Samengevoegde reacties op de openbare consultatie voor SAML v2.0 van de volgende partijen:

- Kennisnet
- Rijkswaterstaat

KENNISNET

1. Zijn er volgens u in deze toelichting aanvullingen of anderszins wijzigingen nodig, bezien vanuit het doel van het document (het Forum en College Standaardisatie voorzien van een inhoudelijk relevante toelichting op SAML). [paragraaf 1.1 t/m 1.4 van het expertadvies].

- Advies: neem bij de zin *"Door de expertgroep is versie 2.0 van de SAML standaard beoordeeld."* de lijst met daadwerkelijk beoordeelde documenten op en ten minste een link naar het overzicht van de documentatie behorende bij de specificatie (http://saml.xml.org/saml-specifications)

2. Bent u het eens met het door de expertgroep geadviseerde toepassingsgebied van SAML? [paragraaf 2.1 van het expertadvies]

- Het expertadvies biedt onvoldoende houvast
  - De term "single-sign-off" moet volgens mij "single logout" zijn
  - In het advies over toepassingsgebieden zie ik erg weinig referenties naar de exacte onderdelen in de SAML 2.0 specificatie.
  - Het lijkt erop dat er alleen voor de profielen 1a en 1d is gekozen (zie lijst hieronder).

De verschillende profielen in SAML 2.0 zijn:

1. SSO Profiles of SAML
   a. Web Browser SSO Profile
   b. Enhanced Client or Proxy (ECP) Profile
   c. Identity Provider Discovery Profile
   d. Single Logout Profile
   e. Name Identifier Management Profile
2. Artifact Resolution Profile
3. Assertion Query/Request Profile
4. Name Identifier Mapping Profile
5. SAML Attribute Profiles
   a. Basic Attribute Profile
   b. X.500/LDAP Attribute Profile
   c. UUID Attribute Profile
   d. DCE PAC Attribute Profile
   e. XACML Attribute Profile

[bron: http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf

- Het expertadvies lijkt lang niet ver genoeg gaan (onvoldoende profielen aan te bevelen)
  - *hiervoor heb ik een collega om aanvullend advies gevraagd en hij kwam met het volgende antwoord:*

Ik deel je mening dat er zeer summier naar de beschikbare SAML 2.0 profielen is gekeken. Ik adviseer om een aantal generieke use cases uit te werken voor het overheid en op basis hiervan een mapping te maken op de beschikbare SAML 2.0 profielen.

Hierbij kan ik alvast een extra profiel aandragen: het SAML 2.0 Profiel “Assertion Query/Request Profile”. Met dit mechanisme worden additionele attributen van een gebruiker getransporteerd. We zien in het onderwijs dat hier in een federatief verband een sterke behoefte aan is. Hiermee kunnen identiteiten verrijkt worden met (geverifieerde) attributen uit diverse systemen. Hier is vooral in het onderwijs nu een acute behoefte aan, omdat er naast identity providers de rol attribute of autorisation provider sterk vorm neemt.

Buiten het onderwijsveld zie ik hier ook toepassingen voor, bijvoorbeeld: authenticeren met DigiD bij een overheid service provider, deze vraagt bij een andere overheid attribute provider wat gegevens over de persoon uit ten behoeve van zijn eigen dienstverlening.

Het standaardiseren van het protocol hiervoor draagt bij tot een open architectuur.

3. Bent u het eens met het door de expertgroep geadviseerde werkingsgebied van SAML? [paragraaf 2.2 van het expertadvies]

- geen aanvullende opmerkingen

4. Bent u het eens met de conclusie van de expertgroep inzake de openheid van de standaard SAML? [paragraaf 3.1 van het expertadvies]

- -

5. Bent u het eens met de conclusie van de expertgroep inzake de bruikbaarheid van de standaard SAML? [paragraaf 3.2 van het expertadvies]

- Ten aanzien van single logout gaat er bij het op een goede manier implementeren (dus daadwerkelijk werkend) volgens mij nog veel mis, afgaande op presentaties die zijn gehouden op een meeting van EdReNe in Oegstgeest.

6. Bent u het eens met de conclusie van de expertgroep inzake de impact van de standaard SAML? [paragraaf 3.3 van het expertadvies]

- Ik deel de mening van de expertgroep ten aanzien van de risico's van de complexiteit van de standaard.
- Ik deel eveneens de volgende mening van de expertgroep: quote “*federatieve (web)browser-based single-sign-on (SSO) en single-sign-off*”. Mijn verbazing is mede daarom extra groot over het gekozen beperkte toepassingsgebied.

