Difi
Direktoratet for forvaltning og ikt

Justisdepartementets lovavdeling
Postboks 8005 Dep
0030 OSLO

Vår dato	21.12.2017
Vår referanse	17/00008-60

Deres dato	7.9.2017
Deres referanse	17/4746 EP HEA /MEK/bj

Saksbehandler: Jon Berge Holden

Høringssvar - Revisjon av finansavtaleloven (PSD2 og e-ID)

Vi viser til høringen, og avtale om utsatt høringsfrist.

Høringen gjelder gjennomføring av flere direktiver, blant annet det reviderte betalingstjenestedirektivet (PSD2). Departementet peker i høringen på at direktivet på noen punkter kan være utfordrende for eksisterende e-ID-ordninger. Spesifikt pekes det på at direktivet synes forutsette at passord og kode som benyttes for bruk av BankID vil kunne bli tilgjengelig for betalings- og opplysningsfullmektiger, og at det er noe usikkerhet med hensyn til om BankID kan opprettholde vilkår om at passord og kode ikke skal gjøres kjent for uvedkommende.

Beskrivelsen i høringsnotatet uroer oss. Det mest problematiske punkt synes være ovennevnte krav.

Direktivets mål

Et av hensynene i direktivet er at å sikre at det er attraktivt og enkelt for forbrukerne å ta i bruk fullmektiger. Det er derfor stilt krav om at e-ID-løsninger som benyttes for å disponere bankkonto også skal kunne brukes av fullmektigene.

Vi vil imidlertid understreke at direktivets formål neppe bør trekkes så langt at det skal føre til at dagens e-ID-løsninger ikke lenger skal kunne brukes til andre tjenester enn banktjenester.

EU har like før PSD2 ble vedtatt fastsatt en forordning om tillitstjenester og elektronisk identifikasjon (eIDAS, forordning 910/2014). Begrepsbruk og innhold i PSD2 og eIDAS synes være dårlig koordinert. Et formål med eIDAS er å sørge for gjenbruk av e-ID og tillitstjenester på tvers av sektorer og land. PSD2 begrenser seg til å se på konkurransen på betalingsområdet. Vi anbefaler at PSD2 fortolkes innskrenkende, der reglene kommer i konflikt med sektorovergripende mål.

Bruk av e-ID i Norge - særtrekk

Difi har rollen som samordner og premissgiver for tverrgående utfordringer i digitaliseringen av offentlig sektor. Fellesløsninger som ID-porten er et kraftig virkemiddel i etableringen av

Direktoratet for forvaltning og ikt
22 45 10 00
postmottak@difi.no

Besøksadresse Oslo:
Grev Wedels plass 9
0151 Oslo

Besøksadresse Leikanger:
Skrivarvegen 2
6863 Leikanger

Postboks 8115 Dep, 0032 Oslo
Org.nr: NO 991 825 827
www.difi.no

digitale tjenester og gir god ressursutnyttelse ved at fellesbehov løses for alle med én løsning.

ID-porten står for pålogging til 703 offentlige virksomheter og beskytter 1394 digitale tjenester. Det går ca 120 mill påloggінger gjennom ID-porten i 2017. Den er således en svært viktig fellesløsning og en forutsetning for å oppnå digitalt førstevalg.

For å kunne tilby pålogging på høyeste sikkerhetsnivå gjennom ID-porten benytter Difi e-ID fra markedet. BankID benyttes totalt til 70 %[1] av påloggingene gjennom ID-porten og de aller fleste på høyt sikkerhetsnivå. BankID spiller i dag en avgjørende rolle for digitaliseringen av offentlig sektor.

Norge var tidlig ute med bruk av e-ID både til nettbank og offentlige tjenester på nett. BankID ble lansert i 2004 og utviklingen av det som i dag er ID-porten startet i 2006.

I de fleste andre land i EØS kan e-ID-løsningene bare brukes i det konkrete kundeforholdet for én bank. Direktivet tar sikte på å håndtere risiko for misbruk av e-ID i slike situasjoner – risikoen rammer da aktørene som direktivet direkte regulerer, og direktivet har iverksatt tiltak for å håndtere denne risikoen. For norske forhold blir en slik tilnærming for snever: BankID er en fellesløsning både for alle bankene, men også offentlige og private tjenestesteder. Norge skiller seg således ut med stor bruk av e-ID på tvers både i privat og offentlig sektor.

