FS 180314.3C

SAML2.0

Evaluatie

Colofon

DATUM	29-01-2018
VERSIE	Definitief
PROJECT REFERENTIE	BFS Evaluatie Standaarden
TOEGANGSRECHTEN	Openbaar
STATUS	Definitief
BEDRIJF	InnoValor
AUTEUR(S)	Bob Hulsebosch & Melissa Roelfsema

Synopsis

Dit rapport evalueert de SAML2.0 standaard tegen een aantal criteria: toepassingsgebied, relevantie, adoptie en ontwikkelingen. De evaluatie is gebaseerd op interviews met experts en medewerkers van organisaties die SAML hebben geïmplementeerd. Uit de evaluatie komt naar voren dat SAML nog voldoet aan de criteria voor de 'pas toe of leg uit' lijst. SAML wordt door veel overheidsorganisaties toegepast, al wordt de interoperabiliteitswinst wel beperkt door de verschillende profielen en implementaties die in gebruik zijn. De opkomende OpenID Connect standaard kan zich op middellange termijn als een alternatief voor SAML ontwikkelen.

Inhoudsopgave

1 Introductie

1.1 AANLEIDING VOOR DE EVALUATIE

De Security Assertion Markup Language (SAML), is een XML-gebaseerd raamwerk voor het communiceren van claims over de identiteit van gebruikers voor authenticatie- en autorisatiedoeleinden bij webdiensten. Versie 2.0 van de inmiddels 17 jaar oude SAML standaard staat al sinds 2009 op de 'pas-toe-of-leg-uit' (PTOLU) lijst van de Nederlandse overheid.

Rondom de opname van SAML2.0 op de PTOLU-lijst is veel te doen geweest. De standaard is nogal 'ruim' gedefinieerd waardoor het op veel verschillende manieren te implementeren is. Dit komt de interoperabiliteit tussen SAML-gebaseerde oplossingen niet ten goede. In 2014 heeft daarom een keer een hertoetsing plaatsgevonden[1]. Een belangrijke uitkomst van die toetsing was om te standaardiseren op een specifiek SAML-profiel, bijvoorbeeld een overheidsprofiel.

SAML2.0 wordt ook wel aangeduid als een 'dode' standaard[2]. Niet omdat de standaard dood is, maar omdat de standaard zich niet meer verder ontwikkeld. Dit zegt overigens niets over het gebruik van de standaard. In 2013 heeft OASIS nog getracht de specificatie op te schonen en uit te breiden met nieuwe functionaliteit[3]. Hier lijkt echter weinig uit te zijn gekomen.

In Nederland maken de identiteitsstelsels eHerkenning, Idensys, iDIN en DigiD gebruik van SAML2.0. SURFnet en Kennisnet hebben de standaard geadopteerd voor federatieve authenticatie in het onderwijsdomein. In het kader van de implementatie van de Europese eIDAS verordening, die in september 2018 van kracht treedt, is ook SAML gewenst.

De afgelopen jaren zijn er diverse, meer moderne en eenvoudigere alternatieven voor SAML ontwikkeld: OAuth en het hierop gebaseerde OpenID Connect. Deze zijn vooral in de mobiele wereld populair en bieden meerwaarde bij machine-to-machine communicatie. OAuth is onlangs getoetst en het Forum Standaardisatie adviseert om de standaard op de PTOLU-lijst te plaatsen met een overheidsprofiel voor gebruik met (REST) API[4]s. Komt OpenID Connect in aanmerking om SAML te vervangen of is het complementair?

1.2 DOEL

Gezien het bovenstaande heeft het Forum Standaardisatie het nodig geacht om de SAML2.0 te evalueren. De evaluatie heeft tot doel om informatie te verschaffen over de huidige relevantie van de standaard, het toepassingsgebied, en de stand van zaken rond de adoptie van de standaard.

De evaluatie beoogt geen oordeel te geven over de vraag of de standaard wel of niet op de PTOLU-lijst moet blijven staan. De resultaten moeten wel voldoende informatie geven voor Forum Standaardisatie ten aanzien van besluitvorming over het handhaven van de standaarden op de PTOLU-uit'-lijst. De resultaten zullen derhalve adviezen bevatten hoe de resultaten van de evaluatie zouden kunnen worden verwerkt in de PTOLU-lijst.

