JUSTITSMINISTERIET
Lovafdelingen

Folketinget
Retsudvalget
Christiansborg
1240 København K

Dato: 20. oktober 2009
Kontor: Formueretskontoret
Sagsnr.: 2009-792-1040
Dok.: RLM40335

Hermed sendes besvarelse af spørgsmål nr. 1278 (Alm. del), som Folketingets Retsudvalg har stillet til justitsministeren den 18. september 2009. Spørgsmålet er stillet efter ønske fra Peter Skaarup (DF).

Brian Mikkelsen

/

Lars Hjortnæs

Slotsholmsgade 10
1216 København K.

Telefon 7226 8400
Telefax 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 1278 fra Folketingets Retsudvalg (Alm. del):

> ”Ministeren bedes kommentere henvendelserne omdelt som REU alm. del - bilag 655 og 699 og i forlængelse heraf redegøre for, om der er grundlag for de bekymringer ved den digitale tinglysning, som henvendelserne giver udtryk for både i relation til sikkerheden ved digitalsignatur og i relation til visse grupper af borgere.”

Svar:

I advokat Olav Willadsens henvendelse af 29. juli 2009 til Folketingets Retsudvalg (alm. del – bilag 655) adresseres de samme spørgsmål og betænkeligheder ved digital tinglysning, som også dannede grundlag for advokatens brev af 16. juli 2009 til Folketingets Retsudvalg (alm. del – bilag 703).

Justitsministeren har ved besvarelse af spørgsmål nr. 1194 (alm. del) fra Folketingets Retsudvalg kommenteret advokat Olav Willadsens henvendelse af 16. juli 2009, og der henvises derfor til besvarelsen af 28. september 2009 af dette spørgsmål.

For så vidt angår advokat Olav Willadsens bemærkning i henvendelsen af 29. juli 2009 til Folketingets Retsudvalg vedrørende det forhold, at meddelelser fra Tinglysningsretten udfærdiges på dansk, bemærkes det, at det følger af retsplejelovens § 149, stk. 1, 1. pkt., at retssproget her i landet er dansk.

I henvendelsen omdelt som bilag 699 (alm. del), anføres det, at den nuværende digitale signatur, som kan anvendes ved anmeldelse af dokumenter til tinglysning, ikke har den nødvendige sikkerhed.

Til brug for besvarelsen af denne del af spørgsmålet har Justitsministeriet anmodet Ministeriet for Videnskab, Teknologi og Udvikling om en udtalelse om de sikkerhedsmæssige aspekter af den nuværende og den fremtidige digitale signatur.

Justitsministeriet modtog den 7. oktober 2009 en udtalelse fra Videnskabsministeriet. I udtalelsen behandles de sikkerhedsmæssige aspekter ved udstedelse af både person- og medarbejdersignaturer, idet begge disse typer signaturer kan anvendes i det digitale tinglysningssystem.

Af udtalelsen fremgår følgende vedrørende de sikkerhedsmæssige aspekter af den nuværende digitale signatur:

> ”**Personsignatur**
> En digital personsignatur udstedes i dag via en online registreringsprocedure, hvor brugeren indtaster sit cpr-nummer, sit postnummer og sin e-mail adresse. Certificeringscentret (DanID), der har ansvaret for udstedelsen af den digitale signatur indhenter i den forbindelse oplysninger om brugerens navn og folkeregisteradresse i cpr-registeret. Det valideres, om det af brugeren angivne postnummer svarer til folkeregisteradressens postnummer, der er registreret hos CPR. Kun ved sammenfald kan bestillingen gennemføres. DanID udsender herefter et pinkode-brev til brugerens folkeregisteradresse og via en anden kanal – den af brugeren angivne e-mailadresse – en installationsmail. Brugeren kan først installere den digitale signatur, når begge informationer er modtaget. Hermed kontrolleres, at både postadressen og e-mail-adressen hører sammen med modtageren.
>
> Sikkerheden i udsendelsen af pinkode-brevet baseres i dag på cpr-registerets oplysninger og Post Danmarks evne til rettidigt og sikkert at omdele posten. Folkeregisteradressen anvendes i dag bredt af såvel den offentlige som private sektor som en sikker modtager af fortrolig brevveksling.
>
> Videnskabsministeriet kan bemærke, at den omtalte registreringsprocedure er blevet forelagt Datatilsynet, inden den er blevet implementeret. Datatilsynet har fundet proceduren tilstrækkelig sikker til kommunikation og udlevering af følsomme oplysninger omfattet af persondataloven.
>
> Digitale personsignaturer udstedes i dag som en softwarebaseret løsning, hvor den private nøgle gemmes som en krypteret fil på brugerens pc. Filen er beskyttet af en personlig kode, som brugeren selv vælger i forbindelse med installationen. Koden skal leve op til nogle krav, der sikrer den mod kompromittering. Sikkerheden omkring løsningen afhænger af, om uvedkommende får kendskab til brugerens personlige kode og den krypterede fil på brugerens pc.
>
> Det er brugerens ansvar at sørge for, at den personlige kode ikke kommer uvedkommende til kendskab, og at den private nøgle opbevares sikkert og pålideligt på pc’en. Brugeren skal således sikre, at computermiljøet er opdateret med de seneste sikkerhedsopdateringer og er udstyret med virus- og firewallbeskyttelsessoftware. Betingelserne for anvendelse af den digitale signatur er regulerede i DanID’s vilkår for anvendelse af OCES-certifikater, som brugeren accepterer i forbindelse med bestillingen.

