FORUM STANDAARDISATIE

# Expertadvies

# SAML v 2.0

**Auteur(s)**

ir. A.C.M. Smulders, ir D. Krukkert

**Datum**

19 februari 2009

**Versie**

1.2

**Status**

Definitief

# Inhoudsopgave

# Managementsamenvatting

Dit rapport bevat het advies van de expertgroep SAML aan het Forum Standaardisatie en het College Standaardisatie over het opnemen van de SAML v2.0 standaard op de lijst met open standaarden.

De expertgroep is tot de conclusie gekomen dat SAML v2.0 opgenomen kan worden op de lijst met open standaarden.

Belangrijkste punten uit dit advies zijn:

- Door het gebruik van de SAML v2.0 wordt standaard uitwisseling van informatie tussen partijen eenvoudiger en eenduidiger. Dit bevordert interoperabiliteit en reduceert de kans op fouten in de informatievoorziening.
- Met betrekking tot het werkingsgebied van de SAML v2.0 standaard, adviseert de expert groep om geen restricties op te nemen voor het werkingsgebied. Het werkingsgebied is hiermee gelijk aan alle organisaties waarop het comply-or-explain principe van toepassing is, te weten overheden en alle overige (semi-) publieke instellingen.
- Het toepassingsgebied van de standaard betreft federatieve web browser based single-sign-on en single-sign-off. Daar ligt in de praktijk ook het zwaartepunt wat betreft de toepassing van de standaard. Voor andere toepassingsgebieden, zoals enterprise single-sign-on is de standaard niet primair bedoeld.
- De standaard SAML v2.0 voldoet aan de gestelde criteria met betrekking tot openheid, bruikbaarheid en potentieel.
- Het toepassingsgebied heeft impact op de bedrijfsvoering doordat de onderlinge afhankelijkheid toeneemt als gevolg van een nieuwe manier van samenwerken binnen de overheid.
- Het implementeren van de standaard heeft impact op, en dwingt tot het nadenken over, organisatorische inrichting. Onderwerpen die hierbij aan bod zullen komen zijn onder andere welke organisaties welke claims over een persoon kunnen maken, wat de betekenis hiervan is en hoe de controle daarop plaatsvindt.
- SAML v2.0 biedt security functionaliteit en zal dus toegepast worden in gebieden waar security en privacy een rol spelen. Dit betekent dat binnen het toepassingsgebied bij iedere implementatie kritisch gekeken moet worden naar de overwegingen die ten grondslag liggen aan de te maken implementatie keuzes, daar deze grote impact kunnen hebben op security en privacy.

# 1. Doelstelling expertadvies

## 1.1 Achtergrond

De staatssecretaris van Economische Zaken heeft op maandag 17 september 2007 het actieplan open standaarden en open source software aan de Tweede Kamer gestuurd. Het doel van het actieplan is om de informatievoorziening toegankelijker te maken, onafhankelijkheid van ICT-leveranciers te creëren en de weg vrij te maken voor innovatie.

Een onderdeel van het actieplan is het opstellen van een lijst met standaarden, die vallen onder het principe comply or explain. Het College Standaardisatie spreekt zich uit over de standaarden die op de lijst zullen worden opgenomen, o.a. op basis van een expertbeoordeling van de standaard.

De experts zijn verzameld in een afgewogen expertgroep, die de standaard beoordeelt aan de hand van een aantal criteria. Deze criteria - en de uitwerking ervan in de vorm van concrete vragen - worden in het hier voorliggende expertadvies genoemd en behandeld en zijn overgenomen uit het op 14 mei 2008 door het College Standaardisatie geaccordeerde VKA-rapport "Open standaarden: het proces om te komen tot een lijst met open standaarden", te vinden op de website van het Forum Standaardisatie.

De opdracht aan de expertgroep was dan ook om een advies op te stellen over het wel of niet opnemen van de SAML versie 2.0 (hierna te noemen: SAML v2.0), al dan niet onder bepaalde voorwaarden, op de lijst met open standaarden.

## 1.2 Proces

Voor het opstellen van dit advies is de volgende procedure doorlopen.

