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 159 om obligatorisk digital selvbetjening

Lovforslag L 159 indfører obligatorisk digital selvbetjening på fire konkrete områder fra december 2012, og det fremgår af bemærkningerne at der i 2012 (”første bølge”) vil blive indført obligatorisk digital selvbetjening på en række andre områder, hvor dette kan ske med hjemmel i eksisterende lovgivning (for eksempel har skatteforvaltningsloven § 35 siden maj 2010 givet mulighed for at pålægge borgerne digital kommunikation med Skat, men denne bemyndigelse har endnu ikke været udnyttet).

Pligt til at bruge OCES NemID er problematisk

Der er ikke noget specielt ved lovgivning som pålægger borgerne pligter (vi skal alle betale skat). Det specielle og problematiske ved dette lovforslag er at det, i praksis, giver borgerne en pligt til at indgå en aftale med et bestemt privat firma (DanID A/S), og afgive et temmelig vidtgående samtykke til dette firma, for at få OCES NemID.

Denne pligt fremgår ikke direkte af lovforslaget, idet lovforslaget alene specificerer en pligt til at anvende digital selvbetjening. Det er op til de enkelte kommuner at designe deres digitale selvbetjeningsløsninger, men det fremgår af bemærkningerne at disse selvbetjeningsløsninger generelt bruger OCES NemID.

Hvis borgeren ikke har OCES NemID, og ikke kan blive omfattet af undtagelserne fra den obligatoriske digitale selvbetjening, kan borgeren for eksempel ikke overholde CPR lovens krav om flytteanmeldelse eller udnytte sin ret til lægebehandling efter sundhedsloven (sundhedskort kan kun bestilles ved brug af den

obligatoriske digitale selvbetjening). Lovforslaget pålægger ligefrem den enkelte kommune at afvise de henvendelser som ikke indgives digitalt, medmindre altså at borgeren er omfattet af undtagelserne.

For at borgeren kan få OCES NemID skal borgeren indgå en aftale med DanID A/S, og borgeren skal afgive et samtykke til dette firma. Borgeren skal i den forbindelse 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 160).

Tvunget samtykke til et privat firma for at overholde dansk lov

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 159) 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, i dette tilfælde DanID A/S.

Vi er ikke bekendt med anden dansk lovgivning som på samme eksplicitte måde pålægger borgeren at afgive et vidtgående samtykke til et bestemt privat firma. Lov om offentlige betalinger pålægger borgeren at have en bankkonto (NemKonto), og det vil kræve et samtykke til en bank, men det kan ikke sammenlignes med lovforslag L 159. For det første har borgeren valgfrihed mellem 125 danske banker, og det er også muligt at vælge en udenlandsk bank til NemKonto. For det andet risikerer borgeren ikke straf hvis kravet om at have en NemKonto ikke overholdes, og borgeren mister heller ikke nogle rettigheder (et krav på tilbagebetaling af overskydende skat fortabes eksempelvis ikke). Hvis borgeren derimod ikke melder flytning til kommunen rettidigt, kan det udløse bødestraf jf. CPR lovens § 59. Det samtykke som afgives til en bank for at få en bankkonto har et

begrænset omfang, og det kan på ingen måde sammenlignes med det vidtgående samtykke som borgeren skal afgive til DanID A/S for at få OCES NemID (digital signatur).

Det er muligt at designe digitale selvbetjeningsløsninger som ikke kræver et samtykke til en privat tredjepart. Hos Skat kan borgeren foruden NemID (indtil videre) bruge Skats egen TastSelv kode, hvor borgeren ikke tvinges til at involvere en privat tredjepart.

Uklar retsstilling for borgere som ikke frivilligt vil erhverve NemID

I bemærkningerne til lovforslaget virker det som om at Finansministeren gør sig store anstrengelser for ikke at skrive ”pligt til at erhverve NemID”, selv om denne pligt i praksis kommer til at eksistere via den obligatoriske digitale selvbetjening. På side 10 i bemærkningerne til lovforslaget står der eksempelvis

> *Hvis en borger ikke har, men kan få udstedt NemID, og dette er en forudsætning for anvendelse af den konkrete digitale selvbetjeningsløsning, foreslås det, at den offentlige myndighed skal anmode borgeren om at anskaffe sig NemID. Hvis den offentlige myndighed vurderer, at der foreligger særlige forhold, kan myndigheden vælge ikke at kræve anskaffelse af NemID, men lade borgeren ansøge på anden vis.*
>
> *Det er den offentlige myndighed, der i de konkrete tilfælde foretager en vurdering af, om der foreligger særlige forhold. Hvis den offentlige myndighed finder, at der foreligger særlige forhold, skal den offentlige myndighed tilbyde borgeren en anden måde at ansøge, anmelde eller indberette på. Finder den offentlige myndighed, at der ikke foreligger særlige forhold, vil borgeren være henvist til at ansøge, anmelde eller indberette digitalt. Indgives ansøgningen alligevel ikke digitalt, vil kommunen skulle afvise ansøgningen.*

Kommunen kan efter L 159 pålægge borgeren at bruge den digitale selvbetjening (der generelt kræver NemID), men kommunen kan tilsyneladende ikke pålægge borgeren at erhverve NemID? I stedet skal kommunen ”anmode” borgeren om at anskaffe sig NemID.

Denne formulering efterlader borgeren i en besynderlig retstilstand. På den ene side er der måske ikke i L 159 noget eksplicit lovkrav om at erhverve NemID (og afgive det ”frivillige” samtykke til DanID), men på den anden side er borgeren afskåret fra at overholde landets love og gøre brug af lovbestemte rettigheder uden NemID.

