

## NOTAT

**Telefon** 45 11 11 11  
**Direkte** 23 49 42 89  
**Fax** 45 11 11 12  
**Mail** [Koncern-it@regionh.dk](mailto:Koncern-it@regionh.dk)  
**Web** [www.regionh.dk](http://www.regionh.dk)Sagsnr.:  
Arkiv:  
Sagsbeh.: Claus Thorsen  
Deres j. nr./ref.:

Dato: 18. september 2007

### Høringssvar vedr. DK-SAML 2.0

Region Hovedstaden har gennemgået høringsmaterialet omkring dansk SAML 2.0 profil og har følgende kommentarer:

### Indledende overvejelser

#### Regionens anvendelse af DK-SAML 2.0, og krav til dette

Regionen byder IT&Ts arbejde med simplificeringen og national tilpasning af SAML 2.0 velkommen. Det er vigtigt, at dette arbejde sker nu inden der udstilles for mange nationale services.

I hvilken grad Region Hovedstaden vil komme til at anvende DK-SAML 2.0 er afhængigt af den udviklingsretning der aftales i SDSD (tidligere kaldet "den nationale EPJ-organisation"). Det antages i dette dokument, at regionen vil få en anvendelse, hvor DK-SAML 2.0 er central for det kliniske personale daglig adgang til nationale data. Vi vil under alle omstændigheder have brug for tilgang til nationale data – det er kun formen der er usikker.

I vores vurdering af profilen lægges vægt på, at vores kliniske personale har en hverdag der er præget af stor mobilitet, hvor man anvender flere forskellige PC'er og står med meget pressede situationer, hvor tilgangen til data er kritisk (i yderste konsekvens livsvigtige). Løsningens brugervenlighed og effektivitet er derfor afgørende for den værdi, og de anvendelsesmuligheder den giver regionen.

### Kommentarer til høringens punkter

Afsnit	Kommentar
s. 9	Hvorfor understøttes kun portaler og browsere? Det ser ud til at mekanismen er den samme for WS-integration.
s. 9	Regionens ønske en sømløs brugeroplevelse i tilgangen til interne og eksterne services og web sider i vores portal. Hvis kun portaler og browsere understøttes af DK-SAML, kan vi så opnå SSO, når der i samme portal anvendes en blanding af framed

	<p>løsninger og WS integrationer?</p> <p>Det er ikke acceptabelt, hvis klinikkeren skal logge på med sin digitale signatur to eller flere gang for at anvende løsninger i samme portal (en logon til DK-SAML og en/flere til WS).</p>
-	<p>Hvis klinikkeren anvender flere portaler, kan de så dele adgangen (det ser ud til, at det handler om fælles anvendelse af en cookie)?</p>
-	<p>Tankerne om forenkling er gode og understøtter hvidbogens tanker om interoperabilitet, men er det ikke et problem, at vi løsriver os fra Oasis SAML med disse tiltag?</p> <ul style="list-style-type: none"> <li>- Vi kan ikke "blot" satse på at købe produkt der understøtter SAML, men skal specifikt sikre os, at det understøtter DK-SAML</li> <li>- Hvilken opgave omkring løbende vedligehold og compliance påtager vi og resten af DK os hermed?</li> <li>- Har andre (fx USA eller New Zealand) gjort sig erfaringer der understøtter, at dette er den rigtige vej, og kan vi få tyngde i vores valg ved at bygge profilen i fællesskab med dem?</li> <li>- Nogle krav er meget hårde – fx s.30: "All other statements are disallowed" – Uden at have undersøgt det specifikke indhold af felterne, ville det være attraktivt at opbløde dette krav, hvis det er muligt – fx ved at modtager af data skal se bort fra disse data, eller ved at de "skrælles bort" under forsendelsen. Er dette muligt, kan vi potentielt opnå et bredere udvalg af applikationsleverandører.</li> </ul>
s. 26	<p>Hvordan skal klinikkeren vide hvilken IdP han skal vælge? Det giver ikke mening at bede en kliniker om at tage stilling til dette, og i akutte situationer, vil det være en alvorlig stressfaktor. Kan vi finde en anden (teknisk) løsning – fx ved at der i servicekaldet angiver ønsket IdP?</p>
-	<p>Klinikkeren vil skifte pc flere gange på en arbejdsdag. Dette ønsker vi at understøtte ved at samle applikationerne i en portal, og her fastholde kontekst fra session til session. Af nødvendighed er det ok at logge på igen, men er der nogle problemer ved fornyet logon – fx at IdP ikke vil autentificere samme bruger, når vedkommende allerede har en igangværende session?</p>
-	<p>Hvor ligger rettighedsstyringen? Er denne opgave isoleret til det arbejde Økonomiministeriet har i gang, og er det tænkt sammen med dette arbejde? Uden sammenhæng mellem de to projekter er anvendelsesområdet meget begrænset.</p>
s. 46	<p>AttributeQuery – er det overvejet hvilke data man vil overføre her, og hvem + hvordan vedligehold af disse data sker?</p> <p>Man kunne få den tanke at "snige" en form for rettighedsstyring ind</p>

	<p>via attributter. Dette vil hurtigt udvikle sig til en meget problematisk model, og det må anbefales ikke at gå denne vej.</p> <p>Vi kunne hurtigt ønske en masse domaine specifikke attributer. Det skal overvejes, om dette er en hensigtsmæssig løsning på den opgaven man adressere, eller attributter er en "løsnings-rodekasse".</p>
s. 48	Metadata – "All entities supporting the DK-SAML profiles must support the SAML Meta Data Specification" – hvad kræver dette af os som service anvender og som service udstiller?
s. 52	Logon er sat til at time ud efter 15 minutter. Er disse 15 minutter defineret efter vurdering af brugerbehovet? Hvis en klinikker sidder og bearbejder nationalt udstillede data sammen med vores interne data, kan han være løbende aktiv, men uden at ramme nationale services så hyppigt. Det vil være et stort irritationsmoment, hvis han skal logge på op til 4 gang pr. time. Brugerbehovet bør undersøges.
s. 60	Afs. 13.2 Authentication level in requests. Problemet ser ikke ud til at være løst. Hvordan understøttes det, at en service kræver logon på sikkerheds niveau 4, hvis IdPen ikke får denne oplysning og frit kan vælge autentifications niveau?
-	Flere steder får man den overvejelse, om man bør være logget på nationalt fra starten af sessionen. Dette er en uønsket løsning set fra regionen, da systemadgangen er særdeles kritisk. En løsning der adresserede behovet for at være logget på lokalt og nationalt parallelt kunne være at etablere en "bro" mellem den lokale identitet og den nationale identitet.