i 3.4, men formidler vårt syn med noen flere ord, som en bakgrunn.

Sikkerhetsloven med de tilhørende forskriftene gir regler for at målgruppen skal kunne håndtere trusler knyttet til sikkerhetsgradert informasjon og –objekter. Truslene er iht loven representert ved spionasje, sabotasje og terrorhandlinger. Objekt for disse truslene er rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser. Det sentrale virkemiddelet er forebyggende sikkerhetstjeneste som fjerner eller reduserer risiko fra de nevnte truslene (kalt sikkerhetstruende virksomhet).

Statskonsult antar at sikkerhetsgradert informasjon utgjør bare noen få prosent (2 %?) av den totale mengden informasjon som brukes i offentlig forvaltning (stat, fylkeskommuner og kommuner). Vi antar videre at truslene fra spionasje, sabotasje og terrorhandlinger ikke er særlig aktuelle i forhold til offentlig forvaltning, utenfor totalforsvaret.

Offentlig forvaltning og privat sektor, utenfor området for totalforsvaret og rikets sikkerhet/vitale nasjonale sikkerhetsinteresser, har *egne verdier* knyttet til informasjon å ta vare på, med et generelt sett annet trussel- og mulighetsbilde, der informasjonens tilgjengelighet og integritet er de mest typiske behovene som skal ivaretas, for store volumer med informasjon og saksbehandling. I tillegg kommer behovet for konfidensialitet, som tradisjonelt omfatter bare en mindre del av den totale mengden informasjon som forvaltningen håndterer. Dessuten er det fokus på identitet og autentisering, ikke minst i forhold til utviklingen med åpne løsninger hvor forvaltningen flytter sine "skranker" ut på nettet, og kommer publikum og næringsliv i møte på en ny måte, jf arbeidene med offentlige servicekontorer, og måten man gjør offentlig informasjon og tjenester mer tilgjengelige på, via mer eller mindre usikre internettløsninger, mv. Dette aktualiserer også behovet for konfidensialitet og det å kunne identifisere og autentisere deltakere i nye elektroniske sammenhenger. Ulike former for kryptering og bruk av annen

***Statskonsult** er et direktorat for kommunikasjon, kompetanse og forvaltning*
Stensberggt. 25, Postboks 8115 Dep, 0032 Oslo
Telefon: 22 45 10 00, Telefaks: 22 46 94 70
postmottak@statskonsult.dep.no
www.statskonsult.no

sikkerhetsteknologi er/blir i økende grad interessante virkemidler for å gjøre nye tjenester mulig, der de nevnte behovene gjør seg gjeldende.

Selv om området for rikets sikkerhet er stort, og går langt inn i både privat og offentlig sektor/totalforsvaret, vil sikkerhetsloven med forskrifter bare i liten grad direkte angå sivil offentlig og privat sektor. Likevel er det grunn til å tro, som vi har lært av forhistorien, at dette regelverket vil få en betydning langt utover dets rettslige virkeområde. Vi har lang erfaring for at man i offentlig forvaltning misforstår rekkevidden av reglene, - mange tror at de omfatter mer enn de faktisk gjør.

Dette tror vi dels henger sammen med at reglene har en lang forhistorie, med et pionéraktig perspektiv, og en tilsvarende mangel på det samme for den øvrige (og langt større) sivile forvaltningen og privat sektor. For å bøte på manglende tenkning og styring av sikkerhet og informasjonssikkerhet i sivil sektor generelt, har man i mange sammenhenger "frivillig" fulgt reglene for rikets sikkerhet. Dermed har man fått mer omfattende og kostbare løsninger enn behovet strengt tatt har tilsagt. Eller man har fått det andre utslaget: "sikkerhet er for vanskelig og dyrt", så det hopper man over. Etter vår mening er begge deler mulige uheldige utslag av denne situasjonen. Dette er vi redd for er et utviklingstrekk som vil fortsette videre, bl.a. fordi forsvarets regelverk er godt synlige og forvaltes på en aktiv måte, mens annet relevant regelverk er for lite synlig og forvaltes kanskje for forsiktig, eller sagt på den positive måten; har et stort potensiale for bedre og mer aktiv regelforvaltning.

