

**Forum Standaardisatie**

Wilhelmina van Pruisenweg 52  
2595 AN Den Haag  
Postbus 96810  
2509 JE Den Haag

[www.forumstandaardisatie.nl](http://www.forumstandaardisatie.nl)

# notitie

Opname WS-Policy en XACML op de lijst voor  
'pas toe of leg uit'

## FORUM STANDAARDISATIE

|                    |                                                                 |               |     |
|--------------------|-----------------------------------------------------------------|---------------|-----|
| <b>Agendapunt:</b> | 4E                                                              |               |     |
| <b>Bijlagen:</b>   | Expertadvies en consultatiereacties                             |               |     |
| <b>Aan:</b>        | Forum Standaardisatie                                           |               |     |
| <b>Van:</b>        | Stuurgroep open standaarden                                     |               |     |
| <b>Datum:</b>      | 4 oktober 2011                                                  | <b>Versie</b> | 1.0 |
| <b>Betreft:</b>    | Opname XACML en WS-Policy op de lijst voor 'pas toe of leg uit' |               |     |

### **Waarom is een keuze belangrijk?**

Voor zowel XACML als voor WS-Policy wordt geadviseerd deze standaarden nu niet op te nemen op de lijst. Uit de expertprocedure blijkt dat XACML weliswaar een kansrijke standaard voor autorisatie is, maar ook dat de praktijkervaring met XACML nog onvoldoende is. Bovendien zijn de raakvlakken met de SAML-standaard (die staat al op de lijst) niet helder. Daarom worden EL&I en BZK opgeroepen eerst een generieke referentie-architectuur voor 'authenticatie en autorisatie' te ontwikkelen op basis waarvan de standaarden in relatie tot elkaar beoordeeld kunnen worden.

Iets vergelijkbaars speelt bij WS-Policy. De expertgroep stelt dat deze standaard niet losgezien kan worden van andere webservice-standaarden. Geadviseerd wordt de beheerder van Digikoppeling (Logius) te vragen een uitspraak te doen over de bruikbaarheid van WS-policy.

### **Waarom kunt u met een 'gerust hart' ja zeggen tegen deze standaard?**

Een expertgroep is gevraagd een expertadvies te geven over het wel of niet opnemen van WS-Policy en XACML op de lijst voor 'pas toe of leg uit'. Op verzoek van het Forum is niet enkel naar de criteria gekeken, maar ook naar het bredere domein van authenticatie en autorisatie. Na vaststelling van het expertadvies heeft een publieke consultatie plaatsgevonden. De conclusies van de expertgroep werden breed gedeeld door de geconsulteerde partijen.

### **Zijn er risico's verbonden aan de keuze?**

Het domein 'authenticatie en autorisatie' heeft binnen de overheid meer dan één eigenaar. Daardoor bestaat het risico dat het advies niet of gefragmenteerd wordt opgepakt.

**Gevraagd besluit**

**Datum**  
4 oktober 2011

Het Forum Standaardisatie wordt gevraagd:

1. XACML en WS-Policy (nog) niet voor te dragen aan het College Standaardisatie voor opname op de 'pas toe of leg uit' -lijst;
2. De ministeries van EL&I en BZK (ook via de Bestuurlijke Regiegroep) op te roepen om voor 1 juni 2012 een eerste versie te (laten) ontwikkelen van een referentiearchitectuur voor het domein 'authenticatie en autorisatie' om vervolgens op basis daarvan:
  - a. medio 2012 opnieuw de expertgroep te laten bekijken of XACML opgenomen moet worden op de 'pas toe of leg uit' lijst;
  - b. eventueel een aanmelding te doen voor een aangepast functioneel toepassingsgebied voor SAML;
  - c. naast eHerkenning andere plaatsen te identificeren om meer ervaring met XACML op te doen.
3. De beheerorganisatie van Digikoppeling (bij Logius) te vragen voor 1 juni 2012 een uitspraak te doen over de vraag in hoeverre WS-Policy iets toevoegt aan het bestaande WUS-profiel (webservice profiel) en of men mogelijkheden ziet voor zelfstandige toepassing van de standaard.

*Ad 1 en 2)*

Het domein van authenticatie en autorisatie neemt aan belang toe binnen de overheid.

- Op het gebied van generieke authenticatie-oplossingen zijn er diverse initiatieven (o.a. eHerkenning, Rijkspas, DigiD, PKIoverheid).
- Op het terrein van generieke autorisatie-oplossingen zijn er nog weinig initiatieven. Tegelijkertijd neemt het belang hiervan toe, doordat de overheid steeds meer in ketens gaat werken waarin voor de gehele keten autorisatie geregeld moet worden. In de consultatie worden o.a. de basisregistraties als voorbeeld genoemd.

