KITH
INFORMASJONSTEKNOLOGI
FOR HELSE OG VELFERD

Trondheim, 11. mai 2007

Fornyings- og administrasjonsdepartementet
Postboks 8004 Dep
0030 Oslo

Deres ref.:	Deres dato:	Vår ref.:	Vår dato:
200700605-KDB	13.03.2007	118/07	11.05.2007

Høringssvar – ”eID-strategi”

Vi viser til brev av 2.3.2007 om ”Høring – forslag til strategi for bruk av eID og e-signatur i offentlig sektor”, og takker for muligheten til å avgi høringssvar.

Forslagene til strategi for bruk av eID og e-signatur i offentlig sektor virker gjennomarbeidet og grundige, og KITH støtter hovedkonklusjonene i forslaget. Erfaringene med dagens løsninger, særlig knyttet til forretningsmodeller, har tydeliggjort behovet for et selvstendig offentlig initiativ for å sikre en samordnet løsning for sikker elektronisk identitet og signatur.

Langt de fleste tjenester som helsesektoren vil tilby hvor det vil være behov for autentisering, vil kreve sikkerhetsnivå 4 iht. Rammeverket som er vedlagt strategien. Vi vil derfor fokusere våre tilbakemeldinger på dette området, samt virksomhetssertifikater, som har stor betydning for den elektroniske samhandlingen i helsesektoren.

Strategien påpeker også viktige utfordringer knyttet til universell utforming og tilgjengelighet for brukergrupper med spesielle behov, et område hvor dagens sikkerhetsløsninger på mange måter kommer til kort.

Om virksomhetssertifikater
Virksomhetssertifikater er en kritisk del av den infrastrukturen for sikker elektronisk samhandling som helsesektoren har basert seg på. Virksomhetssertifikatene gjør det mulig å utveksle sensitiv helseinformasjon mellom virksomheter i sektoren på en effektiv og trygg måte. Funksjoner for kryptering og signering på virksomhetsnivå er implementert i en rekke løsninger i sektoren, basert på åpne standarder.

Åpne standarder for PKI-løsninger gjør det mulig å implementere tekniske PKI-løsninger uten å tilpasse løsningen til den enkelte PKI-leverandør, så lenge leverandørene støtter de åpne standardene. Så framt en løsning for virksomhetssertifikater som tilbys av Brønnøysundregistrene baserer seg på åpne standarder og profiler som er i bruk i dag, vil en

slik løsning som foreslås i strategien være en effektiv måte å dekke det offentliges behov for virksomhetssertifikater.

Ift. kostnader for virksomhetssertifikater må det legges vekt på at kostnadene bør reduseres betraktelig *eller* tilpasses virksomhetens størrelse. Basert på erfaringene fra helsesektoren ser vi at kostnadene for mindre virksomheter, enkeltmannsforetak osv. i dag er alt for høye. For større virksomheter kan prisen på virksomhetssertifikater være bagatellmessig, men for mindre virksomheter er prisen for sertifikatet betydelig. Vi ser heller ingen påviselige grunner til at prisen på virksomhetssertifikater skal være betraktelig høyere enn prisen for personsertifikater av typen Person-Høyt. Kostnadene for PKI på virksomhetsnivå må ses i sammenheng med den viktige funksjonen disse har for sikker elektronisk samhandling, og må bidra til å redusere terskelen for å ta i bruk nye løsninger.

Om elektronisk signatur
Vi anbefaler at funksjoner for eSignatur knyttes til sikkerhetsnivå 4. Som utredet i ulike sammenhenger er det et fåtall av anvendelser for elektronisk signatur sammenlignet med behovet for autentisering, men i de tilfeller der det har vært ønskelig med signatur, har f.eks. både Lånekassen og NAV stilt krav om sikkerhetsnivå 4. Det synes urimelig å åpne for at borgere skal kunne signere, med de forpliktelser dette innebærer for den enkelte, med mekanismer som ikke tilfredsstiller kravene i lov om elektronisk signatur.

