FORUM STANDAARDISATIE

Aanmeldformulier open standaarden en specificaties

Uw gegevens:

1. Naam organisatie
ComplexIT

2. Naam contactpersoon
[…….]

3. Functie contactpersoon
[…….]

4. Telefoonnummer contactpersoon
[…….]

5. E-mailadres contactpersoon
[…….]

Gegevens standaard of specificatie:

6. Naam standaard of specificatie
WS-Security

7. Versie standaard of specificatie
1.1

8. Naam organisatie die de standaard of specificatie beheert
OASIS (TC WSS)

9. Vindplaats documentatie over standaard of specificatie
http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss

Achtergrondinformatie en motivatie:

10. Toepassingsgebied van de standaard of specificatie: voor welke doeleinden wordt de standaard toegepast, c.q. dient de standaard gebruikt te worden? (zie de basislijst met standaarden voor voorbeelden van toepassingsgebieden van standaarden).
WS-Security wordt toegepast om integriteit, confidentialiteit en authenticiteit van berichten tussen web services te garanderen.

11. Werkingsgebied van de standaard of specificatie: binnen welke organisaties wordt deze al gebruikt, c.q. zou deze gebruikt kunnen worden? (indien bekend graag contactpersonen binnen organisaties specificeren, deze gegevens zullen vertrouwelijk worden behandeld).
o.a. RDW, UZI, BPR, EPD, plus een aanzienlijke hoeveelheid commerciele partijen. Waar SAML wordt gebruikt voor formatering van een token wordt doorgaans WS-Security toegepast voor communicatie van dat token.

12. Is uw organisatie gebruiker van de standaard of specificatie? Zo nee, welke relatie bestaat er tussen uw organisatie en de nu aangemelde standaard of specificatie?
Als IT-Architect specificeer ik doorgaans WS-Security wanneer een beveiligde koppeling noodzakelijk is in een SOA (of specifieker: web service) setting.

13. Waarom zou deze standaard of specificatie moeten worden opgenomen op een lijst met aanbevolen open standaarden? Wat is de toegevoegde waarde van de standaard, welk probleem wordt ermee opgelost?
WS-Security specificeert hoe integriteit, authenticiteit en confidentialiteit gegarandeerd worden op bericht nivo (en koppelt daardoor beveiliging los van het gebruikte communicatiekanaal).

14. Welke impact zou het opnemen van deze standaard als aanbevolen standaard hebben?
Interoperabiliteit. WS-Security is een van de bouwstenen voor single sign on tussen verschillende gedistribueerde systemen, platformen, organisatorische eenheden en organisaties.

15. Zijn u concurrerende standaarden of specificaties bekend? (graag benoemen)
Nee. Hoewel in het toepassingsgebied van SSO (of beter federation) nog hoger gelegen standaarden nodig zijn (WS-Trust, WS-Federation zijn de OASIS standaarden hiervoor). Concurrerend voor federation zijn ID-WSF en Shiboleth. Tussen WS-Federation en ID-WSF is convergentie te verwachten; interoperabiliteit is reeds mogelijk en gedemonstreerd).

16. Welke andere organisatie(s) en/of expert(s) zou(den) betrokken kunnen worden bij de beoordeling van de standaard of specificatie op grond van hun expertise of anderszins? (naam en organisatie opgeven)
Binnen het ICTU is reeds de nodige expertise aanwezig. [….] (sca-alliance) is een goede kandidaat om de functionele kant van het probleem toe te lichten. Voor technische vraagstukken wil ik eventueel toelichting geven.

17. Bent u of is uw organisatie bereid deel te nemen aan een expertgroep die deze standaard gaat beoordelen?
JA