



Afsender:
DK-AAI sekretariatet
sekretariat@dk-aa.dk

Sendt til:
oiostandarder@itst.dk og
Søren Peter Nielsen spn@itst.dk

Høringssvar til høring over Dansk SAML2.0 Profil

DK-AAI har diskuteret DK-SAML2.0 høringsudkastet internt og indhentet kommentarer fra føderationseksperter fra Finland og Norge. Kommentarerne herunder tager udgangspunkt i føderationsarbejdet for videregående uddannelse og forskning, der p.t. har pågået i snart to år.

Vores vigtigste kommentarer er:

- DK-SAML2.0's formelle afgrænsning er ikke tydelig nok (hvordan afgrænses 'offentlige føderationer'?)
- DK-SAML2.0 overholder ikke de officielle krav fra OASIS vedrørende SAML-profilering
- DK-AAI's primære scenarium er ikke dækket i DK-SAML2.0
- DK-SAML2.0 stiller urealistiske krav til den anvendte PKI (obligatorisk brug af OCES-certifikater)

Generelt

I introduktionen lægges ud med at skrive at profilen(DK-SAML2.0) skal bruges til føderationer indenfor den danske offentlige sektor. Afgrænsningen synes ikke at være defineret præcist nok, specielt når man tager de begrænsende valg der foretages i betragtning. DK-SAML2.0 efterlader det indtryk, at dokumentet er skrevet med en bestemt føderation for øje - eller til en gruppe af meget homogene føderationer.

Fokus for DK-SAML2.0 er primært føderationer bestående af offentlige myndigheder, deres ansatte og borgerne. Der er kun lidt fokus på føderationer indholdende private tjenesteudbydere eller føderationer, som går på tværs af landegrænser. Dette gør det formentlig svært at leve op til profilen i alle hjørner af de føderationer, som vil opstå i offentligt regi. Derfor bør scope't enten defineres mere præcist eller også bør visse begrænsninger fjernes.

DK-AAI's brugerscenarium undertøttes ikke

Det primære DK-AAI scenarium er ikke omfattet af de beskrevne scenarier. I DK-AAI er brugerne for det meste anonyme i forhold til SP'en. I nogle tilfælde er der behov for en persistent relation (pseudonym), men ikke nødvendigvis konti-linking. I andre tilfælde er det nok at IdP'en siger god for brugeren og at vedkommende eksempelvis er studerende. I dette tilfælde er der ikke behov for persistering af relationen, men der skal tilgængelig overføres en række rollelignende attributter.

Vidtrækkende generalisering

Følgende tekst er taget fra:

<http://www.oasis-open.org/committees/download.php/11785/sstc-saml-exec-overview-2.0-draft-06.pdf> :

'Generally, a *profile* of SAML defines constraints and/or extensions in support of the usage of SAML for a particular application – the goal being to enhance interoperability by removing some of the flexibility inevitable in a general-use standard. For instance, the Web Browser SSO Profile specifies how SAML authentication assertions are communicated between an identity provider and service provider to enable single sign-on for a browser user.'

Vi mener ikke, at man bør generalisere alle kommende, danske føderationer til 'a particular application', som det eksempelvis gøres ved alene at tillade HTTP-POST (ekskluderer SAML-artefact).

Om SAML2-artifacter

Ifølge dokumentet 'Conformance Requirements for the OASIS Security Assertion Markup Language (SAML) V2.03' lever en given profil ikke op til SAML2-standarden hvis ikke http-artefact understøttes.

SAML-artefact'er anbefales til overførsel af større datamængder, og giver derfor god mening at bruge, hvis der tale om måleresultater, patientjournaler, mediefiler, grid-jobs osv. som ofte udgør større datamængder.

Argumentet om at man i USA har haft problemer med brugen af SAML-artefact er *ikke* fra énsbetydende med, at det samme skulle være tilfældet for alle kommende føderationer i Danmark (afsnit 4.5.4). Manglen på diskussion af baggrunden for dette vigtige fravalg springer i øjnene - især når man tager DK-SAML2.0's generelle karakter i betragtning.



