Ministeren for videnskab, teknologi og udvikling

Udvalget for Videnskab og Teknologi
Folketinget
Christiansborg
1240 København K

Hermed fremsendes svar på spørgsmål nr. 33, 34, 35, 36, 37 og 38 (Alm. del - bilag) stillet af Udvalget for Videnskab og Teknologi den 23. november 2009. Spørgsmålene er stillet efter ønske fra Hanne Agersnap (SF).

Med venlig hilsen

Helge Sander

16. december 2009

Ministeriet for Videnskab
Teknologi og Udvikling
Bredgade 43
1260 København K
Telefon 3392 9700
Telefax 3332 3501
E-post vtu@vtu.dk
Netsted www.vtu.dk
CVR-nr. 1680 5408

Sagsnr.
Dok nr.

Spørgsmål nr. 33, 34, 35, 36, 37 og 38 stillet af Udvalget for Videnskab og Teknologi den 23. november 2009 til Ministeren for videnskab, teknologi og udvikling (Alm. del - bilag).

Spørgsmål 33

Ministeren bedes orientere om sikkerhedssystemerne for NemID?

Svar

Til brug for besvarelsen har jeg indhentet bidrag fra IT- og Telestyrelsen, der udtaler følgende:

Ministeriet for Videnskab
Teknologi og Udvikling
Bredgade 43
1260 København K
Telefon 3392 9700
Telefax 3332 3501
E-post vtu@vtu.dk
Netsted www.vtu.dk
CVR-nr. 1680 5408

Sagsnr. 09-074112
Dok nr. 1158548

”De væsentligste sikkerhedsforbedringer i forhold til den nuværende digitale signatur vedrører registreringsprocessen i forbindelse med udstedelse og opbevaring af den private nøgle, der anvendes til signering.

De nye registreringsprocedurer for NemID er udformet med henblik på at øge sikkerheden og opfylde kravene til identifikation i Lov om forebyggende foranstaltninger mod hvidvask af udbytte og finansiering af terrorisme.

I den kommende NemID vil brugerens private nøgle ikke længere ligge på brugerens pc, men bliver opbevaret sikkert i specielle kryptografiske hardwaremoduler i en central server, der driftes af DanID A/S. NemID til borgerne vil således ikke – som det er tilfældet i den nuværende signatur - være en software løsning, hvor sikkerheden alene er afhængig af, om brugeren kan opretholde et fornuftigt sikkerhedsniveau på pc’en.

NemID vil blive baseret på en såkaldt to-faktor autentifikationsløsning, hvor adgang til anvendelsen af den private nøgle vil være beskyttet af en personlig kode (noget man ved), og en engangskode fra et nøglekort (noget man har). Brugerne skal angive et brugernavn, en personlig unik kode og en engangskode fra et personligt nøglekort (det vil sige et plastikkort med fortrykte engangskoder), hver gang signaturen skal anvendes.

De centralt opbevarede private nøgler vil blive sikret mod misbrug gennem tekniske og proceduremæssige sikkerhedsforanstaltninger, og så længe brugeren holder sin personlige kode hemmelig, vil brugerens digitale signatur være beskyttet mod misbrug.

Endelig kan det tilføjes, at NemID samtidig følger de certifikatpolitikker, der gælder for udbydere af OCES-certifikater. I certifikatpolitikkerne stilles en række krav til udbyderens udstedelsesprocesser, nøglehåndtering, certifikat-håndtering samt styring og drift af det tekniske miljø og de organisatoriske procedurer. Certifikatpolitikkerne forpligter udbyderne af OCES-certifikater til, at der årligt skal gennemføres systemrevision af sikkerheden og udarbejdes en protokol og revisionserklæring af en ekstern statsautoriseret revisor, der for NemID’s vedkommende indsendes til IT- og Telestyrelsens godkendelse.

Certifikatpolitikkerne er udarbejdet efter ”best practice” og krav til sikkerhed, algoritmer med videre. Certifikatpolitikkerne refererer således til internationale og de facto-standarder, der er gældende på området.”

Jeg henholder mig til IT- og Telestyrelsens udtalelse.

Spørgsmål 34

Mener ministeren, at den nye OCES-certifikat-politik, der blev offentliggjort fredag den 2. oktober 2009 følger principperne i Lov om elektroniske signaturer? - herunder §10, stk. 3: Nøglecentre må ikke opbevare eller kopiere de personers signaturgenereringsdata, som nøglecentret gennem udstedelsen af certifikater måtte have fået kendskab til?

Svar

Til brug for besvarelsen har jeg indhentet bidrag fra IT- og Telestyrelsen, der udtaler følgende:

”Det antages, at spørgeren implicit lægger til grund for spørgsmålet, at Lov om elektroniske signaturer finder anvendelse for NemID. Dette er ikke tilfældet, idet loven hverken finder anvendelse for den nuværende digitale signatur eller den nye NemID. Lov om elektroniske signaturer finder anvendelse på nøglecentre etableret i Danmark, der udsteder kvalificerede certifikater til offentligheden.

Der er på nuværende tidspunkt ikke udbydere i Danmark af kvalificerede signaturer, det vil sige signaturer, der er reguleret af loven, ligesom udbredelsen heraf i EU generelt er meget begrænset.