Hoewel er in Nederland nog weinig initiatieven zijn, lijkt XACML wel een kansrijke standaard op het gebied van autorisatie. Dit wordt onderschreven in het expertadvies en de consultatie. eHerkenning richt zich primair op authenticatie, maar past XACML inmiddels toe in samenhang met SAML voor een beperkt toepassingsgebied.

Opname van XACML op de lijst voor 'pas toe of leg uit' is echter weinig zinvol indien niet vooraf bekend is in welke context de standaard ingezet kan worden. Met andere woorden: hoe wil de overheid omgaan met centrale/gefedereerde autorisatie (en authenticatie)? Deze vraag moet volgens de experts eerst beantwoord worden, voordat een uitspraak over XACML gedaan kan worden. Bovendien is ook de praktische ervaring met XACML in het overheidsdomein nu nog beperkt.

*Referentiearchitectuur 'authenticatie en autorisatie'*

Geadviseerd wordt daarom om de beleidsverantwoordelijke ministeries op te roepen een eerste versie van een generieke referentiearchitectuur voor het domein 'authenticatie en autorisatie' te (laten) ontwikkelen. Dit zou praktisch gezien belegd kunnen worden bij de daaronder ressorterende organisaties (bijv. eHerkenning en/of Logius).

Deze referentiearchitectuur zou ten minste moeten omvatten:

**Datum**  
4 oktober 2011

- Definities van begrippen;
- Architectuurprincipes en visueel model;
- De afbakening van en samenhang tussen authenticatie en autorisatie;
- De invulling in de verschillende, aanverwante domeinen (ambtenaren, burgers, bedrijfsleven).

Voor een dergelijke referentiearchitectuur biedt het voorliggende expertadvies reeds enkele bouwstenen (zoals de op ISO/IEC 10181-3 gebaseerde figuur).

De ambitie hoeft nu nog niet te zijn een bindend architectuurraster op te stellen ('NORA katern'), met alle gerelateerde governance aspecten. Wel zal er medio 2012 een versie moeten (kunnen) zijn, die voldoende substantie en draagvlak heeft om een expertgroep een uitspraak te laten doen over de opname van XACML en de positionering ten opzichte van SAML.

*Ad 3)*

Opname van WS-Policy moet volgens de expertgroep gezien worden in de context van andere webservice-standaarden. Voor de overheid is het WUS-profiel van Digikoppeling hierbij een leidend profiel, waarin wordt beschreven hoe (en: welke) webservice-standaarden ingezet moeten worden.

Mogelijk kan het zinvol zijn om WS-Policy toe te voegen aan het Digikoppeling WUS-profiel. De beste plek om dit te beoordelen lijkt dan ook de beheerprocedure van Digikoppeling te zien. Mocht dit leiden tot een nieuwe versie van het WUS-profiel, dan kan deze indien nodig weer worden aangemeld voor de lijst met open standaarden voor 'pas toe of leg uit'.

De Kamer van Koophandel heeft in de consultatieronde aangegeven dat men ook toepassingsmogelijkheden ziet los van Digikoppeling. Men wijst op de beperkte scope van het WUS-profiel op de lijst met open standaarden voor 'pas toe of leg uit' (kort gesteld: uitwisseling tussen sectoren en met basisregistraties). In de praktijk is de toepassing van het WUS-profiel breder dan enkel dit vastgestelde domein. Om recht te doen aan de opmerking van de Kamer van Koophandel wordt voorgesteld om Digikoppeling ook te vragen op dit punt (toepassing buiten het WUS-profiel) een expertopinie te geven.

## **Toelichting**

*Waar gaat het inhoudelijk over?*

Steeds vaker worden authenticatie en autorisatie van gebruikers van ICT-systemen afgehandeld door een centraal systeem. Dit kan een centraal systeem zijn binnen één organisatie of binnen een groep van organisaties. Deze ontwikkeling wordt ook wel 'externalisering' genoemd. Een voorbeeld hiervan is het gebruik van DigiD als centrale inlogmethode op websites van de overheid.

WS-Policy en XACML zijn twee standaarden die binnen dit domein een rol kunnen spelen. WS-Policy richt zich op het toepassen van beleidsregels (bijvoorbeeld rondom privacy) bij geautomatiseerde berichtenuitwisseling tussen systemen. XACML is een standaard waarmee regels voor autorisatie vastgelegd en uitgewisseld kunnen worden.

*Hoe is het proces verlopen?*

De standaarden zijn aangemeld door Centric. Op basis van de aanmelding is gezocht naar een sponsor binnen de overheid. eHerkenning is bereid gevonden op te treden als sponsor. Vervolgens is een expertgroep geformeerd die heeft gekeken naar de aanmelding en – op verzoek van het Forum – ook in brede zin naar afspraken en standaarden binnen het domein van authenticatie en autorisatie.