Beskyttelsesinstruksen er så vidt vi vet de eneste konkrete reglene staten generelt har for behandling av informasjon som er taushetsbelagt iht lov. Dette er i seg selv et tankekors. Et annet er at beskyttelsesinstruksen neppe er i bruk i det omfanget den opprinnelig er tiltenkt, eller rettslig sett må anses å omfatte. Vi *tror* generelt at bare noen få statlige virksomheter er aktive brukere av beskyttelsesinstruksen (for eksempel Utenriksdepartementet/utenrikstjenesten, deler av politiet, Forsvarsdepartementet (på administrativt område som ikke har med rikets sikkerhet å gjøre), Statsministerens kontor, og kanskje enkelte flere). En medvirkende grunn til dette kan være at Statsministerens kontor neppe kan sies å ha lagt vekt på å forvalte beskyttelsesinstruksen på en aktiv måte i sivil statlig sektor, og at praksisen fortsetter med å "sette den bort" til Forsvarets overkommando/Sikkerhetsstaben (NSM) i forhold til elektronisk behandling og kommunikasjon (som jo er blitt vanlig). Dermed er visse deler av sikkerhetsloven og tilhørende forskrift om informasjonssikkerhet for å forebygge trusler fra sabotasje, spionasje og terror gjort gjeldende på området for beskyttelsesinstruksen. Man skal ikke se bort fra at dette i seg selv kan føre til at noen unnlater å gradere iht beskyttelsesinstruksen, og nøyer seg med å følge de vanlige reglene for unntatt offentlighet iht offentlighetsloven. Offentlighetsloven og forvaltningsloven har ikke selv noen konkrete regler om *hvordan* man skal ivareta hensynet til konfidensialitet (taushetsplikt og "gråsonen" ellers kalt u.off.), verken i en papirbasert eller elektronisk forvaltning. I forvaltningslovens regel om taushetplikt er det formulert et krav om at opplysningene må oppbevares på betryggende måte. Den nevnte forskrift om elektronisk kommunikasjon med og i forvaltningen har noen supplerende regler, men går ikke langt på dette området. Sikkerhetsloven med forskrift har til gjengjeld så mange, omfattende og til dels strenge regler at mange sikkert lar seg skremme. Og det er ingen som forstyrrer roen til de som velger ikke å etterleve reglene, som de i utgangspunktet har plikt til å følge.

Statskonsult tror det er et stort misforhold mellom antall taushetsplikter og mykere konfidensialitetshensyn på den ene siden (i form av andre grunner til å unnta fra offentlighet enn lovpålagt taushetsplikt), og antall etterlevelser av beskyttelsesinstruksen (med tilhørende regler for elektronisk håndtering iht sikkerhetsloven med forskrifter) på den andre siden.

I tillegg til forvaltningslovens generelle regler om taushetsplikt, minner vi om at det finnes en mengde andre lover på ulike særområder som pålegger taushetsplikt. Vi tror dette dreier seg om minimum rundt 80 paragrafer fordelt på et noe mindre antall lover, jf lovsamlingens fotnote nr 2 til straffelovens § 121, som gir eksempler på lovbestemmelser med taushetsplikt i forhold til tjeneste eller arbeid for statlig eller kommunalt organ. I tillegg kommer alle de taushetsplikter som er og blir pålagt med hjemmel i (gyldig)

instruks. Det er neppe grunn til å tro at dette er færre i antall enn de tilfellene som har hjemmel i lov. Sannsynligvis er dette et betydelig høyere antall.

Når man har med informasjon å gjøre der det kan oppstå en skadevirkning hvis innholdet i informasjonen blir kjent, er det slik vi oppfatter reglene *alltid* en plikt i staten til å *vurdere* om gradering iht beskyttelsesinstruksen skal anvendes og evt hvilken av de to graderingene informasjonen skal merkes med (som igjen evt utløser plikt til å følge de mange og konkrete behandlingsreglene i angitt forskriften under sikkerhetsloven. Dette må skje innenfor de rammene offentlighetsloven setter, med bl a plikt til å vurdere meroffentlighet når man er utenfor området for lovbestemt taushetsplikt (som jo alltid skal unntas).

Det er en forvaltningspolitisk stor målsetting å øke mengden elektronisk saksbehandling, og å gjøre den til en hovedform for saksbehandling både internt og i forholdet til publikum og næringsliv. Elektronisk forvaltning er et uttrykt og høyt profilert politisk mål, der brukervennlige IKT-baserte tjenester vil stå sentralt.

