

Fornyings- og administrasjonsdepartementet
Postboks 8004 Dep
0030 OSLO

Deres ref:
200700605-KDDB

Vår ref:
glin

Dato:
11. mai 2007

Høringsvar - forslag til strategi for eID og e-signatur i offentlig sektor

Vi viser til Deres høringsbrev av 12. mars 2007 med tilhørende forslag til strategi for eID og e-signatur i offentlig sektor. Innledningsvis vil vi gjerne få takke for anledningen til å komme med våre vurderinger og innspill. Vårt høringssvar består av dette brevet og et vedlegg med kommentarer til konkrete punkter i høringsdokumentet.

Omfattende infrastrukturer er etablert

Aktører i markedet har etablert omfattende eID og e-signatur infrastrukturer. Buypass har per dags dato over 1,8 millioner kunder med Buypass ID på smartkort og i mobil, som benyttes over 10 millioner ganger per måned. Antallet Buypass IDer i markedet øker fortsatt med flere tusen hver uke. Dette innebærer at mer enn 50 % av Norges befolkning over 18 år har en Buypass ID. I tillegg til dette volumet kommer utbredelsen av BankID. Utbredelsen av eID og e-signatur i Norge er dermed langt over kritisk masse. Like viktig, disse eIDene er knyttet til tjenester med høy bruksfrekvens.

Fornyings- og administrasjonsdepartementet, Nærings- og handelsdepartementet og markedsaktørene har i felleskap (SEID prosjektet) etablert norske versjoner av internasjonale tekniske standarder (ETSI med mer) som infrastrukturleverandørene baserer sine løsninger på.

Leverandører som tilbyr eID og e-signatur løsninger og tjenester til offentlig sektor må tilfredsstille et omfattende sett av krav regulert i Lov om e-signatur, selvdeklarasjonsordningen for sertifikatutstedere og Kravspesifikasjon for PKI i offentlig sektor. Buypass' virksomhet, eID og e-signatur løsninger og tjenester etterlever disse regulatoriske kravene gjennom registrering og selvdeklarerer hos Post- og teletilsynet. Buypass er, som et av 15

selskaper i Norge, sertifisert av Det Norske Veritas i henhold til standard for informasjonssikkerhet ISO/IEC 27001. Se http://www.buypass.no/nyhet_070419.htm

Norsk innovasjon og verdiskaping

Buypass med partnere og andre markedsaktører har investert betydelige beløp i de nevnte løsninger og infrastrukturer (~X00 MNOK) over de siste 8 årene. Vi har grunn til å tro at vi er helt i tetsjiktet internasjonalt med hensyn til teknologi, løsninger, utbredelse, bruk og aktive kunder.

Utviklingen av vår teknologi, våre løsninger og tjenester er basert på innovasjon i samarbeid med norske partnere. Et fokus er å tilfredsstille de ønsker og krav som offentlige virksomheter har. Offentlig sektor, med sine åpenbare behov og store potensielle effektiviseringsgevinster gjennom digitalisering av tjenester og arbeidsprosesser, har vært og er en viktig driver for denne innovasjonen. Det nye strategiforslaget kan komme til å legge en betydelig demper på slik innovasjon. Tydelige og varige rammebetingelser som muliggjør lønnsom forretningsutvikling er viktige forutsetninger for videre innovasjon og verdiskaping på området.

Offentlige virksomheter benytter eksisterende løsninger

Mange offentlige virksomheter har allerede foretatt store investeringer i integrering av eksisterende eID og e-signaturløsninger og ytterligere omfattende prosjekter pågår. En overgang til nye offentlige eIDer vil innebære at deler av disse investeringene går tapt, at nye investeringer i migrering må påregnes, og at prosjekter blir utsatt. Dette betyr videre at betydelige effektiviseringsgevinster utsettes i flere år og muligens ikke oppnås.

Siden lanseringen av Buypass' produkter og tjenester i det norske markedet i 2001 har Buypass opplevd en stadig større interesse for eID og e-signatur fra offentlige virksomheter. Noen eksempler:

- Buypass har utstedt ca. 3.000 eIDer til virksomheter (virksomhetssertifikater), hvor majoriteten er utstedt i prosjekter knyttet til offentlig virksomhet. Vi utsteder nå gjennomsnittlig 300 virksomhetssertifikater per måned
- Buypass' virksomhetssertifikater benyttes for å sikre flere hundre tusen transaksjoner/meldinger per måned
- Buypass har inngått avtaler med majoriteten av leverandørene av elektroniske pasientjournalssystemer (EPJ) til helsesektoren. Det er så langt levert over 10.000 sertifikater, både personsertifikater (Person Høyt) og virksomhetssertifikater til helsesektoren
- Buypass har inngått rammeavtale for leveranse av personsertifikater, virksomhetssertifikater og tilhørende produkter/tjenester med Helse Øst v/Nye Ahus på vegne av Nasjonal IKT. Rammeavtalen kan benyttes av hele helsesektoren

- Buypass har fra 2003 levert eID og e-signaturtjenester til Altinn for elektronisk innrapportering. Over 10 % av alle pålogginger fra bedrifter i Altinn gjennomføres med Buypass Smartkort. I tillegg til andre typer Buypass Smartkort som benyttes i Altinn er det i løpet av første kvartal 2007 utstedt over 2.000 personsertifikater (Person Høyt) på "Altinn smartkort" til profesjonelle avgivere (primært regnskapsbyråer). Se <https://www.altinn.no/cms/1044/altinn/Lar+a+bruke+Altinn/Smartkort.htm>

Buypass produkter og tjenester for eID og e-signatur benyttes i tillegg av en rekke andre offentlige virksomheter. Noen eksempler er: Kredittilsynet (egen løsning i tillegg til Altinn), Posten, Norsk Tipping, Mercell (offentlige anbud), Gassco, Luftfartstilsynet, MinJournal-prosjektet, samt flere kommuner og fylkeskommuner.

Foreslått strategi kan medføre at nye potensielle tjenesteytere og offentlige virksomheter inntar en "vente-og-se" holdning. Strategiforslagets fremdriftsplan medfører en betydelig risiko for at utviklingen av nye offentlige bruksområder må utsettes i flere år. Dette innebærer også en høy risiko for at eksisterende leverandører av eID og e-signatur vil prioritere andre markeder.