1.3 AANPAK

Voor het evalueren van de standaard is de volgende aanpak gehanteerd:

[1] Expertadvies adoptie SAML 2.0, versie 1.0, Forum Standaardisatie, april 2014, ref FS 49-04-05A, voor meer informatie zie https://www.forumstandaardisatie.nl/sites/bfs/files/proceedings/FS_49-04-05A_Expertadvies_adoptie_SAML.pdf.
[2] SAML is dead. Long live SAML!, KuppingerCole, 2012, zie https://www.kuppingercole.com/events/n40173.
[3] OASIS SAML2.1 wiki, zie https://wiki.oasis-open.org/security/SAML21.
[4] Forum Standaardisatie OAuth, 2017, zie https://www.forumstandaardisatie.nl/standaard/oauth.

1. In overleg met het bureau Forum Standaardisatie (BFS) zijn de evaluatiecriteria opgesteld. Deze komen in grote lijnen overeen met de criteria die worden gehanteerd bij de beoordeling van de standaard om op de PTOLU-lijst te komen.
2. Door de onderzoekers is een eerste evaluatie gemaakt.
3. Een tweede evaluatie is gedaan middels interviews met experts of met medewerkers van organisaties die SAML2.0 hebben geïmplementeerd.
4. De uitkomsten van beide evaluatieactiviteiten zijn verwerkt en gereviewd door medewerkers van het Bureau Forum Standaardisatie.

De volgende partijen zijn geïnterviewd:

- Belastingdienst;
- SURFnet;
- Logius (DigiD en ETD-stelsel);
- Nederlandse Betaalvereniging;
- Ministerie van Defensie;
- RDW;
- ZmartZone (digitale identiteiten experts en ook betrokken geweest bij de toetsing van SAML);
- Anoigo (specialisten op het gebied van SAML integratie/interoperabiliteit);
- InnoValor.

2 Evaluatie

2.1 CRITERIA

De evaluatie heeft tot doel om informatie te verschaffen over de huidige relevantie van de standaard en het toepassingsgebied, en de stand van zaken rond de adoptie van de standaard. De evaluatie concentreert zich met name op de volgende criteria:

- Het *toepassingsgebied*: is deze duidelijk en zo concreet mogelijk geformuleerd en in lijn met de criteria zoals toegepast in de ideaaltypische syntactische structuur[5]. Weet een potentiële gebruiker wanneer de standaard van toepassing is?
- Het *gebruik*: hoe staat het met gebruik van de standaard, waar wordt deze met name toegepast binnen de overheid en wat zijn de toekomstige ontwikkelingen? Wat zijn de ervaringen?
- Het *belang*: heeft de standaard nog toegevoegde waarde? Welk probleem heeft het opgelost?
- Openstaande *adoptiepunten*: bij verschillende standaarden zijn bij opname adviezen meegegeven door het Forum om de adoptie te bevorderen. Zijn deze adviezen opgevolgd en of zijn er nieuwe adoptieadviezen mee te geven?
- Lopende *ontwikkelingen*: wat zijn de toekomstige ontwikkelingen met betrekking tot de standaard en het interoperabiliteitsprobleem dat het oplost? Heeft dit impact voor de positie van de standaard op de lijst? Zijn er ondertussen andere standaarden ontwikkeld die een soortgelijk toepassingsgebied hebben?

De volgende secties evalueren SAML tegen deze criteria.

2.2 TOEPASSINGSGEBIED

De functionele scope van de standaard is in het expert adviesdocument, bij plaatsing op de PTOLU-lijst, als volgt gedefinieerd: “het uitwisselen van autorisatie en authenticatie data tussen security domeinen.” Het toepassingsgebied is als volgt gedefinieerd: “federatieve (web)browser-based single-sign-on (SSO) en single-sign-off”.

Belangrijke elementen in deze definities zijn ‘authenticatie’, ‘federatieve’, ‘web’ en ‘SSO’. Hiermee worden de scope en het toepassingsgebied voldoende volledig en eenduidig afgebakend. Uit de evaluatiegesprekken met de stakeholders komt naar voren dat iedereen redelijk tevreden is met deze twee definities. Twee verbeteringen zijn voorgesteld.

Ten eerste is de scope van ‘browser’-gebaseerde SSO mogelijk iets te nauw; web-gebaseerde SSO dekt het toepassingsgebied wellicht beter af. Dit omdat authenticatie jegens een mobiele/native app onder water vaak via web-gebaseerde standaarden plaats vindt. Een tweede verbeterpunt betreft de term ‘SSO’ in de definitie. Het vigerende normenkader voor betrouwbaarheidsniveaus van het Stelsel voor Elektronische Toegangsdiensten, waaronder eHerkenning en Idensys vallen, staat niet toe dat SSO plaats vindt op de hogere niveaus (LoA3 en 4)[6]. Sectie 2.3.1 lid 2 op niveau LoA3 van het normenkader zegt hierover het volgende: “De toegang tot diensten van elke afzonderlijke dienstverlener MOET het aanloggen met behulp van het authenticatiemiddel vereisen.” SSO is dus niet toegestaan voor LoA3 en dientengevolge ook LoA4. De reden

[5] Ideaaltypische syntactische structuur, 2017, zie https://www.forumstandaardisatie.nl/sites/bfs/files/proceedings/FS%20170419.2D%20Advies%20verduidelijking%20toepassingsgebieden%20v1%200.pdf.