**Datum**  
4 oktober 2011

De expertgroep bestond uit 23 experts uit het bedrijfsleven, wetenschap en de overheid.

*Wat is de conclusie van de expertgroep?*

De expertgroep adviseert af te zien van afzonderlijke opname van WS-Policy. Deze standaard richt zich op elektronische berichtenuitwisseling op basis van webservices. Daarvoor is reeds een overheidsbreed profiel ontwikkeld in de vorm van Digikoppeling; dit profiel wordt al verplicht via het 'pas toe of leg uit' regime. De waarde van het zelfstandig opnemen van WS-Policy is daardoor beperkt. Het lijkt de expertgroep dan ook verstandig de keuze over het wel of niet toepassen van WS-Policy als verplichte standaard over te laten aan Digikoppeling.

XACML wordt door de expertgroep bestempeld als kansrijke standaard voor autorisatie. De ervaring met deze standaard is echter nog beperkt. Bovendien ontbreekt het bredere plaatje (referentiearchitectuur) waarin de standaard ingezet zou moeten worden. Daarom wordt geadviseerd de standaard nu nog niet op te nemen op de lijst voor 'pas toe of leg uit'.

*Welke additionele adviezen zijn er?*

De expertgroep onderstreept het belang van samenhang op het gebied van authenticatie en autorisatie. Voor een belangrijk deel zijn er eerst nog onderzoeks- en ontwikkelvraagstukken die opgelost moeten worden, voordat gekeken kan worden naar standaardisatie van het geheel.

De expertgroep noemt de volgende punten:

*De ervaring met externalisering van autorisaties is nog beperkt, het belang van dit onderwerp neemt toe, XACML is een kansrijke standaard*

1. Start met een aantal overheidsorganisaties en marktpartijen pilot trajecten om meer ervaring op te doen bij het gebruik van XACML in de praktijk, deel de resultaten.
2. Onderzoek via deze pilot trajecten in hoeverre het noodzakelijk is om behalve XACML ook specifieke attributen te standaardiseren. Mogelijk is de conclusie dat het noodzakelijk is een profiel te ontwikkelen voor de Nederlandse overheid.
3. Onderzoek via deze pilottrajecten of XACML voorgeschreven moet worden als definitietaal voor autorisatieregels of als protocol voor de uitwisseling daarvan, of voor beide.
4. Onderzoek of versie 2.0 (huidige versie) of juist versie 3.0 (verwachte versie) in aanmerking zou moeten komen voor de lijst voor 'pas toe of leg uit'.

Er is een relatie tussen identificatie, authenticatie en autorisatie en de daarin gebruikte standaarden, in het bijzonder SAML (voor authenticatie) en XACML (voor autorisatie).

**Datum**  
4 oktober 2011

5. Onderzoek of het toepassingsgebied van SAML op de lijst voor 'pas toe of leg uit' verbreed moet worden ten opzichte van de huidige formulering. Bij dit onderzoek zou nadrukkelijk het beschikbare SAML-profiel van XACML betrokken moeten worden.

Er is samenhang gewenst

6. Ga op basis van de ervaringen van overheidsorganisaties na of er noodzaak bestaat tot het voorschrijven van standaarden voor identificatie, authenticatie en autorisatie *binnen* organisaties. De verwachting is dat een infrastructuur voor identificatie, authenticatie en autorisatie binnen een organisatie in toenemende mate ook geschikt moet zijn om met andere organisaties samen te werken.
7. Ontwikkel een referentiearchitectuur voor identificatie, authenticatie en autorisatie binnen de overheid.

Dit laatste punt (referentiearchitectuur) vormt het kernpunt van het advies. In het advies aan het Forum Standaardisatie is dit dan ook als vertrekpunt geformuleerd.

*Wat zijn de reacties in de consultatieronde?*

In de consultatieronde zijn de volgende reacties binnengekomen:

#### Digikoppeling

In een informele reactie geeft Tom Peelen, architect bij Digikoppeling, aan zich te kunnen vinden in het resultaat. Daarnaast complimenteert hij het Forum Standaardisatie met het gevoerde proces inzake deze standaarden.

#### Programmabureau Nederland Open in Verbinding

Het programmabureau Nederland Open in Verbinding heeft kennis genomen van het advies. Aangezien men echter geen kennis/ervaring heeft van de standaard onthoudt men zich van commentaar.

#### Capgemini

Capgemini steunt het expertadvies. Men geeft een aantal extra inhoudelijke aandachtspunten:

- Men onderstreept het belang van een referentiearchitectuur en gemeenschappelijk berichtenkader.
- Het scheidsvlak 'tussen organisaties' en 'binnen organisaties' verdwijnt naar hun mening, door de steeds intensievere samenwerking in ketens en netwerken.
- Men wijst op het belang van voorzieningen/standaarden bij gemeenten voor authenticatie, autorisatie en beveiliging bij gemeenten, o.a. gegeven de ontwikkeling van mGBA.