Visjonen – én eID for bruk i alle tjenester

Undersøkelser viser at en internetbruker i dag må forholde seg til omlag 20 ulike brukernavn, passord, engangskoder og kodegenerasjoner. I "eNorge 2009 – det digitale spranget" står dette problemet omtalt i kapittel 3.1 side 26. Et mål er å forenkle og samtidig øke sikkerheten ved identifikasjon og autentisering for både brukere og tjenesteytere. Med andre ord - etablere én eID som kan benyttes i alle tjenester, uavhengig av tjenestenes varierende krav til sikkerhet. Buypass arbeider med dette som et viktig mål.

Målet om én eID til alle tjenester er ikke til hinder for fri konkurranse mellom leverandører av allment aksepterte eIDer og e-signaturer, hvor brukerne fritt kan velge mellom disse. Dette kan sammenliknes med at en kunde idag fritt kan velge mellom flere betalingsmidler ved kjøp av en vare.

Etablering av en ny eID på et nytt lavere sikkerhetsnivå, nivå 3, som ikke kan benyttes i alle tjenester er å gå i motsatt retning av målet om én eID for alle tjenester.

Vi erkjenner at det i en overgangsperiode må finnes alternativer med lavere sikkerhetsnivå inntil infrastrukturene på nivå 4 har full utbredelse hos landets innbyggere. I denne overgangsperioden mener vi at de eksisterende alternativene er tilstrekkelige, som for eksempel bruk av "skatte-PIN".

Forsyning av innbyggere med eID og e-signatur

Eksisterende elektroniske offentlige tjenester som krever identifisering av sluttbruker benytter i dag hovedsakelig eID på nivå 1 (brukernavn/passord), eID på nivå 2 (skatte-PIN etc) eller eID på nivå 4 (selvdeklart PKI). Buypass er som nevnt skeptiske til en etablering av ny eID på nivå 3:

- eID nivå 3 er ikke spesifisert og størrelse og omfang på investeringer og driftskostnader er ikke estimert
- Investeringer som et offentlig brukersted vil måtte foreta for å benytte felles eID på nivå 3 er ikke estimert
- Etablering og bruk av felles eID på nivå 3 forutsetter integrasjon mot offentlig samtrafikknave, og kan tidligst tas i bruk medio 2008

Buypass mener at det ikke foreligger et tilstrekkelig beslutningsgrunnlag for å kunne konkludere med effektiviseringsgevinster relatert til en etablering av en ny midlertidig infrastruktur av eID på nivå 3.

Etter vår oppfatning bør en forsyningsstrategi av eID og e-signatur til innbyggere ta hensyn til at det er ulike brukergrupper med ulike behov som skal betjenes:

- De som i kraft av sin profesjon skal benytte tjenester fra offentlig virksomhet. Innen helsesektoren er dette leger og annet helsepersonell. For en rekke andre offentlige tjenester er dette typisk profesjonelle avgivere som eksempelvis regnskapsførere, revisorer og advokater. Dette er alle målgrupper som er klart definerte. Målgruppene har ofte hyppig bruk av tjenestene og representerer en viktig del av effektiviseringspotensialet. Vi antar at dette er årsaken til at en rekke offentlige virksomheter i første rekke har hatt fokus på forsyning av eID og e-signatur til disse målgruppene for å effektivisere store transaksjonsvolumer. For disse er det naturlig å benytte eID på nivå 4, da dette vil gi dem tilgang til alle offentlige tjenester.
- Sluttbrukere/innbyggere/privatpersoner. Denne gruppen bruker offentlige tjenester sjelden, og bør betjenes gjennom eksisterende og/eller kommende infrastrukturer av eID på nivå 4. En privatpersons interesse for å anskaffe og benytte en eID er blant annet relatert til bruksområder, brukshyppighet og brukerterskler for anskaffelse og installasjon. Undersøkelser fra andre land viser at en egen offentlig eID til privatpersoner primært for bruk mot offentlige tjenester benyttes sjelden. Det er derfor helt avgjørende at en privatperson kan benytte en eID som benyttes til andre daglige/hyppige formål.

Forsyning av virksomheter med eID og e-signatur

Med bakgrunn i arbeidsgruppens estimater på volum av virksomhetssertifikater til offentlige virksomheter, kan vi ikke se at dette forsvare kostnadene relatert til en etablering av en offentlig utsteder. Offentlige virksomheters behov for virksomhetssertifikater er pr. i dag godt dekket gjennom tilbud fra leverandører i markedet.

Flere samtrafikknave er etablert

Vi ser behovet for tekniske samtrafikknave som gir tilgang til flere eID-er og e-signaturer i markedet. Det eksisterer allerede en rekke slike samtrafikknave, både under offentlig kontroll (i Altinn og i MinSide) og hos private leverandører (for eksempel Kantega, Sem & Stenersen Prokom, More, BBS). Disse benyttes både av offentlige og private virksomheter.

Buypass er positiv til å inngå én avtale som omfatter alle virksomheter i statlig og kommunal sektor, og som dekker behovet for forutsigbare kostnader.

Hvis det allikevel skal utvikles et nytt offentlig samtrafikknave, må eksisterende eID-er og e-signaturer kunne benyttes. Buypass mener følgende avklaringer og forutsetninger bør vurderes ved en eventuell etablering av et nytt offentlig samtrafikknave:

- Det bør kun være en teknisk løsning for formidling av transaksjoner som er usynlig for sluttbruker. Det må ikke konkurrere med leverandører av eID og e-signatur, eller være til hinder for innovasjon og nye tjenester fra disse
- For å sikre lave priser til offentlige virksomheter og brukersteder bør det være fri konkurranse mellom tilbydere av samtrafikknave
- Eksisterende eID og e-signaturløsninger, tilgjengelig i flere alternative samtrafikknave, vil gjøre det langt lettere å realisere effektiviseringsgevinster. Offentlig sektor vil også kunne redusere sin risiko betraktelig ved å åpne generelt for bruk av allerede utstedte eID-er
- Både våre egne og andres erfaringer tyder på at kostnadene ved et nytt offentlig samtrafikknave med tilhørende tjenester er estimert for lavt

En rekke offentlige virksomheter har i dag fokus på forsyning av eID og e-signatur til målgrupper som har hyppig bruk av tjenestene og dermed representerer en betydelig del av effektiviseringspotensialet. Flere av disse offentlige virksomhetene har integrert eID og e-signaturløsningene inn i sine respektive fagapplikasjoner. Helsesektoren er et eksempel på dette hvor eID og e-signaturløsningene er tungt integrert i det enkelte fagsystem. Disse løsningene dekker det behovet helsesektoren har uten bruk av samtrafikknave.

