Kommunaludvalget
Folketinget, Christiansborg
1240 København K

IT-Politisk Forening
c/o Niels Elgaard Larsen
Århusgade 35, 1.
2100 København Ø

E-mail : bestyrelsen@itpol.dk
Web : http://www.itpol.dk

Dato : 24. april 2012

Henvendelse fra IT-Politisk Forening om lovforslag L 160 om Offentlig Digital Post

Lovforslag L 160 indfører i § 3 stk 1 en pligt for borgerne til at være tilsluttet Offentlig Digital Post. Pligten indtræder på et fremtidigt tidspunkt som Finansministeren fastsætter, og bemærkningerne til lovforslaget nævner november 2014. Samtidig giver lovforslaget Finansministeren bemyndigelse til at vælge en (enkelt) digital postløsning og udpege en systemansvarlig som kan være et privat firma.

Offentlig Digital Post eksisterer allerede i dag med frivillig tilslutning, og firmaet e-Boks A/S varetager driften af systemet via webportalen www.borger.dk og integration med det "private" e-Boks system på www.e-boks.dk.

Borgerne skal fremover afgive samtykke til private firmaer for at læse deres egen post

Lovforslag L 160 forholder sig generelt ikke til hvordan borgeren skal kunne læse den post som fra november 2014 afleveres i den digitale postløsning, uanset om borgeren ønsker dette eller ej. Efter § 10 er brevene i juridisk forstand kommet frem til borgeren når de er afleveret til den digitale postløsning (hvilket i bemærkningerne benævnes "tilgængelige for borgeren"), og det er borgerens eget ansvar at skaffe sig adgang til at læse disse breve, ligesom det er borgerens eget ansvar løbende at holde øje med om der er nye breve i den digitale postkasse.

For at bruge den nuværende offentlige digitale postløsning skal borgeren indgå en aftale med firmaet e-Boks A/S. Borgeren skal i den forbindelse acceptere de betingelser som e-Boks har fastsat for den digitale postløsning, for eksempel at borgeren ikke kan

holde e-Boks ansvarlig for manglende tilgængelighed ved driftsforstyrrelser. E-Boks kan i øvrigt frit ændre disse betingelser på et senere tidspunkt. Borgeren skal også acceptere at være dataansvarlig for egne breve når de opbevares hos e-Boks, og at e-Boks er databehandler for borgeren i den henseende.

For overhovedet at komme så langt skal borgeren have OCES NemID, hvilket kræver en aftale med firmaet DanID A/S og et temmelig vidtgående samtykke til dette firma. Borgeren skal acceptere de betingelser som DanID har fastsat for brugen af NemID tjenesten, og borgeren skal konkret acceptere at den private PKI nøgle (borgerens ”digitale underskrift”) opbevares på DanIDs servere. Der er desuden en række sikkerhedsproblemer ved NemID, og dem accepterer borgeren ved at afgive et samtykke til DanID. IT-Politisk Forening har tidligere kritiseret NemID som vi mener er en meget dårlig teknisk løsning. Vi har lavet en opsummering af denne kritik i et appendiks til dette brev (samme appendiks som i vores henvendelse om lovforslag L 159).

Problematisk at der er tvungne samtykker til private monopolfirmaer

På Datatilsynets hjemmeside er der under ”ordbog” en definition af begrebet ”samtykke” i forbindelse med persondataloven. Centrale elementer i denne definition er at et samtykke efter persondataloven skal være frivilligt, og at det skal være muligt at trække samtykket tilbage. Hvis der er en lov (for eksempel L 160) som i praksis pålægger borgeren at bruge OCES NemID, er denne frivillighed og mulighed for at trække samtykket tilbage en illusion. Der bliver tale om et ”afpresset” samtykke til en privat tredjepart.

IT-Politisk Forening er ikke bekendt med anden dansk lovgivning som på samme eksplicitte måde pålægger borgeren at afgive et vidtgående samtykke til et bestemt privat firma. I dette tilfælde er der endda tale om ”afpressede” samtykker til to forskellige firmaer (DanID A/S og e-Boks A/S).