De expertgroep is begonnen met het individueel scoren van SAML v2.0 op basis van een vragenlijst. Deze vragenlijst bevat de criteria zoals beschreven in het hierboven genoemde rapport. Op basis van de verkregen antwoorden heeft de voorzitter van de expertgroep de verschillende knelpunten geïdentificeerd.

Vervolgens is de expertgroep op 19 januari 2009 bijeen gekomen om met elkaar de bevindingen in het algemeen, en de geïdentificeerde knelpunten in het bijzonder, te bespreken. Tijdens deze bijeenkomst zijn ook het toepassings- en werkingsgebied vastgelegd.

De uitkomsten van de expertgroep zijn door de voorzitter en begeleider verwerkt in dit advies rapport. Een eerste conceptversie is aan de leden van de expertgroep gestuurd met verzoek om

reactie. De ontvangen reacties zijn verwerkt en het rapport is afgerond en ingediend voor de publieke consultatieronde.

## 1.3 Samenstelling expertgroep

Voor de expertgroep zijn personen uitgenodigd die vanuit hun persoonlijke expertise of werkzaamheden bij een bepaalde organisatie direct of indirect betrokken zijn bij de standaard. Daarnaast is een onafhankelijke voorzitter aangezocht om de expertgroep te leiden en als verantwoordelijke voor het uiteindelijke expertadvies.

Als voorzitter is gekozen ir. Andre Smulders. Hij is senior consultant bij NO Informatie- en Communicatietechnologie. In zijn huidige rol heeft hij te maken met informatie-beveiligingsprojecten variërend van technologisch tot strategisch niveau. Tevens is hij coauteur van een basisboek over informatiebeveiliging dat onder een “creative commons” licentie is uitgebracht. De expertgroep is begeleid door ir. Dennis Krukkert, consultant bij TNO Informatie- en Communicatietechnologie.

Aan de expertgroep hebben deelgenomen:

- Jeroen de Beer (Anoigo)
- Lex Borger (Logica)
- Hans Bos (Microsoft)
- Marnix Dekker (GBO, programma DigiD)
- Barry Dukker (IVENT)
- Henk Geurtsen (UWV WERKbedrijf)
- Bart Kerver (ICTU, programma PIP)
- Rene Klomp (SUN Microsystems)
- Bart Knubben (VKA)
- Jacqueline Kok (Atos Origin)
- Jaap Kuipers (Surf)
- Jeroen de Miranda (Siemens)
- Rob van der Staaij (Atos Origin)
- Peter Valkenburg (Everett)
- Ton Verschuren (Innofusie)

- Erik Vullings (TNO)
- Maarten Wegdam (Telematica Instituut)
- Hans Zandbelt (Surf)
- Frank Zwart (ICTU, programma PIP)

## 1.4 Toelichting SAML[1]

De beoordeelde standaard is ontwikkeld door het Security Services Technical Committee van Organization for the Advancement of Structured Information Standards (OASIS). De Security Assertion Markup Language (SAML), is een XML-gebaseerd raamwerk voor het communiceren van gebruikers authenticatie, rechten, en attribuut informatie. SAML biedt organisatie entiteiten de mogelijkheid om claims te maken over de identiteit, attributen en rechten van een subject (een entiteit welke vaak een menselijke gebruiker is) aan andere entiteiten zoals Internet applicaties of diensten. Een voorbeeld van een authenticatieclaim is:

*"Om 09:03 is subject Bob geauthenticeerd op basis van een X.509 certificaat."*

SAML definieert de syntax en bewerkingssemantiek van claims over een subject door een system entiteit. In het proces van het vaststellen van of afhankelijk zijn van deze claims, kunnen SAML systeem entiteiten gebruik maken van andere protocollen (zoals SOAP) om over een claim te communiceren of over het subject van een claim.

Door de expertgroep is versie 2.0 van de SAML standaard beoordeeld.

