Skattedirektoratet

Saksbehandler
Svein Mobakken

Telefon
22 07 74 50

Deres dato
12.03.2007

Deres referanse
200700605-KDB

Vår dato
16.05.2007

Vår referanse
2007/111107/SKD-IT/SMO/008

Fornyings- og administrasjonsdepartementet
Postboks 8004 Dep
0030 Oslo

Uttalelse om forslag til strategi for bruk av eID og e-signatur i offentlig sektor

Skattedirektoratet stiller seg positiv til forslaget om statlig utstedelse av eID. I videreføringen av arbeidet med eForvaltning vil etablering av en felles løsning for e-signatur og eID være av stor betydning. Fravær av en klart formulert strategi på dette området har bidratt til at Norge har falt nedover på internasjonale eGovernmentrangeringer. Foreliggende forslag vil kunne medvirke til å snu denne trenden, og føre til et grunnlag for utvikling og tilbud om mer omfattende og komplette elektroniske tjenester til publikum og næringsliv.

Direktoratet har vært aktiv bidragsyter i utformingen av høringsutkastet.

Overordnede kommentarer til rapporten

Den vanlige bruker av etatens tjenester har relativt sjelden kontakt med Skatteetaten. For den store majoritet skjer det kun i fbm innlevering av selvangivelse, endring av skattekort, flyttemelding m.m. Vi er derfor opptatt av hvordan de konkrete løsningene utformes og tilbys. Det er av største betydning at sikkerhetsløsningene kan fremstå som enkelt tilgjengelig, både bruksmessig og kostnadsmessig, slik at utbredelse og anvendelse sikres best mulig. Alternativet vil fort kunne innebære tilbakefall til papirbaserte alternativer med de kostnadsmessige og kvalitetsmessige konsekvenser dette vil kunne ha. Generelt mener vi derfor at strategien bør ha et sterkere fokus på brukervennlighet og tilgjengelighet som vi anser å være en kritisk suksessfaktor.

Videre er det viktig at innføring av løsningene gjøres på en måte som kan ivareta tilstrekkelig sikkerhet i fht til tjenestens reelle innhold. Med det menes bl a at det kan gis handlingsfrihet til å kunne velge enklere løsninger for tjenester på et lavere sikkerhetsnivå.

Skatteetaten benytter i dag med stor suksess PIN-kodebasert pålogging for de store publikumstjenestene, og har oppnådd en svært høy andel elektronisk innlevering. Det skyldes etter vårt skjønn et strengt fokus på at løsningene må være enkle i bruk samtidig som løsningene gir tilstrekkelig sikkerhet. Vi mener sikkerheten i dagens påloggingsrutiner er forsvarlige for de tjenester som etaten tilbyr, og vi ser ikke at det vil være behov for vesentlige endringer i nær fremtid. Skatteetaten har derfor for tiden ingen planer om tjenester som vil kreve eID på nivå 4.

Postadresse
Postboks 6300, Etterstad
0603 Oslo
skattedirektoratet@skatteetaten.no

Kontoradresse
Fredrik Selmers vei 4
Org. nr.:974761076

Sentralbord
22 07 70 00
Telefaks

Det må fortsatt være etatenes egen oppgave å definere nivået for akseptabel risiko. Det er viktig at valgt strategi for e-id ikke svekker muligheten til å opprettholde en enkel påloggings-mekanisme. Elektroniske løsninger konkurrerer med papirbaserte løsninger – det enkleste er gjerne det beste. Vi oppfatter strategien slik at det ikke legges opp til utfasing av etablerte etatsspesifikke løsninger før nivået av utbredelse og dekningsgrad for nye sikkerhetsløsninger er tilfredsstillende, og før en helhetlig vurdering av brukervennlighet og kostnadseffektivitet tilsier dette. (ref s. 15, 2. avsnitt). Skattedirektoratet er enige i denne presiseringen.

Generelt stiller Skatteetaten seg positiv til forslaget om at nasjonalt ID-kort brukes som bærer av eID nivå 4, gitt at dette kommer i henhold til tidsplan, og at det gjøres tiltak for å oppnå høy utbredelse.