Formelt giver L 160 måske ikke borgeren en pligt til at acceptere betingelserne for brugen af Offentlig Digital Post (e-Boks) og OCES NemID, men det er alligevel den praktiske realitet af loven. Det vil være umuligt for borgeren at læse sin egen post fra det offentlige medmindre der indgås aftaler med de private firmaer, som af Finansministeren har fået opgaven med at administrere borgerens digitale post (e-Boks) og borgerens digitale underskrift (DanID).

Det fremgår også af bemærkningerne (side 19 i lovforslaget) at Offentlig Digital Post kan omfatte stort set alle henvendelser fra det offentlige, hvis den offentlige myndighed vælger at bruge systemet (der er ikke noget krav om dette, idet L 160 kun definerer nye pligter for borgeren). Der kan altså være tale om breve med væsentlig information til borgerne, eller breve som pålægger borgerne en konkret handlepligt efter lovgivningen. Der kan i øvrigt også være tale om breve med følsomt indhold som borgeren ikke ønsker opbevaret hos et privat firma.

Men borgeren har ikke noget valg. Finansministeren (oprindeligt ITST) har først givet et privat firma monopol på at opbevare borgernes digitale post fra det offentlige, og derefter vil Finansministeriet tvinge alle borgere til at blive ”kunder” hos dette firma. Hvis der skal indføres en pligt for borgerne til at modtage post digitalt, bør ordningen være baseret på fri konkurrence så borgeren frit kan vælge postudbyder. I Danmark kan borgerne frit skifte bank eller teleselskab (og beholde deres telefonnummer), og den samme valgfrihed bør gælde for modtagelse og opbevaring af digital post.

Misvisende sammenligning med fysiske postkasser bruges som begrundelse

Bemærkningerne til lovforslaget forholder sig stort set ikke til ovenstående problemer, og ordet ”samtykke” nævnes ikke en eneste gang i bemærkningerne. Brevene er afleveret til borgeren når de er i den digitale postløsning, og det er fuldstændigt underordnet om borgeren er i stand til at læse brevene eller ej (medmindre borgeren kan blive fritaget for den digitale postordning, hvilket der ikke er noget retskrav om). På side 10 i bemærkningerne står der således

> *Det vil ikke være til hinder for offentlige afsenderes mulighed for at sende digital post til fysiske personer og juridiske enheder, der omfattes af obligatorisk tilslutning, at disse ikke har været logget ind i postløsningen og således ikke i praksis anvender postløsningen. Det er således op til de pågældende fysiske personer og juridiske enheder selv at skaffe sig adgang til de dokumenter, som sendes til dem, ved at logge på postløsningen.*
>
> *Dette svarer på mange punkter til den praksis og retstilstand, der gælder ved levering af papirbreve i fysiske postkasser tilhørende fysiske personer og juridiske enheder, hvor det tilsvarende er modtagerens eget ansvar*

at tømme postkassen og gøre sig bekendt med indholdet af meddelelser, der er kommet frem til den pågældende, jf. bemærkningerne til lovforslagets § 10.

Sammenligningen med borgerens fysiske postkasse er efter vores mening en meget dårlig analogi. Det kræver ikke et samtykke til privat(e) tredjepart(er) at opsætte en fysisk postkasse, og der er ingen problematikker i forhold til borgerens privatlivsbeskyttelse når posten er afleveret i den fysiske postkasse.

Borgeren har også selv mulighed for at bestemme sikkerheden for opbevaring af sin egen post når den er afleveret i den fysiske postkasse. Med Offentlig Digital Post skal borgeren acceptere den sikkerhed som e-Boks og NemID tilbyder. Det tekniske design af NemID giver desværre mange muligheder for at andre (f.eks. kriminelle) kan aflure borgerens adgangskoder via såkaldte phishing angreb. Vi kommer ind på dette i nedenstående appendiks.

Appendiks: IT-Politisk Forenings kritik af NemID [1]

Sårbar overfor man-in-the-middle-angreb

DanIDs tekniske løsning er meget sårbar overfor såkaldte man-in-the-middle angreb, hvor en hacker giver sig ud for at være DanID og bruger en falsk NemID side til at aflure borgerens password og papkort-koder i takt med at de skal bruges. Hvis borgeren kan lokkes ind på en falsk NemID side, er der reelt fri adgang til at misbruge borgerens digitale signatur. Det samme kan ske på en legitim side, som benytter NemID, for eksempel en sportsklub, hvis hackeren har angrebet denne side.