#### Belastingdienst

De Belastingdienst deelt de opvatting van de experts en onderstreept het belang om hier – bij verdere volwassenheid en draagvlak – nogmaals naar te kijken.

Axiomatics**Datum**

4 oktober 2011

De heer Gaehtgens werkt bij het bedrijf Axiomatics; dit bedrijf levert software voor autorisatieoplossingen op basis van XACML.

In zijn reactie gaat hij in op een aantal aspecten:

- Naar zijn mening is XACML als standaard rijp genoeg voor 'pas toe of leg uit'.
- Hij stelt als belangrijke randvoorwaarde voor het invoeren van geëxternaliseerde autorisatie, dat softwareapplicaties hier klaar voor moeten zijn. Ondanks dat XACML misschien op korte termijn nog niet breed toegepast wordt, zou daarvoor een 'pas toe of leg uit' regime moeten gelden.
- Hij stelt dat er niet een 'one size fits all' is, maar dat er in verschillende situaties verschillende architecturen moeten kunnen zijn.
- Naar zijn mening is versie 3.0, ondanks dat deze nog niet is vastgesteld, al redelijk stabiel. Nieuwe mogelijkheden van versie 3.0 lijken hem van groot belang.

Kamer van Koophandel

De Kamer van Koophandel is het eens met de conclusies ten aanzien van XACML, maar niet eens met de conclusies en voorstellen ten aanzien van WS-Policy. Het expertadvies stelt dat primair bij Digikoppeling de afweging moet worden gemaakt of WS-Policy iets toevoegt aan de overige webservice standaarden voor berichtuitwisseling. De Kamer van Koophandel is echter van mening dat deze afweging door het Forum Standaardisatie gemaakt zou moeten worden. In dit verband wijst men op het feit dat er ook berichtenuitwisseling plaatsvindt, waarbij geen gebruik wordt gemaakt van het Digikoppeling profiel.

Ministerie van EL&I

Door de concernarchitect wordt aangevoerd dat invoering van standaarden als WS-Policy en XACML voorlopig inderdaad nog te ver voert. Men geeft aan dat er mogelijk (voor de korte termijn) eenvoudigere mechanismes zijn.

Direct na binnenkomst van de consultatiereactie is bij het ministerie van EL&I de vraag uitgezet welke mechanismes dit dan zouden kunnen zijn. Bij de verzending van deze oplegnotitie was hier echter nog geen reactie op ontvangen.

*Wat betekenen deze reacties voor het advies?*

Deze reacties ondersteunen in belangrijke mate het advies. Hoewel Axiomatics als leverancier aangeeft dat 'de techniek' er klaar voor is, blijkt dat het voor veel overheidsorganisaties nog te ver voert. Er moet een minimale context zijn. De centrale vraag is dan ook hoe een standaard als XACML – door iedereen als kansrijk bestempeld – ingezet kan worden.

In de opvolging van het expertadvies wordt dan ook voorgesteld primair onderzoek te doen naar (een eerste versie van) een referentiearchitectuur, waarbinnen de diverse standaarden (XACML, SAML) geplaatst kunnen worden. De inhoudelijke opmerkingen (o.a. versie 2.0 of 3.0, rol voor de diverse overheidslagen, etc.) kunnen daarbij betrokken worden.

Door de expertgroep wordt de afzonderlijke toegevoegde waarde van WS-Policy, in tegenstelling tot de Kamer van Koophandel, in twijfel getrokken. Immers: voor webservices geldt dat het WUS-profiel van Digikoppeling voor uitwisseling tussen

organisaties erg gebruikelijk is (en voor veel toepassingen zelfs verplicht via 'pas toe of leg uit'). Desalniettemin wordt voorgesteld om bij de beheerorganisatie Digikoppeling de vraag breder neer te leggen: zijn er mogelijkheden/wenselijkheden voor toepassing binnen Digikoppeling en eventueel ook daarbuiten. Afhankelijk van de uitkomst kan het resultaat meegenomen worden in de gebruikelijke procedure voor de lijst voor 'pas toe of leg uit' (bijvoorbeeld: een nieuwe versie van Digikoppeling, waar ook WS-Policy onderdeel van uit maakt).

**Datum**  
4 oktober 2011

**Bijlagen**

**Datum**  
4 oktober 2011

- Expertadvies Expertadvies WS-Policy en XACML, standaarden voor authenticatie en autorisatie, 5 augustus 2011
- Overzicht reacties consultatieronde
  - Digikoppeling
  - Programmabureau Nederland Open in Verbinding
  - Capgemini
  - Belastingdienst
  - Axiomatics
  - Kamer van Koophandel
  - Ministerie van EL&I