DET KONGELIGE FORNYINGS-
OG ADMINISTRASJONSDEPARTEMENT

Finansdepartementet
Postboks 8008 Dep
0030 OSLO

Deres referanse	Vår referanse	Dato
07/3692 FM PCB	200702415-/AKH	16.10.2007

Høring av NOU 2007: 10 Om tiltak mot hvitvasking og terrorfinansiering (gjennomføring av EØS-regler tilsvarende EUs hvitvaskingsdirektiv i norsk rett)

Vi viser til Finansdepartementets (FIN) brev av 24.8.2007 om ovennevnte.

Fornyings- og administrasjonsdepartementet (FAD) har merknader knyttet til personvernspørsmål og forholdet mellom elektronisk og fysisk legitimasjon.

Personvernvurderinger
Vi savner en nærmere redegjørelse for personvernvurderingene som er foretatt ved utforming av forslaget. Det fremgår av mandatet at utvalget skulle vurdere hvordan hensynet til personvernet kan ivaretas på en hensiktsmessig måte. De overveielser som er gjort fremgår imidlertid bare sporadisk og ytterst kortfattet av utredningen.

Generelt legges det opp til utvidet plikt til kundekontroll, alle kontanttransaksjoner på over 40 000 kroner krever identitetskontroll av kunden, og økt bruk av risikobasert kontroll. Dette er endringer som utfordrer personvernet. Flere opplysninger vil bli registrert og risikovurderinger er av natur usikre.

I de økonomisk/administrative vurderinger savner vi en redegjørelse av eventuelle kostnader knyttet til ivaretakelse av personvernet. Når flere opplysninger skal registreres, kan det være behov for en mer finmasket tilgangskontroll hos aktørene. Bruk av automatiserte systemer for å vurdere risiko må utformes slik at de registrertes personvern varetas, jf. personopplysningsloven § 25.

Postadresse	Kontoradresse	Telefon	Administrasjonsavdelingen	Saksbehandler
Postboks 8004 Dep	Akersg. 59	22 24 90 90	Telefaks	Anne Kristine Hage
N-0030 OSLO		Org no. 972 417 785	22 24 27 14	22 24 48 51

Vedrørende elektronisk legitimasjon – til NOU kap. 4.4.3.2
FAD støtter utvalgets forslag om å foreslå en prinsipiell likestilling mellom elektronisk legitimasjon og fysisk legitimasjon.

Som ansvarlig for koordinering av IT-politikken i Norge vil FAD påpeke at økonomisk samkvem i stor grad allerede foregår, og vil i økende grad skje fremover, via Internett (s.k. digital økonomi). En slik elektronisk samhandling krever bl.a. pålitelig identifikasjon av samhandlende parter, s.k. elektronisk legitimasjon. Det er samtidig viktig at regelverket tilrettelegger for elektronisk kommunikasjon i størst mulig grad. Allerede i 2001 la Nærings- og handelsdepartementet (NHD), som da var ansvarlig for IT-politikken, frem Ot.prp. nr. 108 (2000-2001) som gjennomførte endringer i 39 eksisterende lover og senere i en rekke forskrifter, med tanke på å fjerne hindringer for elektronisk kommunikasjon. Forslagene i utvalgets utredning er i således i tråd med denne prinsipielle tenkningen.

Elektronisk legitimasjon (e-ID) er et spørsmål som FAD har arbeidet med i flere år, både med fokus på bred bruk i samfunnet generelt og bruk i forbindelse med utvikling av elektroniske tjenester fra forvaltningen. Disse to bruksområder henger tett sammen, da innbyggere gjerne vil benytte færrest mulig identifikasjoner ved elektronisk kommunikasjon over Internett (unngå "PIN-kodekaoset"), uansett type tjeneste en benytter.

