

Afdeling:	IT - Strategi og Arkitektur	Udarbejdet af:	Esben Dalsgaard , Jan Riis og Thomas Sonne Olesen
Journal nr.:		E-mail:	Esben.Dalsgaard @regionsyddanmark.dk
Dato:	19. september 2007	Telefon:	76631746

Høringssvar i forbindelse med DK-SAML 2.0 profilen

Indledning

Region syddanmark takker for muligheden for at afgive høringssvar på udkastet til en national standard for en dansk SAML 2.0 profil for web-browser-baserede applikationer. Regionen har gennem SOSI-projektet (se: <http://www.sosi.dk>) opnået en del erfaring med SAML 2.0, om end denne standard her er benyttet til web-service-baseret systemintegration.

Relevans og nødvendighed

Region Syddanmark er af den opfattelse, at dansk standardisering - så vidt det er muligt - skal ske indenfor rammerne af internationale standarder, således at mulighederne for at anskaffe og benytte produkter fra et internationalt marked ikke begrænses.

Regionen noterer sig med tilfredshed at It- og Telestyrelsen har bestræbt sig på at følge internationale standarder og retningslinier i videst muligt omfang ved fastlæggelsen af DK-SAML. Et godt eksempel herpå, er processen omkring valg af autenticitetsniveauer, hvor man har baseret sig på arbejde fra det amerikanske "National Institute of Standards and Technology" (NIST).

Når man baserer sig på internationale standarder, er der ofte indbygget fleksibilitet i standarderne, der gør det muligt at repræsentere de samme informationer på mange forskellige måder. Med ukoordineret anvendelse af standarderne, vil to anvendere af de samme standarder derfor sjældent blive interoperable. Det er således både relevant og nødvendigt, at der etableres danske profiler omkring anvendelse af internationale standarder på dette område.

I nærværende DK-SAML profil finder regionen, at det er lykkedes ganske godt, at indsnævre fortolknings- og repræsentationsmuligheder, så interoperabilitet kan opnås - uden at fleksibilitet mistes på væsentlige områder (afsnit 7.4).

En forudsætning for, at nationale og internationale standarder tages i bred anvendelse, er at standarderne viser sig anvendelige i praksis. Det er derfor vigtigt, at praktiske erfaringer med anvendelsen af standarden opsamles og at disse erfaringer anvendes til at udvikle og modne standarderne. Region Syddanmark finder, at It- og Telestyrelsen spiller en central rolle i at opsamle erfaringerne på nationalt plan, at justere i nationale standarder såfremt erfaringerne påpeger nødvendigheden heraf, samt at benytte de praktiske erfaringer og ønsker om ændringer til at påvirke det internationale standardiseringsarbejde, således at der skabes de bedst mulige rammer for det nationale standardiseringsarbejde.

Forestående anvendelse

I høringsbrevet nævnes det, at DK-SAML profilen bliver det tekniske fundament for en kommende fællesoffentlig brugerstyringsløsning. Med dette tænkes en fællesoffentlig brugerstyringsløsning for web-browser-baserede applikationer, og i forhold til dette, finder regionen arbejdet med DK-SAML grundigt og konsistent.

Region Syddanmark finder, at arbejdet med fællesoffentlig brugerstyring for web-browser-baserede applikationer – herunder fastlæggelsen af en dansk SAML 2.0 profil for disse, samt arbejdet med fællesoffentlige portaler (borger.dk, sundhed.dk og miljøportalen) og integration mellem disse, giver et godt grundlag for at arbejde med it-understøttelse af kommunikation mellem borgere og den offentlige sektor (herunder udvikling af selvbetjeningsløsninger, hvor det er muligt) på en måde som styrker borgerens oplevelse af en sammenhængende offentlig sektor.

Hovedparten af sundhedessektorens tjenester er imidlertid ikke digitale og vil langt hen ad vejen ikke blive det. Kerneydelser som behandling og pleje er noget som gives af mennesker. Skal borgeren opleve sammenhæng i disse ydelser, er det vigtigt at skabe sammenhæng i de systemer (f.eks. den elektroniske patientjournal), der understøtter de kliniske fagpersoner i deres arbejdsprocesser – på tværs af organisationer og sektorer. Da disse fagsystemer er ikke er web-browser-baserede (og ofte er for interaktive til at blive det) vil den foreslåede DK-SAML 2.0 profil ikke hjælpe til at skabe sammenhæng mellem sådanne fagsystemer.

Sundhedsområdet arbejder p.t. på at skabe sammenhæng mellem fagsystemer ved at etablere nationale web-services. I samarbejde med Lægemiddelstyrelsen og MedCom er der således ved at blive etableret nationale web-services der muliggør etableringen af en fælles nationalt medicinkort (Lægemiddelstyrelsens pilotprojekt vedr. det fælles medicingrundlag og MedComs FAME-projekt).