Tidsplanen skissert i figur 1, "Gjennomføringsplan" antyder at eID på nivå 3 vil kunne gjennomføres umiddelbart (inneværende år) basert på en utsendelse av Skattekort PIN for Skattekort 2008. Vi vil peke på at dette anses å være en stram plan som, basert på beslutninger som ennå ikke er fattet vil ha en høy risiko for forsinkelse. En første versjon, basert på løsninger tilknyttet MinID kan redusere denne risikoen noe, men beslutninger vedrørende Skattekort PIN for 2008 må kunne fattes kort tid etter høringsfristens utløp.

Skatteetaten registrerer at det er foreslått å etablere E-id nivå 3 basert på Skatteetatens distribusjon av PIN koder og at Skatteetaten utvikler, utsteder og distribuerer denne basert på finansiering innenfor rammen av egne budsjetter. Dette, også sammen med en videreutvikling av et forslag om statlig utstedelse av eID basert på Det sentrale folkeregister, og dermed fødselsnummer, hilser vi velkommen. Dette sikrer at hver borger får en unik eID. Gjennomføring av disse ordningene vil imidlertid forutsette samtykke i Finansdepartementet.

Skatteetaten er enig i at anvendelse av sikkerhetsløsninger på et høyere nivå også skal kunne brukes for å få tilgang til tjenester på et lavere nivå (ref. s. 60). Vi ser det imidlertid ikke som hensiktsmessig å legge unødig høye krav på enklere tjenester der brukervennlighet og effektivitet er viktig for å få høy bruksfrekvens.

I det etterfølgende drøftes noen utvalgte temaer i mer detalj.

Samordning av MinId og Altinn

I dag fungerer både MinId og Altinn som "samtrafikknav" ved at ulike offentlige tjenesteeiere/etater kan utnytte e-idene som er tilgjengelige i disse løsningene. Skattedirektoratet støtter rapportens anbefaling om en samordning mot disse to påloggingsløsningene.

I dag vedlikeholdes to brukerdatabaser, en i MinSide og en i Altinn, med hvert sitt datasett: statisk passord, e-postadresse og mobilnummer på alle registrerte brukere. Fra et bruker-vennlighetsperspektiv og kvalitetsperspektiv er det ønskelig med et felles vedlikehold av disse påloggingsløsningene.

I den sammenheng vil vi også peke på at det når det gjelder digitalt arkiv, må dette koordineres med tilsvarende tjenester i Altinn slik at det ikke opprettes uhensiktsmessig overlappende offentlige tilbud på dette området.

Vi ser positivt på etablering av et samtrafikknav med et enkelt sett av avtaler for de enkelte aktører, men at dette må samordnes med de offentlige portalene Altinn og Min Side på en slik måte at ikke overlappende ressurskrevende tjenester oppstår.

Risikovurdering og redegjørelse for utenlandske løsninger

Sikkerhetsnivåene er i rapporten ikke forankret i en risikovurdering. Det gjør det vanskelig å vurdere hvilke trusler som reduseres ved å gå opp til et høyere sikkerhetsnivå, herunder om forskjellene er relevante og signifikante.

Eksempelvis er skillet mellom dynamiske og statiske passord primært knyttet til faren for gjenbruk av passordet f. eks. ved avlytting av kommunikasjonen. Gitt tilfredsstillende skall- og kommunikasjonssikring (som forutsettes i rammeverket) er det uklart hvilke trusler som vil kreve dynamisk passord[1] i stedet for statisk passord. Skrapelodd (s 80) er ikke kopierbare, men den som har mulighet til å kopiere passordet, vil også ha mulighet til å skrape frem et nytt passord[2].

Strategien begrunner behovet for høyere sikkerhetsnivåer delvis med teknologiutviklingen og økt nettkriminalitet (s 15 tredje avsnitt). Slik vi forstår det, er imidlertid disse trusler som langt på vei er upåvirket av rammeverket, jf. at angrepet på nettbanker nylig skyldtes skreddersydde trojanere – som rammer skall- og kommunikasjonssikkerheten, og ikke påloggingsmetoden. Det er behov for en nærmere analyse av hvilke trusler som rammeverket tar sikte på å verne mot.