I 2005 la FAD (daværende Moderniseringsdepartementet, MOD) frem Kravspesifikasjon for PKI i forvaltningen, utarbeidet av en bred sammensatt arbeidsgruppe, der bl.a. NHD, Skattedirektoratet, Rikstrygdeverket, Brønnøysundregistrene, SSØ, Domstolsadministrasjonen, SSB, Trondheim kommune, mfl. deltok. Kravspesifikasjonen bygger på norsk lovgivning (bl.a. e-signaturloven, hvitvaskingsloven) og en rekke internasjonale standarder for PKI-basert e-signatur og e-ID. Daværende Moderniseringsdepartementet besluttet i 2005 at Kravspesifikasjonen skal gis status som forvaltningsstandard og gjelde for alle anskaffelser av PKI i offentlig sektor. Beslutningen er hjemlet i forskrift til forvaltningsloven om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften), 2004.06.25 nr 0988 og Vedtak om etablering av koordineringsorgan for forvaltningens bruk av sikkerhets-tjenester og -produkter ved elektronisk kommunikasjon med og i forvaltningen 2005.10.07 nr 1117. Kravspesifikasjonen er av KS anbefalt som standard for anskaffelse av PKI til alle landets kommuner.

I oppfølgingen av arbeidet med Kravspesifikasjonen har den samme arbeidsgruppen lagt frem Strategi for utbredelse av PKI-anvendelser i forvaltningen. En av anbefalingene i denne strategien var at det skulle etableres en godkjenningsordning for leverandører av PKI til forvaltningen.

Denne anbefalingen ble sett i sammenheng med Næringsdepartementets oppfølging av stortingsvedtaket av 16. juni 2003 med anmodning om å legge frem tiltak for likestilling

av fysisk og elektronisk legitimasjon. NHD fulgte opp vedtaket ved å legge frem forslag til endring av e-signaturloven med innføring av ny § 16a, som gir hjemmel for innføring av frivillige sertifiserings-, godkjennings- og selvdeklarasjonsordninger for sertifikatutstedere.

NHD og MOD utarbeidet så i fellesskap forskrift av 21.11.2005 nr. 1296 til e-signaturloven om frivillige selvdeklarasjonsordninger. Forskriften bygger på Kravspesifikasjon for PKI i forvaltningen, ved å vise til Kravspesifikasjonen og sertifikatklasser med tilhørende krav som er definert i den. Post- og teletilsynet ble utpekt til å forvalte selvdeklarasjonsordningen som ble operativ fra 1.1.2006. Ved en endring av eForvaltningsforskriften[1] som trådte i kraft 1.12.2005 ble FAD gitt hjemmel til å pålegge bruken av selvdeklarasjonsordningen ved anskaffelse av PKI-basert e-ID og e-signatur til forvaltningen. Pålegget ble gitt i brev av 20.9.2006 til alle statlige virksomheter.

Det er per i dag registrert 9 leverandører av e-ID i ordningen, herunder bl.a. Bankenes ID-tjeneste AS med sertifikatklassen Person Høyt.

Til NOU kap. 4.4.3.4
Med utgangspunkt i ovenstående faktainformasjon ser FAD det som forunderlig og lite gjennomtenkt av utvalget å foreslå en regulering av krav til e-ID som skal benyttes i forbindelse med kundekontroll i medhold av hvitvaskingsloven, som bryter med etablert regulatorisk rammeverk for e-ID i Norge.

FAD vil støtte tanken om at sikkerhetskravene til gyldig elektronisk legitimasjon baseres på sertifikatklassen Person Høyt, men vi kan ikke finne en begrunnelse for at kun enkelte av kravene til denne sertifikatklassen tas ut og foreslås regulert direkte i hvitvaskingsforskriften, men andre, tildels viktige krav ikke tas med. Det må etter FADs menig være bedre å vise til det fullstendige settet med krav som finnes i Kravspesifikasjonen, dersom det er ønskelig med en e-ID med høyt sikkerhetsnivå.

