JUSTITSMINISTERIET
Lovafdelingen

Folketinget
Udvalget for Videnskab og Teknologi
Christiansborg
1240 København K

Dato: 22. oktober 2008
Kontor: Strafferetskontoret
Sagsnr.: 2008-792-0674
Dok.: RAJ40725

Hermed sendes besvarelse af spørgsmål nr. 219 (Alm. del), som Udvalget for Videnskab og Teknologi har stillet til justitsministeren den 19. september 2008.

Brian Mikkelsen

/

Lars Hjortnæs

Slotsholmsgade 10
1216 København K.

Telefon 7226 8400
Telefax 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 219 fra Udvalget for Videnskab og Teknologi (Alm. del):

> ”Vil ministeren oplyse, under hvilke omstændigheder politiet kan anvende borgernes nye digitale signaturer?”

Svar:

Justitsministeriet har til brug for besvarelsen af spørgsmålet indhentet en udtalelse fra IT- og Telestyrelsen, der har oplyst følgende:

> ”DanID, der er valgt som leverandør af den nye digitale signatur, har på IT- og Telestyrelsens foranledning oplyst følgende:
>
> > ”Indledningsvis skal det bemærkes, at fastlæggelsen af løsningens endelige tekniske udformning og design ikke er afsluttet. Det ligger dog allerede fast, at den nye digitale signatur fra DanID vil blive tilbudt i to forskellige udgaver:
> >
> > 1. Digital signatur centralt placeret på en signaturserver hos certificeringscentret (DanID)
> > 2. Digital signatur placeret på en elektronisk enhed, der opbevares hos borgeren.
> >
> > *Ad 1.*
> > De centralt opbevarede digitale signaturer vil blive sikret mod misbrug gennem tekniske og proceduremæssige sikkerhedsforanstaltninger, der er underlagt intern og ekstern revision samt krav til certificering fra IT- og Telestyrelsen.
> >
> > Borgerne skal angive et brugernavn, en personlig unik kode og en engangskode fra et personligt nøglekort (dvs. et plastikkort med fortrykte engangskoder), hver gang signaturen skal anvendes. Den personlige unikke kode kendes kun af borgeren, og det vil ikke umiddelbart være teknisk muligt for DanID at genskabe eller fremfinde borgerens personlige kode.
> >
> > Borgerne vil kunne tilvælge en funktion, hvor signaturen desuden kan anvendes til kryptering af data og mails. Når denne funktion anvendes af borgerne, vil det ligeledes ikke umiddelbart være teknisk muligt for DanID at genskabe nøglen til dekryptering af borgerens krypterede data eller mails.
> >
> > Så længe borgeren holder sin personlige unikke kode hemmelig, vil uautoriserede således ikke kunne anvende borgerens digitale signatur eller dekrypteringsnøgle bortset

fra i tilfælde af, at der er utilsigtede sårbarheder i systemet eller de generelle krypteringsalgoritmer kan knækkes.

Det bemærkes, at hvis DanID ved lov eller en dommerkendelse blev tilpligtet at skabe adgang til anvendelse af en borgers digitale signatur, ville DanID ved at omgå de etablerede tekniske og proceduremæssige sikkerhedsforanstaltninger gennem modificering af den etablerede løsning kunne muliggøre afluring af borgerens personlige kode, som efterfølgende kan anvendes til aktivering af borgerens digitale signatur eller dekrypteringsnøgle.

Ad 2.
Borgerens digitale signatur vil i denne udgave være genereret og placeret på en særlig elektronisk enhed (f.eks. et smartcard eller mobiltelefonens SIM-kort), der opbevares af borgeren. Anvendelse af signaturen på den elektroniske enhed vil kræve, at borgeren angiver en personlig kode (PIN-kode).

Signaturen vil både kunne anvendes til signering/logon og til kryptering af data og mails. DanID eller andre har ikke mulighed for at få adgang til anvendelse af signaturen eller genskabelse af dekrypteringsnøglen.

Så længe borgeren holder sin personlige kode hemmelig, vil uautoriserede således ikke kunne anvende borgerens digitale signatur eller dekrypteringsnøgle bortset fra i tilfælde af, at der er utilsigtede sårbarheder i systemet eller de generelle krypteringsalgoritmer kan knækkes."

IT- og Telestyrelsens konklusion på DanID's redegørelse i relation til spørgsmål nr. 219-221 fra Udvalget for Videnskab og Teknologi er, at det ikke umiddelbart vil være teknisk muligt for DanID at få adgang til at anvende borgernes digitale signatur til signering eller logon på it-systemer eller dekryptering af data og mails uden borgerens aktive medvirken, medmindre der er utilsigtede sårbarheder i systemet eller de generelle krypteringsalgoritmer kan knækkes eller løsningen modificeres som beskrevet ovenfor."

