

**DET KONGELIGE FORNYINGS-,
ADMINISTRASJONS- OG KIRKEDEPARTEMENT**

Nærings- og handelsdepartementet
Postboks 8014 Dep
0030 OSLO

Deres ref.
201203327-1/LHW

Vår ref.
12/2748 AKH

Dato
06.12.2012

Europakommisjonens forslag til forordning om eID og e-signatur m.m.

Vi viser til Nærings- og handelsdepartementets brev av 13. september og 25. oktober 2012 om ovennevnte høring.

Fornyings-, administrasjons- og kirke departementet (FAD) har fulgt arbeidet med forordningen siden forslaget ble offentliggjort i juni. Vår overordnede oppfatning er at forslaget er positivt og peker i riktig retning, men at flere praktiske avklaringer av stor betydning gjenstår. Slik vi forstår det, vil norske tillitstjenester kunne brukes som notifiserte tjenester, under visse vesentlige forutsetninger. Vi vil gå gjennom følgende områder:

- Sikkerhetsnivåer
- Markedspåvirkning
- Juridisk ansvar for tjenestene
- Praktisk tilrettelegging for utenlandske tjenester
- Kontroll av tillitstjenester
- Juridisk status for signatur
- Virksomhetssertifikat / eSeals
- Dokumentutveksling
- Personvern
- Delegerte rettsakter
- Oppsummering, anbefaling

Interesse og status for Norge

Norge vil, slik vi bedømmer det, ha stor nytte av å delta i samarbeid om digitale tillitstjenester. Dette vil legge grunnlaget for tverrnasjonal tjenesteproduksjon, og vi har allerede et godt utgangspunkt som vi bør bygge videre på.

Postadresse
Postboks 8004 Dep
N-0030 OSLO
postmottak@fad.dep.no

Kontoradresse
Akersg. 59

Telefon
22 24 90 90
Org. nr.
972 417 785

Administrasjonsavdelingen
Telefaks
22 24 27 14

Saksbehandler
Anne Kristine Hage
22 24 48 51
akh@fad.dep.no

Forordningen omtaler ikke assosierte stater, bare tredjeland, dvs. at dette vil bli Norges status i samarbeidet. Dette er prinsipielt problematisk. På den annen side framholder artikkel 10 i den grad åpning for normal deltakelse for tredjeland, at det i praksis ikke framstår som problematisk. Det vil likevel være viktig fortsatt å sørge for at Norge deltar i de fora der beslutninger om framtidige ordninger blir framforhandlet.

Oppgaveløsning

De nye oppgavene som oppstår gjennom forordningen er primært godkjenning/kontroll og praktisk implementering. Vi tror i utgangspunktet det er naturlig at Post- og teletilsynet fortsetter sin rolle, tilpasset det nye regelverket. Vi tror videre i utgangspunktet det er naturlig at ID-porten (Difi) har ansvaret for praktisk implementering. Altinn ville vært et alternativ, ettersom Altinn er Point of Single Contact, men det er behov for autentiseringstjenestene også utenfor Altinn.

Det er tidlig å vurdere økonomiske og administrative konsekvenser for Difi. Vi vil her vise til Difis høringsuttalelse. I utgangspunktet tror vi ikke ressursbruken i Difi vil øke dramatisk, men dette avhenger både av god, praktisk tilrettelegging på europeisk nivå, og visse avklaringer rundt tekniske løsninger.

Sikkerhetsnivåer

All form for teknisk spesifisering er i kommisjonens forslag henvisning til delegerte- eller gjennomføringsrettsakter. Dette framstår i utgangspunktet hensiktsmessig, ettersom teknologisk utvikling vil kunne medføre behov for raske tilpasninger. Samtidig gjør fraværet av teknisk spesifisering at det er vanskelig å planlegge konkret eller forutse praktiske konsekvenser. Det er uklart om de to sikkerhetsnivåene i ID-porten vil kunne benyttes.

Av praktisk hensyn bør det etableres sikkerhetsnivåer i rettsaktene. Disse bør ikke være teknisk spesifikke, ettersom ulike løsninger kan fungere like godt, men være koblet til en felles, faglig vurdering av sikkerhetsnivået. Dette vil gjøre det enklere å vurdere hvilke offentlige tjenester en gitt autentiseringsløsning kan benyttes mot.

Andre praktiske utfordringer vil også kreve avklaring i den videre prosessen: (1) ID-porten benytter personnummer/D-nummer som identifikator. Dette er ikke nødvendigvis tilfelle for utenlandske tjenester, og vil kreve tilrettelegging. (2) Forutsatt at ID-porten blir norsk knutepunkt mot utenlandske notifikasjonstjenester, vil implementeringen avhenge av koordinerte fellestjenester på europeisk nivå. Hvis ikke vil antall integrasjoner bli uhåndterbart.