Dette krever konkrete løsninger på områder for elektronisk kommunikasjon og autentisering, inkludert sikring av konfidensialitet. Behovene vil variere mht hvor sterk sikkerhet som er nødvendig. De store volumene med saksbehandling vil generelt sett trenge enkle, eller *vanlige* sikkerhetsløsninger, som konkrete risikovurderinger på de aktuelle områdene kan bidra til. Regelverkene gir utgangspunkter for slike vurderinger, men ikke mer. Risikoanalyse i det enkelte tilfellet, overfor konkrete opplysningstyper, i forhold til den funksjonen som skal ivaretas, og sammenheng til saksgangen forøvrig, vil avgjøre "hvor høyt man skal legge listen".

Vi slutter oss til beskrivelsen av utfordringer i kapittel 4, og legger til at det som er nevnt ovenfor utgjør ytterligere utfordringer i forhold til det som allerede står i punkt 4.4.

Til kap 5 (om ansvar for og koordinering av IT-sikkerhet)

Vi tror ikke betegnelsen **"bør"** bare brukes slik det står innledningsvis i kapitlet, om tiltak som fremmes som et resultat av arbeidet med den nasjonale strategien. Vi slutter oss til intensjonen med en slik klargjøring, men tror en gjennomgang og revurdering er på sin plass.

I beskrivelsen av sektorovergripende myndigheter, sentrale aktører mv. (5.1) kan vi ikke se at Arbeids- og administrasjonsdepartementet og dets ansvarsområde (samt underliggende virksomheter, inkludert Forvaltningstjenestene og Statskonsult) er nevnt på en tilstrekkelig måte. Så vidt vi kan forstå hører vårt departement så avgjort med i det helhetsbildet man prøver å gi i kapittel 5. I all beskjedenhet synes vi Statskonsult også hører med som aktør, som en del av AAD-familien, innenfor departementets ansvarsområde for koordinering og samordning av informasjonssikkerhet i statlig sektor. Både AAD og Statskonsult har lange tradisjoner med aktiviteter på området for informasjonssikkerhet. Og Forvaltningstjenestene er sentrale for ikke minst departementenes informasjonssikkerhet.

I kapittel 5.1.4 hører også Arbeids- og administrasjonsdepartementet etter vår mening med i oversikten over det som kalles de "vesentligste myndigheter i denne sammenheng". Ved siden av sitt tverrgående ansvar overfor hele statlig sektor, forvalter AAD nå to sentrale regelverk på området for informasjonssikkerhet, jf forskriften til personopplysningsloven og forskriften om elektronisk kommunikasjon med og i forvaltningen. I tillegg har AAD et administrativt ansvar for Datatilsynet. På personvernområdet er med andre ord AADs ansvarsområde betydelig utvidet i forhold til tidligere, ved at hele landet, privat og offentlig sektor, er målgruppen for personopplysningsforskriften. Ved sitt ansvar for forskriften om elektronisk kommunikasjon med og i forvaltningen er også ansvaret utvidet til å inkludere kommuner og fylkeskommuner, som i tillegg til statlig sektor er målgruppe for forskriften.

Vi ser at AAD er nevnt som en viktig samarbeidspartner, i kap. 5.2.1, for tiltak av tverrsektoriell natur innen IT-sikkerhet i statlig sektor. Dette understreker etter vår mening at departementet også må tas med i oversikten i kap. 5.1 over viktige aktører.

5.1.3 Samarbeidsarenaer
Det fins flere organisasjoner som er i bruk for norske representanter som samarbeidsarenaer for informasjonssikkerhet i dag. Av nasjonale organisasjoner er det naturlig å nevne Norsk Teknologisenter (NTS) og Den norske dataforening (DnD). Av internasjonale organisasjoner kan vi nevne ISO, CEN, ETSI ESI, W3C, IETF. I tillegg fins det mye samhandling mellom forvaltningsorganer på tvers innenlands og over landegrensene, f.eks. PKI Government.

Til kap 6 og 7 (om regelverk)

Ut fra dette kunne man i **kapittel 6 og 7 følge opp med forslag til strategier og tiltak**:

Statskonsult foreslår at det settes i gang et arbeid i forhold til regelverk for informasjonssikkerhet, for å få de eksisterende reglene i bedre, praktisk bruk, og eventuelt gi bedre grunnlag for fornyelse av dem, på en samordnet, harmonisk måte.

