Ministeren for videnskab, teknologi og udvikling

Udvalget for Videnskab og Teknologi
Folketinget
Christiansborg
1240 København K

11. november 2010

Hermed fremsendes svar på spørgsmål nr. 15, 16, 17 og 18 (Alm. del) stillet af Udvalget for Videnskab og Teknologi den 14. oktober 2010. Spørgsmålene er stillet efter ønske fra Yildiz Akdogan (S).

Med venlig hilsen

Charlotte Sahl-Madsen

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. 10-096251
Dok nr. 1582055

Spørgsmål nr. 15, 16, 17 og 18 stillet af Udvalget for Videnskab og Teknologi den 14. oktober 2010 til Ministeren for videnskab, teknologi og udvikling (Alm. del).

Spørgsmål 15

Ministeren bedes udarbejde en opgørelse over de tilfælde, hvor banker har lavet i fejl i sikkerhedsprocedurer omkring NemID?

Svar

Til brug for besvarelse af spørgsmålet har jeg indhentet en udtalelse fra IT- og Telestyrelsen, som oplyser, at styrelsen ikke har kendskab til tilfælde, hvor banker har lavet fejl i sikkerhedsprocedurer udover de tilfælde, som har været omtalt i medierne. Konkret drejer det sig om tre tilfælde. IT- og Telestyrelsen har desuden indhentet information fra DanID, der over for IT- og Telestyrelsen har oplyst, at udover de sager, der har været omtalt i medierne, har DanID konkret kendskab til tre andre tilfælde, hvor medarbejdere i en banks supportfunktion ikke har overholdt kravene til autentifikation i forbindelse med telefoniske henvendelser. Autentifikation betyder måden medarbejderen i banken skal identificere borgeren på. Alle tre tilfælde handler om, at en supportmedarbejder ikke har levet op til kravet om stærk autentifikation i forbindelse med telefonisk henvendelse. Stærk autentifikation stiller flere krav til legitimering af borgeren, som fx supplerende spørgsmål om kundens konti.

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

Herudover har jeg indhentet følgende udtalelse fra Økonomi- og Erhvervsministeriet, som er ansvarlig for tilsyn med finanssektoren:

”Økonomi- og Erhvervsministeriet har oplyst, at Finanstilsynet har kendskab til enkelte tilfælde, hvor en bank fejlagtigt har udleveret nøglekort og pinkode til en forkert person. Udleveringen var sket i strid med gældende fælles procedurer for udlevering, hvilket banken har erkendt over for tilsynet. Banken har endvidere meddelt Finanstilsynet, at den har indskærpet de gældende procedurer overfor sine medarbejdere.”

Jeg henholder mig til oplysningerne fra IT- og Telestyrelsen og udtalelsen fra Økonomi- og Erhvervsministeriet.

Spørgsmål 16

Er ministeren tryg ved bankernes praksis i forbindelse med udlevering af koder til NemID?

Svar

For at kunne udstede OCES-certifikater skal udbyderen DanID indgå en OCES-standardaftale med Videnskabsministeriet. I denne aftale forpligter certifikatudsteder (CA) sig bl.a. til at overholde kravene i OCES-certifikatpolitik for personcertifikater for udstedelse og udlevering af NemID til borgerne og at underlægge

sig IT- og Telestyrelsens kontrol af, at kravene opfyldes, herunder at gennemføre ekstern systemrevision af en statsautoriseret revisor. DanID har indgået OCES-standardaftale med Videnskabsministeriet.

DanID har desuden indgået den kontrakt om indførelse og drift af NemID, som Videnskabsministeriet har været i EU-udbud med. I denne kontrakt forpligter DanID sig til at have en OCES-standardaftale med Videnskabsministeriet og overholde kravene heri i hele kontraktperioden.

I forbindelse med udstedelse af certifikater kan DanID ifølge certifikatpolitikken benytte sig af eksterne registreringsenheder, som bankerne er at betragte som i denne sammenhæng. Det fremgår af certifikatpolitikken, at *"Registreringsenheden (RA) kan enten være nøje knyttet til CA, eller den kan være en selvstændig funktion. CA hæfter under alle omstændigheder for RA's opfyldelse af de stillede krav og forpligtelser på ganske samme måde som for sine egne forhold"*. DanID er således ansvarlig for registreringsenhedens virke og bankernes funktion som registreringsenhed er således underlagt samme kontrol og revisionskrav som DanID selv. DanID har indgået aftaler med registreringsenhederne (RA-aftaler), hvoraf bl.a. fremgår, at udover, at DanID selv fører kontrol med bankernes registreringsenheder, revideres den samlede udstedelsesprocedure ligeledes af ekstern statsautoriseret revision, og der rapporteres til IT- og Telestyrelsen, som påser, at kravene i certifikatpolitikken overholdes.

Herudover har jeg indhentet følgende udtalelse fra Økonomi- og Erhvervsministeriet, som er ansvarlig for tilsyn med finanssektoren:

"Finanstilsynet kan alene forholde sig til pengeinstitutternes anvendelse af NemID i forbindelse med brug af netbank m.m. I disse tilfælde skal pengeinstitutterne leve op til høje krav om identifikation af den pågældende kunde, inden engangskoder og nøglekort udleveres. På denne baggrund og på baggrund af at ministeriet kun har kendskab til enkelte tilfælde, hvor der er begået fejl, finder ministeriet, at pengeinstitutternes udleveringsprocedure må kunne anses for betryggende.