Det skal nævnes at andre lande bruger i øvrigt SAML-artefact'er i deres bruger-scenarier for uddannelsessektoren, f.eks. <http://www.e.govt.nz/standards/e-gif/authentication/nzsams/chapter17.html>.

For stærk binding til OCES

Vi spørger os selv om, hvorfor man ønsker at tvinge udbredelsen af OCES signatur via dette initiativ? De direkte og afledte krav til brugerne, IdP'erne og SP'erne vedrørende brug af OCES-certifikater volder problemer i forhold til profilens generelle anvendelse. Her tænkes særligt på eksisterende PKI'er, som fungerer til alles tilfredshed.

Også det faktum at relativt store beløb allerede er investeret i certifikater og abonnementsordninger vil konflikte med de mange krav om brug af OCES-certifikater. Billedet kompliceres yderligere i et internationalt miljø som det akademiske, hvor interføderering, dvs. sammenkobling af eksisterende føderationer, allerede er igangsat.

Endelig er der mange IdP'er som ikke bruger OCES i dag, da mobilitetsproblematikken med OCES endnu ikke er løst for de fleste brugere, ikke mindst i uddannelsessektoren. Og så skal det nævnes, at DK-AAI-brugeren ofte er anonym i forhold til SP'eren hvorfor overførelse af CPR-nummer eller PID derfor være uaktuelt.

Level of authentication understøttes ikke

I afsnit 4.4.2 står der at en IdP gerne må supportere forskellige autentifikationsmekanismer, men "level of authentication" må ikke angives i forespørgslen. Der skal i stedet anvendes forskellige logiske IdP'er - hvilket ikke giver mening, da auth-niveauer dermed alligevel skal konfigureres. Vi forstår ikke hvorfor ikke auth-level ikke tillades i authn-request. Det bør efter vores mening være op til den enkelte føderation at definere. At enkelte stykker software har svært ved at håndtere forskellige 'levels of assurance', LOA, bør ikke gå ud over alle. DK-AAI har påvist, at systemopsætningen på IdP-siden kan være ganske begrænsende for udbredelsen af føderationen. At bede hver enkelt IdP om at opsætte og administrere flere logiske IdP'er svarende til multiple auth-niveauer tror vi vil være direkte hæmmende - ikke mindst når man tager SAML2-understøttelsen for auth-levels i betragtning.

Men også fravalg af fx "level of authentication" eller tilvalget af "Identity Discovery profile" volder problemer i forhold til føderationer med partnere som ikke er en dansk myndighed. Mere herom nedenfor.

Restriktioner i Single Logout profilen

Argumentationen i afsnit 6 for at anvende HTTP Redirect binding til single-logout er problematisk.

Hvis man vil fastholde front-channel, skal argumentet være, at man har mulighed for at prompte brugeren for, om han virkelig vil logge ud. Brugerens identitet kan også videregives via SOAP binding.

Hvad er SP'ere's 'Common domain'

"Common domain" og dermed brugen af "Identity Discovery profile", beskrevet i afsnit 4.2, giver fint mening hvis en SP'er kun er medlem af få forskellige føderationer. I DK-AAI vil der være kommercielle (udenlandske) SP'ere, som udbyder deres tjeneste til mange føderationer. Det bliver svært at kræve, at disse skal håndtere mange "common domains", idet de allerede i dag anvender andre "discovery" mekanismer, som passer ind i deres forretning for fødereret adgang til deres tjenester.

For højt påkrævet sikkerhedsniveau?

DK-SAML2.0 sætter et meget højt sikkerhedsniveau.

I Afsnit 4.3.3, 10.8, 10.9 og 11.5 beskrives det, at data på "message level" både skal signeres og krypteres.

Da DK-AAI-brugeren ofte er anonym i forhold til SP'erne, bør et lavere sikkerhedsniveau i forhold til kryptering kunne anvendes - det skal i øvrigt siges, at alle attributoverførsler sker via sikre, krypterede forbindelser.

Navngivning attributter

Navngivningen af unikke, sektorspecifikke attributter bør bindes til DNS-navngivningen af føderationen (se afsnit 7.4, bullet 2).