

Fornyings- og administrasjonsdepartementet
Postboks 8004 Dep
0030 Oslo



Saksbehandler:
Ragnhild Olin Amdam 21.05.07

Vår dato:

Vår referanse:
2007/133-2

Deres dato:
12.03.2007

Deres referanse:
200700605-KDB

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

Vi viser til Deres høringsbrev av 12. mars i år der De ber om kommentarer til overnevnte høringsforslag. Etter samtale med Katarina de Brisis fikk Forbrukerrådet utsatt høringsfristen til 21. mai 2007.

Forbrukerrådet er i utgangspunktet positive til at stadig flere offentlige tjenester tilbys via Internett, og at dette på sikt vil inkludere tjenester som krever høyere sikkerhet enn det som tilbys i dag. Mange brukergrupper oppfatter Internett som en enkel og effektiv måte å kommunisere med det offentlige på. Skal disse ha tillit til løsningen som velges og skal denne reelt sett være sikker i bruk, kreves det imidlertid at en rekke hensyn må ivaretas og utredes ytterligere. Dette gjelder særlig sikkerhet hos sluttbruker, tilgjengelighet og valgfrihet.

Sikkerhet hos sluttbruker

Høringen legger til grunn at *"Begge parter må ha maskinvare og programvare med støtte for felles autentiseringsprotokoller og nødvendige brukerdiallog. Partenes utstyr må være sikret mot uautorisert tilgang og bruk"*. Det legges imidlertid ingen strategi til grunn for hvordan dette skal sikres hos sluttbruker, og hvem som har erstatningsansvar hvis uautorisert tilgang og bruk likevel skulle inntreffe. Dette utgjør også en svakhet i "Vedlegg 1", som kun tar for seg den delen av sikkerhetsrammeverket som går på autentisering og uavviselighet. Vi legger til grunn at vi får en ny mulighet å uttale oss om disse aspektene når veilederen det henvises til i vedlegget foreligger.

Den siste tid har stadig flere nettbankløsninger vært utsatt for datainnbrudd med den konsekvens at konti har blitt tappet, på tross av at bankenes høye IT-sikkerhet og kvalifisert personell til å overvåke eventuelle dataangrep. Offentlige nettbaserte tjenester er attraktive å benytte seg av, og man må derfor være åpen for at også disse løsningene kan bli utsatt for ulike typer angrep som sluttbruker ikke vil ha kontroll over. Dette kan også ramme sluttbrukere med oppdatert virusprogramvare, brannmur og annen sikkerhetsprogramvare som har all grunn til å tro at utstyret er sikret mot uautorisert tilgang og bruk.

For at befolkningen skal ha tillit til den nettbaserte løsningen må det utredes hvordan ulike typer angrep og eventuelle misbruk skal håndteres. Dette gjelder både eventuelle svakheter ved eID eller e-signatur, og sluttbrukers datasikkerhet både på datamaskin og Internett i et stadig skiftende trusselbilde. Virus, phishing og hacking utgjør en økende trussel, og konsekvensene av eID på avveie og eventuelle identitetstyveri kan være store. Den enkelte sluttbruker har begrenset tilgang på kvalifisert personell som kan ivareta sikkerhetshensyn i det daglige. Det bør utredes om det i det hele tatt er realistisk at sluttbruker har kompetanse til å ivareta et slikt sikkerhetsansvar på egenhånd, og eventuelle tiltak for å ivareta dette.

Store deler av befolkningen vil foretrekke å ha kontakt med det offentlige via Internett fremfor alternative kanaler, og dette utgjør i seg selv en stor samfunnsmessig besparelse. Det er samfunnet som legger til rette for og oppmoder til bruk av offentlige selvbetjeningsløsninger på nett, og det bør overveies om det derfor ikke også er samfunnet som bør betale prisen ved eventuelle angrep og misbruk.

Tilgjengelighet og valgfrihet

Universell utforming

Høringen påpeker at forslagene i strategien også må konsekvensvurderes i forhold til krav til universell utforming, med tanke på de med nedsatte funksjonsevner. Det er viktig at denne tilretteleggingen inkluderer grupper som har lese- og skrivevansker og de som innehar begrenset digital kompetanse. Språket bør derfor være enkelt, navigasjonen mest mulig intuitiv og det er særlig viktig at det er lett for sluttbruker å kunne verifisere at et sertifikat faktisk er gyldig.

I høringsbrevet påpekes det at hvordan kravene til universell utforming skal oppfylles først vil bli avklart etter denne høringen og i dialog med brukerorganisasjonene. Vi anser oss selv som en slik organisasjon, og ønsker å få en ny anledning til å uttale oss når disse kravene foreligger.