Dette må inkludere å lage en *oversikt* over reglene for informasjonssikkerhet, lage praktiske *veiledninger* og gjennomføres *kurs og opplæringstiltak*, ikke som et skippertak, men på fortløpende basis. Målgruppen for disse regelverkene må være målgruppen for slike tiltak. Videre bør det vurderes *sammenhenger* mellom regler knyttet til identitet og autentisering, signering, tilgjengelighet og integritet, samt konfidensialitet, med fokus på harmoni mellom regelverkene, for lettere etterlevelse. Vi tenker eksempelvis på reglene om informasjonssikkerhet i sentrale lover for forvaltningen og deler av privat sektor; personopplysningsloven med forskrifter, forvaltningsloven, forskrift om elektronisk kommunikasjon med og i forvaltningen, offentlighetsloven, lov om elektronisk signatur, beskyttelsesinstruksen, samt relevant sektorregelverk. Til sammen gir disse en rekke regler om forebyggende informasjonssikkerhet.

Videre *foreslår* Statskonsult at det i strategien oppfordres til at den enkelte regelverksforvalter *systematisk* innhenter opplysninger som kan si hvordan regelverkene faktisk virker i praksis, og periodevis vurderer behovet for endringer i regelverket. Den nye forskriften om elektronisk kommunikasjon med og i forvaltningen er et eksempel i så måte, med sin § 29, som sier at forskriften opphører etter to år hvis den ikke uttrykkelig fornyes. Arbeids- og administrasjonsdepartementet har dermed lagt inn en såkalt solnedgangsregel, som krever nettopp slike aktiviteter som vi foreslår over, for at denne regelen ikke skal bli redusert til en formalitet, med "automatisk" fornyelse eller opphør. Dette mener vi kan være et eksempel til etterfølgelse, og som den nasjonale strategien for informasjonssikkerhet kan bidra til.

De aktuelle regelverkene må identifiseres og synliggjøres på en betydelig mer aktiv måte enn det som er tilfellet i dag. Videre må grensegangen mellom dem gås opp. Dette krever kunnskap og bevissthet. Det må gis god informasjon om hva aktuelle lover med forskrifter faktisk regulerer, og hva som ikke reguleres. Dessuten må de som skal etterleve de enkelte regelverkene, og ikke minst flere overlappende/tilgrensende regelverk, få hjelp til dette, ved bl.a. god opplæring og veiledning.

En liten illustrasjon: vi gikk inn på nettsidene til Statsministerens kontor, og fant ingen opplysninger om beskyttelsesinstruksen (heller ikke hos Forsvaret) (men i instruksbasen til Lovdata fant vi selve instruksen). Tilsvarende fant vi ingen opplysninger på nettsidene til Arbeids- og administrasjonsdepartementet eller Datatilsynet om hvem som har ansvaret for å forvalte personopplysningsforskriften. Disse opplysningene fant vi heller ikke i departementenes telefonkatalog, som ellers gir mange opplysninger om hvem som har ansvar for hva. Det er viktig å ha klare ansvarforhold, men en må ikke glemme å formidle informasjon om det, som er lett å finne.

Statskonsult slutter seg til forslaget i 6.1.3, men vil hevde at behovet er tilsvarende for ikke-samfunnskritisk infrastruktur, der sikkerhetsloven ikke kommer til anvendelse (i forhold til metode for risikovurdering. På det ikke-kritiske området kommer da andre myndigheter inn i bildet, i forhold til det vi kan kalle "vanlig sikkerhet". Både NHD og AAD har ansvar her.

Både offentlig og privat sektor bedriver elektronisk saksbehandling i utstrakt grad. Det er store volumer av dokumenter og informasjon som mottas, behandles, lagres og videreformidles elektronisk. Behovet for *vanlig* IT-sikkerhet og fornuftige administrative rutiner er derfor stort for all saksgang. Vi setter pris på at dette kommer fram i punkt 6.1.4, og støtter forslaget, hvor også Arbeids- og administrasjonsdepartementet er identifisert som ansvarlig aktør. Vi er litt usikre på hva som ligger i at normene baseres på klassifisering av informasjon, systemer og infrastruktur (for hhv konfidensialitet, integritet og tilgjengelighet), men regner med at man kommer tilbake til dette. Vi viser imidlertid til sammenhengen mellom dette forslaget i 6.1.4 om å utarbeide generelle normer for IT-sikkerhet, og hvilke regelverk som legger hvilke overordnede føringer i det enkelte tilfellet. Hvis man på et slikt IT-sikkerhetspolicy-nivå kan forene behov under flere regelverk, ville dette være en praktisk og effektiv løsning.

