DIGITALISERINGSSTYRELSEN

Bilag 1

6. februar 2020

Digitaliseringsstyrelsens vurdering af de beskrevne problematikker i SOU-spm. 195 af 17. december 2019

Til besvarelsen af Social- og Indenrigsudvalgets spørgsmål nr. 195 af 17. december 2019 fremgår herunder en beskrivelse af brugen af kryptering af datakommunikation i regi af NemID, samt en redegørelse for vurderingen af, hvorledes NemID kan kategoriseres som en avanceret elektronisk signatur med deraf følgende retsvirkning.

TLS er en protokol, som muliggør kryptering af forbindelsen mellem en klient og en server. Når forbindelsen til en hjemmeside er sikret med TLS, vil hjemmesiden typisk i browseren vise "https:" samt en hængelås i adresselinjen, som gør det tydeligt for brugerne, at hjemmesidens identitet er valid, og at kommunikationen krypteres.

NemID-oplysninger, der indtastes i NemID-klienten, er netop via implementering af TLS sikret af en sådan tunnelløsning til NemID-backenden, hvor der altid benyttes TLS-krypteret kommunikation og certifikat i kommunikationen med NemID-backenden. Yderligere kryptografiske teknikker sikrer adgangskoder og andre sensitive oplysninger. Disse bidrager til det høje niveau af sikkerhed i løsningen.

For langt størstedelen af offentlige selvbetjeningsløsninger, finder login sted via NemLog-in, som er en fællesoffentlig login-løsning. NemLog-in anvender TLS-certifikater, og brugerens kommunikationen er derved TLS-krypteret, uafhængigt af hvilken selvbetjeningsløsning brugeren benytter, og om denne anvender TLS. Dette bidrager yderligere til et højt sikkerhedsniveau. Langt de fleste private tjenesteudbydere, der tilbyder login med NemID, anvender også TLS-certifikater, uden at der dog stilles specifikt krav herom.

HTTPS og TLS kan have en effekt, hvis borgeren er opmærksom på dette. Det forudsætter dog, at borgeren er opmærksom på hængelåssymbolet, som borgeren præsenteres for ved hjemmesidens adressefelt. Det er vurderingen, at synligheden af en hængelås (TLS) i browseren ikke kan betragtes som en sikkerhedsgaranti, da kriminelle kan anskaffe TLS-certifikater til falske og kompromitterede hjemmesider. TLS i sig selv sikrer således ikke, at falske hjemmesider kan undgås.

Som i andre tilfælde hvor it-kriminelle udvikler falske sites, fx som led i forsøg på svindel gennem såkaldte phishing-angreb, kan det være en udfordring, hvis kriminelle laver noget, der visuelt kunne ligne en NemID login-klient på et illegitimt

website. Sådanne sites kan af de it-kriminelle sikres med HTTPS som led i at forsøge at skabe tillid til det falske site.

Digitaliseringsstyrelsen ser hele tiden på at styrke sikkerheden. Derfor ses der i den nye MitID-løsning bl.a. på at gøre det nemmere for brugere at tjekke, om en given hjemmeside er legitim. Med NemID i dag er det de enkelte tjenesteudbydere, der viser login-siden. Fremover med MitID vil der være en række certificerede brokere, der viser klienten. Offentlige og private tjenesteudbydere skal i fremtiden tilsluttes via en sådan broker, før de kan tilbyde log-in med MitID til deres brugere. Derfor stilles der i den nye MitID-løsning skærpede sikkerhedskrav til brokere, og de skal certificeres i henhold til en række krav. Dermed vil det blive nemmere at tjekke, om en given hjemmeside er legitim.

I forhold til anvendelsen af NemID til at underskrive dokumenter eller kontrakter, er det Digitaliseringsstyrelsens vurdering, at relevante krav følges. Det bemærkes, at det af eIDAS-forordningen fremgår, at et dokument med en elektronisk signatur, fx NemID, ikke må nægtes retsvirkning, alene af den grund, at den er i elektronisk form, eller at den ikke opfylder alle kravene til en kvalificeret elektronisk signatur. Det, der er afgørende for retsvirkning, vil være, om det er muligt at bevise ægtheden af signaturen, om den er elektronisk eller skriftlig, og rigtigheden af indholdet i dokumentet, uanset om signaturen er elektronisk eller skriftlig.

Desuden bemærkes det, at NemID baserer sig på en teknologi kaldet Public Key Infrastructure (PKI). I PKI er det et afgørende element, at brugeren er den eneste, der har kontrol over den private nøgle. I NemID er brugerens private nøgle opbevaret på en central signaturserver hos Nets, og generering, og anvendelse af den private nøgle kan kun foregå i specielle sikrede kryptografiske hardwaremoduler under brugerens fulde kontrol. Nets har i sin tid fået lavet en uvildig juridisk vurdering, der fastslår, at den centrale signaturløsning ikke er i strid med den tidligere Lov om elektronisk signatur.

Ligeledes fremgår det i den nuværende eIDAS-forordning, at en central signaturserverløsning som NemID er en fuldt kompatibel signaturløsning. Dertil bemærkes, at borgere kan vælge løsningen "NemID på hardware", hvor slutbrugeren kan erhverve særlig hardware til selv at generere og opbevare den private nøgle, der ligger bag den offentlige digitale signatur (denne løsningsmulighed foreligger ikke for bankernes brug af NemID). Denne løsning er relevant for de få brugere, der ønsker at undgå opbevaring på den centrale signaturserver.

NemID kan med henvisning til eIDAS-forordningen således teknisk og funktionelt kategoriseres som en avanceret elektronisk signatur med deraf følgende retsvirkning.