NOTAT

Den 15. december 2014

Sags ID: SAG-2013-07863
Dok.ID: 1951921

ALB@kl.dk
Direkte
Mobil 2939 3723

Weidekampsgade 10
Postboks 3370
2300 København S
Telefon

www.kl.dk

Bilag 6 – opsamling på høringssvar fra netværket til sikkerhedsmodel for sårjournalen

(Bilag til dagsordenpunkt 7, Føderative sikkerhedsmodeller til Sårjournalen og andre nationale it-løsninger på sundhedsområdet)

Lars Nico Høgfeldt, Odense Kommune

Odense Kommune fremsender hermed høringssvar. Odense Kommunes høringssvar indeholder dels en generel indledning og bemærkninger og dels specifikke bemærkninger.

Generel indledning og bemærkninger

Odense Kommune anser høringen som relevant i forhold til sikring af, at det kommunale sundhedspersonale fortsat vil få mulighed for at tilgå oplysninger i Sårjournal systemet på en sikker måde.

Odense Kommune har selv deltaget med en it-arkitekt i arbejdsgruppen og mener, at dokumentet er gennemarbejdet og tilgodeser kommunale behov i forhold til en ny sikkerhedsmodel.

Det skal dog bemærkes, at dokumentet primært har til formål at beskrive hvorledes at sikkerhedsmodellen kan forbedre og understøtte authentificering af brugere for således at understøtte bl.a. fælles offentlige standarder og rammearkitekturen. Dette betyder dog, at der i dokumentet ikke er behandlet emnet beskedfordeling, som er relevant i forhold til den kommende beskedfordeler støttesystem komponent fra KOMBIT. Der nævnes kort i dokumentet funktionalitet med links i korrespondancebeskeder, men det skal afklares hvorledes at denne funktionalitet nærmere fungere og om det kan understøtte beskedfor-

deling. Ligeledes skal det undersøges om funktionaliteten med beskedfordeling kræver stærk authentification og hvorledes dette håndteres.

Der savnes en generel beskrivelse af indholdet og mulighederne i Sårjournal systemet, evt. blot ved en henvisning til en vejledning som denne fra MedCom http://www.medcom.dk/dwn6336

Scenarierne i kapitel 2 er godt beskrevet, der savnes dog relation til hvilke parter(Regioner, Kommuner eller private) de hver især dækker. Der er ligeledes kort nævnt et scenarie angående adgang fra mobile devices, men det skal undersøges nærmere hvorledes at stærk authentification kan understøttes på en brugervenlig måde på mobile devices.

Der savnes en overordnet konklusion for hvilken model der anbefales, men der nævnes dog at de kan kombineres. Set fra et kommunalt perspektiv, så vil det være modellen beskrevet i afsnit "4.3 Passiv fødereret model" som fortrækkes da denne understøtter Rammearkitekturen og KOMBIT's støttesystem på sikkerhed og vil på sigt også muliggøre borgeradgang. Det skal dog afklares om der gives direkte borgeradgang til systemet eller om borgerne altid skal gå ind via sundhed.dk

Kommunerne skal dog være opmærksomme på, at KOMBIT's støttesystem først vil være tilgængeligt for tilkobling af andre systemer fra år 2017, hvilket betyder at hvis Sårjournal systemet implementerer den nye sikkerhedsmodel i år 2015 skal det sikres, at kommunerne fortsat vil kunne få adgang til løsningen.

Specifikke bemærkninger:

Side 6 afsnit 2.2 Link tilgår sundhedsperson….:

Bemærkninger:

Er en "korrespondancemeddelelse" en mail?

Eller et advis i fagsystemet?

Gerne lidt mere beskrivelse af hvorledes korrespondancemeddelelser tænkes anvendt?

Hvad kræves for anvendelse af disse korrespondancemeddelelser?

Odense kommune ser funktionaliteten med korrespondancemedelelser som vigtig i forhold til de fremadrettede arbejdsgange med Beskedfordeler komponenter i de enkelte domæner, og sikring af en mere effektiv arbejdsgang.