Det skal bemærkes at denne sikkerhedsrisiko ikke er et teoretisk problem: der har allerede være to angrebsbølger mod netbank-udgaven af NemID, hvor bankkunder er blevet afluret password og papkort-koder. Efterfølgende er penge overført fra disse kunders bankkonti.

For de borgere, der har OCES NemID, vil denne slags angreb ikke blot kunne misbruge bankkonti, men også offentlige tjenester. Dette vil også blive et mål for kriminelle.

Identitetstyveri er et stort ”forretningsområde” for den internationale organiserede kriminalitet, og der er desværre mange andre muligheder som kan give store problemer for borgeren.

Brugen af Java er en IT-sikkerhedsrisiko

NemID kræver Java i webbrowseren — en snart 15 år gammel teknologi, som af mange betragtes som forældet. Nye mobile devices som smartphones og tablets understøtter ikke Java i deres webbrowsere.

Java i webbrowseren er plaget af en række sikkerhedsproblemer, og der bliver hele tiden fundet nye alvorlige sikkerhedshuller. En del sikkerhedseksperter anbefaler direkte folk at de-aktivere Java i deres webbrowser, eller helt at afinstallere denne software-komponent (som stort set ikke bruges mere). Det kan den danske befolkning imidlertid ikke gøre, da de så ikke kan bruge NemID.

1 Dette appendiks er identisk med appendiks i vores henvendelse til Kommunaludvalget om lovforslag L 159.

NemID snager i din computer

Java-appletten i NemID giver DanID mulighed for at læse borgernes filer, og starte egne programmer på borgernes computere — eventuelt på vegne af en statslig myndighed som beder DanID om dette.

IT-Politisk Forening påpegede dette forhold i august 2010, men DanID afviste pure at det skete. Efterfølgende har det dog vist sig at DanID faktisk bruger NemID Java appletten til at køre programmer på borgernes computere for at indsamle visse oplysninger om dem.

Det er i forvejen unødvendigt og betænkeligt, at DanID skal have mulighed for at infiltrere borgernes computere med NemID Java appletten. Når DanID så ovenikøbet misinformerer om, hvordan de bruger denne adgang, må man som borger alvorligt overveje, om man kan have tillid til løsningen.

NemID bryder med gængse sikkerhedsprincipper

En digital signatur består teknisk set af to dele: En privat nøgle og en offentlig nøgle. Når borgeren underskriver et dokument digitalt, bruges den private nøgle. For at kontrollere om det er borgerens underskrift, bruges den offentlige nøgle. Hvis borgeren er den eneste som kan bruge den private nøgle, er en digital underskrift et matematisk bevis for at borgeren har skrevet meddelelsen.

Den offentlige nøgle må alle kende, men i sagens natur er det altafgørende at borgeren har den fulde kontrol over sin egen private nøgle, da man ellers ikke kan vide om det er den pågældende borger eller en anden person, der har skrevet meddelelsen. I så godt som alle digital signatur systemer sikres dette ved at borgeren selv opbevarer sin private nøgle, og den private nøgle beskyttes mod kopiering med password, eller andre sikkerhedsmekanismer som opbevaring på hardware tokens (den digital underskrift foretages på et hardware token, og den private nøgle kan slet ikke kopieres).

Vigtigheden af at borgeren har den fulde kontrol over sin egen private nøgle ses også af § 10, stk 3 i lov om elektroniske signaturer, der forbyder nøglecentre at *"...opbevare eller kopiere de personers signaturgenereringsdata, som nøglecentret gennem udstedelsen af certifikater måtte have fået kendskab til."*

OCES NemID, altså den digitale signatur, er desværre ikke baseret på dette princip. I stedet opbevares den private nøgle hos DanID. Borgeren tilgår den private nøgle via en hjemmeside, og adgangen til den private nøgle er sikret med et password og en kode fra et papkort.

OCES NemID opfylder ikke de krav, der stilles i Lov om elektroniske signaturer. Det retslige grundlag for OCES NemID er alene certifikatpolitikken ”Offentlige Certifikater til Elektronisk Service, version 4”, som er defineret af IT- og Telestyrelsen uden direkte involvering af Folketinget.