Erfaringsmessig vil ikke fagapplikasjoner/systemer kunne utnytte et samtrafikknave for informasjonsutveksling mellom de ulike etatene og fagapplikasjonene.

Oppsummering

Mange offentlige virksomheter har allerede tatt i bruk løsninger for eID og e-signatur fra markedsaktører. Vi opplever en stadig økende interesse fra offentlige virksomheter som umiddelbart ønsker å benytte Buypass ID og e-signaturløsninger. Det er derfor svært viktig at *Strategi for bruk av eID og e-signatur i offentlig sektor* ikke bidrar til å bremse denne positive utviklingen av gode elektroniske tjenester som effektiviserer offentlig sektor.

Valg av strategi bør:

- legge til rette for at offentlige virksomheter og innbyggere kan fortsette å benytte eksisterende løsninger for eID og e-signatur (gjelder også MinSide)
- være i henhold til gjeldende lover og regler, herunder konkurranselovgivning
- tilrettelegge for rask vekst i nye tjenester og bruksområder

Vi kjenner ikke til at tilsvarende strategi som foreslås i høringsdokumentet har lyktes i andre land. Vi antar at dette i hovedsak skyldes at private personer i snitt har kontakt med det offentlige 1 til 2 ganger per år (uavhengig av om det er digitale eller papirbaserte tjenester). Dette er en altfor lav bruksfrekvens for å forsvare investeringer i etablering, vedlikehold og drift av en offentlig eID og e-signatur. Hvem husker koden til en eID som benyttes så sjelden?

Den grunnleggende forutsetningen fra Kravspesifikasjon for PKI i offentlig sektor, datert Januar 2005 (side 5), bør legges til grunn for videre strategivalg: *"Det ligger videre som en forutsetning til grunn om at løsninger for eID og e-signatur skal leveres av markedet i konkurranse. Videre er det forutsatt at den eID som en bruker vil anskaffe skal gi størst mulig nytte, dvs. skal kunne brukes mot flest mulig elektroniske tjenester, både offentlige, men også private, der eID eller e-signatur er påkrevet."*

Myndighetene bør fortsatt fokusere på å regulere markedet, benytte eksisterende infrastrukturer og løsninger, samt sikre like konkurransevilkår for leverandører av eID og e-signatur. Dette vil gi lavere risiko og raskere vekst i byggingen av nye offentlige elektroniske tjenester og bruksområder for publikum og næringsliv.

Vi stiller oss til disposisjon ved et eventuelt behov for ytterligere opplysninger og/eller gjennomgang av høringssvaret.

Med vennlig hilsen

Buypass AS

Gunnar Lindstøl
Administrerende Direktør

Vedlegg: Buypass' kommentarer til konkrete punkter i høringsdokumentet

Vedlegg

Buypass' kommentarer til konkrete punkter i høringsdokumentet

Dette vedlegg belyser problemstillinger og mulige utfordringer relatert til konkrete punkter i høringsdokumentet. Sitater fra høringsdokumentet er skrevet i *kursiv*.

Scenarie 2010 (side 4-5)

I eksempel mellom pasient og fastlege er det benyttet kryptering av e-post for pasientens avlevering av informasjon til lege. I eksemplene for pasientkommunikasjon, egenregistrering og e-Resept vil det, så langt vi forstår, være et krav til kryptering.

Buypass er enig i at det vil være et stort behov for løsninger for sikker kryptering av personsensitive opplysninger, men det er i høringsdokumentet senere forutsatt/avgrenset at kryptering ikke er en del av strategien. Etter vår oppfatning bør kryptering også utredes og være en del av strategien.

Sikkerhetsnivå 4 (side 15)

Det hevdes at markedet er umodent og at dagens etablerte løsninger kun delvis oppfyller offentlige krav, og ikke er selvdeklart.

Buypass produkter og tjenester er selvdeklart og kan således benyttes til alle offentlige tjenester.

Forsyning av virksomheter med eID (side 16)

Det hevdes at forretningspotensialet for markedsaktører er lite.

Buypass har lang erfaring med leveranse av virksomhetssertifikater til blant annet helsesektoren, og ser dette som et interessant satsningsområde. Dette må i mange sammenhenger ses sammen med utstedelse av personsertifikater (eksempelvis legekontorer) og i sum gir dette et vesentlig forretningspotensiale.

Etablering av et offentlig samtrafikknavn for eID og e-signatur (side 17-18)

"Offentlige virksomheter som har tjenester på nett vil imidlertid pålegges å legge til rette for bruk av felles eID på nivå 3 og 4, så snart ordninger for å utstede disse er operative. Dette pålegget bør sannsynligvis gis gjennom en forskrift".

Buypass anbefaler at overgang/pålegg konsekvensutredes for etablerte løsninger med bruk av PKI i offentlig sektor. I særdeleshet vil helsesektoren bli sterkt berørt av foreslått overgang/pålegg.

Gjennomføringsplan (side 22)

Etter det Buypass erfarer korresponderer ikke tidspunkter i foreslått gjennomføringsplan med planer som foreligger i eksisterende og planlagte prosjekter for bruk av PKI i offentlig sektor. Dette gjelder eksempelvis flere prosjekter i ulike deler av helsesektoren. Den foreslåtte tidsplan bør konsekvensutredes ift eksisterende og planlagte prosjekter med bruk av PKI i offentlig sektor.

Offentlig bruk av eID/e-signatur – NAV/Helsevesenet (side 27-28)

"Helsevesenet har derfor ikke sett behov for egne ansattsertifikater for elektronisk kommunikasjon mellom virksomheter".

Deler av behovene i helsesektoren kan løses ved bruk av kun personlige sertifikater, men helseforetakene ønsker å utstede ansattsertifikater til sine ansatte (både kvalifiserte og ikke-kvalifiserte). Dette både for bruk internt og for kommunikasjon mellom virksomheter både i og utenfor helsesektoren.