[1] Tekst is afgeleid van: "S. Cantor et al. Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS SSTC, March 2005. Document ID samlcore-2.0-os. See http://www.oasis-open.org/committees/security/." En: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

# 2. Toepassings- en werkingsgebied

Van overheidsorganisaties wordt verwacht dat zij de lijst met open standaarden hanteren bij aanbestedingstrajecten volgens het comply-or-explain principe. Afhankelijk van de aan te schaffen functionaliteit zal bepaald moeten worden welke koppelvlakken geïmplementeerd moeten worden, en welke standaarden uit de lijst hiervoor ingezet dienen te worden. Om dit te kunnen doen heeft de expertgroep gekeken in welke gevallen SAML v2.0 functioneel gezien gebruik moet worden (toepassingsgebied), en door welke organisaties SAML v2.0 gebruikt zou moeten worden (werkingsgebied)

## 2.1 Toepassingsgebied

De expertgroep heeft ervoor gekozen om de functionele scope van SAML intact te houden. Dit betekent dat SAML v2.0 ingezet kan worden voor (uit SAML standaard): het uitwisselen van autorisatie en authenticatie data tussen security domeinen.

Als toepassingsgebied heeft de expertgroep gekozen voor “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.

Bij het vaststellen van het toepassingsgebied heeft de expertgroep de volgende aspecten in beschouwing genomen:

- SAML standaard heeft in potentie een breed toepassingsgebied. Zo biedt SAML v2.0 meer functionaliteit dan alleen SSO. Het biedt ook de mogelijkheid tot het delen van attributen en kan (eventueel in combinatie met eXtended Access Control Markup Language (XACML) die hiertoe meer gedetailleerde mogelijkheden biedt) ingezet worden voor toegangscontrole en autorisatie.
- In de praktijk blijkt echter dat het toepassingsgebied van deze standaard hoofdzakelijk ligt in het toepassen van SAML in federatieve browser based single-sign-on. Daarbij wordt opgemerkt dat SAML tevens de basis biedt voor single-sign-off, waarmee een gebruiker zich dus via één actie bij alle ingelogde applicaties kan uitloggen, ook weer binnen de afbakening van federatieve browser based informatiesystemen.
- Voor andere functionele toepassingsgebieden zoals bijvoorbeeld enterprise single-sign–on en web service security zijn ook andere standaarden in ontwikkeling of voorhanden. De expertgroep is van mening dat voor deze andere toepassingsgebieden een comply-or-explain principe voor SAML v2.0 te zwaar is, en geen recht doet aan de overige standaarden zoals Kerberos en WS-federation. Op dit moment zijn ontwikkelingen gaande om compatibiliteit

tussen SAML v2.0 en WS-federation te verwezenlijken. Daardoor is op dit moment nog geen uitspraak te doen over welke standaard in dat toepassingsdomein het meest geschikt is.

## 2.2 Werkingsgebied

In relatie tot het gekozen toepassingsgebied is er volgens de expert groep geen nadere afbakening van het werkingsgebied noodzakelijk. Het werkingsgebied is hiermee gelijk aan alle organisaties waarop het comply-or-explain principe van toepassing is, te weten: overheden en instellingen uit de (semi-) publieke sector[2].

2 Zoals vastgelegd in het actieplan “Nederland Open in Verbinding”

# 3. Toetsing van standaard aan criteria

Om te bepalen of SAML opgenomen moet worden op de lijst met open standaarden is deze getoetst aan een aantal criteria. Deze criteria staan beschreven in het rapport, *"Open standaarden, het proces om te komen tot een lijst met open standaarden"*. Dit rapport, d.d. 23 april 2008 is opgesteld door Verdonck, Klooster & Associates. Het resultaat van de toetsing zal in dit hoofdstuk per criterium beschreven worden. Voor de volledigheid is de definitie van elk criterium tevens opgenomen (*cursief*).

## 3.1 Openheid

**Goedkeuring en handhaving**

*De standaard is goedgekeurd en zal worden gehandhaafd door een non-profit organisatie. De lopende ontwikkeling gebeurt op basis van een open besluitvormingsprocedure die toegankelijk is voor alle belanghebbende partijen (consensus of meerderheidsbeschikking enz.);*

De SAML 2.0 standaard wordt goedgekeurd en gehandhaafd door het non-profit consortium OASIS (Organization for the Advancement of Structured Information Standards). OASIS streeft naar convergentie en adaptatie van open standaarden op het gebied van web services. OASIS is opgericht in 1993 en telt meer dan 5000 deelnemers uit ruim 600 organisaties en individuele leden in 100 landen.