[6] Afsprakenstelsel ETD, Normenkader voor betrouwbaarheidsniveaus, zie https://afsprakenstelsel.etoegang.nl/display/as/Technische+specificaties+en+procedures+voor+uitgifte+van+authenticatiemiddelen

hiervoor is dat het betrouwbaarheidsniveau met SSO tussen dienstverleners te veel wordt ondermijnd omdat de transactie kwetsbaar wordt voor Man-in-the-front en Man-in-the-browser aanvallen. Daarnaast accepteren Dienstverleners in formeel juridische zin een authenticatie en daarmee kan SSO tussen dienstverleners op LoA3 en LoA4 niet alleen meer een oplossing zijn voor gebruiksgemak. Desondanks wordt in de ETD-stelsels SAML gebruikt als standaard voor het uitwisselen van identiteitsverklaringen, en is het wenselijk dit ook zo te doen. Verder is er een opmerking gemaakt over de termen 'autorisatie en authenticatie data'. Wellicht is dit te specifiek en is een beter alternatief om de term 'identiteitsverklaring' te gebruiken.

De definitie van het toepassingsgebied voldoet niet helemaal aan de "Toets ideaaltypische syntactische structuur"[7]. Een mogelijke herdefinitie conform de toets zou als volgt zijn:

"SAML2.0 moet worden toegepast op (1) de uitwisseling van autorisatie en authenticatie data (i.e. identiteitsverklaringen) tussen (2) security domeinen ten behoeve van (5) federatieve web-gebaseerde toegang."

2.3 GEBRUIK

De afgelopen jaren is het gebruik van de SAML-standaard behoorlijk toegenomen. Overheidsvoorzieningen als DigiD, Idensys en eHerkenning voor het authentiseren van burgers en ondernemers/bedrijven zijn allen gebaseerd op SAML2.0. Op deze voorzieningen zijn enkele honderden dienstaanbieders en enkele tientallen authenticatiediensten, makelaars en registers aangesloten[8]. Voor DigiD valt een kanttekening te plaatsen: ongeveer de helft van de ruim 850 aansluitingen is nog gebaseerd op de voorloper van SAML, A-Select[9]. Deze aansluitingen zijn voornamelijk te vinden bij de grote uitvoeringsorganisaties.

De authenticatie-infrastructuur van de banken, iDIN, is ook gebaseerd op SAML. Echter, in iDIN worden SAML-verklaringen 'verpakt' in op iDeal gebaseerde berichtuitwisselingen. Dit betekent dat partijen extra handelingen moeten plegen voordat ze met de SAML verklaringen aan de slag kunnen gaan. De Belastingdienst voert momenteel een pilot uit met iDIN.

Ook de onderwijsfederaties voor primair en voortgezet onderwijs (Kennisnet Entree) en het hoger onderwijs en onderzoek (SURFconext) maken gebruik van SAML. Kennisnet Entree ontsluit meer dan 90% van de scholen in het VO en MBO. Ook steeds meer scholen in het PO melden zich aan. Ruim 100 aanbieders van digitale leermaterialen, van overheid tot uitgeverijen, gebruiken Entree Federatie voor het ontsluiten van hun educatieve diensten.[10] Op SURFconext zijn meer dan 140 instellingen (meer dan 1 miljoen gebruikers) en meer dan 170 clouddiensten aangesloten[11]. Over de hele wereld zijn meer dan 40 van dergelijke SAML onderwijsfederaties te vinden (waaronder landen als Zwitserland, Denemarken, Spanje, Verenigd Koninkrijk, Verenigde Staten, Canada, Brazilië en Australië)[12]. Sommige van deze landen maken gebruik van Shibboleth, een specifiek profiel van SAML (b.v. Zwitserland en de Verenigde Staten).

Daarnaast participeert bijvoorbeeld het Ministerie van Defensie in SAML-gebaseerde federaties als NAVO en Transglobal Secure Collaboration Program (www.tscp.org).

---

[7] Toets ideaaltypische syntactische structuur, 2017, zie https://www.forumstandaardisatie.nl/sites/bfs/files/proceedings/FS%20170614.5A%20Toets%20syntactische%20structuur%20toepassingsgebieden.pdf.