Videre savnes en redegjørelse for utenlandske løsninger for felles e-id. I Danmark finnes blant annet fellesløsningene "Den fælles pin-kode" og "OCES-sertifikater". I det videre arbeid bør det foretas en vurdering av disse løsningene i fht det foreslåtte rammeverk.

Rammeverkets begrensninger og avgrensninger

I rapporten presiseres det at skallsikringen ikke inngår i rammeverket (ref. s 77), og at *"partenes utstyr må være sikret mot uautorisert tilgang og bruk"* (s 76). Dette hviler på forutsetninger som neppe er til stede hos et stort antall av innbyggerne:

- En stor andel av brukerne har ikke oppdatert antivirusbeskyttelse.
- Vesentlige deler av infrastrukturen er i dag usikker.
- Det må legges til grunn at det kan være vanskelig for mange brukere å skille mellom ekte og falske nettsider, de er således sårbare for villedende nettsider (phishing).
- Det vil alltid være et tidsspenn mellom når virus lages og når vaksine er distribuert.

Mye kan tale for at de viktigste sikkerhetsutfordringer – i alle fall for tjenester som krever autentisering på sikkerhetsnivå 3 eller 4, – ligger i skall- og kommunikasjonssikring. Dette vil fremkomme i de konkrete risikovurderinger som etatene gjør.

Avgrensning mot konfidensialitet – uavviselighet og konfidensialitet gir forskjellige sikkerhetsbehov

Rammeverket avgrenser seg (s 75 andre avsnitt) mot konfidensialitet. Det er logisk sett fornuftig, jf. at rammeverkets fokus på uavviselighet – som er en egenskap knyttet til bevisføring for *disposisjoner*. Bevis for uavviselighet (ekthet/autentisitet) forutsetter både tilfredsstillende identitetskontroll (autentisering) og tilfredsstillende bevisføring

---

[1] I alle fall med rammeverkets definisjoner, hvor også gjenbrukbare "engangs"passord/passord med kort levetid inngår.

[2] Muligheten til misbruk er således omtrent like stor, mens det *kan* være ulikhet mht. oppdagelsesrisiko – avhengig av om innehaveren holder rede på hvilke passord som er skrapet eller ikke. (Liknende oppdagelsesrisiko kan sikres gjennom varsling av siste pålogging/innsynsrutiner).

(integritetssikring, uavviselighet). Konfidensialitetsinteressen er knyttet til *innsynstjenester*, og stiller ikke i seg selv krav til uavviselighet på samme sikkerhetsnivå.

Vi ser imidlertid ikke at strategien er konsekvent i forhold til denne avgrensningen mot konfidensialitet, jfr. at man begrunner behovet for e-ID på nivå 4 med at NAV skal tilby tjenester med *sensitive* helseopplysninger. Det må skyldes behovet for høyere konfidensialitetsvern.

Vi tror imidlertid et slikt rammeverk vil kunne brukes både i forhold til å sette autentiseringskrav pga konfidensialitet (innsynstjenester) og pga behov for uavviselighet (disposisjoner). Uavviselighetskravet vil da vises som kombinasjonen av et krav til uavviselighet (siste kolonne i tabellen på side 82) og et krav til autentisering (de øvrige kolonner).

Det er i så fall viktig at det gjøres klart at tjenestene må plasseres i disse dimensjoner, og at det kan føre til at autentiseringen (qua innsynstjeneste) må skje på nivå 4, mens behovet for uavviselighet tilsier nivå 2 eller 3 (qua disposisjon).

Virksomhetssertifikater

For Skatteetaten antar vi at behovet for virksomhetssertifikater primært vil være knyttet til samhandling mellom og fra offentlig myndigheter.

Vi ser et fremtidig behov for å kunne håndtere utenlandske virksomheter, og ev. virksomhetssertifikater utstedt av utenlandske utstedere, og mener dette bør vurderes i forhold til samtrafikknavets oppgaver.

Med hilsen

Reidar Nybø
Avdelingsdirektør
IT-avdelingen

Svein Mobakken

Kopi: Finansdepartementet