DIGITAL SUNDHED
SAMMENHÆNGENDE DIGITAL SUNDHED I DANMARK

Islands Brygge 67
DK-2300 København S
www.sdsd.dk

EAD / 25. Januar 2008

Høringssvar: Signatur- og systembevis

1. Indledning

Digital Sundhed takker for muligheden for at afgive høringssvar vedrørende vejledning om Signatur- og systembevis. Generelt finder Digital Sundhed, at materialet har en høj kvalitet. Specielt giver materialet en god teoretisk introduktion til de mange modeller for sikring af signatur- og systembeviser. Det teoretiske niveau er desværre også svagheden ved det foreliggende materiale, idet det bærer præg af mere at være en gennemgang af forskellige muligheder, frem for at vejlede læseren i, hvilke modeller og midler der bør bringes i anvendelse, når forskellige kriterier er opfyldt.

2. Relevans og nødvendighed

Digital Sundhed finder materialet både relevant og nødvendigt. Sikring af signaturbevis er en problemstilling, der skal arbejdes med i forbindelse med opbygningen af sikkerhedsarkitekturen for en kommende national infrastruktur for udveksling af sundhedsdata. Der er allerede arbejdet med en identitetsservice[1] (Secure Token Service, STS) der opbevarer de akkreditiver (digital signatur), som en bruger har præsenteret, for at få udstedt et security token. Fremover skal der arbejdes med services vedr. afgivelse- / nægtelse af samtykke, bemyndigelser samt håndtering af den i sundhedsloven angivne "værdispringsregel" (tiltvungen adgang til data). Alt sammen områder, hvor signaturer og systembeviser har relevans.

3. Afgrænsning eller mangel

Dokumentet behandler kun modtagers muligheder for at bevise, at der er modtaget et dokument fra afsender. Man burde måske nævne sikring af bevis for at noget er udført eller afsendt af en bestemt signerende person eller myndighed. I tilfælde af at en handling skal være udført eller en meddelelse afgivet inden en frist, kan dette være af stor betydning. Dette kan i nogle tilfælde gøres med signerede kvitteringer, men der er mange situationer, hvor dette ikke er muligt eller tilstrækkeligt. F.eks. hvis modtager ikke kan svare inden for kort tid.

4. Specifikke kommentarer

Mangel på afsnitsnumre i materialet gør det lidt svært præcist at udpege passager. I det følgende benyttes derfor overskrifter, bullet-numre etc. for at udpege sætninger.

Model 1 første afsnit linie 2: "evt." bør muligvis slettes. Det tilhørende certifikat, eller alternativt en entydig reference til certifikatet, der gør det muligt at rekvirere certifikatet

[1] Se www.sosi.dk

fra et passende arkiv, bør vel altid gemmes sammen med signaturen, så signaturen kan reproduceres/reverificeres.

Model 1, Ulemper, bullet 1. Det bør måske uddybes at holdbarheden retter sig mod signaturafgiverens mulighed for at påstå, at signaturmodtager har produceret en ny signatur med en beregnet privat nøgle (brud på uafviselighed).

Model 1, Ulemper, bullet 3, under-bullet 2. At inkludere tidsangivelse i det dokument der signeres er en så væsentlig styrkelse at bevisværdien, at det bør trækkes frem. Det fungerer næsten på niveau med en tidsstemplingsservice, da afsenderen jo skriver under på tidsstemplets korrekthed. Det vil i øvrigt også kunne imødegå sammensværgelses scenariet, der er nævnt overfor. Metoden nævnes også under ″Fremtidige modeller″,Model 5, afsnit 2, som værende effektiv i en række situationer.

Model 1, Punkt 1 i listen der starter med ″Tidspunkt for verifikation ...″. Det bør pointeres at tidspunktet skal være i UTC eller alternativt med eksplicit tidszoneangivelse.

Model 2, afsnittet ″Indholdet af et signaturbevis″. Afsnittet giver tre eksempler på, hvad andre projekter eller vejledninger peger på, at et signaturbevis skal indeholde. Hvis materialet skal være en teknisk vejledning, bør det pege mere præcist på, hvilke elementer der bør indgå, såfremt de er tilgængelige i det pågældende system. Hvordan forholder vejledningen sig præcist til det på eDag2 anbefalede?

Afsnittet ″Fremtidige modeller″. Disse modeller er teoretisk interessante, men bør ikke være i den endelige vejledning, med mindre der er konkrete vejledninger for disse fremtidige modeller.
Undtagelsen er den ovenfor nævnte beskrivelse i Model 5, afsnit 2 om brug af tidsstempler i det dokument, der underskrives. Punktet er vigtigt og har intet med fremtid at gøre.

Kapitlet ″Sikring af logfilers integritet″, ″Tilgængelighed″, afsnit 2. Dette bør afvejes mod privacy-hensyn.

Såfremt der skulle være behov for uddybning af ovenstående høringssvar, er IT- og Telestyrelsen meget velkommen til at henvende sig til undertegnede.

Med venlig hilsen

Esben Dalsgaard
Chef IT-arkitekt,
Leder af SDSD's enhed for arkitektur og sikkerhed
Mobil: 25 10 75 08
E-mail: ead@sst.dk