[8] Logius jaarverslag 2016, zie https://logius.online-magazine.nl/nl/magazine/11769/818895/digid.html.

[9] Bron: Logius, inventarisatie die gemaakt is in het kader van routeringsvoorziening.

[10] Zie voor meer informatie https://www.kennisnet.nl/entree-federatie/aangesloten-partijen/.

[11] Dienstbeschrijving SURFconext, 2017, zie https://www.surf.nl/binaries/content/assets/surf/nl/2015/dienstbeschrijving_surfconext.pdf.

[12] EduGain interfederatie, zie https://www.geant.org/Services/Trust_identity_and_security/eduGAIN/Pages/About-eduGAIN.aspx.

Ook Gartner geeft aan dat SAML een 'winner' is voor het realiseren van toegang en bevestigt dit door in zijn Magic Quadrant for Access Management 2017 veel waarde te hechten aan commerciële SAML enterprise oplossingen.

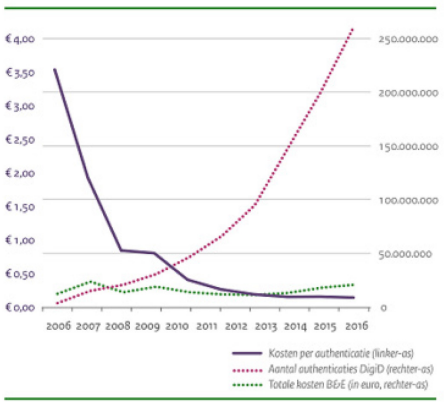
Tot slot is de huidige infrastructuur voor grensoverschrijdende authenticatie in het kader van de Europese eIDAS verordening ook primair op SAML gebaseerd[13]. Alle publieke diensten van de Europese lidstaten die een substantiële of hoge mate van identiteitszekerheid vereisen zullen voor mei 2018 op deze infrastructuur aangesloten moeten zijn. Het Verenigd Koninkrijk heeft een nationale federatieve eID infrastructuur die te vergelijken is met Idensys. Ook deze infrastructuur is op SAML gebaseerd.

Kortom het gebruik van de SAML standaard door overheidsorganisaties, dienstaanbieders en leveranciers in het algemeen is de afgelopen jaren flink toegenomen. Dit gebruik lijkt voorlopig nog toe te nemen, mede door toekomstige ontwikkelingen als eIDAS.

Wel zijn er enkele kanttekeningen te plaatsen bij het gebruik van de standaard. De ervaring leert dat SAML een behoorlijk complexe standaard is. Het vereist specialistische kennis om de standaard op een goede manier te implementeren. Deze kennis is dun gezaaid bij overheidsorganisaties en daardoor duur. Hoewel uit de evaluatie blijkt dat de standaard zelf veilig is, kunnen er kwetsbaarheden ontstaan door fouten in implementaties van de standaard. De gevolgen kunnen, gezien de aard van de standaard, zeer ernstig zijn (denk daarbij aan identiteitsfraude en/of verlies van privacy).

2.4 BELANG

Authenticatie is een essentiële functionaliteit bij digitale dienstverlening. Zonder authenticatie ligt een groot deel van de Nederlandse e-overheid stil. SAML, als standaard voor het uitwisselen van authenticatiegegevens, speelt daarbij een belangrijke, zo niet een essentiële rol. Het staat toe dat burgers en ondernemers hergebruik kunnen maken van hun authenticatiemiddelen. Daarmee verkleint het de digitale sleutelbos, biedt het gebruikersvriendelijkheid, creëert het meer veiligheid en reduceert het kosten. Dit laatste is bijvoorbeeld goed te zien bij DigiD (zie Figuur 1 hieronder). SAML heeft dus wel degelijk een toegevoegde waarde.



Figuur 1: Kosten DigiD vs gebruik ervan. Bron: Jaaroverzicht Logius 2016.

Veel van die toegevoegde waarde komt uit de interoperabiliteit die SAML creëert tussen typisch de authenticatiedienst aan de ene kant en de dienstverlener aan de andere kant. Dit werkt zo bij DigiD, eHerkenning, Idensys, eIDAS, SURFconext, Entree, iDIN en NAVO. Echter, tussen deze verschillende oplossingen is de interoperabiliteit beperkt. De SAML implementatie van DigiD is op onderdelen anders dan die van Idensys

[13] Merk op dat de verordening zelf niets zegt over welke technische standaarden gebruikt moeten worden.

of SURFconext of NAVO. Dienstaanbieders die op meerdere oplossingen zijn aangesloten dienen vaak protocoltranslaties te doen om de ontvangen authenticatiegegevens goed te kunnen verwerken in de achterliggende systemen. Veelal is dit laatste sowieso vereist omdat het SAML-profiel van de achterliggende (enterprise) systemen vaak niet aansluit op het SAML-profiel van de genoemde oplossingen. Dit komt doordat de SAML-standaard door zijn breedheid veel implementatieruimte biedt.