Som led i dette, arbejdes med fælles brugerstyring indenfor sundhedsområdet. P.t. har der primært været arbejdet med identifikation og autentifikation, men Styregruppen for Digital Sundhed i Danmark (SDSD) er ved at se på sikkerhedsområdet generelt, hvorfor der inden længe vil blive skabt løsninger der fokuserer på sikring af autorisation og relevans (eksempelvis må en kliniker kun se information om patienter som vedkommende aktuelt har i behandling).

DK-SAML i relation til web-services

Som skrevet indledningsvis, er der allerede erfaring med at benytte SAML 2.0 til identitetssikring i forbindelse med web-service-baseret integration indenfor sundhedsområdet. Det såkaldte SOSI-projekt (SOSI = Service Orienteret System Integration) har i samarbejde med MedCom fastlagt en standard for web-services ("Den Gode WebService"), der v.h.a. SAML 2.0 og en Identity Provider komponent (IdP) / Secure Token Service (STS) udviklet i SOSI-projektet skaber en føderation for simplified signon (SSO) baseret på offentlige digitale certifikater (OCES).

I samråd med It- og Telestyrelsen har SOSI-projektet valgt, at den kommunikation der skal foregå med centrale identitetssikringsmekanismer for web-services (IdP/STS) ikke baseres på SAML. I skrivende stund ser det ud til, at standarderne konvergerer mod, at denne kommunikation bliver reguleret i WS-Trust standarden.

I SOSI-projektet har man betragtet nedbringelsen af antallet af gange en bruger skal foretage sign-on som en forudsætning for en succesfuld implementering af en serviceorienteret arkitektur på sundhedsområdet. Ligeledes har der været fokus på at minimere antallet af eksterne opslag af

brugeroplysninger – såvel for det system, der skal anvende en service, som for det system, der udstiller en service. Endelig er der brugt megen tid på at tilrettelægge arkitekturen, så et evt. udfald af centrale sikkerhedsløsninger i *mindst muligt* omfang påvirker systemintegration mellem systemer i sundhedssektoren. Man har med andre ord forsøgt at undgå ”single points of failure”.

Hvor man internt på sundhedsområdet er langt i forhold til opbygningen af standarder for web-service-baseret kommunikation, er der en udfordring, når man skal kommunikere med andre sektorer (fødselsanmeldelser til kirkeministeriet etc.). Da man ikke her følger fælles standarder for etablering og anvendelse af web-services, må der etableres specifikke integrationer fra gang til gang. Hvis sikkerhedsmekanismen omkring den specifikke service kræver sikring af autentifikation gennem brug af en digital medarbejder signatur, da vil det ikke engang være muligt at etablere en sådan integration gennem en standardiseret national service på sundhedsområdet.

Region Syddanmark opfordrer It- og Telestyrelsen til at arbejde på en national SAML 2.0 profil for web-services (eller flere nationale profiler, der tillader etablering af tillidsforhold, ”trusts” mellem de forskellige sikkerhedsdomæner / føderationer). Regionen opfordrer endvidere Styrelsen til at lade et sådant arbejde tage afsæt i erfaringerne fra sundhedsområdet. Endelig vil Region Syddanmark opfordre It- og telestyrelsen til at arbejde for, at viden om det anvendelsesscenarium for SAML 2.0 indenfor sundhedssektoren (med minimering af antallet af signon’s og antallet af eksterne opslag) bibringes relevante internationale fora, idet problemstillingerne indenfor it-understøttelsen af sundhedsområdet må antages at være parallelle med problemstillinger i andre lande.

Når It- og Telestyrelsen fastlægger en arkitektur for sikkerhedshåndtering i forbindelse med kommunikation baseret på web-services, da skal man være opmærksom på, at resultater og løsninger fra arbejdet med fælles brugerstyring og DK-SAML 2.0 for web-browser-baserede løsninger ikke nødvendigvis kan overføres til web-service området.

Eksempelvis vil der være stor forskel på de risikovurderinger der ligger til grund for web-browser-baserede løsninger og for fagsystemer, der integreres via web-services. Et skrækszenarium i sundhedssektoren er, at en læge ikke kan få adgang til vital information i (evt. flere) tilgængelige fagsystemer, fordi lægen ikke kan ”logges ind” eller autoriseres pga. nedbrud i fællesoffentlige tjenester. Dette kan i yderste instans have fatale følger for patienter.

Vi anbefaler derfor, at man i etablering af en fællesoffentlig brugerstyringsløsning for web-service-baserede løsninger, baserer arkitekturen på fornyede risikovurderinger. Dette kan give anledning til overvejelser om, der kan være sektorer, f.eks. sundhedssektoren, hvor der er så specielle tilgængelighedskrav, at der skal etableres specielle driftsmæssige løsninger for den pågældende sektor. Eller hvor der er behov for at udarbejde specielle beredskabsprocedurer for disse sektorer, f.eks. ”nød-adgang” ved mangelfuld sikring af autorisation, evt. kombineret med forøget logning og kontrol.

Såfremt It- og Telestyrelsen måtte gå videre med dette arbejde, stiller Region Syddanmark og SOSI-projektet sig gerne til rådighed med praktiske erfaringer.