Norge skiller seg også ut med at man i større grad benytter nettsentriske løsninger (sentrallagrede nøkler, sentrallagret pki) også på høyeste sikkerhetsnivå. BankID er en slik løsning. Det har gitt en helt annen fleksibilitet i brukervennlighet og gjenbruk på tvers, enn løsninger i andre land. BankID kan for eksempel brukes til det aller fleste finanstjenester som å opprette konto, gi tilgang til nettbank og inngå låneavtaler. Fleksibiliteten gir også mange bruksområder i offentlig sektor som tilgang til tjenester på alle sikkerhetsnivåer og mulighet til å automatisere tjenester ved brukervennlig autentisering og digitale signaturer.

Siden Norge er et foregangsland som står temmelig alene om utstrakt bruk av sentrallageret PKI er det trolig at utfordringer PSD2 gir for denne type løsninger er tillagt mindre vekt i arbeidet med direktivet. Smartkortbaserte og app-baserte løsninger, som er utstrakt bruk i andre land, kommer for eksempel utenom direktivets krav om fallback-løsninger. For Norge er det imidlertid ikke tilstrekkelig, jf. at BankID har en sentrallageret løsning.

Sentralt i suksessen i bruken av BankID står brukernes tillit. Difi brukerundersøkelser viser at innbyggeren har svært høy tillit til ID-porten og BankID. Norge er således i en særstilling i forhold til de fleste andre land i EØS, hvor det er en ukjent tanke at en e-ID fra bank også skal tilgang til andre tjenester i samfunnet.

Sikkerhetsutfordringen

I høringsnotatet er det uttalt at «Dersom en kunde med BankID skal benytte seg av en kontofullmaktstjeneste, må kunden oppgi passord og koder til BankID til tilbyderen av slike tjenester, som på den måten får tilgang til å hente opplysninger eller initiere en betaling fra kundens betalingskonto.» (pkt 4.5.2.2, vår utheving)

[1] Tall for hittil i 2017, hhv. 45% på BankID, 25% BankID mobil.

Dersom dette er riktig, vil det innebære et alvorlig brudd på sikkerhetskravene til dagens løsning. Elektroniske identifikasjonsordninger baserer seg på at delte hemmeligheter, som passord og koder, bare er tilgjengelig for kunden og e-ID-utstederen (i eksemplet: BankID). Dersom gjennomføringen av PSD2 innebærer at passord og koder skal kunne oppgis til andre enn e-ID-utstederen vil det svekke tilliten til den aktuelle e-ID-ordningen. Resonnementet er like enkelt, som det er gammelt: «Det ein veit um, er utrygt hjå tvo, det tri veit um, veit alle»[2].

Et krav om deling vil høyst sannsynlig innebære at løsningen verken vil oppfylle krav til høyeste sikkerhetsnivå iht. dagens norske rammeverk, eller EUs nylig definerte sikkerhetsnivåer for e-ID[3]. For e-ID-løsninger som er basert på kvalifiserte sertifikater, som i dag er et krav for høyeste e-ID-sikkerhetsnivå, vil det formodentlig også føre til at kvalifisert-statusen – og muligheten for å bruke e-ID-en til å lage avanserte signaturer – vil opphøre, jf. at deling av hemmelighetene vil føre til at kravet til «enekontroll» over privatnøkkelen ikke lenger er oppfylt.

I høringsnotatet anerkjennes denne utfordringen, men antydes det at utfordringen kan løses ved at det utstedes nye e-ID-er, en «gjestenøkkel» med begrenset funksjon. Omtalen av spørsmålet er knapp, og ikke fyldestgjørende. Vi kan ikke se hvordan dette er mulig å oppnå, dersom *de samme hemmeligheter* skal gi tilgang til både «hovednøkkel» og «gjestenøkkel». Dersom kunden skal utstyres med *ulike passord og koder* for hhv. «hovednøkkel» og «gjestenøkkel» vil det erfaringsmessig innebære store utfordringer, både med å utbre løsningene, få dem tatt i bruk og holdt vedlike – et sannsynlig utfall er at begge løsninger taper både brukere og bruk, og at det største tapet oppstår for den av nøklene som brukes minst.