"Imidlertid har anskaffelse av PKI-løsninger for alle ansatte vist seg å være svært kostbart. Nye Ahus har valgt enklere løsninger for ansattsertifikater for intern bruk".

Det er korrekt at Helse Øst v/Nye Ahus har inngått en rammeavtale med Buypass som kan benyttes av alle helseforetak og øvrige virksomheter i helsesektoren. Avtalen inneholder alle produkter og tjenester som helsesektoren har vurdert som dekkende for aktuell bruk av virksomhetssertifikater, serversertifikater og personsertifikater. Etter kundens oppfatning er denne løsningen verken kostbar eller "enkel", men gir snarere den nødvendige fleksibilitet for å dekke helsesektorens behov.

Fremtidig behov for eID i offentlig sektor (side 29-31)

Mye av det som fremkommer i dette punkt er riktig og begrunner behov for sikkerhetsløsning på nivå 4, men ordet fremtidig i overskriften blir misvisende. Behovet er der nå, og mange prosjekter/prosesser er allerede iverksatt.

I tillegg bør en del kommenteres/presiseres:

ebXML-rammeverket er ikke kun for bruk med virksomhetssertifikater. Det fremkommer at det er *begrenset* behov for personlig eID, noe som ikke er korrekt. I praksis er det behov for dette i de fleste tilfeller (det er kun apoteker/poliklinikker som så langt kun benytter virksomhetssertifikater).

"Det antas at dette behovet kan oppfylles gjennom den nye rammeavtalen om ansattkort som sykehuset Ahus nylig har inngått".

Buypass bekrefter at rammeavtalen dekker dette behovet.

"Nye Ahus har inngått en felles rammeavtale for PKI for spesialisthelsetjenesten, til bruk både for autentisering og pålogging til systemer, og for signering. Ved slik bruk av PKI er det viktig at det ikke påløper kostnader per transaksjon, og valideringstjenester bør være tilgjengelig lokalt".

Buypass bekrefter at det for helseforetaket IKKE påløper kostnader per transaksjon og validering. Denne type kostnader er flere ganger i høringsdokumentet benyttet som argument for hvorfor det offentlige skal lage egne løsninger og ikke kjøpe fra markedsaktører.

"Helsevesenet bruk av eID for signering og utveksling av sensitiv informasjon, krever en lokal signeringsløsning. En lokal signeringsløsning stiller krav om lokal oppbevaring og tilgang til egen privat nøkkel over et standardisert grensesnitt. I tillegg stilles det krav til tilgang til offentlig nøkkel for den man samhandler med. Det er derfor avgjørende at PKI-leverandøren tilbyr dette for at et samtrafikknavn skal kunne tilby denne funksjonaliteten. Åpne standardiserte grensesnitt må derfor

vektlegges ved valg av leverandør. Disse grensesnittene må omfatte tilgang til privat nøkkel og tilgang til sperreinformasjon og katalog”.

Buypass bekrefter at rammeavtalen med Helse Øst v/Nye Ahus, samt det som er innført/innføres i andre deler av helsesektoren, allerede støtter ovennevnte funksjonalitet uten bruk av samtrafikknav. Eksisterende løsninger i helsesektoren, er etter Buypass sin oppfatning, ikke avhengig av et samtrafikknav.

”Full innføring av PKI/eID i helsevesenet vil omfatte 2-300 000 profesjonelle brukere i spesialisthelsetjenesten og kommunehelsetjenesten”.

Dette er faktisk en svært betydelig andel av volumet/behovet totalt sett i Norge, og sannsynligvis den del av offentlig sektor som i størst grad de nærmeste årene vil være en pådriver for utrulling av eID på nivå 4. Vi kan ikke se at dette i noen grad er hensyntatt i konklusjoner/anbefalinger vedr. nivå 4 (utstedelse og bruk). Et par eksempler:

- Skal en fastlege eller en lege på et helseforetak (eller andre innenfor helsesektoren) gå til politikammeret for å anskaffe seg et personlig sertifikat som vedkommende skal benytte i sin profesjon?
- Skal helsepersonell ha et kort for intern bruk (pålogging, VPN, e-post etc) og et annet kort for signering?

Fremdrift på etablering av elektroniske tjenester (NAV) (side 31)

”Etaten har, gjennom pensjonsprosjektet forpliktende planer overfor bl.a. Arbeids- og inkluderingsdepartementet og Finansdepartementet, konkretisert og tidsfestet når elektroniske tjenester knyttet til både gammelt og nytt regelverk vil være etablert. Selv om konkretiseringen av nye tjenester foreløpig ikke er uttømmende, foreligger det nå forpliktende planer om når de forskjellige typer tjenester må være ferdigstilt for test mot våre tjenester:

- *Fra 1.5.07 er løsninger som krever autentisering med nivå 3 klare*
- *Fra 2.kvartal 2008 er løsninger som krever autentisering/signering med sikkerhetsløsning på nivå 4 i rammeverket klare”.*

I gjennomføringsplan fremgår det at offentlig utstedelse av eID på nivå 4 tidligst er klart for utstedelse i 2009. Vi anbefaler at konsekvenser for pensjonsprosjektet utredes.

Forsyning av innbyggere med eID på sikkerhetsnivå 4 (side 37-38)

”Det er samtidig nødvendig å fastslå at det ikke er særlig mange e-tjenester etablert i offentlig sektor som per dags dato har behov for en eID på nivå 4. Statens lånekasse for utdanning har en tjeneste som krever eID/ e-signatur på dette nivå. Denne tjenesten innebærer signering av gjeldsbrev elektronisk. Lånekassen løser imidlertid dette i dag ved å benytte de eID’er som tilbys i Altinn. Utbredelsen av den aktuelle eID er imidlertid begrenset, hovedsaklig pga kostnader som påføres brukere ved anskaffelsen”.

Brukerkostnad for Buypass Smartkort er i dag lavere enn det som er foreslått som brukerfinansiert (NOK 340) i høringsdokumentet.

”Videre er identifiserte behov i NAV-etaten noen av hoveddrivere bak ønsket om å sikre forsyning av eID på dette sikkerhetsnivå til bredere lag av befolkningen, gjerne til nærmere definerte målgrupper. For å fremme utvikling av pasienttjenester fra helsevesenet, vil det være viktig å få en felles løsning for distribusjon av eID på sikkerhetsnivå 4. eID på sikkerhetsnivå 3 er ikke aktuelt for tjenester som inneholder pasientinformasjon”.