Kravspesifikasjon for PKI har gjennom selvdeklarasjonsforskriften blitt lagt til grunn for regulering av krav til e-ID på tre viktige områder – elektronisk kommunikasjon med og i forvaltningen (jf. fotnote 1), offentlige anskaffelser[2] og tinglysing[3]. Det er derfor direkte feil av utvalget å hevde at Kravspesifikasjonen kun benyttes i offentlig sektor. Det er riktig at spesifikasjonen ikke i seg selv har status som forskrift (noe som uansett er uvanlig å gjøre i norsk reguleringspraksis), men den vises direkte til i selvdeklarasjons-forskriften, bl.a. gjennom referanse til sertifikatklasser Person Høyt, Standard og Virksomhet. NHD og FAD vurderte i fellesskap, da

---

[1] Tilføyd nytt ledd (4) i §27 i forskriften

[2] Se forskrift om offentlige anskaffelser av 7.4.2006 nr 402, §7-3 , 1. ledd, bokstav a.

[3] Se forskrift om prøveprosjekt for elektronisk kommunikasjon ved tinglysing av 3.5.2007 nr 476, §4, 1. ledd.

selvdeklarasjonsforskriften ble utarbeidet, om sikkerhetskrav til de ulike sertifikatklassene skulle forskriftsfestes direkte. Dette ble ikke valgt, primært av den grunn at PKI/e-ID er et kompleks teknologiområde der utviklingen går raskt og der trusselbildet mhp sikkerhet også er i stadig endring. Det er derfor mye mer hensiktsmessig å håndtere denne dynamikken gjennom en mer teknisk kravspesifikasjon enn direkte i en forskrift.

FAD ser det derfor som underlig at utvalget foreslår en direkte forskriftsfesting av enkelte krav hentet fra Kravspesifikasjonen. Videre er ett av kravene formulert i strid med den fortolkning av personopplysningsloven som Datatilsynet har lagt til grunn når det gjelder bruk av fødselsnummer i sertifikater. Kravspesifikasjon for PKI inneholder referanse til s.k. SEID-standarder som legger til rette for at en unik identifikasjon i sertifikatet kan kobles til et fødselsnummer, uten at dette må ligge i sertifikatet.

En kravspesifikasjon som har status som forvaltningsstandard vil være underlagt prosedyrer for revisjon og oppdatering som ivaretar interesser både til brukere av de aktuelle løsningene og til leverandører i markedet. I tilfellet Kravspesifikasjon for PKI, innebærer dette at det vil bli gjennomført en bred høring med alle aktuelle interessenter før en ny versjon blir fastsatt.

FAD er formell forvalter av Kravspesifikasjonen, i medhold av vedtak 7.11.2005 nr. 1117. Den praktiske siden ved dette ansvaret (utvikling av forslag til nye versjoner, gjennomføring av høringer) vil mest sannsynlig bli delegert til det nye Direktoratet for forvaltning og IKT som skal etableres per 1.1.2008. For å oppnå nødvendig forankring av nye versjoner av standarden vil FAD sørge for regjeringsbehandling før disse fastsettes.

Med disse kjensgjerninger lagt til grunn mener FAD at det burde være formålstjenlig og tilstrekkelig at Kravspesifikasjon for PKI legges til grunn for regulering av krav til e-ID som kan benyttes ved kundekontroll iht. hvitvaskingsregelverket.

Spørsmålet om hvorvidt leverandører av e-ID skal dokumentere at de oppfyller kravene som settes frem i Kravspesifikasjonen gjennom en selvdeklarasjon eller gjennom en sertifisering er svært overfladisk behandlet i utvalgets utredning. Det er ikke gitt noen begrunnelse for hvorfor utvalget mener at en sertifiseringsordning vil være å foretrekke fremfor en selvdeklarasjonsordning, slik den er definert i forskrift av 21.11.2005 nr. 1296.

En sertifisering innebærer en svært fordyrende ordning for leverandører av e-ID, særlig sett i lys av at de fleste aktuelle allerede er registrert hos PT som utstedere av kvalifiserte sertifikater og de er registrert som selvdeklarerte utstedere av e-ID som oppfyller krav i Kravspesifikasjon for PKI.

Sertifisering er i Ot.prp. nr. 74 (2004-2005) definert slik:

Akkreditert sertifisering er sertifisering utført av et akkreditert sertifiseringsorgan. Sertifiseringsorgan som utfører systemsertifisering er vurdert for hver enkelt bransje og kan bare utstede akkrediterte sertifikater i de bransjene der det har dokumentert kompetanse.

