Fra: Thue Janus Kristensen
Date:søn 17. nov. 2019
Subject:Tvangsfuldbyrdelse på grundlag af digitale gældsbreve

Hej Retsordførere.

Som i forhåbentligt ved, så er der et åbent sikkerhedshul i NemID. Jeg har (efter at have fortalt Digitaliseringstyrelsen at jeg at jeg kunne få enhver professor i kryptologi til at sige at NemID er usikker) fået følgende to udtalelser fra Danmarks to mest prominente kryptologer. Begge er med tilladelse, og givet i kontekst af min artikel NemID er ikke kryptologisk sikker - og myndighederne er ligeglade:

Jeg har fremlagt dette for professor Lars R. Knudsen, som er en internationalt anerkendt kryptolog og leder af DTU's kryptologi-gruppe. Knudsen er enig i at NemID har et reelt sikkerhedshul, som ikke findes i andre browser-baserede single sign-on systemer, såsom Google's, og han ”finder det besynderligt at Nets ignorerer dette problem”

Når man beder folk om at taste et password på en webside, så bør man bruge de teknologiske muligheder der findes for at bekræfte identiteten af den webside, der får udleveret passwordet. Det vil i praksis sige TLS som findes i alle moderne browsere. Løsningen er på ingen måde perfekt eller ubrydelig, men klart bedre end ingenting. Det er derfor svært at forstå hvorfor NemID ikke bruger den mulighed. -Ivan Bjerre Damgård

Et særlig retsligt interessant punkt er brugen af NemID som digital signatur. NemID opfylder åbenlyst ikke de funktionelle krav til en digital signatur (i eIDAS kaldet en "avanceret elektronisk signatur"; NemID opfylder ikke eIDAS artikel 26 punkt c)). med andre ord er der ikke nogen meningsfuld teknisk garanti om at en digitalt signeret kontrakt er godkendt af "underskriveren"; hvis en retsinstans fejlagtigt tror at der er en sådan meningsfuld teknisk garanti, så er der muligheden for justitsmord (jeg får associationer til "Teledataskandale er ikke it-systemernes skyld").

Mit spørgsmål er så om de danske fogedretter dømmer ud fra den forkerte antagelse at NemID er en digital signatur. Jeg spurgte Domstolsstyrelsen om dette i maj, men har endnu ikke fået noget svar. Justitsministeriets chefkonsulent Mads Jespersen har "bragt din henvendelse af 24. maj 2019 i erindring" for Domsstolsstyrelsen (vedhæftet), men det har tilsyneladende ikke hjulpet. En yderligere henvendelse til Justitsministeriet i september (vedhæftet) har jeg ikke fået noget svar på; jeg ved ikke om min henvendelse er blevet sendt videre til Justitsministeren.

Så min forespørgsel til retsordførene: **Vil en af jer stille paragraf 20 spørgsmålet "Tvangsfuldbyrder fogedretterne på grundlag af digitale gældsbreve signeret med NemID+OCES?"**

Se min henvendelse til Domsstolsstyrelsen nedenfor for flere detaljer. I er selvfølgelig meget velkomne til at stille opfølgende spørgsmål.

Hilsen
Thue Janus Kristensen

---------- Forwarded message ---------
Fra: Thue Janus Kristensen
Date: fre. 24. maj 2019
Subject: Tvangsfuldbyrdelse på grundlag af digitale gældsbreve
To: <post@domstolsstyrelsen.dk>

Hej Domstolsstyrelsen

Spørgsmål: Tvangsfuldbyrder fogedretterne på grundlag af digitale gældsbreve signeret med NemID+OCES?

Baggrund: Jeg arbejder på en kryptologisk-juridisk analyse af NemID.