Undtagelser fra obligatorisk digital selvbetjening

Det vil aldrig være muligt at opnå 100% digital selvbetjening, fordi der altid (også om 25 år) vil være en række borgere som ikke er i stand til at bruge de digitale selvbetjeningssystemer. Kommunerne skal altså stadig have ”analoge” systemer til at betjene de borgere som ikke kan bruge den digitale selvbetjening.

I bemærkningerne til lovforslaget står der flere steder at mange borgere selv ønsker at bruge den digitale selvbetjening. IT-Politisk Forening er enig i denne vurdering, men det burde rejse spørgsmålet hvad man opnår ved at gøre den digitale selvbetjening obligatorisk? Frivillig digital selvbetjening vil give kommunerne et økonomisk incitament til at udvikle brugervenlige systemer som borgerne ønsker at bruge. Det samme incitament er ikke til stede ved obligatorisk selvbetjening, og alene af den grund kan man frygte dårligere løsninger når grundlaget for den offentlige digitalisering er tvang.

Obligatorisk digital selvbetjening giver desuden en række retssikkerhedsmæssige problemer for de borgere som ikke kan bruge den digitale selvbetjening, og i nogle situationer kan det ende med at blive dyrere for det offentlige end en frivillig ordning.

De borgere, som ikke kan bruge den offentlige digitale selvbetjening, kan efter lovforslaget blive fritaget fra denne pligt, men borgerne har ikke som sådan noget retskrav på dette. Der synes heller ikke at være opstillet tilpas objektive kriterier for om borgerne kan blive fritaget eller ej. Det er op til kommunalbestyrelsen at vurdere om betingelserne for fritagelse er til stede.

Borgere som ikke kan, eller vil, bruge den obligatoriske digitale selvbetjening kommer nærmest til at stå ”med hatten i hånden”, og deres rettigheder i forhold til den offentlige sektor er forringet sammenlignet med de borgere som bruger den digitale selvbetjening (enten fordi de gerne vil eller fordi de accepterer den offentlige tvang, herunder det ”afpressede” samtykke til DanID).

Hvornår har borgeren eksempelvis opfyldt sin pligt til at anmelde flytning hvis dette ikke sker digitalt: når kommunen modtager den ikke-digitale henvendelse eller når kommunen accepterer at borgeren er fritaget fra kravet om digital selvbetjening?

I nogle situationer kan den obligatoriske digitale selvbetjening blive langt dyrere for kommunerne end en frivillig ordning. Hvis en borger for eksempel indgiver en flytteanmeldelse til kommunen per brev, eller via personlig henvendelse, skal kommunen efter lovforslaget afvise denne henvendelse. Det kræver ikke meget fantasi at forestille sig at en afvisning af den ikke-digitale henvendelse kan være dyrere end blot at lade en kommunal medarbejder indtaste den nye adresse i CPR systemet.

En afvisning af en ikke-digital henvendelse er en kommunal afgørelse, som efter forvaltningslovens regler skal begrundes. Hvis borgeren har anført en begrundelse for ikke at bruge den digitale selvbetjening, eller gør dette i efterfølgende korrespondance med kommunen, skal kommunen naturligvis foretage en realitetsbehandling heraf inden en endelig afgørelse om afvisning af den ikke-digitale henvendelse træffes. Derefter har borgeren mulighed for at klage til de kommunale tilsynsmyndigheder og til Folketingets ombudsmand.

Hvis det var frivilligt at bruge den offentlige digitale selvbetjening, ville man ikke forringe rettighederne for visse grupper af samfundet (de ”digitalt svage” borgere), og der ville ikke være nogen risiko for at en banal ekspeditionssag som en flytning kunne eskalere til en langvarig og sikkert bekostelig klagesag.

Software og krav om tilgængelighed for alle borgere

Hvis det skal være obligatorisk for borgerne at bruge den offentlige digitale selvbetjening, bør der tilsvarende være en forpligtelse for kommunerne til at sikre at *alle* borgere kan bruge selvbetjeningssystemerne fra deres egne computere. Det er ikke klart ud fra bemærkningerne til lovforslaget hvordan det skal sikres (eller om det skal sikres?), idet det er overladt til kommunerne at designe de digitale selvbetjeningsløsninger. På side 11 i bemærkningerne, samt i høringsnotatet, nævnes de ”fællesoffentlige tilgængelighedsstandarder, for eksempel WCAG”, men kravene synes ikke særligt konkrete.

På portalen borger.dk er der i dag eksempler på digital selvbetjening som kun kan bruges hvis borgeren anvender

bestemte programmer (software). Selv om vi i Danmark har en folketingsbeslutning om åbne standarder, der blandt andet er udmøntet i et krav om PDF/A for ikke-redigerbare dokumenter, kan man på borger.dk finde PDF blanketter som kun kan læses med Adobe PDF Reader. Sådanne eksempler kan næppe være forenelige med ”åbne standarder” og ”tilgængelighed”.

Det fremgår ikke af lovforslaget eller bemærkningerne hvilke klagemuligheder borgerne har, hvis de oplever at de ikke kan bruge den obligatoriske digitale selvbetjening fra deres egne computere. Det eneste rimelige ville være at give borgerne en fritagelse i sådanne tilfælde, og hvis det var frivilligt at bruge den digitale selvbetjening, ville der slet ikke være basis for denne diskussion.

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 160.

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).