I samarbeid med ulike aktører i helsesektoren, samt leverandører til helsesektoren, utsteder Buypass eID på nivå 4 til definerte målgrupper i helsesektoren. For elektronisk kommunikasjon mellom virksomheter og profesjonsgrupper i helsesektoren er det allerede etablert løsninger (utstedelse og bruk). Buypass og andre markedsaktører forsyner eID på nivå 4 til et bredere lag av befolkningen.

Felles avtale og markedsbasert distribusjon (side 39)

"I denne modellen vil innbyggere kunne ha muligheten til å benytte den/de eID som de anskaffet seg i samband med private tjenester til offentlige formål. Det vil imidlertid være en utfordring at det kan påløpe brukskostnader for sluttbruker dersom eID skal benyttes mot private tjenester, mens det ikke vil være tilfellet i bruk mot offentlige tjenester".

Private brukersteder som pr. i dag benytter eID på nivå 4 belaster ikke sluttbruker for denne type tjenester. Buypass kan ikke se at en offentlig utstedelse av eID på nivå 4 vil kunne påvirke hvorvidt private aktører priser tjenester ovenfor sine kunder/sluttbrukere. Se også siste setning i høringsdokumentets punkt 4.3.3 på side 40.

Valg av modell for forsyning av eID på sikkerhetsnivå 4 (side 41-43)

"Usikkerheten i enkelte aktørers estimater når det gjelder dekningsgraden av godkjente eID-løsninger på nivå 4".

Buypass og andre markedsaktører er tydelige på hva som er utstedt, samt hvilke konkrete planer som foreligger.

"Usikkerheten om fremdriftsplaner for aktører med større utbredelse av eID på nivå 4 hva gjelder deklarasjoner om at felles offentlige krav til eID er oppfylt".

Markedsaktørene har kommunisert tydelig når selvdeklarasjon er på plass. Buypass er allerede selvdeklareret.

"Kostnader ved bruk som vil belastes offentlige brukersteder og offentlig sektors muligheter til å estimere disse i en tidlig fase av bruk (de første 2 årene)".

Buypass kan tilby ulike prismodeller tilpasset offentlige virksomheters behov for forutsigbarhet.

"Ingen utbredelse i dag, krever tilrettelegging av incentiver for rask spredning til aktuelle målgrupper".

Markedsaktørene har utstedt ca. 1 million eID på nivå 4 i Norge pr. i dag. Tiltak mot definerte/viktige målgrupper bør gjøres uavhengig av modell.

Anbefaling – forsyning av innbyggere med eID – nivå 4 (side 44)

"Ettersom markedet knyttet til denne type eID og tilhørende infrastruktur er begrenset og kan karakteriseres som ustabil, er gruppen kommet til at det er formålstjenlig å utnytte muligheten for etablering av et nasjonalt ID-kort til distribusjon av statlig utstedt og kontrollerbar eID".

Det er flere norske markedsaktører som tilbyr eID og tilhørende tjenester på nivå 4. Det er ca. 1 million eID på nivå 4 utstedt til norske borgere pr. i dag. Private og offentlige tjenestetilbydere tilbyr i stadig større grad tjenester med bruk av de nevnte eID på nivå 4.

Forsyning av virksomheter med eID (side 46-50)

"eForvaltningsforskriften til forvaltningsloven anbefaler bruk av virksomhetssertifikat i forbindelse med elektronisk utsendelse av vedtak fra offentlige virksomheter. Nye forskrifter som åpner for elektronisk behandling av offentlige innkjøp forventes å gjelde fra 1. januar 2007. En mulig teknisk infrastruktur for dette vil være basert på virksomhetssertifikater".

Det gjelder fra 1. januar 2007, og det er etablert løsninger med bruk av personsertifikater på nivå 4 (Mercell). Roller/rettigheter er løst med tilknytning mellom person og foretak i bakenforliggende systemer.

"Med utgangspunkt i erfaringer som enkelte etater har høstet, er det imidlertid et svært sentralt krav at det ikke påløper transaksjonskostnader ved bruk av virksomhetssertifikater. Det kan i denne sammenheng stilles spørsmål ved om markedsandelen til offentlig sektors anskaffelser av virksomhetssertifikater vil være tilstrekkelig stor for en rammeavtale i de nærmeste årene, dersom denne skal gi en rimelig avkastning for aktuelle markedsaktører".

Det påløper ingen kostnader fra Buypass ved bruk av virksomhetssertifikater. Buypass ser utstedelse av virksomhetssertifikater som et interessant forretningsområde sammen med andre eID produkter og tjenester.

"Ordningen skal være et tilbud for utstedelse av sertifikater til bruk i privat sektor, i tillegg til tilbudene fra private aktører. For offentlige virksomheter anbefaler gruppen at det er pålagt å benytte ordningen, dersom de skal anskaffe eID for virksomheten, av hensyn til lønnsomhet og kvalitet".

Påstand om bedre lønnsomhet og kvalitet ved kjøp av virksomhetssertifikater fra en statlig monopoltilbyder bør begrunnes/tallfestes.

"Kravet om at offentlige virksomheter skal velge virksomhetssertifikat fra Brønnøysundregistrene innebærer at tjenesten monopoliseres overfor offentlige kjøpere. Overfor de private virksomhetene vil Brønnøysundregistrene tilby sitt sertifikat i konkurranse med private tilbydere i markedet. Dette vil gi en viss fordel for Brønnøysundregistrene. Ut fra at det offentlige ikke representerer noen stor og viktig del av sertifikatmarkedet (drøyt 5000 offentlige virksomheter mot ca 800.000 juridiske enheter innen privat sektor), anses det ikke å være noe stor problem i forhold til konkurransehensyn. Under forutsetning av at man på den annen side ikke tar noe høyere pris av de offentlige virksomhetene enn de private, vil en slik løsning heller ikke vanskeliggjøre en organisering av virksomheten i forhold til statsstøtte.

Eksempelvis har NAV implementert virksomhetssertifikat i etaten ved bruk av kun ett sertifikat for hele virksomheten (som omfatter ca 500 "lokale" enheter)".