I den forbindelse nevner vi som et godt eksempel den i utgangspunktet britiske standarden BS 7799, som også foreligger som norsk standard (fordi den også er gjort til en Internasjonal standard). Ved siden av at den fortjener egen omtale på fremtredende plass (mangler i det foreliggende utkastet), kan den være et sentralt fellesgrunnlag for å håndtere informasjonssikkerhet både i henhold til personopplysningsforskriften og forskriften om elektronisk kommunikasjon med og i forvaltningen. Begge forskriftene pålegger utarbeidelse og jevnlig vedlikehold av sikkerhetsmål og -strategier, med relevante risikovurderinger.

Den nevnte standarden er grunnlag for den norske sertifiseringsordningen av IT-sikkerhet i organisasjoner (administrert av Norsk Akkreditering). Hele denne ordningen bør omtales, og den nasjonale strategien for IT-sikkerhet bør bidra til å gjøre ordningen kjent, og dermed lettere å følge opp.

Verdien av denne standarden er langt større enn som målekriterium i sertifiseringsordningen. Den har antakelig sitt største virkeområde for de mange som ikke ønsker å sertifisere seg, men som likevel vil ha den tryggheten det gir å følge en etablert og internasjonalt anerkjent standard på området (akkurat som for Common Criteria på området for informasjonssikkerhet i produkter og systemer). Strategien bør synliggjøre dette (for begge de nevnte områdene), og styrke bruken av standardene.

I denne forbindelse vil vi også etterlyse en klarere fremstilling av IT-sikkerhetsstandarder, og deres plass i en fremtidig nasjonal strategi. Statskonsult mener standarder på dette området er viktige virkemidler, og at Norge bør styrke deltakelse i de relevante organisasjoner, og bidra til sterkere grad av implementering av standardene enn det tilfellet er i dag. Vi har omtrent samme syn på standardene som på regelverkene, jf foran. Det må formidles med større styrke hvilke standarder som finnes, hva de kan brukes til, og sammenhengene mellom dem. Her har vi i Statskonsult også et ansvar, gjennom Standardiseringssekretariatet, som har sitt mandat fra AAD på bakgrunn av en kgl.res. Dette arbeidet bør styrkes og synliggjøres bedre, som et ledd i en nasjonal strategi for IT-sikkerhet.

Som direktorat med spesiell kompetanse innen området, deltar vi gjerne i arbeidet med å konkretisere slike statlige IT-sikkerhetsnormer som foreslås i 6.1.4.

Grunnlagsdokumentet legger i punkt 5.2.1 vekt på at tillitsdimensjonen er en viktig dimensjon innen IT-sikkerhet. Og i innledningen påpekes det at samfunnet mangler enkle og anvendelige metoder for risiko- og sårbarhetsvurdering. Det er etter vårt syn absolutt tilfelle for flere felt knyttet til offentlig sektor f.eks. digitale signaturer og PKI. Dette gjelder bl.a. fordi man må foreta hver risikovurdering i sin aktuelle

kontekst der tillit til forvaltningen og dens systemer er vesentlig for samfunnet, jf også forslagene i kap 8 om PKI.

Et ledd i slikt arbeid kan også være å analysere og vurdere hvilke informasjonsvolumer som har behov for ulike typer sikkerhetstjenester, om kommunene har særskilte behov som må dekkes på annet vis, eller om de kan omfattes av slike normer (som da kunne bli "offentlige" og ikke bare "statlige").

Statskonsult mener det er viktig med en utvikling på dette området som er og forblir samordnet med andre relevante regelområder. Vi tenker på både området for forvaltningsrett (med regler om taushetsplikt, innsyn og saksbehandling, som også omfatter sikkerhetsaspekter), og på området for personvern (der det er en ny lov og forskrift med klare, direkte reguleringer om informasjonssikkerhet for både offentlig og privat sektor), samt andre sektorområder. Vi vil spesielt fremheve at det finnes tilsvarende klare og direkte regler i den enda nyere forskriften om elektronisk kommunikasjon med og i forvaltningen (i kraft fra 1.7.02), med bl.a. krav om at ethvert forvaltningsorgan som benytter elektroniske signaturer, systemer for innholdskryptering eller andre sikkerhetstjenester (f. eks. for integritet, tilgjengelighet og ikke-benekting), har plikt til å lage sikkerhetsmål og sikkerhetsstrategi for virksomhetens ivaretakelse av informasjonssikkerhet (§ 11). Det er videre et krav i forskriften at sikkerhetsstrategien skal være utarbeidet i henhold til anerkjente prinsipper for informasjonssystemers sikkerhet.

