

Fornyings- og Administrasjonsdepartementet
Postboks 8004 Dep
0030 Oslo
postmottak@fad.dep.no

DERES REF
200700605-KDB

VÅR REF
07/2009

STED, DATO
Oslo, 21.05.2007

Høringsuttalelse – forslag til strategi for bruk av eID og e-signatur i offentlig sektor

Vi viser til departementets (FAD) høringsbrev av 12. mars 2007 vedrørende overnevnte. UDI har lest høringsutkastet til eID strategi og hovedpoengene i vår tilbakemelding er:

- Utredningen er mangelfull mht ansattsertifikater og håndtering/kryptering av E-post
- For mye oppmerksomhet på inngående korrespondanse i forhold til utgående korrespondanse (elektronisk signerte vedtak)
- De strategiske valgene virker ellers fornuftige

Vår høringsuttalelse er bygd opp slik at vi først kommenterer de behov UDI har i forbindelse med bruk av eID og e-signatur. Deretter kommenterer vi de enkelte områdene FAD spesielt ønsket tilbakemeldinger på.

UDIs kommentarer iht egne og Utlendingsforvaltningens behov

Det er mange offentlige etater som samarbeider om å løse utlendingsforvaltningens oppgaver, og dette gjøres med støtte i noen få, felles fagsystemer som deler til dels meget sensitive data lagret i sentrale databaser og elektroniske arkiver. Det er derfor behov for sikre løsninger i forhold til å autentisere flere tusen fagsystembrukere representert ved tilsatte fra 7 forvaltningsorganer; UDI, UNE, UD, IMDi, AID, SKD og Politiet. I tillegg har vi asylmottak og flere av landets kommuner som systembrukere. Flere av brukerne er utenlandske statsborgere ansatt ved norske ambassader og konsulater. Å realisere en to-faktor autentisering av brukere i ulike organisasjoner er avhengig av én standard PKI-løsning for offentlig sektor, en ordning som også omfatter anskaffelser og bruk av ansattsertifikater.

Ansattsertifikater vs virksomhetssertifikater:

Etter UDIs oppfatning hadde det vært ønskelig at strategiutkastet hadde adressert behovet for ansattsertifikater til autentisering og e-signatur. For offentlige organer som ønsker overgang til fullelektronisk saksflyt og samhandling i og mellom organisasjoner enheter i offentlig forvaltning, er en vesentlig forutsetning for realiseringen av fullelektronisk forvaltning ved dette ikke tilfredsstilt.

Et virksomhetssertifikat brukt som et "digitalt segl" kan alene ikke erstatte håndskrevet underskrift gitt at dette utleveres til en person med nødvendig fullmakt. Utlendingsforvaltningen har samlet sett flere tusen saksbehandlere som vil ha ulike nivåer av "signatur-fullmakt" i kraft av sin stilling. Det kan stilles spørsmål ved om et dokument signert av en ikke-identifiserbar

saksbehandler med tilgang til virksomhetens virksomhetssertifikat vil oppfylle kravene til integritet og uavviselig digital signatur av dokumenter.

I bilag 1 til rammeverk for autentisering og uavviselighet henvises det til Ot.prp 82 (1999-2000) om at ”sertifikater utstedet til juridiske personer som for eksempel en bedrift, kan derfor ikke ha status som kvalifisert sertifikat”. Dette understøtter UDIs vurdering av at en fullelektronisk saks- og dokumentbehandling mellom det offentlige (G2G), eller mellom det offentlige og privatpersoner/privat næringsliv (G2P, G2B), er helt avhengig av en individbasert digital signatur i tillegg til at et virksomhetssertifikat (som erstatning for et brevhode/stempel) for å sikre en god elektronisk forvaltning.

Inngående kontra utgående korrespondanse

Det er UDIs oppfatning at høringsutkastet i det vesentligste retter oppmerksomheten på håndtering av ”inngående korrespondanse” (søknader) mellom privatpersoner og det offentlige, og i mindre grad på elektronisk formidling av ”utgående korrespondanse” (vedtak). Dette mener UDI er en vesentlig svakhet med høringsutkastet.

Generell betraktning om ansattsertifikater vs. personsertifikater og fysisk sikring

To-faktor autentisering som ikke bygger på biometri er neppe i alle tilfeller knyttet til autentisering av en fysisk person. For eksempel vil man i en familie med utenlandsk bakgrunn der kun et fåtall personer behersker norsk, sannsynligvis oppleve at de som er norsktalende utfører elektroniske tjenester på vegne av andre fysiske personer i familien. Gjenbruk av slike personsertifikater som ansattsertifikat kan i prinsippet bety en sikkerhetsrisiko, særlig dersom den fysiske sikring som et arbeidssted normalt utgjør (adgangskontroll med mer) ikke lenger hindrer aksess til sensitive opplysninger i arbeidsgivers databaser.