Det fremgår af IT- og Telestyrelsens udtalelse, at hvis borgeren selv opbevarer sin digitale signatur, vil DanID med forbehold for utilsigtede sårbarheder i systemet mv. ikke have teknisk mulighed for at anvende borgerens digitale signatur eller dekrypteringsnøgle. I denne situation vil politiet derfor ikke ved henvendelse til DanID kunne få adgang til den digitale signatur eller dekrypteringsnøgle.

Det fremgår endvidere af IT- og Telestyrelsens udtalelse, at hvis borgeren får opbevaret sin digitale signatur hos DanID, vil DanID med forbehold for utilsigtede sårbarheder i systemet mv. ikke umiddelbart have

teknisk mulighed for at anvende borgerens digitale signatur eller dekrypteringsnøgle. Det vil dog i princippet være teknisk muligt gennem en modificering af den tekniske løsning at "aflure" borgerens personlige kode og dermed få adgang til borgerens digitale signatur og dekrypteringsnøgle. I denne situation vil politiet således i princippet kunne have teknisk mulighed for gennem DanID at få kendskab til borgerens digitale signatur og dekrypteringsnøgle.

Hvis politiet som led i efterforskningen af en straffesag på den beskrevne måde ønsker at få adgang til en persons digitale signatur eller dekrypteringsnøgle, vil der efter Justitsministeriets opfattelse være tale om dataaflæsning, der i retsplejeloven er defineret som "aflæsning af ikke offentligt tilgængelige oplysninger i et informationssystem ved hjælp af programmer eller andet udstyr".

Betingelserne for dataaflæsning fremgår af retsplejelovens § 791 b. Det kræves navnlig, at 1) der er bestemte grunde til at antage, at informationssystemet anvendes af en mistænkt i forbindelse med planlagt eller begået kriminalitet som nævnt i nr. 3, 2) indgrebet må antages at være af afgørende betydning for efterforskningen, og 3) efterforskningen angår en lovovertrædelse, som efter loven kan straffes med fængsel i 6 år eller derover eller en forsætlig overtrædelse af straffelovens kapitel 12 eller 13 (sager om terrorisme mv.).

Afgørelse om dataaflæsning træffes af retten ved kendelse, jf. retsplejelovens § 791 b, stk. 3. Såfremt indgrebets øjemed ville forspildes, dersom retskendelse skulle afventes, kan politiet træffe beslutning om at foretage indgrebet. I så fald skal politiet snarest muligt og senest inden 24 timer fra indgrebets iværksættelse forelægge sagen for retten. Retten afgør ved kendelse, om indgrebet kan godkendes.

Det må afgøres efter de almindelige regler og principper for politiets efterforskning mv., i hvilket omfang politiet har adgang til at anvende en persons digitale signatur til f.eks. at logge på en hjemmeside eller til at anvende en persons dekrypteringsnøgle til at dekryptere en meddelelse, som politiet er i besiddelse af.

Hvis politiet f.eks. som led i efterforskningen af en straffesag i overensstemmelse med retsplejelovens regler om f.eks. ransagning og beslaglæggelse eller indgreb i meddelelseshemmeligheden er kommet i besiddelse af en krypteret meddelelse, kan politiet efter Justitsministeriets op-

fattelse gøre brug af tilgængelige tekniske muligheder for at dekryptere meddelelsen, herunder anvende en dekrypteringsnøgle, som politiet har skaffet sig adgang til i overensstemmelse med retsplejelovens regler om dataaflæsning, jf. ovenfor.

Med hensyn til politiets adgang til at logge på hjemmesider ved at anvende en persons digitale signatur bemærkes, at dette vil afhænge af, hvilke efterforskningskridt mv. politiet ønsker at foretage i den konkrete situation. I en række tilfælde vil der formentlig kunne være tale om dataaflæsning efter retsplejelovens § 791 b, hvilket forudsætter, at de ovenfor beskrevne betingelser er opfyldt. Det bemærkes i den forbindelse, at det formentlig ofte vil være mere nærliggende at pålægge indehaveren af den pågældende hjemmeside at udlevere oplysningerne til politiet efter retsplejelovens regler om edition (dvs. pålæg om at forevise eller udlevere genstande, herunder oplysninger der er lagret i et informationssystem). Afgørelse om edition træffes af retten ved kendelse, medmindre øjemedet ville forspildes, hvis retskendelse skulle afventes, jf. retsplejelovens § 806, stk. 2 og 3.