Een mogelijke oplossing hiervoor is om een specifiek SAML-profiel op de PTOLU-lijst te zetten waardoor Nederlandse overheidsorganisaties er gericht(er) mee aan de slag kunnen gaan. De grote vraag is echter welk profiel het beste is. En als er al een specifiek profiel is gekozen, dan zijn er nog steeds risico's. De keuze van een te specifiek/nauw profiel kan ten koste gaan van de interoperabiliteit met leveranciers van software uit andere landen en er nog steeds protocoltranslaties nodig zijn en het kan leiden tot lock-in situaties. Daarnaast is het nog maar de vraag of en in welke mate een specifiek profiel interoperabel is met de huidige SAML implementaties bij overheidsorganisaties. Ofwel, het opnemen van een nieuw, specifiek SAML profiel op de PTOLU-lijst kan nadelig zijn voor de interoperabiliteit of weinig meerwaarde hebben. Het lijkt er op dat het nu te laat is om nog over te tot een gestandaardiseerd specifiek profiel. Zie verder ook de sectie Openstaande Adoptiepunten hieronder.

2.5 OPENSTAANDE ADOPTIEPUNTEN

Het expertadvies van 2009 bevat naast het opnemen van de SAML op de lijst met standaarden nog een tweede advies rondom de adoptie van de standaard:

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

Ook het "Expertadvies Adoptie SAML2.0" uit 2014 bevat een dergelijk advies. Specifiek zijn daar de volgende adoptiepunten aangedragen:

1. Maak via het eID-traject sluitende afspraken over één SAML deployment profiel (d.w.z. koppelvlakspecificatie) voor dienstverleners in de Nederlandse (semi-)publieke sector [eID];
    - Evaluatie: Hier is werk van gemaakt in het ETD-stelsel. Eind 2015 was men klaar met een specifiek SAML profiel voor de overheid. Adoptie ervan door andere stelsels bleek echter niet haalbaar en is later losgelaten door oplossingen als DigiD en iDIN.
2. Ga bij de ontwikkeling van dit deployment profiel uit van de SAML-standaard (incl. errata) en van industry best practices, met name het Kantara interoperabiliteitsprofiel [eID];
    - Evaluatie: Hier is naar gekeken en rekening mee gehouden bij de specificatie van de SAML-koppelvlakken.
3. Word lid van eGovernment Work Group bij Kantara Initiative en eventueel ook van standaardisatie-organisatie OASIS om te leren en om eigen kennis in te brengen. Zorg er mede daarom voor dat documentatie ook in het Engels beschikbaar is [eID];
    - Evaluatie: Is gedaan; Logius is lid. Een actieve bijdrage is echter nooit geleverd.
4. Houd rekening met samenhang met standaarden voor aanverwante domeinen (elektronische handtekening) en met Europese initiatieven (STORK, eIDAS, mandate M/460) [eID ism Forum Standaardisatie];
    - Evaluatie: Het ETD-stelsel is eIDAS compliant gemaakt; aansluiting op de eIDAS infrastructuur wordt op dit moment getest.
5. Beheer het Nederlandse eID deployment profiel als open standaard en betrek stakeholders (leveranciers, overheidsorganisaties en standaardisatie-experts) actief bij de ontwikkeling [eID];
    - Evaluatie: Hier is geen werk van gemaakt. Zie het eerste adoptiepunt.
6. Vraag aan leveranciers of er behoefte bestaat aan een laagdrempelige testvoorziening waarmee leveranciers eenvoudig hun software compatibel kunnen maken met het deployment profiel [eID];

- Evaluatie: Binnen het ETD-stelsel is een testomgeving ontwikkeld waarmee deelnemers kunnen testen of ze SAML-compatibel zijn.