Hovedparten af tilmeldingerne sker imidlertid igennem DanID, som er et selskab i NETS-koncernen, hvor identifikationen sker ved en eksisterende "netbankkontakt".

Det er på denne baggrund min opfattelse, at det samlede kontrolsystem, som er etableret i forbindelse med udlevering af koder til NemID, er indrettet, så det fungerer og skaber den nødvendige sikkerhed omkring NemID.

Spørgsmål 17

Ser ministeren noget problem i, at banker kan udlevere koder til NemID, når NemID samtidig bruges som adgang til personlige oplysninger i offentlig regi?

Svar

Indledningsvist vil jeg gerne understrege, at hele baggrunden for NemID netop har været at skabe et samarbejde mellem finanssektoren og det fællesoffentlige for at opnå de synergifordele, der er ved et fælles og bredt dækkende system.

Men for forståelsens skyld vil jeg gerne kort forklare sammenhængen mellem NemID og adgang til henholdsvis netbank og offentlig digital signatur. NemID er en fælles sikkerhedsinfrastruktur, der på sikker vis autentificerer borgeren og giver borgeren adgang til netbank eller offentlig digital signatur eller begge dele. For at få adgang til netbank, skal kunden indgå en netbankaftale med en bank, og have denne knyttet til sit NemID. For at NemID skal kunne anvendes til offentlige it-systemer, skal kunden eksplicit acceptere vilkårene for offentlig digital signatur.

Som jeg har redegjort for i mit svar på spørgsmål 16 agerer bankerne som registreringsenhed for DanID, når de udleverer NemID til offentlig digital signatur. I deres egenskab af registreringsenhed er bankerne som nævnt underlagt kravene i OCES-certifikatpolitik for personcertifikater, altså nøjagtig de samme krav og den samme kontrol som DanID ville være underlagt, hvis de selv foretog udleveringen.

I relation til bankens identifikation af deres kunder har bankerne naturligvis herudover et selvstændigt ansvar for at leve op til reglerne i Lov om forebyggende foranstaltninger mod hvidvask af udbytte og finansiering af terrorisme. Finanstilsynet fører tilsyn med bankerne i relation til hvidvaskningsloven.

For at opretholde et ensartet sikkerhedsniveau er der mellem bankerne og den offentlige sektor udarbejdet fælles krav til legitimering af personer i forbindelse med udstedelse af NemID. Disse fælles legitimationskrav opfylder kravene i Lov om forebyggende foranstaltninger mod hvidvask af udbytte og finansiering af terrorisme. Legitimationskravene fremgår bl.a. af DanIDs såkaldte RA-aftaler med registreringsenhederne (borgerservicecentre, skattecentre og banker).

Jeg ser derfor ikke noget problem i, at bankerne optræder som registreringsenhed for DanID i forhold til udlevering af NemID.

Spørgsmål 18

Laver ministeren løbende overvågning af bankernes håndtering af sikkerheden omkring NemID?

Svar

Jeg tillader mig at referere til min redegørelse i spørgsmål 16 og 17 om bankernes rolle som registreringsenhed for NemID og kontrollen hermed.

IT- og Telestyrelsen har desuden indhentet nedenstående udtalelse fra DanID om deres løbende overvågning og kontrol med bankerne som registreringsenhed for DanID:

”I bankernes aftale vedrørende NemID er beskrevet hvilke krav bankerne skal efterleve i forhold til håndtering af kunderne. Kravene falder i 3 hovedområder:

1) Legitimering af kunderne jævnfør gældende lov om forebyggende foranstaltninger mod hvidvask af udbytte og finansiering af terrorisme og de fælles vedtagne legitimationskrav for NemID infrastrukturen.

2) Krav til henholdsvis svag og stærk autentifikation (identificering) af brugerne i forbindelse med support på betryggende vis afspejles i Bankens forretningsgange for brugersupport.

3) Krav i forbindelse med opbevaring og udlevering af nøglekort og midlertidig adgangskode hos en registreringsenhed (bank).

Inden lanceringen af NemID er der udarbejdet instruks til bankerne, der beskriver punkt 2 og 3 ovenfor. Endvidere er der udarbejdet materiale, der kan danne grundlag for den interne uddannelse af de medarbejdere, der skal håndtere NemID fx kunderådgivere og supportmedarbejdere.

De konkrete sager DanID har kendskab til er blevet forelagt bankernes ledelse og har desuden været fremhævet som opmærksomhedspunkter i den fælles gruppe til varetagelse af support.

I forbindelse med bankernes håndtering af rollen som registreringsenhed – såvel som det offentliges – er DanID berettiget til selv eller ved at anvende en uvildig tredjemand (fx DanID’s egen eksterne systemrevisor) at foretage inspektion hos registreringsenheden med henblik på at kontrollere, om registreringsenheden overholder kravene i RA-aftalen.

Såfremt en registreringsenhed ikke lever op til sine forpligtelser og ikke gennemfører de nødvendige tiltag til atter at kunne gøre det, vil DanID kunne begrænse registreringsenheden i sine muligheder for at udstede NemID”.

Jeg kan tilføje, at DanIDs RA-aftaler med registreringsenhederne (borgerservicecentre, skattecentre og banker) kan ophæves af DanID, såfremt registreringsenhederne ikke lever op til kravene heri.

Jeg henholder mig således til min besvarelse af spørgsmål 16 og 17 samt den af IT- og Telestyrelsen indhentede udtalelse fra DanID om praksis i forhold til kontrol med bankerne som registreringsenheder.