7. Bent u het eens met de conclusie van de expertgroep inzake het potentieel van de standaard SAML? [paragraaf 3.4 van het expertadvies]

- De functionele scope (quote "het *uitwisselen van autorisatie en authenticatie data tussen security domeinen.*") lijkt niet tot zijn recht te komen in de toepassingsgebied (qoute “*federatieve (web)browser-basedsingle-sign-on (SSO) en single-sign-off*”)
  Het potentieel van de standaard lijkt met deze afbakening onvoldoende tot zijn recht te komen. (zie opmerkingen bij vraag 2)
- Overigens staat dit in paragraaf 3.3

8. Bent u het eens met de samenvattende overwegingen van de expertgroep? [paragraaf 4.1 van het expertadvies]

- Volgens mij toont de volgende zin een redenatiefout: quote: "*SAML wordt ingezet in omgevingen voor federatieve browser bases SSO, en inzet van deze omgevingen introduceert een zekere afhankelijkheid van andere partijen.*" Het is logisch dat alleen die applicaties die de specifiek gekozen profielen van SAML hebben geïmplementeerd alleen maar zullen werken. Dat is echter niet de vraag. Het is de vraag of de ontwikkeling van de standaard voldoende open gebeurt zodat iedere willekeurige partij deze SAML profielen kan implementeren. Deze opmerking wekt de suggestie dat je met de keuze van SAML aan bepaalde partijen vast zit, wat nu juist niet het geval behoort te zijn met een open standaard.

- Volgende opmerking onderstreept onze mening dat er meer uit SAML te halen valt dan met de huidige afbakening het geval is: "*Afhankelijk van de implementatie van SAML kan het voor de eindgebruiker niet altijd inzichtelijk zijn welke gegevens er verstuurd worden. SAML biedt hiervoor wel mogelijkheden, maar het gebruik daarvan wordt niet afgedwongen.*"

9. Bent u het eens met het advies van de expertgroep aan het Forum en College Standaardisatie? [paragraaf 4.2 van het expertadvies]

- In het advies zou tevens in moeten gaan op de noodzaak om ten minste op termijn aanvullende afspraken te maken over (de invulling van) andere profielen van SAML.
- Het opnemen van SAML op de advieslijst schept verwachtingen ten aanzien van een relatief gemakkelijke uitwisseling van authenticatie en autorisatie informatie. Gezien het huidige gekozen toepassingsgebied is dit echter ver weg van de realiteit.

10. Is/zijn er volgens u nog andere informatie of overwegingen omtrent SAML die aan het Forum en College Standaardisatie zou moeten worden meegegeven voor een besluit over het opnemen van SAML op de lijst met standaarden?

- Het advies is vrij optimistisch opgesteld en lijkt onvoldoende rekening te houden met de vele interpretatieverschillen die er in huidige implementaties zijn.

Aanvullende opmerking ten aanzien van de structuur van het advies:

- Onder toepassingsgebied (paragraaf 2.1) worden zowel de functionele scope als toepassingsgebied benoemd. Waarschijnlijk duidelijker om hier aparte (sub)paragraven voor te gebruiken..

Groetjes,

Jeroen F.M. Hamers
Expert onderwijsstandaarden Stichting Kennisnet

RIJKSWATERSTAAT

Geacht forum standaardisatie,
Onderstaand op verzoek van Andre de Boer namens Rijkswaterstaat reactie op de vragen die het Forum standaardisatie stelt bij de openbare consultatie voor het opnemen van de SAML standaard in de lijst van open standaarden van het Forum standaardisatie.

Vraag:

1. Zijn er volgens u in deze toelichting aanvullingen of anderszins wijzigingen nodig, bezien vanuit het doel van het document (het Forum en College Standaardisatie voorzien van een inhoudelijk relevante toelichting op SAML). [paragraaf 1.1 t/m 1.4 van het expertadvies].

Antwoord: Het is zeer wenselijk om vanuit de NORA een functionele behoefte te beschrijven op grond waarvan het wenselijk is om afspraken te maken over een bepaalde standaard. Daarmee wordt ook de relatie tussen al vastgestelde standaarden en nog te maken afspraken duidelijker.

