DIGITALISERINGSSTYRELSEN

Notat

14. maj 2012

Bilag til svar på Kommunaludvalgets spørgsmål nr. 1 (L159) og spørgsmål 2 (L160) af 24. april 2012 - "Appendiks IT-Politisk Forenings kritik af NemID"

IT-Politisk Forenings appendiks opsummerer en række tidligere kritikpunkter vedrørende NemID. Svarene på de enkelte kritikpunkter opsummeres nedenfor.

Ad: "Sårbar overfor man-in-the-middle-angreb"

Der har været to vellykkede phishing henholdsvis man-in-the-middle angreb, som anført af IT-Politisk Forening, hvor få bankkunder blev franarret deres personlige koder til NemID. Svindlere misbrugte herefter koderne til at overføre penge til egne konti. Disse få angreb skal ses i forhold til et samlet meget stort antal daglige transaktioner. Siden lanceringen af NemID den 1. juli 2010 har der været mere end 700 mio. transaktioner med NemID. Hverken Nets DanID eller Digitaliseringsstyrelsen har kendskab til, at der skulle være sket angreb mod offentlige selvbetjeningsløsninger, hvor NemID er blevet misbrugt.

Der er således ingen tvivl om, at indførelsen af NemID generelt har gjort det vanskeligere for de it-kriminelle, som går efter en hurtig økonomisk gevinst på nettet, set i forhold til netbankernes tidligere sikkerhedsløsninger og den tidligere digitale signatur. Det er dog samtidig nødvendigt at anerkende, at uanset hvilken sikkerhedsløsning man anvender, vil den altid være forbundet med risici og sårbarheder, som løbende skal vurderes og imødegås. NemID er valgt ud fra en nøje afbalanceret afvejning mellem et tilstrækkeligt højt sikkerhedsniveau, høj mobilitet og behovet for stor udbredelse, anvendelse og forståelighed af løsningen i den brede befolkning.

Sikkerhed er således ikke en absolut størrelse. Trusselsbilledet ændrer sig konstant, og det er ikke praktisk muligt at etablere it-systemer, der over tid er 100 % sikre. Risiko for misbrug og svindel eksisterer i den digitale såvel som i den papirbaserede verden, og ligesom i den papirbaserede verden er det nødvendigt at forholde sig til og minimere risici løbende. Identitetstyveri eller økonomiske tab som følge af svindel og misbrug er alvorlige lovovertrædelser, såvel i den digitale som den analoge verden. Sådanne lovovertrædelser er reguleret af og skal retsforfølges efter dansk rets almindelige regler, herunder straffeloven og betalingstjenesteloven.

Der har fra starten været stort fokus på sikkerheden i NemID, og Nets DanID overvåger løbende systemet og iværksætter fornødne sikkerhedsforanstaltninger, hvis det vurderes at blive aktuelt. Desuden foretager bankerne, Nets DanID og

Digitaliseringsstyrelsen løbende risikovurderinger af de aktuelle trusler og afvejer behovet for supplerende sikkerhedsforanstaltninger i forhold til brugervenlighed og økonomi.

De aktuelle få eksempler på vellykkede angreb på netbanker bliver naturligvis taget meget alvorligt, og Digitaliseringsstyrelsen, bankerne og Nets DanID vurderer fortsat, at risikoen for svindel på nuværende tidspunkt er minimal. Borgerne kan derfor fortsat have tillid til NemID.

Ad: "Brugen af Java er en IT-sikkerhedsrisiko"

Valget af Java som det teknologiske grundlag for NemID løsningen blev truffet tilbage i 2008/2009, hvor løsningen blev specificeret. Valget af Java som platform blev truffet på baggrund af erfaringer fra netbankernes tidligere sikkerhedsløsninger og fra den tidligere digitale signatur. Java teknologien passede desuden bedst til den specificerede arkitektur for NemID og tilgodeså samtidig bankernes og den tidligere IT- og Telestyrelses krav til platformuafhængighed og sikkerhed af den samlede løsning.

NemID baseret på Java anses fortsat som sikker, forudsat at brugerne - som ved al anden software - sikrer løbende opdatering med seneste versioner.

Ligesom trusselsbilledet på sikkerhedsområdet ændres, ændrer det teknologiske landskab sig også konstant. Det er derfor vigtigt og nødvendigt at it-løsninger som NemID vurderes løbende, både i forhold til sikkerheden og deres teknologiske robusthed. Digitaliseringsstyrelsen, bankerne og Nets DanID vurderer løbende, om der er grundlag for at ændre den teknologiske platform for NemID.

Ad "NemID snager i din computer"

I NemID løsningen anvendes en såkaldt Java-applet, som afvikles på brugerens pc. Appletten gemmer kode lokalt (cache) på brugerens computer, bl.a. som filer, der ender med "gif". Disse filer benyttes til at beregne en såkaldt pc-checksum, som kan anvendes både præventivt og opklaringsmæssigt i forhold til visse angreb mod brugeren. Nets DanID har ved flere lejligheder beskrevet disse forhold. Dette tiltag er ét blandt mange sikkerhedstiltag, der skal besværliggøre misbrug og udnyttelse af systemet for it-kriminelle. Nets DanIDs privatlivspolitik beskriver, at denne information bliver indsamlet, og at formålet med indsamlingen er efterforskning af misbrug eller forsøg på misbrug af NemID. Nets DanIDs NemID-applet har ikke funktionalitet, der indsamler data fra brugerens pc udover det, der er beskrevet i privatlivspolitikken.