Det vil også kunne virke forvirrende med ulike grader av sikkerhetsløsninger for eSignatur. Vi antar det vil være lettere for borgeren å se og akseptere avveiningen mellom enkelhet/tilgjengelighet på den ene siden og sikkerhet på den andre ved autentiseringsløsninger, og dermed behovet for to nivåer, enn det vil være ved signaturløsninger. Anvendelser som krever en slags ”avsjekking”, aksept av vilkår og betingelser eller bekreftelse på avgitt informasjon kan også likevel implementeres basert på autentisering, jfr. skatteetatens pinkoder for godkjenning av selvangivelsen. På denne bakgrunn finner vi det formålstjenelig å begrense eSignaturbegrepet til sikkerhetsnivå 4.

Om sikkerhetsportal
Vedrørende tjenestetilbudet til en sikkerhetsportal, bør det prioriteres å etablere de tjenester som har høyest nytteverdi, og de tjenester hvor en sikkerhetsportal har klare fordeler framfor desentrale løsninger. Særlig bør tjenestene for formidling av sikker identitet prioriteres, da dette er områder hvor det eksisterer gode tekniske standarder med fungerende implementasjoner. Behovet for signaturtjenester er langt mindre enn tjenester for identitetsformidling, og vi foreslår nedenfor at signaturtjenester bør knyttes til sikkerhetsnivå 4. Etter vår mening bør det derfor heller ikke prioriteres å utvikle signaturtjenester i sikkerhetsportalen i første fase, med mindre disse knyttes til løsninger på nivå 4.

Basert på erfaringene i helsesektoren med implementering av elektronisk signatur stiller vi oss videre tvilende til behovet for en sikkerhetsportal for løsninger for signering i fagapplikasjoner. For det første vil enkelte slike løsninger kunne forutsette at sensitiv informasjon må overføres til en tredjepart for å utføre signaturen. For det andre eksisterer det i dag en rekke gode programmeringsbibliotek og rammeverk for å håndtere signering og verifikasjon av signatur lokalt. Gevinsten ved bruk av en sikkerhetsportal vil derfor være minimal, særlig ift. påføring av signaturer på dokumenter. For verifikasjon av signaturer, særlig kontroll med sertifikatstatus, kan en sikkerhetsportal være gunstig som felles sted for kontroll av status, men også her vil bruk av standardiserte løsninger redusere nytteverdien av sikkerhetsportalens tjenester på området. Tjenestene som sikkerhetsportalen tilbyr bør derfor

være et supplement, og ikke nødvendige for å bruke signaturfunksjonaliteten til de PKI-tjenestene som tilbys gjennom sikkerhetsportalen.

Det bør også vurderes om sikkerhetsportalen kan tilby en felles offentlig tjeneste for tidsstempling av elektroniske dokumenter, i tråd med relevante åpne standarder for dette. En slik tjeneste bidrar til å øke sikkerheten rundt elektroniske signaturer, og bør kunne ha lave investeringskostnader. Tjenesten bør derfor kunne være åpent tilgjengelig.

Om tidsplanen
Den foreslåtte tidsplanen medfører at det ennå vil være en god stund før det offentlige har etablert løsninger på nivå 4, som helsesektoren avhenger av for å kunne etablere løsninger for å gi tilgang til sensitive opplysninger, f.eks. i kommunikasjon med pasienter.

En rekke initiativer er underveis som vil ha behov for sikkerhetsløsninger, som pasienttilgang til reseptinformasjon i eResept og tilgang for pasienter til opplysninger i sin egen kjernejournal. Det vil være uheldig om disse tjenestene ikke kan basere seg på en tilgjengelig offentlig PKI-løsning, og eventuelt etablerer egne løsninger.

Vi aksepterer likevel at behovet for å gjøre et grundig spesifikasjonsløp for å sikre en optimal løsning vil medføre at etableringen av en slik løsning vil ta noe tid. Vi vil derfor anbefale at sikkerhetsportalen inngår avtaler om frikjøp av autentiseringstjenester mot eksisterende PKI-leverandører i markedet fram til en offentlig eID er etablert. En slik løsning vil medføre at tjenestene kan etableres mot *ett felles teknisk grensesnitt* som vil være likt både for dagens løsninger og en framtidig offentlig eID. En slik løsning må forutsette at sikkerhetsportalen kan inngå avtaler som ikke gjør det nødvendig for den enkelte tjenesteleverandør å inngå selvstendige avtaler med PKI-leverandørene.

Med vennlig hilsen

Jacob Hygen
Adm. dir.

Arnstein Vestad
Seniorrådgiver