7. Ontwikkel een planning en strategie voor migratie en uitfasering van 'oude' koppelvlakspecificaties [DigiD, eHerkenning, eID];
    - Evaluatie: Hier is nooit een planning voor gemaakt. Dit heeft voor een groot deel te maken met de onrust/onduidelijkheid over de toekomst van voorzieningen voor digitale identiteiten in de publieke en private sectoren.
8. Monitor en waarschuw over kwetsbaarheden in SAML-implementaties [NCSC i.s.m. Logius];
    - Evaluatie: Concrete afspraken hierover zijn nooit gemaakt tussen beide partijen.
9. Onderzoek hoe de opname op de 'pas toe of leg uit'-lijst van SAML kan worden verbeterd. Bekijk daarbij of het nieuwe eID deployment profiel of het eID stelsel NL een 'pas toe of leg uit'-status kunnen krijgen [Forum Standaardisatie i.s.m. eID];
    - Evaluatie: Bij Logius vindt in het kader van de te ontwikkelen routeringsvoorziening om te ontzorgen op dit moment ook een evaluatie van SAML plaats: Wat is de adoptie en wat zijn eventuele kosten voor een migratie naar een specifiek profiel? De onderhavige evaluatie is een ander voorbeeld.
10. Volg de ontwikkelingen rondom OpenID Connect actief [Forum Standaardisatie i.s.m. eID].
    - Evaluatie: het Forum Standaardisatie volgt de ontwikkelingen van OpenID Connect actief. Onlangs is de standaard nog beoordeeld in het kader van de toetsing van OAuth voor opname op de lijst van standaarden.

Veel van de openstaande adoptiepunten zijn opgepakt. Of deze hebben geleid tot een betere adoptie van SAML2.0 valt te betwijfelen. Met andere woorden, het is moeilijk hard te maken dat ze hebben geresulteerd in meer overheidsorganisaties die SAML toepassen en in een verbetering van de interoperabiliteit/uniformiteit van SAML implementaties.

2.6 ONTWIKKELINGEN

De SAML standaard wordt nog steeds door OASIS beheerd. Veel doorontwikkelingen hebben er sinds versie 2.0 niet plaatsgevonden. Uit de evaluatiegesprekken volgt ook dat dit niet noodzakelijkerwijs nodig is. De standaard doet wat hij moet doen, en doorontwikkeling is niet echt nodig.

Interessanter zijn de authenticatie-ontwikkelingen die komen vanuit de sociale netwerk omgevingen als Facebook en Google. Met name het op OAuth gebaseerde OpenID Connect (OIDC) versie 1.0 kan worden gezien als een serieuze concurrent voor SAML2.0. OIDC is een open standaard en biedt ten opzichte van SAML enkele voordelen:

1. Het is veel eenvoudiger te implementeren waardoor het minder specialistische kennis vereist en goedkoper is. Vooral voor dienstaanbieders is dit interessant. Het verlaagt voor hun de drempel om federatieve authenticatie aan te bieden.
2. Het wordt op dit moment al ondersteund door veel grote partijen (waaronder Google, Twitter, Microsoft en Paypal) wat betekent dat de adoptie groot is en er veel gebruikers mee worden bediend. Andere dienstaanbieders zullen het ook willen gaan gebruiken en leveranciers van oplossingen hiervoor zullen het in hun software integreren.
3. Het biedt ook de mogelijkheid om authenticatie voor niet-web-gebaseerde toepassingen zoals native mobiele apps en single-page applicaties te realiseren.

Ook kleven er enkele nadelen aan OIDC:

1. Het is niet geschikt voor federaties als eHerkenning en Idensys waar meerdere partijen op aangesloten zijn die de gebruiker kunnen authentiseren. SAML biedt hiervoor meer/betere handvatten, bijvoorbeeld via de metadata specificatie.

2. In dergelijke multilaterale federaties is OIDC ook minder geschikt voor single-sign-on (SSO). In het geval er een identity provider / OpenID provider is, is dit geen probleem. Binnen het overheidsdomein kan OIDC heel goed worden ingezet voor SSO.
3. Er zijn kanttekening te plaatsen bij de beveiliging ervan (met de kanttekening dat veel kwetsbaarheden debet zijn aan de onderliggende OAuth standaard).

De vraag is of de voordelen van OIDC opwegen tegen de nadelen van het uitfaseren van SAML.

Net als SAML is ook OIDC op verschillende manieren te implementeren. Een specifiek profiel lijkt dus ook wenselijk voor OIDC.

Het gebruik van OIDC neemt langzaam maar gestaag toe. Bijvoorbeeld, SURFnet heeft het geïmplementeerd in SURFconext.

Een aanpalende ontwikkeling is de Europese betaalrichtlijn Payment Service Directive 2. Onderdeel van deze richtlijn is dat alle Europese banken verplicht zijn om bedrijven toegang te verlenen tot de betaalrekening van klanten. De implementatie hiervan met SOAP is niet triviaal, wat inhoud dat SAML lastig te gebruiken is en banken met het REST-gebaseerde OAuth aan de slag zullen moeten. Een dergelijke ontwikkeling vergroot de kans dat banken over zullen gaan op het op OAuth-gebaseerde OIDC voor authenticatie doeleinden.