OASIS heeft transparante governance en operationele procedures. De technische agenda wordt bepaald door de leden binnen een proces dat gericht is op industrie consensus en focus van inspanningen. Afgerond werk wordt geratificeerd door een open instemmingsronde. Governance is accountable en bevat geen restricties. Leden van zowel het OASIS bestuur als Directeur en technische advies raad worden in een tweejaars cyclus gekozen op basis van een democratisch proces. Consortium leiderschap is gebaseerd op individuele bijdragen en wordt niet beperkt door financiële bijdrage, bedrijfspositie of speciale aanwijzing.

**Beschikbaarheid**

*De standaard is gepubliceerd en over het specificatiedocument van de standaard kan vrijelijk worden beschikt of het is te verkrijgen tegen een nominale bijdrage. Het moet voor een ieder mogelijk zijn om het te kopiëren, beschikbaar te stellen en te gebruiken om niet of tegen een nominale prijs*

De standaard is gratis toegankelijk voor iedereen via de OASIS website.

**Intellectueel eigendom**

*Het intellectuele eigendom – met betrekking tot mogelijk aanwezige patenten – van (delen) van de standaard is onherroepelijk ter beschikking gesteld op een "royalty-free" basis;*

De expertgroep is van mening dat in voldoende mate aan dit criterium wordt voldaan, hoewel strikt genomen patenten niet onherroepelijk ter beschikking worden gesteld.

De expertgroep heeft in haar mening o.a. de volgende aspecten meegenomen:

- Navraag bij OASIS leert dat strikt genomen niet volledig aan dit punt voldaan kan worden, al was het maar omdat eventuele patenten van organisaties buiten OASIS buiten de beïnvloedingssfeer van OASIS zelf liggen. Over het royalty-free beschikbaar stellen van patenten wordt aangegeven dat dit slechts mogelijk is voor organisaties die direct betrokken zijn bij de ontwikkeling van de standaard, en leden van OASIS (die hier een verklaring voor hebben getekend). De expertgroep is echter van mening dat dit niet bezwaarlijk is voor opname op de lijst, mede ook omdat dit voor vrijwel alle standaarden het geval is.
- Om (juridische) zekerheid te krijgen zal er een jurist naar moeten kijken, maar de sterke verwachting is dat niet 100% voldaan kan worden (net zoals dit voor veel standaarden geldt). Over.. Het is niet mogelijk om 100% zekerheid te geven dat er geen enkele organisatie ter wereld ooit een claim zal neerleggen rondom een eventuele patentschending.
- Denemarken hanteert vergelijkbare criteria voor openheid en heeft ook SAML omarmd.

**Hergebruik**

*Er zijn geen beperkingen omtrent het hergebruik van de standaard*

Er worden aan het gebruik van de standaard geen additionele eisen gesteld. Hoewel er in theorie geen garanties gegeven kunnen worden over eventuele patentclaims (zie hierboven), zijn er binnen de expertgroep sinds de introductie van de standaard geen gevallen bekend zijn waarin mogelijke restricties geleid hebben tot conflicten over het gebruik van de standaard.

## 3.2 Bruikbaarheid

**Volwassenheid**

*Is de standaard voldoende uitgekristalliseerd?*

Ja, de standaard heeft een ontwikkeling doorgemaakt naar een versie 2.0. De expertgroep geeft aan dat de standaard daarmee een acceptabele volwassenheid heeft.

*Is verdere ontwikkeling en het onderhoud van de standaard verzekerd?*

Ja, de organisatie die de standaard beheert (OASIS) heeft aangetoond dat zij een stabiele organisatie zijn die over een lange periode in staat is om standaarden te ontwikkelen en beheren.