Åpne standarder

Høringen legger til grunn at det skal benyttes åpne standarder, men det utdypes ikke hvordan dette er tenkt realisert. Det er viktig at de åpne standardene blir implementert på en slik måte at det motvirker innelåsning til bestemte leverandører og at det inkluderer alle relevante plattformer. For eksempel er TCP/IP en åpen og fri standard, men dette forhindrer en ikke i å implementere tjenester som krever Internet Explorer eller Windows. Det skal være en selvfølge at forbrukeren kan bruke de offentlige selvbetjeningsløsningene uavhengig av for eksempel plattform, operativsystem, nettleser eller e-postprogram. På samme måte må det forhindres at sertifikatapplikasjonene ikke er begrenset til kun å støtte ett operativsystem eller kun utvalgte nettlesere. Det er dessuten viktig at løsningen som velges er fremtidsrettet og tar høyde for den hurtige utviklingen av blant annet operativsystemer og programvare.

Nasjonalt ID-kort

FAD ser forsyning av publikum med eID i sammenheng med mulig utstedelse av et nasjonalt ID-kort, og sikkerhetsnivå 4 *"baseres på at det blir etablert en ordning for offentlig utstedelse av eID i regi av Justisdepartementet, som et ledd i etableringen av en frivillig ordning for utstedelse av et nasjonal ID-kort"*.

Vi mener det vil være hensiktsmessig med en offentlig utstedt eID, slik som det blir foreslått. Dette vil kunne gi brukerne gunstigere brukervilkår enn det markedsløsningene tilbyr. Det vil dessuten være hensiktsmessig for brukerne å kun behøve én påloggingsløsning i kontakt med det offentlige via nett. Hvis nasjonalt ID-kort blir primærløsningen, er det imidlertid en forutsetning at det finnes en alternativ løsning for de som ikke ønsker eller oppfyller kravene til å inneha dette kortet, men som har behov for kontakt med det offentlige. Den alternative løsningen må også inkludere de som av ulike årsaker ikke innehar fødselsnummer eller D-nummer men som er avhengig av kontakt med det offentlige. Dette kan blant annet gjelde foreldre til asylbarn i skolepliktig alder, som har rett på innsyn i barnas opplysninger men gjerne ikke innehar kravene som stilles for å få tildelt fødselsnummer eller D-nummer.

Alternative kommunikasjonskanaler

I blant annet eNorge-planen foreslås incentiver som kortere saksbehandling ved innsending av søknader på nett. Dette vil utgjøre en reell forskjellsbehandling for de som frivillig eller ufrivillig ikke bruker Internett. Det er viktig at det finnes alternative kommunikasjonskanaler med det offentlige for disse ikke-brukerne, gjennom for eksempel opprettholdelse av dagens telefontjenester og offentlige kontorer i nærmiljøet. Det bør heller ikke knyttes vesentlige ulemper til å ikke basere seg av disse løsningene, som for eksempel uforholdsmessig lengre saksbehandlingstider på papir enn på nett.

Et eksempel på et tiltak vi i Forbrukerrådet har god erfaring med er Forbrukerinfo. Dette er en veiledningstjeneste som er tilgjengelig på 148 steder i Norge gjennom bibliotek og servicekontorer, hvor ansatte har fått opplæring av Forbrukerrådet i grunnleggende juridiske ferdigheter. Slik kan de som har behov for veiledning og som av ulike årsaker ikke kommer i kontakt med Forbrukerrådet via andre kanaler likevel få den hjelpen de trenger. Totalt dekker vi over 2,2 millioner innbyggere på denne måten, og kostnadene med tilbudet til nå har vært svært lave sammenlignet med effekten. Ta gjerne kontakt med oss for mer informasjon om hvordan en slik tjeneste kan tilrettelegges.

Andre hensyn

For at brukerne skal ha tillit til løsningen er det også viktig at teknologien som ligger til grunn gir muligheter for ettersporbarhet og gjennomsiktighet. Dette er for det første viktig for at både sluttbruker og relevant sikkerhetspersonell til enhver tid har oversikt kan få oversikt over hvilken tilgang noen på forskjellige tidspunkt har hatt til de forskjellige dataene. Slik vil man ha oversikt over både bruk og dermed også potensielt misbruk. For det andre er dette viktig for at den enkelte sluttbruker skal kunne undersøke grunnlaget for eventuelle rettsvirkninger, og kunne avdekke svakheter i blant annet helautomatiserte saksbehandlingssystemer. Dette vil blant annet kunne avdekke tilfeller hvor man har fått avslag på en søknad man hadde hatt rett til å få innvilget.

Med hilsen

for Forbrukerrådet

Audun Skeidsvoll
avdelingsdirektør

Benedicte Bergseng Mælan
underdirektør