Uit de evaluatiegesprekken met experts en stakeholders blijkt wel dat men verwacht dat OIDC in de toekomst SAML zal gaan vervangen. De vraag is hoe daar mee om te gaan in de context van de PTOLU-lijst. Verschillende opties zijn mogelijk:

1. Vervang SAML2.0 door OIDC1.0 op de lijst.
2. Plaats beide standaarden op de lijst maar met een verschillend toepassingsgebied.
3. Houd SAML2.0 voorlopig op de lijst en wacht de ontwikkelingen rondom OIDC1.0 nog even af.

Optie 1 heeft als nadeel dat overheidsorganisaties die al SAML2.0 hebben geïmplementeerd, bij nieuwe aanbestedingen aan de slag moeten met OIDC1.0 terwijl ze hiervoor ook SAML2.0 hadden kunnen gebruiken. Deze organisaties moeten in dat geval twee totaal verschillende software-stacks implementeren wat onwenselijk is, tenzij ze gebruik maken van commerciële producten die beide standaarden implementeren (en veel producten doen dat). Bovendien gaat Nederland met OIDC1.0 voorlopen op de rest van Europa/wereld als het gaat om toegang tot publieke diensten. Rondom eIDAS interoperabiliteit kunnen dan problemen ontstaan. Bij overgang van SAML2.0 naar OIDC1.0 is er dus een bepaalde periode waarin organisaties beide standaarden zullen moeten ondersteunen om interoperabel te zijn.

Optie 2 is ook niet optimaal. Ook hier kan de situatie ontstaan dat een organisatie beide standaarden moet ondersteunen om interoperabel te zijn, terwijl het in principe met één standaard had gekund. Dit omdat de toepassingsgebieden van beide standaarden overlappen; iets wat je niet weg kan nemen door een bepaalde definitie van het toepassingsgebied. Bijvoorbeeld, waar SAML zich richt op web-gebaseerde toegang, zou OIDC voor niet-weg-gebaseerde toegang op de lijst kunnen worden gezet. Dit dwingt partijen die beide typen dienstverlening aanbieden tot het gebruik van beide standaarden, terwijl ze OIDC ook voor web-gebaseerde toepassingen hadden kunnen inzetten.

Optie 3 is misschien de verstandigste. Voorlopig SAML2.0 aanhouden als verplichte standaard en organisaties die aan de slag willen met OIDC1.0 en hiervoor een goede reden hebben dit toestaan om te doen (‘leg uit’). Voorwaarde hiervoor is wel dat dit niet ten koste mag gaan van de interoperabiliteit. Een risico hier is dat organisaties een eigen implementatie van OIDC1.0 gaan maken/gebruiken. Enige sturing hierin zou wenselijk zijn. Het Forum Standaardisatie zou daarbij een rol kunnen spelen. Wellicht in de vorm van een concrete uitwerking van het expert advies rondom de toetsing van OAuth. Hiervoor is ook aangegeven dat er een specifieke profiel moet komen voordat de standaard op de lijst komt. OIDC1.0 zou hiervan een invulling kunnen zijn.

De huidige ‘leg uit’ optie komt mogelijk te vervallen met de komst van de nieuwe wet Generieke Digitale Infrastructuur. In de laatste versie van deze wet lijkt het gebruik van bepaalde standaarden een meer verplichtend karakter te krijgen[14]. Onduidelijk is nog of SAML onderdeel gaat uitmaken van de standaarden die onder de wet vallen. Vooralsnog lijkt het voorlopig om een beperkte set internet veiligheidstandaarden te gaan.

Een andere ontwikkeling die van belang is op de positie van SAML als PTOLU-lijst standaard, is de huidige Nederlandse situatie rondom digitale identiteiten. En deze wordt gekenmerkt door veel activiteiten en veel onzekerheden. De overheid is druk bezig om DigiD te verbeteren met Substantieel en Hoog. Daarnaast loopt er een marktconsultatie rondom een alternatief middel[15]. Onduidelijk is of dit middel gebaseerd is op SAML. Als gevolg van de marktconsultatie is het onzeker wat er met Idensys gebeurd. Daarnaast zijn veel organisaties druk om te voldoen aan de in 2018 in werking tredende EU eIDAS-verordening. Gezien deze ‘rumoerige’ situatie van Nederlandse eID markt is het niet verstandig om ook nog te gaan tornen aan standaarden voor eID uitwisseling. Veel organisaties hebben op dit moment een afwachtende houden en zitten niet te wachten op nieuwe ontwikkeltrajecten.