Ligeledes skal der ses på om alle beskeder er så følsomme, at de kræver stærk authentification eller om der sendes beskeder/meddelelser til både medarbej-

dere og borgere som ikke kræver stærk authentification, og dermed kan fx læses nemt på mobile devices.

Side 7 afsnit 1. Anvendelse af Sårjournalen….:

Bemærkning:

Afsnittet hænger ikke sammen med de øvrige afsnit, så er det et separat scenarie som skulle være angivet som afsnit 2.4?

Side 9 øverst:
Der står scenarium 7 og 8.

Bemærkning:
Der må menes scenarium 6 og 7 fra afsnit 2.6 og afsnit 2.7?

Side 9 linie 5, *….at der allerede eksisterer en sikkerhedsmodel.***:**

Bemærkning:
Der må gerne være en henvising til hvor man kan finde de eksisterende sikkerhedsmodeller.

Side 10, linie 3, *... nogle fornuftige veldefinerede rammer.*

Bemærkning:
Ordet *af* bør være et *og* i stedet for.

Side 11 afsnit 3.6 Løsningen må ikke være unødigt svær at administrere:

Bemærkning:
Sidste sætning i afsnittet antyder, at der ikke ønskes opkobling til lokale kommunale IdP/STS løsninger, men at der ønskes opkobling til fælles kommunal knudepunkt, hvilket for kommunerne vil være KOMBIT's støttesystem.

Odense kommune er enig i at opkobling til en fælles kommunal IdP/STS løsning (KOMBIT's løsning), vil medføre mindre administration, men KOMBIT's fælles kommunale IdP/STS vil først kunne anvendes til opkobling af fx Sårjournal systemet fra år 2017, idet at KOMBIT's IdP/STS frem til 2017 er reserveret udelukkende til Monopolsbruds løsningerne(KY, KSP og SAPA).

Dette vil betyde, at hvis NSI indfører denne sikkerhedsmodel for fx Sårjournal systemet i år 2015/2016 så vil det ikke være muligt for de enkelte kommuner at koble sig på Sårjournal systemet via en tilkobling fra deres lokale IdP/STS.

Det skal derfor sikres, at kommunerne fortsat frem imod år 2017, vil enten kunne koble sig på Sårjournal systemet lokalt eller på anden vis kunne tilgå Sårjournal systemet.

Så fra hvornår forventes ændringen af sikkerhedsmodellen for Sårjournal systemet at træde i kraft?

Side 12 linie 4, Modellerne illustreres i deres anvendelse fra en…**:**

Bemærkning:
Er opmærksom på, at modellerne beskrevet i kapitel 4 ikke gensidigt udelukker hinanden, men vil være rigtig godt hvis det i hver modelbeskrivelse fremgik hvilken part(regional, kommunal, privat) at den pågældende model kunne tænkes at anvendes hos eller passe til.

Side 12 afsnittet "Midlertidig accept af lille risiko for…":

Bemærkning
Det er korrekt, at der ikke for kommunerne i dag er etableret hardware sikkerhedsmodul(HSM) løsninger, men HSM er en option i KOMBITs sikkerheds støttesystem, det vil derfor være fornuftigt at stille krav til KOMBIT om at det bliver aktiveret fra starten af i KOMBITS støtte system.

Det er derfor vigtigt, at dette evt. kommende krav om HSM prioriteres og sikres at budskabet om dette HSM krav formidles til KOMBIT. Etablering af HSM er dog en dyr, men sikker løsning, men før implementering skal det analyseres nærmere om indførelse af HSM vil stille yderligere krav til infrastrukturen hos de enkelte 4/5 kommuner, idet mange kommuner måske allerede har eller skal til at investere i infrastruktur til understøttelse af en fødereret sikkerhedsmodel for tilkobling op imod KOMBIT støttesystemerne. En konsekvens af ikke at indføre HSM i KOMBITs løsning fra start kan være, at man skal hen at skifte certificater for alle kommuner senere.

Odense Kommune vil derfor anbefale, at konsekvenserne af HSM analyseres nærmere og at resultatet af en sådan analyse koordineres tæt med KOMBIT's støttesystem løsning.

Side 13 afsnit 4.2 Aktiv SAML login model – Sikker Browseropstart:

Bemærkninger:
Vil dette kun gælde for Regionerne eller vil det også kunne gøres for kommunerne?

