Notitie College Standaardisatie

FORUM STANDAARDISATIE

Agendapunt:	??		
Bijlagen:	Rapport Expertgroep SAML		
Aan:	College Standaardisatie		
Van:	Forum Standaardisatie		
Datum:	20 augustus 2009	**Versie**	0.2
Betreft:	Toevoeging SAML aan lijst met open standaarden voor pas toe of leg uit.		

Waarom is een keuze belangrijk?
De standaard maakt het gebruikers mogelijk om op één plek in te loggen en vervolgens direct toegang te krijgen (zonder opnieuw in te loggen) tot meerdere systemen van verschillende organisaties. Deze functionaliteit wordt beschouwd als randvoorwaarde voor het bereiken van een eenvoudige toegang tot diensten van verschillende overheidsorganisaties en het bieden van integrale dienstverlening vanuit de overheid.

Kunt u met een gerust hart "ja"zeggen?
Het voorliggende advies is het resultaat van een uitgebreid expertonderzoek, een publieke consultatie en bespreking in het Forum Standaardisatie. Daarnaast wordt in Europees verband gekozen voor SAML 2.0, maakt Mijn Overheid hier gebruik van en zal SAML 2.0 ook gebruikt worden binnen DigiD.

Zijn er risico's verbonden aan de keuze?
SAML is een redelijk complexe standaard, en de implementatie daarvan introduceert dus ook risico's. Daarnaast kunnen met SAML privacy gevoelige gegevens uitgewisseld worden, wat vereist dat een organisatie die de standaard implementeert gedwongen wordt tot het nadenken over een geschikte inrichting. Deze risico's worden echter veel lager ingeschat dan de risico's die samenhangen met het alternatief, niet kiezen voor de SAML v2.0 standaard en daarmee de optie openlaten om voor verschillende niet interoperabele standaarden te kiezen.
De risico's worden beperkt doordat er alleen overgestapt moet worden bij nieuwbouw of vervanging van systemen; dit maakt geleidelijke migratie mogelijk.

Doel
Het College Standaardisatie wordt gevraagd in te stemmen met:

1. de opname van de SAML v2.0 standaard op de lijst met open standaarden;
2. het door de expertgroep gedefinieerde toepassingsgebied en organisatorisch werkingsgebied.

Toelichting

Ad. 1
SAML is een internationaal (door OASIS) erkende standaard die het gebruikers mogelijk maakt om op één plek in te loggen en vervolgens direct toegang te krijgen (zonder opnieuw in te loggen) tot meerdere systemen van verschillende organisaties. Dit wordt single-sign-on genoemd. Deze functionaliteit wordt beschouwd als randvoorwaarde voor het bereiken van

een eenvoudige toegang tot diensten van verschillende overheidsorganisaties, en het bieden van integrale dienstverlening vanuit de overheid.

Toevoeging van SAML aan de lijst met open standaarden voor pas toe of leg uit betekent dat van alle overheidsorganisaties wordt verwacht dat zij voor deze standaard een 'pas toe-of-leg uit' beleid gaan toepassen.

Door een expertgroep is de standaard beoordeeld op de vastgestelde criteria: openheid, potentieel, bruikbaarheid en impact. Over alle vier de criteria is positief geadviseerd. In een daaropvolgende openbare consultatie zijn een aantal opmerkingen gemaakt die geen aanleiding vormen tot het herzien van het expertadvies.

Ad. 2
Het toepassingsgebied is: Federatieve (web)browser-based single-sign-on (SSO) en single-sign-off. Dat wil zeggen dat een gebruiker na eenmalig inloggen via zijn browser toegang krijgt tot verschillende diensten van verschillende partijen[1].

Het organisatorische werkingsgebied is:overheden en instellingen uit de (semi-) publieke sector.

Welk probleem wordt daarmee opgelost?
De inzet van SAML maakt het mogelijk voor organisaties om in een federatie integrale dienstverlening in te richten en aan te bieden aan de klant / burger. Zonder een federatieve aanpak ervaart de burger nog steeds de verzuilde organisaties.

De expertgroep constateert dat de standaard zowel een bijdrage levert aan het vergroten van interoperabiliteit tussen overheidsorganisaties als aan leveranciersonafhankelijkheid. Voorts verwacht de expertgroep dat de standaard bijdraagt aan de versnelling van de e-overheidsdoelstellingen.

Waar gaat het inhoudelijk over?
SAML is een standaard om autorisatie[2] en authenticatie[3] gegevens tussen security domeinen[4] uit te wisselen. Met gebruik van SAML kan een (overheids)organisatie informatie over een gebruiker en zijn rechten doorgeven aan een andere (overheids)organisatie, zonder dat de gebruiker zich bij laatstgenoemde opnieuw moet authenticeren.

Zijn er alternatieven voor de voorgestelde keuze?
Binnen het gekozen toepassingsgebied zijn er door de expertgroep geen gelijkwaardige concurrerende standaarden gevonden. Wel zijn er standaarden bekend (Kerberos, WS-federation) die buiten het gekozen toepassingsgebied overlap met SAML vertonen.

---

[1] Bijvoorbeeld: iemand meldt zich aan bij de website van de gemeente met DigiD. Wanneer vervolgens doorverwezen wordt naar de website van de IB-Groep, dan hoeft de gebruiker zich daar niet opnieuw aan te melden.

[2] Autorisatie:de bevoegdheid tot het uitvoeren van een handeling (*Verkenning authenticatie*, KPMG Information Risk Management Amstelveen, maart 2007)

[3] Authenticatie: het bewijzen van een geclaimde identiteit (*Verkenning authenticatie*, KPMG Information Risk Management Amstelveen, maart 2007).

[4] Security domeinen zijn bijvoorbeeld verschillende organisaties.

Schets van de expertgroep en de consultatie
De leden van de expertgroep waren afkomstig uit de voornaamste belanghebbende organisaties uit zowel de private als publieke sector, waaronder GBO (DigiD), ICTU (PIP), IVENT en het UWV.
Na opstelling van het rapport heeft een openbare consultatie plaatsgevonden. Van twee partijen is in de consultatie een reactie ontvangen over o.a. het maken van verregaandere afspraken. Deze reacties vormen geen aanleiding voor het herzien van het expertadvies.

Mogelijke consequenties van opname op de lijst met standaarden
Opname van SAML versie 2.0 op de lijst met standaarden maakt het uitwisselen van authenticatie en autorisatie mogelijk op basis van een gestandaardiseerde manier. Dit introduceert gemak voor een eindgebruiker (de burger), omdat hij niet bij webdiensten van samenwerkende organisaties telkens opnieuw hoeft in te loggen. Door te kiezen voor één standaard wordt de interoperabiliteit tussen verschillende organisaties vergroot.

SAML is een redelijk complexe standaard, en de implementatie daarvan introduceert dus ook risico's. Daarnaast kunnen met SAML privacy gevoelige gegevens uitgewisseld worden, wat vereist dat een organisatie die de standaard implementeert gedwongen wordt tot het nadenken over een geschikte inrichting.

Aangezien "pas toe of leg uit" geldt voor nieuwbouw of vervanging van systemen, zal er een geleidelijk migratiepad zijn per betrokken organisatie.

Communicatie
Zowel het Forum Standaardisatie als het Programmabureau Nederland Open in Verbinding zullen aandacht besteden aan de opname van SAML versie 2.0 op de lijst met standaarden.