Sertifisering er en prosedyre der en tredjepart skriftlig bekrefter at et produkt, en prosess eller en tjeneste oppfyller spesifiserte krav. Med sertifisering menes når en tredje part gir en attestasjon/bekreftelse av produkter, prosesser, systemer og personer. Sertifisering omfatter alle typer av samsvarsvurderinger unntatt samsvarsvurdering av organet selv.

En sertifiseringsordning som vil måtte etableres vil kreve ressurser og kompetanse, i et tilstrekkelig omfang. Sertifisering i praksis innebærer at sertifiseringsorganets representanter vil måtte gjennomgå prosedyrer, rutiner og tekniske løsninger hos aktuelle leverandører for deretter å foreta en vurdering opp mot en fastsatt standard, og så utstede et sertifikat. Den sertifiserte leverandøren må som regel betale for sertifiseringen, og deretter et årlig gebyr for å vedlikeholde den. Vedlikeholdet består i at sertifiseringsorganet kommer på anmeldte eller uanmeldte besøk og verifiserer at prosedyrer etc. fortsatt er i samsvar med krav i standarden. Sammenlignbare ordninger er f.eks. Sertifiseringsordningen for informasjonssikkerhet i organisasjoner (ISO 17799), der gjennomsnittlig prising av sertifisering kan variere mellom 100.000 og 500.000 kroner, avhengig av størrelsen på den sertifiserte organisasjonen.
FAD mener at det er rimelig opplagt at kostbare sertifiseringer vil drive prisen på en e-ID opp og derigjennom skape hindringer for utbredelse av sikker elektronisk legitimasjon i samfunnet.

Videre vil utvalgets krav om at selve e-ID (sertifikatet) skal være merket som sertifisert føre til enda dyrere elektronisk legitimasjon, da et slikt krav vil medføre at alle eksisterende og utrullede e-ID som leverandørene har i markedet vil måtte inndras og utstedes på nytt. Kostnaden ved en slik operasjon må kunne anses som betydelig.

Merverdien av sertifisering fremfor selvdeklarasjon, basert på registrering som kvalifisert utsteder (når det gjelder sertifikatklassen Person Høyt), er overhodet ikke dokumentert i utvalgets utredning, og må anses som tvilsom.

I lys av ovenstående vil FAD sterkt fraråde at krav til e-ID som skal kunne godkjennes som gyldig elektronisk legitimasjon ifm. kundekontroll i henhold til hvitvaskingsregelverket, forskriftsfestes slik utvalget foreslår.

FAD vil i stedet foreslå at krav til e-ID baseres på Kravspesifikasjon for PKI i forvaltningen, sertifikatklasse Person Høyt, og med godkjenning gjennom registrering og selvdeklarasjon i Post- og teletilsynets eksisterende ordninger.

Merknader til de foreslåtte bestemmelser

Til lovutkastet § 4 annet ledd nr. 3 - Senking av beløpsgrensen til 40 000 kroner

Etter gjeldende rett skal identitetskontroll foretas for alle kontanttransaksjoner på minst 100 000 kroner, samt mistenkelige transaksjoner i området 40000 kroner til 100 000 kroner. Kundens fødselsnummer eller annen entydig kode skal registreres.

Utkastet foreslår å senke beløpsgrensen til 40 000 kroner. Man går her lengre enn hvitvaskingsdirektivet, som har en grense på EUR 15 000.

Dette innebærer en utvidet registrering – både ved at flere ikke-mistenkelige transaksjoner skal registreres, og ved at kundens identitet skal registreres entydig. Vi savner en nærmere vurdering av de personvernmessige konsekvenser av forslaget.

Som det påpekes av utvalget, er grensen på 100 000 kroner 4 år gammel. Antallet transaksjoner som gjennomføres i området 40 000 kroner til 100 000 kroner må antas å ha økt betydelig siden den gang, jf. lønns- og prisutviklingen de siste år. Senking av beløpsgrensen vil således medføre en betydelig utvidet registrering av ikke mistenkelige transaksjoner.