Ad: "NemID bryder med gængse sikkerhedsprincipper"

NemID baseret på OCES-standarden bygger på en teknologi kaldet Public Key Infrastructure (PKI). Det indebærer, at brugeren får udstedt en digital signatur, der består af en privat nøgle og et certifikat med en offentlig nøgle. PKI er en anerkendt sikkerhedsmodel.

I PKI er det afgørende, at kun brugeren selv har kontrol over den private nøgle.

I NemID sikres denne kontrol ved, at det alene er brugeren, der – via to-faktor sikkerhed har adgang til den private nøgle, som ligger på specielle sikrede kryptografiske hardware-moduler. Disse moduler er forsvarligt aflåst, og driftes og vedligeholdes af Nets DanID A/S.

Den private nøgle kan ikke anvendes i hardwaremodulet uden anvendelse af data dannet på baggrund af brugerens personlige adgangskode. DanID har på intet tidspunkt brugerens personlige adgangskode.

Tilgangen til brugerens private nøgle er baseret på en sikker protokol, der har været gennemgået af førende internationale sikkerhedseksperter.

I forhold til IT-Politisk Forenings reference til Lov om elektroniske signaturer bemærkes, at NemID udstedes på baggrund af OCES-standarden, som er fastlagt i OCES-certifikatpolitik for personcertifikater og er således ikke omfattet af Lov om elektroniske signaturer. Det skal dog også bemærkes, at den beskrevne teknologiske løsning for NemID efter Digitaliseringsstyrelsens opfattelse ikke strider mod § 10, stk. 3 i loven, idet løsningen sikrer, at brugeren har den fulde kontrol over sin egen private nøgle.

Ad: "DanID overholder ikke sine forpligtelser"

DanIDs forpligtelser fremgår dels af OCES-certifikatpolitikken, dels af kontrakt indgået med staten den 21. august 2008 på baggrund af et EU-udbud. Den hardwareløsning, som omtales i appendikset, er ikke et krav i OCES-certifikatpolitikken, men stammer fra kontrakten med Digitaliseringsstyrelsen.

Det er forventningen, at den hardwarebaserede løsning vil blive lanceret ultimo november 2012. Det er kontraktligt aftalt, at denne løsning vil blive tilbudt til de borgere, der er interesseret i denne løsning og ønsker at betale herfor.

I forhold til henvisning til Datatilsynets udtalelse om privacy, skal det bemærkes, at Digitaliseringsstyrelsen tidligere har besvaret denne og meddelt, at beslutningen om at tilbyde en løsning med opbevaring af nøgler på hardware ikke er begrundet hverken i sikkerhedsmæssige eller privacymæssige hensyn, idet den eksisterende løsning med central opbevaring af den private nøgle fuldt og helt sikrer brugerens

enekontrol. For yderligere detaljer henvises til besvarelsen af it-politisk foreningens kritikpunkt "NemID bryder med gængse sikkerhedsprincipper".

Ad: "DanID's interesser tilgodeser ikke borgernes sikkerhed"

Opgaven om at udvikle, implementere og drive den offentlige digitale signatur infrastruktur på vegne af den offentlige sektor har været konkurrenceudsat ved et EU-udbud. DanID varetager således i forhold til udstedelse af den offentlige digitale signatur en opgave på vegne af den offentlige sektor reguleret i henholdsvis OCES-certifikatpolitikken og den mellem parterne indgåede kontrakt. Alle hensyn og krav i relation til certifikatpolitik og kontrakt relaterer sig til den opgave, der leveres til den offentlige sektor, herunder også sikkerhedsmæssige spørgsmål, og medvirker til, at borgerne kan være trygge ved, at Nets DanID varetager hensynet til borgernes sikkerhed.

Det er helt sædvanligt, at private virksomheder har ansvaret for implementering, drift og vedligeholdelse af sikkerhedsløsninger for den offentlige sektor.

Nets DanID er desuden underlagt Digitaliseringsstyrelsens tilsyn, herunder ekstern systemrevision ved statsautoriseret systemrevisor, som en gang årligt afgiver systemrevisionserklæring til Digitaliseringsstyrelsen om, hvorvidt Nets DanID har overholdt kravene i OCES-certifikatpolitikken.

Endelig er Nets DanID naturligvis, lige som enhver anden virksomhed forpligtet til at leve op til gældende lovgivning, herunder persondataloven.

Ad: "DanID bliver et tvunget monopol"

Som anført i svarene på spørgsmål 159 og 160 er den til enhver tid gældende standard for offentlig digital signatur den identifikationsløsning, som den offentlige sektor har valgt at basere sig på. Det er således korrekt opfattet, at i det omfang obligatoriske digitale selvbetjeningsløsninger kræver, at borgeren identificerer sig selv, vil de borgere, som kan, være nødt til at få NemID.

Det skal endvidere bemærkes, at forudsætningen for at kunne udstede digitale signaturer efter OCES-standarden er, at udsteder har indgået aftale med Digitaliseringsstyrelsen, bl.a. om at overholde OCES-certifikatpolitikken og underlægge sig Digitaliseringsstyrelsens tilsyn.

Med hensyn til IT-politisk foreningens kritik af lovforslagenes konsekvenser henvises til hovedsvarene.