[14] Wet generieke digitale infrastructuur, augustus 2017, zie https://www.rijksoverheid.nl/documenten/publicaties/2017/08/30/wetsontwerp-generieke-digitale-infrastructuur-gdi.
[15] Marktconsultatie eID, 2017, zie https://www.digitaleoverheid.nl/nieuws/start-marktconsultatie-eid/.

3 Conclusies

Uit de evaluatie blijkt dat SAML2.0 een relevante standaard is voor de uitwisseling van authenticatie-informatie ten behoeve van federatieve en web-gebaseerde toegang. Veel publieke en semi-publieke organisaties maken er gebruik van. Kanttekens kunnen worden geplaatst bij de vraag of het plaatsen van SAML op de PTOLU-lijst heeft geresulteerd in betere interoperabiliteit. Door de complexiteit en breedte van de standaard zijn er diverse implementaties in gebruik en wordt er door organisaties regelmatig gebruik gemaakt van protocoltranslatie-functionaliteit. Het ultieme doel van de standaard, maximale interoperabiliteit, is dus ten dele gerealiseerd.

Het standaardiseren van een specifiek SAML profiel kan hier verbetering in brengen. De vraag is echter of dit niet te laat komt. Bovendien blijkt het lastig om tot een bepaald profiel te komen die voorziet in alle eisen, wensen en mogelijkheden van de betrokken organisaties. Daarnaast is er een opkomende standaard, OpenID1.0 Connect, die qua toepassingsgebied grotendeels overlapt met en zelfs meer biedt dan SAML2.0. OpenID Connect wordt door iedereen als een toekomstige standaard voor authenticatie gezien. De vraag is of beide standaarden naast elkaar op de PTOLU-lijst kunnen staan. Een kunstmatig onderscheid tussen beide standaarden is te creëren door de toepassingsgebieden verschillend te definiëren. Maar erg wenselijk is dit niet omdat het organisaties dwingt om in sommige gevallen beide standaarden te gebruiken terwijl ze met één klaar hadden kunnen zijn.

Verstandiger lijkt om SAML2.0 voorlopig op de PTOLU-lijst te houden en organisaties die hier vanaf willen wijken door OpenID Connect te gebruiken te gedogen. Wel is sturing op de juiste implementatie ervan vereist om toekomstige interoperabiliteit en standaardisatie te borgen. Aandachtspunt hier is de aankomende wet Generieke Digitale Infrastructuur. Daarin lijkt het verplichtende karakter voor het gebruik van bepaalde standaarden belangrijker te zijn geworden en lijkt er minder ruimte voor ‘leg uit’ om af te zien van een bepaalde verplichte standaard. Voor SAML en de opkomst van OpenID Connect lijkt dit niet wenselijk (i.e. dat SAML verplicht wordt gesteld).

Andere overwegingen voor het Forum Standaardisatie die uit de evaluatie volgen zijn:

- Overweeg het toepassingsgebied van SAML aan te scherpen. Overweeg daarbij om te abstraheren van een specifieke authenticatiestandaard. De PTOLU-lijst zal hierdoor minder standaard-oriënterend zijn, maar veel meer een lijst eisen waaraan standaarden moeten voldoen. Bijvoorbeeld: “Er zullen standaarden worden ingezet voor het uitwisselen van identiteitsverklaringen voor federatieve toegang”. Technische standaarden waarmee dit ingevuld kan worden zijn: SAML2.0, OpenID Connect1.0, OAuth,…. Dit zal ten koste gaan van de interoperabiliteit, maar biedt partijen de keuze om zelf te bepalen met welke standaard(en) ze aan de slag wil(len) gaan. Daarnaast wordt voorkomen dat ze gedwongen worden om één bepaalde standaard te implementeren (omdat de PTOLU-lijst dat voorschrijf) die niet optimaal voorziet in de behoefte, of worden ze gedwongen om meerdere standaarden te implementeren terwijl het met een standaard had gekund.
- Geef meer support nadat een standaard op de PTOLU-lijst is geplaatst. Denk hierbij aan handreikingen, (technisch) advies, een referentie-implementatie, een toolkit / SDK, etc. Dit helpt organisaties om sneller en effectiever met een standaard aan de slag te gaan en voorkomt dat er diverse verschillende implementaties ervan ontstaan. Concreet voor SAML lijkt er veel vraag te zijn naar een technisch specialist die partijen adviseert hoe zij het beste de standaard op een interoperabele manier kunnen implementeren. Deze specialist borgt een meer uniforme implementatie van de standaard bij overheidsorganisaties.

- Denk na over hoe een PTOLU-standaard uit te faseren ten faveure van een nieuwe, moderne standaard. Wat is een goed moment? Wat betekent het voor de interoperabiliteit? Is er een overgangssituatie, en zoja, hoelang duurt deze situatie?