IT-Politisk Forening har tidligere kritiseret den centrale nøgle-opbevaring. Den bryder med det mest grundlæggende princip for digitale signaturer. I princippet kan DanID udgive sig for en vilkårlig borger uden dennes vidende. Vi er klar over, at denne risiko er teoretisk, men det skaber utryghed, at man har valgt en teknisk løsning med central opbevaring af de private nøgler.

DanID overholder ikke sine forpligtelser

Efter certifikatpolitikken version 4, og aftalen med staten, er DanID forpligtet til at tilbyde borgerne en digital signatur hvor den private nøgle opbevares på et smartcard (hardware token). Det var oprindeligt meningen at denne løsning skulle være tilgængelig i december 2010, men den er blevet forsinket ad flere omgange, og i skrivende stund er den muligvis udsat på ubestemt tid. Derudover bliver smartcard løsningen ikke gratis for borgerne, hvis den altså kommer. Det er heller ikke klart om borgeren får den fulde kontrol over den private nøgle, eller om der fortsat vil eksistere kopier andre steder i DanIDs systemer.

Datatilsynet har flere gange kritiseret udskydelsen af muligheden for at borgeren kan opbevare sin egen private nøgle, senest i høringssvaret om lovforslag L 159, hvor de skriver:

> *Tvungen brug af selvbetjeningsløsninger baseret på NemID aktualiserer en problemstilling, som tilsynet tidligere har påpeget overfor IT og Telestyrelsen omkring opbevaring af borgernes private nøgle.*
>
> *Datatilsynet udtalte bl.a. følgende i brev af 3. marts 2009 til IT og Telestyrelsen:*
> *”[…] Det er endvidere Datatilsynets opfattelse, at et*

generelt hensyn til brugernes privacy taler for, at brugerne skal have et valg med hensyn til, hvor deres nøgle opbevares.

Datatilsynet skal derfor opfordre til, at der hurtigst muligt skabes mulighed for egen opbevaring af den private nøgle.

Datatilsynet skal endvidere anbefale, at det overvejes, om ikke muligheden for egen opbevaring af den private nøgle bør være gratis, eller at prisen i det mindste bliver så lav som muligt og alene kommer til at afspejle omkostningerne. […]"

DanID's interesser tilgodeser ikke borgernes sikkerhed

DanID er ejet af Nets, som igen ejes af bankerne. Det er tydeligt, at DanID's sikkerhedsvurderinger er set ud fra bankernes behov, ikke borgernes.

I bankverdenen vurderer man traditionelt sikkerhed ud fra ren økonomi: Hvis det er billigere at udbetale erstatning til ofrene for et sikkerhedshul end at lappe hullet, så vælger man det første. Det giver god mening for både banker og kunder, fordi banksikkerhed netop kan gøres op i kroner og øre.

Men det giver ikke mening ved brug som digital signatur overfor det offentlige. Følgerne af identitetstyveri, brud på privatlivets fred osv. kan ikke umiddelbart gøres op i kroner og øre.

DanID mener, at deres løsning er "sikker nok", men det er vurderet ud fra et rent økonomisk perspektiv, ikke ud fra borgernes interesser.

DanID bliver et tvunget monopol

Hvis det var frivilligt at bruge OCES NemID, kunne man sige at ovenstående kritikpunkter er noget som den enkelte må tage hensyn til, hvis han/hun beslutter sig for at bruge NemID. Sådan er det med så mange andre "gratis" services på internettet, for eksempel Facebook der tilbyder brugerne en række fordele, men også har en række problemer for privatlivsbeskyttelsen. Hvis man ikke har tillid til Facebook, kan man lade være med at oprette en Facebook konto.

Men hvis lovforslag L 159 eller L 160 vedtages, er det reelt ikke længere frivilligt om den danske befolkning vil bruge OCES NemID. Medmindre borgeren er så heldig at kunne blive undtaget fra den obligatoriske digitale selvbetjening, og den digitale postordning, vil det være nødvendigt at erhverve OCES NemID for at overholde landets love.

Det er således et meget vidtgående skridt at Finansministeren nu agter at tvinge borgerne til at afgive et ”frivilligt” samtykke til et bestemt privat firma (DanID), når dette samtykke reelt indebærer at det private firma kommer til at administrere borgernes digitale ”identitet” (som den private nøgle reelt er).