Både den nuværende digitale signatur og NemID er således alene reguleret af OCES-certifikatpolitikkerne samt udbyderens kontraktuelle forpligtelse over for IT- og Telestyrelsen med hensyn til at overholde OCES-certifikatpolitikkerne.

Det giver således ikke mening at besvare spørgsmålet i relation til NemID. Nedenfor gives i stedet en generel besvarelse af spørgsmålet, om en central nøgleopbevaring er i modstrid med Lov om elektronisk signaturer. Spørgsmålet er blandt andet behandlet af en af Danmarks førende eksperter på området professor, dr. jur. Henrik Udsen fra Københavns Universitet, der i et notat konkluderer:

”Sammenfattende giver hverken loven, lovens forarbejder eller direktivet noget sikkert svar på, hvordan forbuddet mod certifikatudstederens opbevaring af private nøgler skal forstås, Spørgsmålet er heller ikke behandlet i retspraksis fra EF-domstolen eller fra danske domstole. Selvom der således ikke kan gives et sikkert svar på spørgsmålet, er det ud fra det ovenstående min vurdering, at lovens § 10, stk. 3, ikke forbyder brug af centrale nøgleservere i certifikatudstederens besiddelse.”

Notatet er i sin fulde længde offentliggjort på:
https://danid.dk/export/sites/dk.danid.oc/da/dokumenter/henrik_udsen_notat.pdf

En tilsvarende fortolkning af EU-direktivet, der ligger til grund for Lov om elektroniske signaturer, er udarbejdet i regi af standardiseringsorganet CEN.

Baseret på ovenstående vurderinger er det ministeriets opfattelse, at Loven om elektroniske signaturer ikke forhindrer en løsning baseret på kvalificerede certifikater med central opbevaring af private nøgler."

Jeg henholder mig til IT- og Telestyrelsens udtalelse.

Spørgsmål 35

Vil ministeren oplyse, hvornår og hvordan ordførerne er blevet informeret om denne ændring i certifikatpolitikken?

Svar

Ordførerne er ikke blevet orienteret om denne ændring i certifikatpolitikken.

Kravene til sikkerheden for NemID-løsningen er generelt fastlagt i OCES-certifikatpolitikkerne, der administreres af IT- og Telestyrelsen. Første version af certifikatpolitikkerne blev udarbejdet primo 2003 med henblik på at fastlægge krav til den nuværende digitale signatur. Siden 2003 har certifikatpolitikkerne undergået flere revisioner, og i forbindelse med kravspecifikationen til den nye digitale signatur blev fjerde version af OCES-certifikatpolitik for personcertifikater udarbejdet. Alle revisioner af certifikatpolitikkerne er gennemført efter en bred offentlig høring.

Jeg har ikke forestillet mig, at ordførerne har haft interesse i at blive orienteret om alle de tekniske detailændringer, der gennem årene er foretaget i certifikatpolitikkerne. Men jeg vil naturligvis gerne orientere ordførerne om alle fremtidige tekniske ændringer i certifikatpolitikkerne, hvis der er et ønske herom.

Spørgsmål 36

Hvad er begrundelsen for, at brugere af digital signatur ikke tilbydes at få mulighed for at få en digital signatur på et personligt, elektronisk nøglekort på samme tid som den centrale løsning udbydes?

Svar

Da det er et stort og meget komplekst system, der er under udvikling, har det ud fra en risikobetragtning været hensigtsmæssigt at opdele projektets leverancer i flere faser. Dette er god praksis for at kunne styre udviklingen og implementeringen af store it-projekter.

Den tidsmæssige prioritering af de forskellige leverancer er foretaget ud fra en nytteværdibetragtning, idet nytteværdien af den centrale løsning er vurderet langt større end løsningen med digital signatur på et elektronisk nøglekort. Den centra-

le løsning vil i modsætning til signaturen på nøglekortet kunne anvendes til netbankerne, den er mobil, og den er vederlagsfri for borgerne. Af samme årsager forventes efterspørgslen på løsningen med digital signatur på nøglekort at blive meget lille.

Spørgsmål 37

Finder ministeren denne tidsforskydning mellem de to systemer rimelig?

Svar

Ja, idet jeg henviser til mit svar på spørgsmål 36.

Spørgsmål 38

Vil der blive en overgangsordning, hvor de "gamle" digitale signaturer og netbankordninger fungerer, så borgerne ikke behøver at gå over på NemID, før den decentrale løsning udbydes?

Svar

Når den centrale løsning med NemID lanceres, vil der ikke længere blive udstedt flere af de nuværende digitale signaturer. Den decentrale løsning forventes at blive tilbudt til borgerne et halvt år efter, at den centrale løsning er sat i drift. De nuværende digitale signaturer har en gyldighed på to år og vil ikke blive spærret som følge af, at NemID idriftsættes. Det indebærer, at alle de nuværende signaturer, der er udstedt eller fornyet halvandet år før den centrale løsning sættes i drift, vil kunne anvendes indtil den decentrale løsning tilbydes.

Der vil således blive en overgangsordning, hvor både NemID og den nuværende digitale signatur fungerer i forhold til de offentlige myndigheder.

Hvad angår bankerne, kan jeg kun oplyse, at de ikke modtager den nuværende digitale signatur i deres netbank-løsninger. Spørgsmålet om overgangsordninger i netbankerne ligger uden for mit ressortområde at besvare.