Ikke teknologinøytral sekundærlovgivning

Sekundærlovgivningen for PSD2, kommisjonens delegerte rettsakt 2017/2055 av 27.11.2017[4], stiller krav til grensesnittet for bruk av e-ID. Det forutsettes her blant annet at tilgang skal skje uten videresending – se artikkel 32. Det er dette kravet som innebærer at hemmelighetene vil komme under fullmektigens kontroll. Direktivet stille rettslige krav til at fullmektigen ikke selv skal misbruke opplysningene (herunder lagre dem, art 66/67 nr 3 e) og til at den skal hindre at andre får tilgang (art 66/67 nr 3 b). Det endrer imidlertid ikke det grunnleggende problem: at tilliten til e-ID-løsningen står og faller på tilliten til at fullmektigene (i prinsippet et ubegrenset antall aktører) klarer å etterleve pliktene.

Det er en bestemmelse som i praksis diskriminerer mellom lokale, pki-baserte løsninger (som gir lokal tilgang via assymetriske nøkler, i praksis smartkort og app-baserte løsninger) og nettsentriske e-ID-løsninger (symmetriske eller assymetriske). Bestemmelsen bryter etter vårt skjønn med kravet til teknologinøytralitet.

---

[2] Håvamål, strofe 63

[33] Se eIDAS-forordningen artikkel 8, jf. gjennomføringsrettsakt 2015/1502; eIDAS ventes tatt inn i norsk rett i nær framtid.

[4] C(2017) 7782 final, basert på EBAs utkast til krav.

Mulige negative konsekvenser av gjennomføringen

I Difi brukerundersøkelser for ID-porten svarer 81% av brukeren at det viktig for dem å ha en e-ID som kan brukes til alle digitale tjenester. All erfaring viser også at det er e-ID-en som brukes ofte, som er både den mest brukervennlige og mest sikre løsningen. Blir konsekvensen av direktivet at BankID ikke lengre kan oppfylle kravene til høyt sikkerhetsnivå, og således ikke kan brukes på tvers i samfunnet, vil det føre til et betydelig tap og hindre digitaliseringsarbeidet i det offentlige.

Fører direktivet til at det er nødvendig å utbre en ny e-ID på høyt sikkerhetsnivå vil kostnadene bli betydelige og tidshorisonten for full utrulling lang. De største kostnadene med en e-ID er knyttet til utlevering og identitetskontroll. Som eksempel kan nevnes Postens PUM tjeneste som vil kunne oppfylle deler av utleveringskravet. Denne er alene priset til over 300 kr per utlevering. Utrullingen av nasjonalt ID-kort, som kan dekke deler av behovet, har en lang tidshorisont, da den følger takten på utlevering av nye pass.

Dersom BankID ikke lengre vil kunne oppfylle kravene til høyt sikkerhetsnivå, kan det bli nødvendig å sette digitaliseringsprosjekter i det offentlige på vent. Eksempler på dette kan være tjenester innenfor helse og sosiale ytelser og som krever e-ID på høyt sikkerhetsnivå for å beskytte de taushetsbelagte opplysningene. Dette kan ha stor påvirkning på digitaliseringen i sektorene.

Mulig løsning

Vi mener imidlertid direktivets formål vil kunne oppnås uten at man bryter med god praksis for håndtering av hemmeligheter. Det forutsetter imidlertid at man ivaretar sikkerhetsbehovene til e-ID-løsninger som benyttes også utenfor finanssektoren, og ikke stiller krav om at hemmelighetene skal deles med andre enn e-ID-utstederen. En mulig løsning vil her være å akseptere omdirigering for slike løsninger; mao. at det både for smartkortbaserte, app-baserte og nettsentriske løsninger aksepteres at hemmelighetene oppgis i grensesnitt som e-ID-utstederen har kontroll over.

Difi ønsker å bli involvert i det videre arbeidet med gjennomføring av direktivet, jf. at en uheldig gjennomføring kan gi store negative konsekvenser for digitaliseringen av offentlig sektor.

Vennlig hilsen
for Difi

Steffen Sutorius
direktør

Tor Alvik
fagdirektør

Dokumentet er godkjent elektronisk og har derfor ingen håndskrevne signaturer.

Kopi til:

Kommunal- og moderniseringsdepartementet	Postboks 8112 Dep	0032 OSLO