*Is er een methode waarmee conformiteit aan de standaard bepaald kan worden?*

Ja, er zijn voldoende methoden om de conformiteit aan de standaard te beoordelen. In vergelijking met andere standaarden is dit een indicatie dat de volwassenheid van SAML v2.0 ruim voldoende is.

Binnen de expertgroep worden de volgende manieren genoemd waarmee conformiteit bepaald kan worden:

- Op basis van het conformiteitsdocument dat door OASIS beschikbaar is gesteld (http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf). Toetsing op basis van het conformiteitsdocument past weliswaar niet helemaal binnen het toepassingsgebied (aangenomen wordt dat de gehele standaard wordt geïmplementeerd), maar biedt desalniettemin ruim voldoende mogelijkheden. Binnen OASIS wordt gewerkt aan een conformance toetsing die meer overeenkomt met het praktijkgebruik van SAML v2.0, waarmee verwacht wordt dat voor het toepassingsgebied op termijn specifiekere testen komen.
- XML berichten kunnen tegen de SAML XSD worden gecontroleerd
- Implementaties kunnen middels het Liberty Interoperable programma worden gecontroleerd:http://projectliberty.org/index.php/liberty/liberty_interoperable
- Door middel van testen

*Is er voldoende praktijkervaring met het gebruik van de standaard?*

Ja, de standaard wordt ook opgenomen in veel standaard producten en de meeste leveranciers die actief zijn in het relevante werkveld bieden ondersteuning.

Naast haar eigen kennis en ervaring wordt vanuit de expertgroep een aantal zaken benoemd die dit onderschrijven:

- De Liberty Alliance organisatie concludeert (in haar nieuwsbrief “Liberty alliance global adoption newsletter volume VI fall 2007”) dat er een toenemende adaptatie door overheden (Verenigde Staten, Denemarken, Australie en Nieuw-Zeeland) is van de SAML 2.0 standaard. Daarmee komen ook specifieke overheidsprofielen beschikbaar. De Liberty

Alliance geeft aan dat hoewel een grote uitdaging er een grote kans ligt in het ontwikkelen van een overheid geaccordeerd “overheidsprofiel”.

- Binnen Nieuw-Zeeland loopt al geruime tijd de ontwikkeling van een deployment profiel van de SAML v2.0 specificatie. Het resultaat omvat gebruikergecontroleerde, privacy gebaseerde beleids- en ontwerpbeslissingen.
- Ook op Europees niveau heeft SAML v2.0 de aandacht. ENISA heeft een rapport gepubliceerd over de toepasbaarheid van SAML v2.0 voor het uitdrukken van “Authentication Assurance Levels” (AAL). Het rapport geeft gehoor aan een oproep door het Interoperable Delivery of European e-government services to public Administrations, Businesses and Citizens (IDABC). Het IDABC is een programma dat gemanaged wordt door het Directoraat-Generaal voor Informatica van de Europese Commissie. Het IDABC heeft een voorstel gepubliceerd voor een set van vier Authentication Assurance Levels (AAL), welke ieder een bepaalde sterke karakteriseren voor een authenticatie proces. Het doel van het ENISA rapport is om meer kennis te verkrijgen over de beschikbare opties om AAL uit te drukken in termen van SAML v2.0.
- Toepasbaarheid van SAML v2.0 wordt ook onderzocht binnen het door IDABC gemanaged project, eID/STORK. Het doel daarvan is het onderzoek naar de mogelijkheden van een implementatie van een EU breed inter-operabel systeem voor herkenning van eID en authenticatie. Dit wordt gezien als enabler voor bedrijven, burgers en overheid werknemers om hun nationale elektronische identiteiten in iedere lidstaat te kunnen gebruiken.
- Hoewel er leveranciers zijn die producten leveren die (deels buiten het gekozen toepassingsgebied) meerdere standaarden ondersteunen, doet dit niets af aan de praktijkervaring met de SAML standaard.

*Is er nu en in de toekomst voldoende ondersteuning door (meerdere) marktpartijen voor de standaard?*

Ja, steeds meer marktpartijen gaan dit implementeren, vooral doordat gebruiksorganisaties de standaard ook omarmen. Zie ook hierboven.