Her fremstilles offentlig sektor som en liten innkjøper av virksomhetssertifikater. Dette er ikke et korrekt bilde av følgende årsaker:

- Prosjekter i offentlig sektor har allerede resultert i leveranse av flere tusen virksomhetssertifikater. Markedsaktørene har derfor hatt stor fokus på å tilrettelegge systemer og løsninger, samt tilfredsstille alle krav som offentlig sektor har på området.

- Prosjekter i offentlig sektor setter ofte standarden for alle aktører som kommuniserer elektronisk med det angjeldende prosjektet. Eksempelvis har det ene sertifikatet hos NAV resultert i leveranse av ca. 1.500 virksomhetssertifikater til andre virksomheter (poliklinikker, apoteker, primærleger etc).

I tillegg er det verdt å bemerke at programvare fra flere store internasjonale programvareleverandører (Cisco, CheckPoint m.fl.) krever at virksomhetssertifikat og personsertifikat, som benyttes for sikker kommunikasjon mellom virksomhet og person, kommer fra en og samme CA.

"Et minimumsalternativ er å overlate anskaffelsen til hver enkel offentlig virksomhet som har behov for dette, med utgangspunkt i krav stilt i Kravspesifikasjon for PKI i offentlig sektor, som bl.a. innebærer at informasjon fra Enhetsregisteret skal benyttes ved utstedelsen av sertifikatene".

Hvorfor skal dette betegnes som et minimumsalternativ? Det er slik det er etablert i dag, og så langt vi erfarer fungerer dette godt for de offentlige virksomheter som kjøper og benytter virksomhetssertifikater. Det er allerede et krav i Kravspesifikasjon for PKI i offentlig sektor at utsteder av virksomhetssertifikater må validere virksomhetsinformasjon mot Enhetsregisteret.

"Som forvalter av Enhetsregisteret er Brønnøysundregistrene i en unik posisjon når det gjelder å borge for identiteten av norske virksomheter. Brønnøysundregistrene har allerede i dag en funksjon som en attestant for dette, gjennom utstedelse av firmaattest. Det er derfor nærliggende å tenke utvidelse av denne rollen til også å kunne sertifisere elektronisk identitet for virksomhetene".

Det er en pågående prosess mellom etablerte utstedere av virksomhetssertifikater og Brønnøysundregistrene for å bedre den elektronisk tilgjengeligheten til informasjon fra Enhetsregisteret ifm utstedelse av virksomhetssertifikater. Det er derfor nærliggende å fokusere på å forbedre eksisterende tjenester fremfor å etablere nye tjenester.

"Statlig ansvar for en slik rolle innebærer også at staten vil ha sterkere styringsmuligheter når det gjelder hvilke forretningsmodeller og betalingsstrukturer som skal legges til grunn ved anskaffelse og bruk av virksomhetssertifikater, spesielt når det gjelder offentlige virksomheter. Prising mot ev. private kunder vil måtte ta alminnelige hensyn til konkurransen i markedet og basere seg minimum på medgåtte kostnader til drift av tjenesten".

De eksisterende forretningsmodeller og betalingsstrukturer er helt i tråd med de krav og ønsker som offentlige virksomheter har etterspurt. Buypass ønsker gjerne tilbakemeldinger på hva som eventuelt ønskes endret ift dagens løsninger. Pris på virksomhetssertifikater er pr. i dag på et lavere nivå enn de estimerte kostnader til drift av en statlig utstedervirksomhet fordelt på estimert antall sertifikater utstedt fra denne.

"Delvis er dette forslaget begrunnet i at utstedelse kun til offentlige virksomheter vil omfatte så få virksomheter at nytten ikke oppveier kostnadene. Samtidig er det et sentralt poeng ved ordningen at den også skal brukes mellom næringslivet og offentlig sektor. Dersom alle virksomheter får sertifikater vil elektronisk kommunikasjon (dokumenthåndtering) kunne få et betydelig omfang og gi gevinster både hos private og offentlige virksomheter".

Buypass ønsker fortsatt å være leverandør av virksomhetssertifikater til offentlig virksomheter. Med effektive systemer og rutiner for slik utstedelse vil det fortsatt være et interessant forretningsområde. Vi tar til etterretning at arbeidsgruppen mener at nytteeffekt ved etablering av statlig utsteder ikke oppveier kostnadene. Effektiviseringsgevinster ved bruk av elektronisk kommunikasjon mellom virksomheter (offentlige og private) er de samme helt uavhengig av hvem som utsteder virksomhetssertifikatene.

Samtrafikknnav for bruk av eID og e-signatur i offentlig sektor (side 51-56)

I høringsdokumentet er det foreslått at det etableres et offentlig samtrafikknnav som forvaltes av Brønnøysundregistrene. Navet skal tilby følgende funksjonalitet i første versjon:

- *Autentisering med statlig utstedt eID på sikkerhetsnivå 3 og 4, som også vil omfatte validering av sertifikater for sikkerhetsnivå 4 og fødselsnummeroppslag.*
- *Signering av webskjema og lokalt (grensesnitt for integrasjon i fagsystemer), med bruk av felles løsninger.*
- *Digitalt arkiv for signerte dokumenter/dokument-hash.*
- *Videreformidling av ferdig validert eID (felles pålogging), som en generell funksjonalitet.*

"Hvorvidt bruk av samtrafikknnavet skal være pålagt eller valgfritt bør vurderes nærmere, herunder ev. hvilke tjenester som det ev. skal pålegges bruk av".

I forhold til eksisterende og planlagte løsninger i offentlige virksomheter bør følgende hensyntas og/eller konsekvensutredes:

- Kryptering tilbys ikke i første versjon
- Bruk av virksomhetssertifikater tilbys ikke i første versjon
- Integrasjon i fagsystemer (ift signering og kryptering) er ikke beskrevet
- Responstider og skaleringssevne for store transaksjonsvolumer vil påvirkes ved bruk av et ekstra systemledd. Eksempelvis er det slik at de fleste meldinger/transaksjoner i helsesektoren går direkte fra avgiver (apotek, pirmærleger etc) til mottager (NAV, eResept etc)

Pålagt bruk eller valgfrihet for offentlige virksomheters bruk av et eventuelt samtrafikknnav bør ses i lys av de ovennevnte kommentarer.

Forretningsmodeller for offentlig eID – premisser og forutsetninger (side 57-61)

I høringsdokumentet behandles 5 prinsipper. Under har vi kommentert noen av disse.