Vil understøttelsen af den nye sikkerhedsmodel gøre det muligt ikke at være afhængig af sundhedsdatanettet(SDN), som det ellers er beskrevet sidst i afsnit 4.2 på side 13?

Side 14 midt på siden afsnittet "Sårjournalen har nu….":

Bemærkning:
I parentesen er nævnt "*sundhedsfaglig autorisation*" som egenskab/information om brugeren. Når der ikke køres over sundhedsdatanettet(SDN) hvorledes

sikres det så, at brugerens *"sundhedsfaglige autorisation"* kan valideres og leveres med i SAML-tokenet?

Vil der blive stillet en service til rådighed hvor denne information kan hentes fra uden at kommunerne skal være koblet op på SDN?

Side 15 afsnit 4.3 linie 7 – (IP range eller lignende):

Bemærkning:
For de kommunale aktører skal det undersøges om KOMBIT's støttesystem kan forespørge/levere oplysninger om organisatorisk tilknytning. Oplysninger om organisatorisk tilknytning og hvorledes de kan tilvejebringes bør ligge i aftalen etableret imellem KOMBIT's støttesystem løsning og den fælles nationale sundhedsservice.

Der tænkes anvendt and unik ID for organisatorisk tilknyt end IP range.

Side 16 figur 3:

Bemærkning:
I forhold til opnåelse af stærk authentifikation hos parterne kan dette opnås ved enten at den lokale IdP stiller videre til NemLogin eller at KOMBIT's støtte system etablerer forbindelse til NemLogin.

Side 18 nederst / side 19 øverst:

Bemærkning:
Er denne bemærkning om væsentlig udviklingsaktiviteter kun gældende for afsnit 4.4 eller er den gældende for både afsnit 4.3 og 4.4?

For Odense kommune vil foretrække modellen beskrevet i afsnit 4.3, og ser derfor behov for uddybelse af hvad "væsentlige udviklingsaktiviteter" indeholder.

Side 19 afsnittet Tokenformat og -indhold:

Bemærkning:
Kommunerne og KOMBIT bør indgå i denne analyse for at sikre, at det er muligt for os at understøtte dette evt. med en yderligere attribut som medsendes i SAML tokenet.

I forhold til brugerstyring er der ikke i Arkitekturrapporten henvist til støtte

Side 19 afsnittet Håndtering af links i det aktive login scenarium ("sikker browseropstart"):

Bemærkning:

I forhold til dette ses en relation til Adviser og Beskedfordeleren fra KOMBIT. Det er en vigtig funktionalitet i forhold til arbejdsgangene i mellem Regionerne og Kommunerne.

Som udgangspunkt kræves der til dette stærk authentifikation, idet at det jo er personfølsomme oplysninger som udveksles, men det kan tænkes at der på sigt vil blive behov for udveksling af mindre følsomme oplysninger som ikke vil kræve stærk authentification og som dermed brugervenligt vil kunne tilgås fra mobile devices.

Side 21 – proces figur 6 og teksten nederst på siden

Bemærkning

Kommunerne skal indgå i dette arbejde, idet sårjournalen ikke vil være det eneste system med en sådan problemstilling.

Anders Malling Aaboer, Esbjerg Kommune

Hermed Esbjerg Kommunes høringssvar på NSI's oplæg til føderative sikkerhedsmodeller for Sårjournalen.

Helt overordnet mangler vi at få tydeliggjort,

- Hvad er NSI's planer ift. fremtidige løsninger.
- Hvad er NSI's holdning ift. sikkerhedsmodellerne for Sårjournalen.
- Hvad forventer NSI egentligt af os, som kommune ift. at kommentere på de fremlagte sikkerhedsmodeller.

Det er vanskeligt præcist at tyde, hvad man skal forholde sig til. Høringsmaterialet virker uoverskueligt i sin struktur.

- I materialet listes en række løsningsforslag til sikkerhedsmodeller op, uden tydelig angivelse af hvilken model der er i spil og anbefales.
- Der er store spring i detaljeringsgrad, fx nævnes ganske kort i pkt. 2.5 sundhedspersoners adgang til Sårjournalen via mobile devices, ligesom BYOD nævnes endnu mere. Det virker slet ikke tydeligt, hvilke overvejelser man har gjort ift. dette og vi antager derfor, at det ikke er noget der ligger indenfor dokumentets scope og vi undlader derfor at forholde os til det.