Markedspåvirkning

Vi har drøftet i hvilken grad forordningen vil støte på statsstøtteproblematikk. Uansett er det et åpent spørsmål hvordan markedsaktørene vil bli påvirket av forordningen. Dette må undersøkes nærmere.

I tilfellene der ID er et rent nasjonalt anliggende, utviklet eller anskaffet for bruk på egne tjenester, vil ikke markedet påvirkes nevneverdig. Innkjøperen (staten) er både den som velger og som betaler. Noen kostnader ved egne innbygges bruk av tjenestene i utlandet vil neppe framstå urettferdig.

Dersom markedet for autentiserings- og andre tillitstjenester blir mer internasjonalt, kan det oppstå nye situasjoner. Sett at en av de store nettaktørene (Amazon, Google, Facebook osv.) utvikler autentiseringsløsninger som tilfredsstillende sikkerhetskravene, og at ett land velger å benytte og notifisere denne tjenesten. Da vil formodentlig også mange, f.eks. norske innbyggere antakelig velge å bruke denne innloggingsløsningen framfor de tjenestene ID-porten har egen avtale med. Hvordan dette vil slå ut, er vanskelig å vurdere, men det virker åpenbart at dette kan ha konsekvenser både for ønsket om å notifisere og for markedsforholdene for tillitstjenesteleverandørene. Det vil også kunne oppstå spørsmål knyttet til statsstøtte i en slik situasjon, men det er vanskelig å overskue uten at vi har et klart bilde av hvordan finansieringsstrømmene vil arte seg.

Juridisk ansvar

Forordningen sier at tjenestene må være utstedt av, eller på vegne av nasjonale myndigheter. Teksten kan tolkes slik at de private løsningene i ID-porten derfor ikke omfattes. Dette spørsmålet må avklares, samtidig som det må vurderes om staten eventuelt kan eller bør overta tjenestene gjennom avtale om dette. For øvrig bør det påpekes at forordningen knytter et ubegrenset erstatningsansvar til feil i tjenestene, og at dette punktet under enhver omstendighet krever en særskilt vurdering sett i sammenheng med hvilket ansvar staten bør påta seg.

Signatur

Sikkerhetsnivå for elektronisk signatur er relativt åpent i forordningen: Man skal akseptere signaturer på samme sikkerhetsnivå som man selv aksepterer. I følge norsk rett er en avtale i utgangspunktet bindende, uavhengig av hvordan avtalen er inngått, eller formen på signaturen eller avtalen. I tillegg er det i følge norsk rett også fri bevisførsel. Det innebærer fri bevisførsel i en eventuell rettssak. Dette er ulikt rettstilstanden i mange av våre europeiske naboland, der formkrav til avtaler i større grad er avgjørende for om avtalen er gyldig. Det er viktig at man i det kommende arbeidet med regulatorisk implementering ikke svekker signaturens rettslige status i norsk sammenheng, ved å tilpasse seg europeiske formkrav rundt signatur.

eSeals, tilsvarende virksomhets sertifikat

Reguleringen av såkalte eSeals, som er autentisering for juridiske personer, er et skritt i riktig retning. Samtidig må teksten leses i lys av at mange land har lover som tilsier at en avtale ikke er gyldig uten et segl. Dette betyr at behovet ikke er tilsvarende stort i Norge. Dette er likevel ikke å anse som et problem.

Dokumentutveksling

Reguleringen av dokumentutveksling framstår noe umoden, og muligens uheldig. Per i dag er det en uoversiktlig flora av samhandlingsarenaer for standardisering av dokumentutveksling. Norge har vært tett involvert i PEPPOL, og har vært tidlig ute med å etablere en infrastruktur basert på adresseregister og standardisering av sending gjennom slik infrastruktur, en tilnærming som åpner for en fleksibel og konkurransefremmende utbygging. Definisjonen av dokumentutveksling i artikkel 3(28) er snever i så måte. Hovedutfordringen er at det beskrives som én tjeneste, i entall, der vi mener at det like godt kan være en infrastruktur med mange tjenesteleverandører som opererer med koordinerte standarder og protokoller. Alt i alt er vi usikre på om det er klokt å regulere dokumentutveksling med den grad av umodenhet vi observerer.