Generelt kan det i forhold til systemets samlede sikkerhed bemærkes, at DanID – ligesom eventuelle andre certificeringscentre, der måtte ønske at udstede digitale signaturer under OCES-standarden – er underlagt OCES-certifikatpolitikkernes krav til infrastruktur og sikkerhed. Alle procedurer hos certificeringscenteret er i overensstemmelse med certifikatpolitikkernes bestemmelser herom underlagt revision af ekstern statsautoriseret revisor. Revisor skal kontrollere, at den samlede sikkerhed hos certificeringscenteret lever op til certifikatpolitikkens krav og skal årligt afgive erklæring herom til IT- og Telestyrelsen.

Medarbejdersignatur

En virksomhed, der ønsker digitale medarbejdersignaturer, skal indgå en aftale med DanID om at få oprettet en såkaldt LRA (Lokal Registrerings Autoritet).

I forbindelse med bestillingen skal virksomheden angive cvr-nummer på virksomheden, navn og e-mail adresse på virksomhedens "Lokaladministrator" samt navn på den tegningsberettigede person fra virksomhedens ledelse, der underskriver bestillingen. Lokaladministratoren bemyndiges til at bestille, ændre og nedlægge medarbejdersignaturer på vegne af virksomheden. I forbindelse med bestillingen indhenter DanID oplysninger om virksomheden i cvr-registeret. I bestillingsprocessen skal aftalen udskrives på papir, underskrives af den tegningsberettigede og efterfølgende indsendes til DanID. DanID foretager en manuel behandling af bestillingen, hvor blandt andet cvr-oplysningerne samt den tegningsberettigedes fysiske underskrift kontrolleres.

Når bestillingen er godkendt udsender DanID et pinkode-brev til virksomhedens postadresse adresseret til den, der er angivet som bemyndiget (Lokaladministrator). Samtidigt udsendes en installations-e-mail til den angivne e-mail-adresse. Lokaladministratoren kan først installere den digitale signatur, når begge informationer er modtaget. Hermed kontrolleres, at både postadressen og e-mailadressen hører sammen med modtageren.

Sikkerheden i udsendelsen af pinkode-brevet baseres i dag på cvr-registerets oplysninger og Post Danmarks evne til rettidigt og sikkert at omdele posten.

Når aftalen er på plads, initieres udstedelse af en digital medarbejdersignatur af den bemyndigede via et online registreringsmodul. Lokaladministratoren skal først installere sin egen digitale signatur og har herefter mulighed for via LRA-modulet at bestille, ændre og nedlægge medarbejdersignaturer for medarbejdere i virksomheden. Udstedelse af medarbejdersignaturer til andre medarbejdere i virksomheden fore-

går på samme måde som for lokaladministratoren, hvor der udsendes et pinkode-brev og en installationsmail til medarbejderen.

I relation til anvendelse af medarbejdersignaturer, hvor det er afgørende at kunne knytte ansvar til en entydigt identificeret person i virksomheden – som for eksempel digital tinglysning – er det muligt at bestille en særlig type medarbejdersignaturer, hvor medarbejderens cpr-nummer bliver knyttet til medarbejdersignaturen.