Signering og kryptering av e-post - funksjonalitet i et offentlig samtrafikknavn

UDI mener det i vurderingen av et ”minste felles multiplum” av funksjonalitet i et samtrafikknavn hadde vært ønskelig at man hadde inkludert funksjonaliteten ”Signering og kryptering av e-post”. Det finnes i dag ingen gode løsninger på hvordan fortrolig og/eller personsensitiv informasjon kan formidles via e-post på en måte som sikrer konfidensialitet. En løsning som hadde støttet slik e-post kommunikasjon mellom ulike juridiske personer i et samtrafikknavn ville for Utlendingsforvaltningen kunne medført betydelig besparelser og gitt økt sikkerhet. I dag er det en praksis i forvaltningen at slik informasjon i tillegg til brev også i noen grad oversendes pr. fax eller åpen e-post, noe som utgjør en sikkerhetsrisiko.

Basert på denne argumentasjonen mener UDI at konfidensialitet bør inn som en del av sikkerhetsrammeverket, jfr. begrensningen angitt på side 75, 2. avsnitt.

UDIs kommentarer til de områdene FAD spesielt ønsker tilbakemelding på

I forhold til rammeverket for autentisering og uavviselighet (Vedlegg 1);

Rammeverket tar ikke hensyn til utlevering av ansattsertifikat. Vi synes heller ikke rammeverket er fleksibelt nok med hensyn på fremtidige behov for rollebasert autentisering eller ”single sign-on” løsninger.

I forhold til strategiens hoveddokument;

Nasjonalt ID kort som primær strategi for å realisere eID på sikkerhetsnivå 4 (Kapittel 4)

Det kan virke som om arbeidsgruppen ikke i stor nok grad har vurdert de tekniske sidene ved å la Nasjonalt ID kort være bærer på eID. Smartkort teknologien kan for eksempel sette begrensinger for antall sertifikater eller type sertifikater som skal installeres på kortet. Utlendingsforvaltningen har konkrete problemstillinger som må belyses for at Nasjonalt ID kort skal kunne benyttes opp mot fagsystemene.

UDI viser også til egen høringsuttalelse i forbindelse med sluttrapporten fra den interdepartementale arbeidsgruppen som skulle utrede behovet for Nasjonalt ID kort. Fristen på den høringen er satt til 4. juni 2007.

Behovet for et samtrafikknave – ønsket funksjonalitet (Kapittel 6)

Digitalt innsynsarkiv:

UDI mener det bør gjøres en del avklaringer knyttet til begrepet "Digitalt Arkiv - innsynsarkiv", jfr. kap 6.2 s 52. UDI stiller spørsmål ved om det medfører riktighet at det er tilstrekkelig at brukerstedet (virksomheten) selv kan velge å ta i bruk et slikt felles arkiv så lenge de opererer innenfor rammene av arkivlovens og personopplysningslovens bestemmelser. Vi vil anta at selve den tekniske løsningen "Digitalt arkiv" i seg selv som teknisk løsning må oppfylle NOARK-4 /5 - krav, og være godkjent av Riksarkivet for bruk i den gitte kontekst.

Se også kommentar under "Signering og kryptering av e-post – funksjonalitet i et offentlig samtrafikknave" høyere opp.

Hvordan passer det skisserte tidsløpet inn i UDIs planer?

UDI har allerede utsatt en del arbeid med eID, e-signatur og PKI, på grunn av at man ønsket å satse på Sikkerhetsportalen. Vi synes de skisserte tidsfristene kan virke for optimistiske. Ytterligere forsinkelser vil skade tiltroen til strategien og føre til at alternative løsninger vil bli vurdert.

Hvorvidt de planer som er skissert passer med UDIs planer, så synes vi at de strekker seg for langt frem i tid. Vi har behov for slike løsninger i dag og skulle helst ha vært i gang med arbeidet allerede. Samtidig ser vi fordelene av å benytte en felles løsning for offentlig sektor så dette vil være en avveining. Vi er også usikre på om en felles offentlig løsning vil være obligatorisk å bruke slik at dette vil også spille inn når vi foretar våre valg.

Et annet moment som vil være med på å bestemme om vi må vurdere egne løsninger eller ikke, er hvorvidt strategien vil omhandle ansattsertifikater. Hvis ikke strategien blir mer klar på dette punktet, ser ikke UDI at Utlendingsforvaltningen har så mye å hente på å vente på realiseringen av løsninger vi bare delvis kan benytte oss av. UDI kan da tvinges til selv å måtte vurdere utredning av en felles PKI-løsning for utlendingsforvaltningen

I forhold til forretningsmodeller;

UDI er på generelt grunnlag enig i de strategiske valg som arbeidsgruppen har tatt. Dette gjelder både:

- Brønnøysundregistrenes rolle i forhold til å forsyne virksomhet med virksomhetssertifikater, jfr kap. 5.4
- Samtrafikknave som et offentlig drevet tilbud, jfr. kap 6.4
- Sentralisert forretningsmodell, jfr kap 7.4.

At staten her tar sentral styring anses som en grunnleggende forutsetning for å sikre en rask og enhetlig utbredelse av eID og virksomhetssertifikater i det offentlige, og derigjennom kunne realisere de antatt store samfunnsøkonomiske gevinster som vil ligge i disse tiltakene.

Med hilsen

Ida Børresen
direktør

Tore Dælin
avdelingsdirektør