Gratis bruk for innbyggere og næringsliv.

Det er allerede slik at bruk av eID mot offentlige tjenester er kostnadsfritt for innbyggere og næringsliv (selv om det er kostnader for noen ifm anskaffelse/etablering).

Arbeidsgruppen hevder at kostnader ved anskaffelse av eID må prises lavt. Dette er senere i høringsdokumentet tallfestet til NOK 340 (personlig eID nivå 4). Markedsaktørenes eksisterende priser på tilsvarende er lavere. I høringsdokumentets punkt 1.2 hevder arbeidsgruppen at markedsaktørers høye priser er årsak til manglende utbredelse, og dermed et argument for statlig utstedelse.

Konsistens i forhold til (gjen)bruk i offentlig sektor.

"Det skal ikke utvikles egne etatsspesifikke løsninger i offentlig regi for eID for elektronisk kommunikasjon med offentlig sektor. De etablerte etatsspesifikke eID-løsninger skal etter en

overgangsperiode (med parallelle løsninger) fases ut, avhengig av andel distribuerte eID-er relatert til det nivået av utbredelse og dekningsgrad av målgruppen som tjenesten krever. Allerede etablerte e-tjenester hos etaten vil med andre ord i en "mellomfase" eksistere parallelt med fellesløsninger for eID".

Buypass anbefaler at dette punkt konkretiseres ytterligere mht tidspunkter og konsekvenser/kostnader. Offentlige virksomheter som har og/eller er i ferd med å implementere løsninger vil bli berørt. Dette gjelder spesielt for helsesektoren med flere løsninger på dette området (NAV, eResept, Helseforetak m.fl.).

"Mandatet fremhever at forretningsmodell må sikre spredning og bred bruk, prinsippet om konsistens og tilgjengelighet relaterer seg særlig til spørsmålet om bred bruk".

Dagens løsninger fra markedsaktørene på anskaffelse og bruk av eID på nivå 4 sikrer bred bruk gjennom kombinasjon av private og offentlige bruksområder. I høringsdokumentets punkt 7.1 (siste avsnitt) er det konkludert med at offentlige utstedte eID'er i første fase kun skal benyttes mot offentlige tjenester, ikke mot private brukersteder. Dette av hensyn til lovverk ift statsstøtte.

Videre er det verdt å merke seg følgende avsnitt i punkt 4.1 i høringsdokumentet:

*"Statistiske undersøkelser i andre land indikerer at antallet offentlige elektroniske tjenester som innbygger vil komme i kontakt med gjennom et år er forholdsvis lavt. Dette taler sterkt for at det i nye strategier **ikke sperres** for muligheten for slik flerbruk av eID, inkludert bruk av eID mot private tjenester, samtidig som det foreligger et valg å kunne skaffe seg flere forskjellige eID til ulike formål."*

Vi ser ikke sammenheng mellom ovennevnte og arbeidsgruppens anbefalinger.

"Bruker kan benytte de eID typene som er definert på alle offentlige tjenester avhengig av nivå. Dette medfører at bruker ikke fritt kan velge eID løsning i markedet, men den/de eID som blir besluttet (jfr kap 4), kan til gjengjeld brukes mot alle offentlige tjenester".

Konklusjonen/anbefalingen fra arbeidsgruppen er bruk av statlig utstedt eID for personer og virksomheter. Vi tolker dette dithen at en eID utstedt fra en markedsaktør ikke kan benyttes i og/eller mot offentlige tjenester.

"De eID-leverandører som vil være koblet til samtrafikknivet er de som blir besluttet for elektronisk kommunikasjon med offentlig sektor".

Konklusjonen/anbefalingen fra arbeidsgruppen er kun å tillate bruk av statlig utstedt eID for personer og virksomheter. Vi tolker dette dithen at samtrafikknivet ikke vil støtte bruk av eID utstedt fra markedsaktører.

"Samtrafikknivet er et viktig virkemiddel for å sikre konsistens overfor sluttbruker, samt et effektiv teknisk bidrag for å integrere felles eID-løsninger hos brukerstedene. Integrering mot sikkerhetsnavet er i utgangspunktet valgfritt for brukersted, men ut fra samfunnsøkonomiske vurderinger og hensiktsmessighet anses det som en viktig forutsetning at flest mulig integrerer seg mot denne felles løsningen og ikke utvikler egne samtrafikkløsninger".

I høringsdokumentet er det flere steder antydnet at samtrafikknivet ikke er valgfritt, mens det i ovennevnte avsnitt er valgfritt for offentlig virksomhet. Vi anbefaler en presisering og tydeliggjøring av hva som er arbeidsgruppens anbefaling.

Økonomisk forutsigbarhet

Begrepet økonomisk forutsigbarhet benyttes både i høringsdokumentet og i mandatet til arbeidsgruppen. Arbeidsgruppen har videre brukt begrepet som et argument for valg av forretningsmodell. Etter vår oppfatning bør dette begrepet forklares og presiseres. Så langt vi har forstått av høringsdokumentet er begrepet kun relatert til kostnader og det er ikke hensyntatt korresponderende besparelser (effektiviseringsgevinster, kostnadsreduksjon pr. transaksjon etc). Det hevdes at fast pris pr. transaksjon, der hvor antall transaksjoner ikke er kjent på forhånd, gir økonomisk uforutsigbarhet. I slike tilfeller, der hvor besparelsene kan tallfestes (hvilket er gjort i de fleste offentlige prosjekter), vil de etablerte forretningsmodellene mellom offentlige virksomheter og markedsaktører ha nødvendig økonomisk forutsigbarhet. Der hvor besparelse er større en kostnad vil positiv nettoeffekt for den offentlige virksomhet øke i takt med transaksjonsvolum.

Økonomiske og administrative konsekvenser (side 65-73)

"I tillegg til å oppnå forenklingsgevinster for innbyggere (fordi forsyning av felles eID vil føre til at brukere ikke må forholde seg til flere ulike eID løsninger fra offentlige virksomheter), vil etablering av felles eID for innbyggere (henholdsvis på nivå 3 og 4) og virksomheter medføre besparelser for alle de offentlige virksomhetene som i dag foretar egne forsyninger av eID løsninger (f.eks NAV, SKD, Lånekassen, Altinn samt enkelte kommuner), ettersom disse løsningene kan fases ut".