*Is de verwachting van het toekomstig gebruik van de standaard positief?*

Ja, zie ook hierboven

**Functionaliteit**

*Wat zijn de functionele eisen die aan de werking van de standaard gesteld worden binnen het voorgestelde toepassingsgebied?In welke mate voldoet de standaard aan deze eisen?Hoe verhoudt zich dit tot concurrerende standaarden?*

Met de aangebrachte afbakening van het toepassingsgebied wordt dat deel van de functionaliteit binnen de standaard geselecteerd dat momenteel in de praktijk het meest toegepast wordt. De algemene consensus dat op basis van deze afbakening er geen concurrerende standaarden zijn. Buiten de gestelde afbakening zijn er wel concurrerende standaarden (zie hieronder)

**Concurrerende standaarden**

*Zijn er concurrerende standaarden?Zo ja, welke en door wie worden die gebruikt?Wat zijn de voor- en nadelen van deze standaard ten opzichte van concurrerende standaarden?*

Nee, bij de gekozen functionele afbakening zijn er geen omvattende alternatieven. WS-federation is voor een deel van het toepassingsgebied een alternatief, maar wordt vrijwel alleen toegepast in Microsoft-omgevingen en heeft nog niet het volwassenheidsniveau van de SAML v2.0 standaard.

## 3.3 Potentieel

*Draagt het opnemen van de standaard op de lijst bij aan het vergroten van de leveranciersonafhankelijkheid?*

Ja, met het opnemen van de standaard op de lijst neemt de uitwisselbaarheid van producten van verschillende leveranciers alleen maar toe neemt.

*Draagt het opnemen van de standaard op de lijst bij aan het vergroten van de interoperabiliteit?*

Ja, het opnemen van de standaard op de lijst draagt bij aan het vergroten van de interoperabiliteit.

Naast het opnemen van de SAML op de lijst met standaarden geeft de expertgroep het volgende advies:

- Door additionele afspraken te maken over bepaalde implementatiekeuzes die SAML nog biedt, kan de interoperabiliteit nog verder vergroot kan worden.

## 3.4 Impact

*De gestelde vragen rondom impact kunnen we als volgt samenvoegen:*

*Wat is de impact van de standaard op de bedrijfsvoering, informatievoorziening, ICT en beveiliging en privacy van de gebruikers van de standaard? Hoe gemakkelijk is de migratie naar de standaard?.*

Het voornaamste risico bij federatieve browser based SSO is de toenemende mate van afhankelijkheid van anderen. Wanneer bijvoorbeeld de centrale Identity Provider (IdP) niet werkt, kan er bij geen enkele Service Provider ingelogd worden. In de bedrijfsvoering zal aandacht moeten zijn voor deze afhankelijkheid die echter niet primair het gevolg van de SAML v2.0 standaard is, maar veel meer samenhangt met de nieuwe manier van samenwerken binnen de overheid. Daarnaast concludeert de expertgroep dat de risico's in de standaard vooral voortkomen uit het de complexiteit van de SAML v2.0 standaard. Net als met elke andere (complexe) standaard brengt dat risico's voor de (technische) implementatie met zich mee.

Het implementeren van de standaard dwingt dat er nagedacht wordt over organisatorische inrichting. Onderwerpen die hierbij aan bod zullen komen zijn onder andere welke organisaties welke claims over een persoon kunnen maken, wat de betekenis hiervan is en hoe de controle daarop plaatsvindt.

SAML v2.0 biedt security functionaliteit en zal dus toegepast worden in gebieden waar security en privacy een rol spelen. Dit betekent dat binnen het toepassingsgebied bij iedere implementatie kritisch gekeken moet worden naar de overwegingen die ten grondslag liggen aan de te maken implementatie keuzes. Daarnaast zijn op het gebied van security en privacy SAML v2.0 specifieke risico's (en maatregelen) aan te wijzen. Binnen de standaard wordt daar ook aandacht aan geschonken in het document: http://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf

Veel van de hierboven genoemde risico's gelden voor alle toepassingen waar identiteits (gerelateerde) gegevens worden verwerkt. In het algemeen worden deze risico's door de expertgroep veel lager ingeschat dan de risico's die samenhangen met het alternatief, niet kiezen voor de SAML v2.0 standaard.