Personvern

Fra et personvernperspektiv er de foreslåtte reglene gjennomgående positive. Tillit og sikkerhet er begge viktige hensyn for ivaretagelse av personvern, og disse er sentrale også i EU-kommisjonens forslag til forordning om eID og e-signatur m.m. FAD er positiv til en videreføring av reglene om behandling av personopplysninger som foreslått i artikkel 11, og særlig videreføringen av regelen om at medlemsstatene ikke skal kunne forhindre bruken av pseudonymer i stedet for navn ved digitale tillitstjenester.

Det er positivt at det søkes å innføre mer detaljerte felleseuropeiske regler på området for digitale tillitstjenester, ettersom nettbaserte tjenester i stadig større grad krysser landegrensene. Det at erstatningsansvaret og tilbydernes plikter er skjerpet, er også positivt. Disse endringene kan bidra til at innbyggerne får større tillit til både offentlige myndigheter og private næringsdrivende over landegrensene, og forhåpentligvis slik gi større elektronisk samhandling. Dette er en viktig del av regjeringens digitale agenda.

Delegerte rettsakter

Europakommisjonen er gjennom forordningen gitt en vid adgang til å fastsette delegerte rettsakter. Dette gjelder særlig definisjoner og tekniske spesifikasjoner. Adgangen til å fastsette delegerte rettsakter kan være nødvendig for en reell samordning mellom landene, som er et av hovedformålene med forordningen. Denne adgangen kan imidlertid få stor betydning for hvilket handlingsrom Norge får ved en eventuell implementering av de nye reglene. Det bør i det videre forordningsarbeidet rettes oppmerksomhet mot de mulige konsekvenser av adgangen til å fastsette delegerte rettsakter. Særlig viktig vil det i denne sammenheng være å sørge for at ikke det sikkerhetsnivået som norske tilbydere av digitale tillitstjenester holder i dag, svekkes.

Oppsummering / anbefaling:

- Økonomiske og administrative konsekvenser*
I utgangspunktet mener vi at de nye oppgavene i forordningen bør legges til hhv. ID-porten og Post- og teletilsynet.

Forordningen vil, forutsatt at praktisk koordinering og grunnleggende felleskomponenter etableres på europeisk nivå, ha begrenset betydning for ID-portens ressursbruk. Det er likevel vanskelig å estimere dette per nå, ettersom disse avklaringene ikke foreligger. Vi antar at økt ressursbruk først og fremst vil finne sted hos Post- og teletilsynet.

2. Særnorske interesser

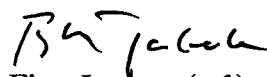
Særnorske interesser rundt forordningen knytter seg slik vi ser det til to forhold: (a) Statusen som tredjeland. Slik vi vurderer det gir artikkel 10 i praksis tilstrekkelig grad av deltakelse. (b) Signatur. Implementeringen av forordningen bør innebære at retten til fri bevisførsel også gjelder elektroniske signaturer i avtalerett. Vi tror ikke det fordrer særlige endringer, så lenge avtalen reguleres av norsk rett, men dette bør kvalitetssikres.

3. Områder som bør følges opp

De øvrige kommentarene er ikke av særnorsk karakter. De må avklares, men det er ikke gitt at Norge bør føre an. I all hovedsak mener vi forordningen er et godt forslag, og vi bør møte den mest mulig konstruktivt.

- (a) Tekniske sikkerhetsnivåer må avklares. Det er akseptabelt at deler av dette er delegert, men for praktisk tilrettelegging er det nødvendig å få signaler. Videre må metodikk for koordinering mellom ulike identifikatorer (eg. personnummer) avklares. Det vil også være svært hensiktsmessig om man på europeisk nivå etablerte ulike sikkerhetsnivå av koordineringshensyn.*
- (b) Markedspåvirkning. Vi må undersøke nærmere (1) om utenlandske autentiseringsløsninger vil kunne benyttes via ID-porten mot private tjenesteeiere, og (2) hvordan bruk av utenlandske tjenester teoretisk vil kunne påvirke markedssituasjonen, og (3) om dette vil relatere til statsstøtteproblematikk.*
- (c) Hvilken type ansvar som må overføres fra private autentiseringsløsninger og liknende til staten, og på hvilken måte. Videre bør Norge støtte et krav om at erstatningsansvar begrenses oppad, ettersom det i teorien kan oppstå svært høye erstatningskrav ved teknisk svikt.*
- (d) Dokumentutveksling, artikkel 3(28) bør utvides til å gjelde ikke bare enkelttjenester som sender dokumenter fra avsender til mottaker, men systemer for samhandling mellom ulike aktører. Hvis ikke dette er akseptabelt, bør dokumentutveksling fjernes fra forordningen.*

Med hilsen


Finn Jensen (e.f.)
avdelingsdirektør


Anne Kristine Hage
rådgiver