I klartekst betyr dette i praksis en eller flere av versjonene Britisk Standard 7799 A Code of Practice for Information Security Management, ISO/IEC 17799 eller den norske varianten NS

Det er mange som vil bli berørt av ulike sikkerhetsregler av overlappende karakter, fordi de er underlagt flere regelsett på sine respektive områder. Da er det viktig at det foregår en samlet vurdering fra regelgivernes side, slik at trykket fra ulike sektorregelverk ikke gjør at regeletterlevelsen blir tyngre enn nødvendig.

Dette gjelder ikke minst når det nå er utviklet regelverk for hele eller deler av fagområder (sikkerhet, informasjonssikkerhet mv) sett fra henholdsvis sivil offentlig forvaltning, personvernet og rikets sikkerhet mv. Regulering av terminologi, ansvarsforhold, plikter og tiltak bør ikke bare passe for den enkelte sektor, men også i et helhetlig perspektiv på tvers av de aktuelle sektorene og områdene, så langt dette er hensiktsmessig. Regelverkene må ikke umotivert utformes og praktiseres ulikt, men være tilbørlig samordnet. Dette krever samordnet regelutvikling og –forvaltning, i regelverkenes levetid.

I en slik sammenheng er det viktig å være bevisst på de ulike sektorenes kjerneområder og særpreg, fellestrekk/fellesområder, og grensene mellom dem, både for regelutformerne/giverne, regelforvalterne og alle de som skal etterleve de mange og ulike reglene.

Statskonsult savner en sterkere fokusering på slike aspekter i grunnlagsmaterialet, og vi er usikre på om grenseflatene mellom sikkerhetsregler for henholdsvis personvernet og for sivil offentlig og privat sektor utenfor området for rikets sikkerhet vil bli tilstrekkelig ivaretatt i prosessen videre. En enkel måte å bidra til slik ivaretakelse er å støtte dette i strategiarbeidet, ved understreking av at regelforvaltningsansvaret skal /bør inkludere f eks regelmessige kontaktmøter mellom de berørte regelforvalterne og -brukere, i det videre arbeidet med å forvalte og etterleve regelverkene, samt tilhørende veiledninger, osv.

7.1.4 Forskning og utvikling innen IT-sikkerhet
Punkt 3 nevner forskningsprogrammer som er relevante for det offentlige. Vi foreslår et selvstendig punkt for offentlig sektor, for å få bedre frem at offentlig sektor har særtrekk som skiller den fra privat sektor, og disse særtrekkene må identifiseres og håndteres. Offentlig sektor har mange datasystemer som er spesielle og eksplisitt knyttet til realisering av et regelverk. Ofte fins det for eksempel bare ett tolldeklarasjonssystem i et land, og det kan i tillegg være vanskelig å sammenlikne med andre lands systemer fordi lovgivningen er ulik. Det fins lite forskning på området for offentlig sektors spesielle behov og sektoren trenger støtte for å lage gode og effektive systemer for sin saksbehandling.

Til kap 8, En samfunnsinfrastruktur for elektronisk signatur med mer

I kapittel 8 står det at "PKI er per i dag den eneste kommersialiserte teknologien for å tilby kvalifiserte elektroniske signaturer som sikrer ikke-benekting slik det er definert i lov om elektronisk signatur". I og med at det ikke står noe i loven om ikke-benekting foreslår vi en endring av denne setningen: "PKI er per i dag den beste teknologien for å tilby kvalifiserte elektroniske signaturer som støtte for ikke-benekting".

Under punkt 8.2 er det listet en rekke aktiviteter som bør utføres. Som punkt 7 foreslås det at felles behov bør identifiseres. Det er uklart for oss om dette gjelder alles behov eller bare offentlig sektors behov. I alle tilfeller foreslår vi at punktet flyttes høyere opp på lista ettersom det bør danne grunnlaget for hvor hva slags PKI som bør implementeres i første omgang. Gartner påpeker at hittil er det bare lukkete PKI som har lykkes. I samme prosess bør det også utføres nytte-kostnadsanalyser med tilhørende risikovurderinger, jfr. utredningsinstruksen.

Med hilsen

for For Guri Verne
Avdelingsdirektør

Anne Karen Bonnevie Seip
Seniorrådgiver