Door het gebruik van de SAML v2.0 standaard wordt uitwisseling van informatie tussen partijen eenvoudiger en eenduidiger. Dit reduceert de kans op fouten in de informatievoorziening.

De standaard biedt de mogelijkheid om anoniem te authenticeren[3]. Dit is een implementatieoverweging. De wenselijkheid zal vooral gebaseerd moeten worden op de eisen vanuit de overheid en de kaders die hiervoor gelden, zoals de Wet bescherming persoonsgegevens. Daarnaast biedt de SAML v2.0 standaard de ruimte om de standaard op verschillende manieren te implementeren. Voorbeelden hiervan zijn anonimiteit en pseudonimiteit. Het is voor de gebruiker niet altijd inzichtelijk welke gegevens verstuurd worden. SAML v2.0 biedt wel de mogelijkheden om dit inzichtelijk te maken, maar bij de implementatie moet hier wel rekening mee worden gehouden (dit probleem is echter generiek voor dit soort systemen). Volgens de expertgroep zijn de grootste privacy risico's te verwachten bij de centrale IdP rol.

Voor wat betreft de migratie van bestaande diensten naar deze standaard, afhankelijk van de inrichting hoeft het niet per definitie zo te zijn dat legacy applicaties aangepast moeten worden. Het is ook mogelijk om bestaande applicaties in te pakken zodat naar buiten toe SAML v2.0 "gepraat" kan worden. In sommige gevallen zal rekening gehouden moeten worden met backwards compatibility van bijvoorbeeld voorzieningen als DigiD. Dit zal bij een migratie naar SAML v2.0 de nodige aandacht vragen.

3 Wel is de identiteit ook in dit geval bekend bij de Identity Provider.

# 4. Advies aan Forum en College

## 4.1 Samenvatting van de toetsingscriteria

Samengevat is het oordeel op de toetsingscriteria als volgt:

- *Openheid*

De standaard voldoet aan de criteria van openheid. Weliswaar wordt er strikt genomen niet voldaan aan “royalty-free” beschikbaar stellen van alle mogelijk aanwezige patenten, omdat dit voor een deel buiten de beïnvloedingssfeer van de beherende organisatie ligt. Het is immers niet te garanderen dat er nooit een organisatie zal opstaan die een patentclaim neerlegt. Dit vormt echter geen belemmering voor opname op de lijst, mede omdat bij de expertgroep geen gevallen bekend zijn waarin restricties geleidt hebben tot conflicten.

- *Bruikbaarheid*

SAML is een volwassen standaard, die inmiddels brede ondersteuning krijgt en waar veel praktijkervaring mee is opgedaan. SAML voldoet aan de eisen die gesteld worden binnen het gekozen toepassingsgebied, en binnen dit toepassingsgebied is er geen alternatieve standaard die dezelfde functionaliteit en volwassenheidsniveau bereikt.

- *Potentieel*

SAML heeft voldoende potentieel wanneer het gaat om het verbeteren van de interoperabiliteit. De leveranciersonafhankelijkheid wordt bovendien versterkt.

- *Impact*

SAML wordt ingezet in omgevingen voor federatieve browser bases SSO, en inzet van deze omgevingen introduceert een zekere afhankelijkheid van andere partijen. Tevens spelen in dit soort omgevingen aspecten als security en privacy een belangrijke rol. Dit is niet direct het gevolg van een keuze voor SAML, maar vraagt wel een kritische blik bij het maken van implementatiekeuzes.

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.

De risico’s van bovengenoemde aspecten worden door de expertgroep lager ingeschat dan die van het alternatief: niet kiezen voor SAML.

## 4.2 Advies

De expertgroep adviseert het college op SAML v2.0 op te nemen op de lijst met open standaarden. Wel zijn er enkele kleine punten geïdentificeerd, maar deze vormen geen belemmering voor opname.