Medarbejdersignaturer udstedes som en softwarebaseret løsning. Løsningen er teknisk den samme, som beskrevet ovenfor. Med hensyn til sikkerheden på medarbejderens pc, er det virksomhedens ansvar via it-sikkerhedspolitikker og procedurer at opretholde den fornødne sikkerhed."

For så vidt angår den fremtidige digitale signatur bemærker Videnskabsministeriet i udtalelsen, at implementeringen heraf ikke er endeligt afsluttet, og at der stadig kan ske mindre tilpasninger i udformningen af den endelige løsning. Endvidere oplyses det, at Datatilsynet endnu ikke har afsluttet sin vurdering af de nye registreringsprocedurer. Vedrørende de sikkerhedsmæssige aspekter af den fremtidige digitale signatur anføres herefter følgende i udtalelsen:

"**Personsignatur**
Med hensyn til registreringsprocedurerne kan det oplyses, at sikkerheden er hævet i forhold til den eksisterende løsning. Som ekstra sikkerhed skal brugeren i forbindelse med online bestilling foruden cpr-nummeret angive pas- eller kørekortnummer. I forbindelse med aktivering skal brugeren indtaste såvel midlertidig adgangskode som engangskode fra nøglekort, som begge er udsendt til folkeregisteradressen ved to separate forsendelser. Bestillingen kan kun gennemføres, hvis pas- eller kørekort er udstedt til rette cpr-nummer og kortet er gyldigt.

De fastsatte registreringsprocedurer 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 fremtidige løsning vil den digitale personsignatur ikke være en softwarebaseret løsning, hvor sikkerheden alene er afhængig af brugerens pc. Løsningen vil blive baseret på en såkaldt ægte to-faktor sikkerhedsløsning, hvor adgang til signaturen vil være beskyttet af en personlig kode (noget man ved) og en engangskode på et nøglekort (noget man har). Da brugerens digitale signatur ikke længere ligger på brugerens

pc, men er sikkert opbevaret i kryptografiske moduler på en central server, bliver det lettere at fastholde et højt sikkerhedsniveau frem for, når signaturen ligger på den enkelte pc.

Medarbejdersignatur
I den fremtidige løsning på erhvervsområdet forventes der ikke foretaget tilsvarende ændringer som for personsignaturer, hverken på registreringsdelen eller den tekniske udformning af løsningen. Bestillingen af medarbejdersignaturer vil også fremover foregå via LRA-modulet, og medarbejdersignaturer forventes også fremover i overvejende grad at være softwarebaserede signaturer. Det vil dog også blive muligt at bestille medarbejdersignaturer, der baserer sig på to-faktor sikkerhed."

Vedrørende sikkerheden ved den digitale signatur i forhold digital tinglysning har Videnskabsministeriet endvidere anført følgende:

"I relation til sikkerheden omkring den digitale tinglysning kan Videnskabsministeriet henvise til rapport af 21. februar 2005 udarbejdet af konsulenthuset Deloitte i forbindelse med udvalgsarbejdet om digital tinglysning. Rapporten konkluderer, at ved anvendelse af en digital signatur, baseret på OCES-certifikater, har en digitaliseret og automatiseret tinglysning et sikkerhedsniveau, som er fuldt på højde med sikkerhedsniveauet for den papirbaserede tinglysning.

Da sikkerhedsniveauet for den fremtidige digitale signatur er hævet i forhold til den eksisterende løsning, vurderer Videnskabsministeriet, at rapportens konklusion også er gældende for den fremtidige digitale signaturløsning."

Vedrørende sikkerheden ved anvendelsen af den nuværende digitale signatur har Videnskabsministeriet endvidere supplerende oplyst, at der ikke er kendte eksempler på, at det er muligt at bryde de koder, der sikrer autenticiteten og integriteten af et digitalt dokument, der er påført en digital OCES-signatur.

Der henvises i øvrigt til vedlagte besvarelse af spørgsmål nr. 8 fra Folketingets Retsudvalg vedrørende lovforslag nr. L 199 (folketingsåret 2005-06), som vedrører spørgsmålet om sikkerheden ved den nuværende digitale signatur.