Som kommune, savner vi at se ambitioner om en generisk sikkerhedsmodel for adgang til nationale sundhedsdatabaser via føderation. Det gælder såvel FMK og Sårjournalen, som fx Shared Care og KHI. Vi må forvente, at antallet af sundhedsfaglige databaser vil stige i antal i de kommende år – og dette bør tænkes tidligt ind i arkitekturen for sikkerhedsmodellerne.

Modellen skal være gennemtænkt ift. forskellige typer sundhedspersonales adgang til de sundhedsfaglige databaser, herunder også problematikken omkring medarbejdere, der arbejder på vegne af sundhedsfagligt personale eller blot med ledelsens accept. Problematikken er aktuel ift. adgang til FMK i kommunerne, men bør kunne løses ensartet på tværs af løsninger.
Via en generisk sikkerhedsmodel, vil man kunne undlade at skulle lave en ny sikkerhedsløsning til hver ny national løsning, der skal implementeres. Det synes, at man ift. Sårjournalen opbygger en ny sikkerhedsmodel, som er snævert rettet mod Sårjournalen. Det er ikke tydeligt for os, hvad det er, der gør Sårjournalen særlig ift. andre løsninger. Det undrer, at man ikke anvender den model, der er udviklet til FMK. Dette skaber en mistanke om at sikkerhedsmodellen for FMK ikke vurderes at være i orden / den optimale og derfor må tilrettes?
I forbindelse med adgang til FMK er den sundhedsfaglige autorisationskode vigtig, men det er ikke tydeligt om det også er gældende for Sårjournalen og vil være det for fremadrettede løsninger. Såfremt denne kode er vigtig efterspørger vi en mere smidig løsning, således at fagsystemerne som tilgår nationale databaser ikke skal registrere denne kode.

Det er vores opfattelse, at NSI opbygger sikkerhedsstruktur som er forskellig fra den fælleskommunale eller andre fællesoffentlige løsninger. Vi kan kun opfordre til, at lave en løsning, der kan genbruges på tværs. Det synes ikke, at der i høringsmaterialet genbruges nævneværdigt ift. de tanker, der er gjort i relation til kommunernes støttesystemer.

Som kommune, kan vi kun være fortaler for en mere åben model. Vi skal selv kunne vælge autentifikationsmetode, når metoden overholder det krævede niveau af sikkerhed. Vi vil altså gerne selv kunne bestemme, hvorvidt, vi vil anvende fx ADFS eller medarbejdersignatur

Generelt har vi det forbehold ift. anvendelse af dedikerede medarbejdersignaturer, at disse signaturer meget hurtigt bliver vanskelige at administrere. Udsigten til at vi skal håndtere en vifte af forskelle signaturer til forskellige fagsystemer og sundhedsfaglige funktioner, fx til EOJ/FMK, Sårjournal m.v., giver bange anelser om at der opbygges modeller, der i praksis vil blive overordentligt komplekse at administrere.

I Danmarks Miljøportal har man etableret en rollebaseret indgang til en lang række miljødatabaser. Dette er gjort via en serviceprovider, der ligger foran databaserne. Via definerede roller gives adgang via serviceprovideren til de underliggende data. En tilsvarende løsning kunne være en mulighed ift. sundhedsfaglige databaser, som fx Sårjournalen.

Esbjerg Kommune indgår gerne i dialog med NSI, vedr. ovenstående bemærkninger. Vi uddyber også gerne vores synspunkter, hvis det er et ønske.

Kirsten Skovrup, Aalborg Kommune

Aalborg kommune har læst materialet om Føderative sikkerhedsmodeller til sårjournalen. Det er vigtigt for kommunen, at modellerne er fleksible i forhold til de sikkerhedsløsninger som de enkelte organisationer har. Det ser ud til at materialet lever op til det. Vi synes dog, at der i begreber/termer mangler EOJ, omsorgssystemer i kommunerne.