Samme resultat kan oppnås tidligere ved bruk av de allerede etablerte løsninger fra markedsaktørene.

"Det er i dag utviklet enkelte løsninger som gjør bruk av eID på nivå 4, eksempelvis Lånekassen og NAV/helse (jfr kap 3.3). Disse løsningene fungerer teknisk sett bra, men tjenestene sliter med "underforbruk" fordi utbredelsen av godkjent eID blant aktuelle målgrupper (studenter og leger) er for liten. Dette vil kunne avhjelpes ved en offentlig distribuert eID".

Markedsaktørene har utstedt ca. 1 million eID på nivå 4 i Norge pr. i dag. Et viktig tiltak for å sikre bruk vil derfor være å åpne for at alle eID på nivå 4 som er utstedt fra markedsaktørene kan benyttes mot aktuelle offentlige tjenester. Svært mange legekontorer har anskaffet sertifikater, tilknytning til NHN og nødvendig signeringsfunksjonalitet i sitt EPJ-system.

"Felles strategi for forsyning av eID vil gi gevinster i form av økt bruk av eksisterende elektroniske tjenester og derved økt potensial for å hente ut gevinster av investeringer i disse tjenestene. I tillegg vil man ved felles forsyning av eID gi incentiver for utvikling av nye tjenester, som vil sikre merbruk/gjenbruk av eID".

Arbeidsgruppen har anbefalt en frivillig utrulling av eID til personer og virksomheter (brukere av offentlige tjenester). Dette er tilsvarende modell som for anskaffelse og bruk av sertifikater utstedt fra etablerte markedsaktører. Eventuelle gevinster vil kunne oppnås tidligere ved fortsatt bruk av markedsaktørenes løsninger.

"NAV arbeider med å sikre at en størst mulig andel benytter de elektroniske tjenester som tilbys. Dette er en forutsetning for organisering av de framtidige pensjonsoppgavene i etaten. Dersom det ikke etableres sentrale felles løsninger som dekker behovet, må etaten gjennom pensjonsprosjektet vurdere utvikling av alternative og/eller supplerende løsninger i samforståelse med de departementer som følger opp arbeidet med realiseringen av reformen. Behovet retter seg først og fremst mot forsyning av eID på sikkerhetsnivå 4 til innbyggerne".

Arbeidsgruppens foreslåtte tidsplan og modell for forsyning av statlig utstedt personlig eID på nivå 4 tilsier ikke at NAV sitt behov dekkes gjennom arbeidsgruppens forslag. Dette begrunnes med:

- Frivillig ordning for innbyggernes anskaffelse
- Pris på NOK 340 for smartkort med eID på nivå 4
- Uavklarte modeller for distribusjon, priser etc på smartkortlesere
- Ikke omtalt utvikling og distribusjon av klientprogramvare (inkl. priser etc)
- Usikkerhet på volum og tidspunkter (det anslås av FAD og Justisdep. et volum på ca. 150.000 pr. år, med start tidligst 2009).

Konsekvenser av forsyningsstrategi – virksomhets-eID (side 69-70)

"I kommunesektoren etterspørres det muligheter for å sikre den elektroniske kommunikasjonen mellom enhetene enklere og rimeligere enn ved hjelp av VPN (Virtual Private Network) tilknytning. Dette viser at det er et behov for virksomhetssertifikater også på bedriftsnivået".

Dette gjelder også tilsvarende for alle offentlige virksomheter i tillegg til kommunesektoren. Programvare for VPN fra flere store internasjonale programvareleverandører (Cisco, CheckPoint m.fl.) krever at virksomhetssertifikat og personsertifikat, som benyttes for sikker kommunikasjon mellom virksomhet og person, kommer fra en og samme CA. En konsekvens av dette vil være at offentlige virksomheter også må kjøpe personsertifikater fra den statlige utsteder av virksomhetssertifikater. Så langt vi kan se av høringsdokumentet er ikke dette vurdert.

Mandat for strategiarbeidet (side 21 og 88-89)

I mandatet til arbeidsgruppen for strategiarbeidet, punkt b, fremkommer det at arbeidsgruppen skal utrede gjenbruk av eksisterende autentiserings- og signeringsløsninger fremskaffet i statlig regi (f.eks. skattePIN som skal benyttes i forbindelse med MinSide, Altinns løsninger og e-signaturløsninger som benyttes av helsesektoren og NAV.).

Vi kan ikke se at gjenbruk av løsninger/avtaler mellom Buypass og Helse Øst v/Nye Ahus, Buypass og EPJ-leverandører, samt Buypass og andre aktører i helsesektoren er utredet og/eller vurdert i høringsdokumentet.

I arbeidsgruppens fortolkning av mandatet er interne behov for elektronisk kommunikasjon i offentlig sektor ikke vurdert. Dette er etter vår oppfatning blant de viktigste områder å effektivisere, noe eksempelvis helsesektoren har startet et omfattende arbeid på. Dette bør ikke ses adskilt fra de øvrige områder, da løsningene i mange tilfeller må ses i sammenheng for å oppnå målsetninger om effektiv elektronisk ende-til-ende-kommunikasjon. eResept-prosjektet er etter vår oppfatning et godt eksempel på dette.

Justisdepartementets høring om nasjonalt ID-kort

Vi henviser til vårt høringsvar til Justisdepartementet, men tar med et punkt som kan ha juridisk betydning ift anbefalinger fra FAD sin arbeidsgruppe. Følgende avsnitt er tatt fra punkt 13.4 i Justisdepartementets høringsdokument:

"Til forskjell fra utstedelse av et offentlig og allment tilgjengelig identitetsdokument med eller uten EU/Schengen reisefunksjonalitet, vil en utstedelse av eID skje i konkurranse med private aktører. En ordning med offentlig utstedt eID vil derfor måtte gjennomføres i tråd med konkurranselovgivningens prinsipper. En offentlig utstedelse av eID for bruk mot offentlige tjenester som for øvrig er åpne for konkurrerende private løsninger, antas ikke å være i strid med disse prinsippene. En offentlig subsidiering av ordningen for å øke utbredelsen, vil imidlertid raskt kunne være i strid med de nevnte prinsipper."

Vi tolker dette dithen at det kan reises juridiske spørsmål knyttet til hvorvidt offentlige tjenester kun skal/kan være tilgjengelig med bruk av en offentlig utstedt eID.