2. Bent u het eens met het door de expertgroep geadviseerde toepassingsgebied van SAML? [paragraaf 2.1 van het expertadvies]

Antwoord: ja

3. Bent u het eens met het door de expertgroep geadviseerde werkingsgebied van SAML? [paragraaf 2.2 van het expertadvies]

Antwoord: ja

4. Bent u het eens met de conclusie van de expertgroep inzake de openheid van de standaard SAML? [paragraaf 3.1 van het expertadvies]

Antwoord: ja

5. Bent u het eens met de conclusie van de expertgroep inzake de bruikbaarheid van de standaard SAML? [paragraaf 3.2 van het expertadvies]

Antwoord: Op grond van onderzoek in onze eigen organisatie hebben we eind 2008 in samenwerking met de Gartner geconcludeerd, dat rijkswaterstaat op dit moment nog niet klaar is voor brede uitrol van SAML. Dat heeft zowel met organisatorische aspecten te maken als met de beschikbaarheid van SAML kennis bij marktpartijen in Nederland. Wel hebben we SAML geschikt bevonden voor pilot projecten binnen onze organisatie. Als het comply or explain principe er toe zou leiden dat er druk ontstaat om de standaard te implementeren voor de organisatie er klaar voor is, dan kan dat risco's opleveren voor de kwaliteit van de implementatie van het beveiligingsbeleid binnen de nederlandse overheid. Inpassing in een binnen het NORA passende beveiligingsarchitectectuur die zowel business, informatie als technische aspecten beschrijft achten wij dan ook wenselijk.

Gezien onze eigen ervaringen zijn wij het op dit moment dan ook niet eens met de conclusie van de expertgroep.

6. Bent u het eens met de conclusie van de expertgroep inzake de impact van de standaard SAML? [paragraaf 3.3 van het expertadvies]

Antwoord Rijkswaterstaat: Gedeeltelijk, het expertpanel benoemt risico's op het gebied van technische en organisatorische implementatie. Deze risico's kunnen aanzienlijk zijn bij de implementatie van deze standaarden. Dit impliceert dat het "comply or explain" principe met voorzichtigheid moet worden gehanteerd omdat het voor een uitvoeringsorganisatie een aanzienlijke inspanning vereist om te voldoen aan het "comply" beleid.

7. Bent u het eens met de conclusie van de expertgroep inzake het potentieel van de standaard SAML? [paragraaf 3.4 van het expertadvies]

Antwoord Rijkswaterstaat: ja

8. Bent u het eens met de samenvattende overwegingen van de expertgroep? [paragraaf 4.1van het expertadvies]

Antwoord Rijkswaterstaat: t.a.v. de bruikbaarheid: er wordt gesteld dat er veel praktijkervaring mee is opgedaan, we zouden graag inzicht krijgen in de ervaringen die bij een grote overheidsorganisatie in Nederland zijn opgedaan en zijn dan met name geïnteresseerd in de organisatorische aspecten en de ondersteuning vanuit de markt.

9. Bent u het eens met het advies van de expertgroep aan het Forum en College Standaardisatie? [paragraaf 4.2 van het expertadvies]

Antwoord: alleen als het forum aan kan tonen dat er voldoende ondersteuning is binnen de Nederlandse ICT-markt, of als het forum aangeeft dat de uitvoeringsorganisaties voldoende tijd krijgen om pilots te starten voordat er gestuurd wordt op compliance op de standaard.

10. Is/zijn er volgens u nog andere informatie of overwegingen omtrent SAML die aan het Forum en College Standaardisatie zou moeten worden meegegeven voor een besluit over het opnemen van SAML op de lijst met standaarden?

Antwoord: Inzichtelijk maken hoe kandidaat standaarden in de NORA passen, zou helpen om de samenhang tussen de lijst open standaarden en wat we er mee willen bereiken in het oog te houden. Door onderscheid te maken tussen te handhaven standaarden en kandidaat standaarden, kan dit mogelijk opgelost worden. Dan kunnen organisaties wel anticiperen op het gebruik en de nodige organisatorische maatregelen treffen, maar wordt er niet overhaast zonder architectuursturing geimplementeerd.

Met vriendelijke groet,
Ardy Siegert
namens
Andre de Boer
Directeur Informatie en Rapportage
Staf DG Rijkswaterstaat

Ardy Siegert
Sr. Adviseur ICT strategie en sturing
Rijkswaterstaat staf DG