Som i forhåbentligt ved, så er der et åbent sikkerhedshul i NemID. Jeg har (efter at have fortalt Digitaliseringstyrelsen at jeg at jeg kunne få enhver professor i kryptologi til at sige at NemID er usikker) fået følgende to udtalelser fra Danmarks to mest prominente kryptologer. Begge er med tilladelse, og givet i kontekst af min artikel NemID er ikke kryptologisk sikker - og myndighederne er ligeglade:

Jeg har fremlagt dette for professor Lars R. Knudsen, som er en internationalt anerkendt kryptolog og leder af DTU's kryptologi-gruppe. Knudsen er enig i at NemID har et reelt sikkerhedshul, som ikke findes i andre browser-baserede single sign-on systemer, såsom Google's, og han ”finder det besynderligt at Nets ignorerer dette problem”

Når man beder folk om at taste et password på en webside, så bør man bruge de teknologiske muligheder der findes for at bekræfte identiteten af den webside, der får udleveret passwordet. Det vil i praksis sige TLS som findes i alle moderne browsere. Løsningen er på ingen måde perfekt eller ubrydelig, men klart bedre end ingenting. Det er derfor svært at forstå hvorfor NemID ikke bruger den mulighed. -Ivan Bjerre Damgård

Mens dette gør at brug af NemID bryder diverse love, så er det jo specifikt relevant for jer, at sikkerhedshullet gør at NemID+OCES ikke er en digital signatur. At NemID+OCES ikke er en digital signatur er ret uheldigt, da der er krav om digital signatur i den kryptologiske forstand i lovgivningen. For eksempel var der jo relativt for nyligt sagen om tvangsfuldbyrdelse af gældsbreve, hvor Fogedretten ikke måtte tvangsfuldbyrde på baggrund af digitale dokumenter underskrevet med NemID+OCES. Så blev loven ændret, og mens lovteksten i sig selv er unødvendig uklar, så fremgår det af lovbemærkningerne at loven kræver kryptologisk sikker digital signatur med et PKI-system, dvs kryptologisk uafviselighed.

For lige at minde om konteksten, så er den centrale egenskab ved en digital signatur *uafviselighed*. Her er definitionen fra side 18 i Henrik Udsen's *Den digitale signatur – ansvarsspørgsmål:*

Uafviselighed (engelsk: non-repudiation) kan defineres som informationsmodtagerens sikkerhed for, at den person, der har vedstået sig indholdet, ikke efterfølgende kan fragå sig denne vedståelse; eller med andre ord informationsmodtagerens sikkerhed for, at det efterfølgende kan bevises, at modparten har vedstået sig indholdet.

I en normal digital signatur så opbevarer jeg jo selv min privatnøgle, og har ansvar for at holde den hemmelig. Denne hemmelighed+PKI-systemets egenskaber giver min digitale signatur den kryptologiske egenskab uafviselighed. Mens for NemID er min privatnøgle opbevaret af Nets, og jeg har jeg i stedet for en hemmelig privatnøgle mit hemmelige NemID-password og engangskoder. Når jeg vil underskrive noget (eller logge ind), så skal jeg kommunikere password+engangskode til software kontrolleret af Nets, og denne kommunikation er som Damgård skriver ovenfor kryptologisk beskyttet af "ingenting". Da disse passwords som en konsekvens af Net's design ikke er beskyttet af en kryptologisk garanti når jeg bruger dem, er de ikke hemmelige, og en "underskrift" dannet af NemID+OCES har derfor åbenlyst ikke egenskaben uafviselighed (eller autentifikation, for den sags skyld), og er derfor ikke en digital signatur. Bemærk at der er lavet demonstrationer af angrebet.

Digitaliseringstyrelsen har sagt at hvadsomhelst kan være en digital signatur, tilsyneladende også ting som ikke er kryptologisk sikre (der er noget begrebsforvirring, i det "digital signatur" nogen gange af folk som ikke aner hvad de taler om bruges om ikke-kryptologiske konstruktioner). Men lovbemærkningerne til loven stiller altså krav om at en konstruktion som bruges til tvangsfuldbyrdelse skal være kryptologisk sikker. Og rent logisk og rettighedsmæssigt, efter noget analyse, er det åbenlyst at kun en digital signatur med en meningsfuld kryptologisk garanti giver mening.

Hilsen Thue Janus Kristensen

PS: Digitaliseringsstyrelsen har sagt at NemID med NemID-app er mere sikker. Hvis i er interesserede i lovlighed og sikkerhed, så arbejder jeg på et lille foredrag om de åbne sikkerhedshuller i NemID-appen og de love brug af denne usikre løsning bryder.