Vi ber departementet vurdere om endringen kan begrenses til de sektorer hvor risikoen for hvitvasking er særlig høy, jf. hvitvaskingsdirektivets risikobaserte tilnærming.

Til lovutkastet § 7 og § 11
FAD støtter flertallets forslag til formulering av § 7 om kundekontroll og likedan vil FAD uttrykke støtte til utvalgets forslag til formulering av § 11 om utkontraktering av gjennomføring av kundekontroll.

Til lovutkastet § 8 – registrering av adresser
Etter utkastet til § 8 skal unntaket fra registreringsplikt for *fortrolige* adresser utvides. I dag gjelder dette unntaket bare for banker. Utvalget foreslår å utvide unntaket for fortrolige adresser til alle registreringspliktige.

Etter vårt skjønn bør departementet samtidig vurdere om det er nødvendig at adresse registreres, uavhengig av om adressen er fortrolig eller ikke. Etter gjeldende rett skal både navn, entydig identitetskode (fødselsnummer/d-nr/organisasjonsnummer) og adresse registreres. Kunden vil således entydig kunne identifiseres gjennom identitetskoden, adressen er ikke nødvendig til identifiseringsformål. Direktiv 2006/1208/EF synes heller ikke å kreve at adressen registreres, jf. at nasjonalt fødselsnummer m.v. regnes som et fullgodt alternativ etter artikkel 4 nr. 2. Adresse skal imidlertid registreres i henhold til FATFs spesialanbefaling pkt VII, men denne gjelder kun finansinstitusjoner mv. Registrering av adresse krever ressurser og vil dessuten representere en personvernulempe for registrerte fysiske personer. Det må legges til grunn at personer med god grunn ikke ønsker å spre opplysninger om sin faste adresse, eksempelvis fordi den røper andre opplysninger som sivilstand, institusjonsopphold eller annet.

Adresseopplysningene fremgår heller ikke av vanlige legitimasjonsdokumenter som bankkort og førerkort. Det er således usikkert om datakvaliteten er tilfredsstillende, når man baserer seg på opplysninger innhentet fra kunden.

Vi viser også til at det for "reell rettighetshaver", jf. utkastet til § 8 siste ledd, ikke er stilt krav om at adresse registreres; kravet er at han entydig kan identifiseres.

Vi ber derfor departementet vurdere erfaringene med registrering av adresse – og om det er nødvendig at adressen registreres for fysiske personer som er registrert med entydig identitetskode, ev. om registreringsplikten kan begrenses til bestemte sektorer.

Til forskriftsutkastet § 4
FAD vil foreslå alternativ formulering i denne paragrafen, som følger:

"Gyldig legitimasjon for fysiske personer er elektronisk signatur som oppfyller kravene i forskrift 21. november 2005 nr. 1296 om frivillig selvdeklarasjonsordning § 3 og som er oppført på publisert liste i henhold til § 11 første ledd i nevnte forskrift."

Når det gjelder krav som fremsettes i forslagets 2. ledd, mener FAD at det må være tilstrekkelig at det fremgår av sertifikatet at det er kvalifisert (dette er et krav iht. en internasjonalt standard, som de fleste aktuelle leverandører allerede har ivaretatt), det foreligger ingen dokumentasjon i utvalgets utredning om at merking som sertifisert i tillegg til kvalifisert vil gi økt sikkerhet, derimot vil slik merking være svært fordyrende, jf. betraktninger tidligere i dette svaret.

Når det gjelder krav i forslagets 3. ledd om å gjennomføre tiltak som nevnt i hvitvaskingsloven § 7 første ledd nr. 1 og 2 og oppbevare dokumenter og opplysninger i samsvar med hvitvaskingsloven § 21, vil FAD peke på at disse kravene allerede er ivaretatt i Kravspesifikasjonen for PKI, punkt 4.2.6, der det vises til aktuelle paragrafer i hvitvaskingsregelverket.[4]

Med hilsen

for Bjørn Magnus Jakobsen (e.f.)
kst. avdelingsdirektør

Anne Kristine Hage
rådgiver

[4] Henvisningene vil måtte oppdateres når revidert lov og forskrift blir vedtatt.