Expertadvies adoptie SAML 2.0

Forum Standaardisatie

Versie:	1.0
Status:	Definitief
Datum:	3 april 2014

Colofon

Projectnaam	Expertadvies adoptie SAML 2.0
Versienummer	1.0 definitief
Organisatie	Forum Standaardisatie Postbus 96810 2509 JE Den Haag forumstandaardisatie@logius.nl

Auteurs	Dennis Krukkert (TNO) Martijn Oostdijk (InnoValor, voorheen: Novay) Bart Knubben (BFS)

Inhoudsopgave

1 Inleiding 4

1.1 Aanleiding 4

1.2 Eerdere adoptie-activiteiten Forum Standaardisatie 4

1.3 Proces adoptie-evaluatie 5

1.4 Geïnterviewde experts 5

2 Over de standaard SAML 6

2.1 SAML 2.0 6

2.2 Profielen voor SAML 7

2.3 Relatie met andere standaarden 8

3 Stakeholderanalyse 10

4 Analyse van de adoptie: kansen en drempels 11

4.1 Bekendheid van de standaard 11

4.2 Kennisdimensie 11

4.3 Technische dimensie 12

4.4 Financiële dimensie 13

4.5 Organisatorische dimensie 13

4.6 Maatschappelijke ontwikkelingen 14

4.7 Internationale ontwikkelingen 14

5 Conclusies en adoptie-adviezen 15

5.1 Conclusies 15

5.2 Adoptie-adviezen 15

1 Inleiding

1.1 Aanleiding

Het Forum heeft in zijn vergadering van 29 oktober 2013 besloten om de adoptie van SAML versie 2.0 formeel te evalueren en te bezien of aanvullende adoptie-maatregelen nodig zijn.[1] Deze standaard is sinds 2009 opgenomen op de lijst met open standaarden voor 'pas toe of leg uit' met als functioneel toepassingsgebied "federatieve (web)browser-based single-sign-on (SSO) en single-sign-off".[2] Dit adoptie-expertadvies geeft invulling aan het besluit van het Forum.

1.2 Eerdere adoptie-activiteiten Forum Standaardisatie

Het Forum Standaardisatie heeft sinds de opname van SAML op de 'pas toe of leg uit'-lijst de onderstaande activiteiten die verband houden met SAML uitgevoerd:

- Twee SAML-kennissessies in 2010 en 2011[3];
- Forum-advies (FS 32-06-07) n.a.v. 2de SAML-kennissessie;
- Toetsing van XACML-standaard (autorisatie-gegevens);
- Toetsing eHerkenning overheidskoppelvlak[4];
- 3de SAML-kennissessie en oprichting Community Identitymanagement, Standaarden & Interoperabiliteit (semi-)Publieke sector (CISIP) in 2013;
- Internationale expertsessie rondom eID in 2013.

SAML wordt inmiddels toegepast door o.a. DigiD, DigiD Machtigen, eHerkenning, SURFconext, Kennisnet Entree en in shared services van het Rijk en zal naar verwachting ook binnen het eID-stelsel relevant zijn. Een belangrijk thema tijdens de kennissessies was het voorkomen van uiteenlopende implementatie-keuzes van de standaard. Gepoogd is om door onderlinge kennisuitwisseling de verschillen te minimaliseren. Daarbij is o.a. gewezen op het Kantara interoperabiliteitsprofiel waarop verschillende deployment profielen in het buitenland zijn gebaseerd. Bij de toetsing van het Koppelvlak eHerkenning in 2012 is naar voren gekomen dat er desondanks uiteenlopende keuzes zijn gemaakt, die hinderlijk kunnen zijn voor de interoperabiliteit en adoptie.

Forum Standaardisatie vervult een formele adviesrol met betrekking tot interoperabiliteit en standaarden in het traject rondo het Nederlandse eID-stelsel.[5] De uitkomst van de voorliggende adoptie-evaluatie van SAML zal ook in dat kader worden gebruikt.

---

[1] Forum-notitie FS 46-10-04, *http://www.forumstandaardisatie.nl/fileadmin/os/Vergaderstukken/FS_46-10-04_Oplegnotitie_Adoptie_open_standaarden.pdf*

[2] 'Pas toe of leg uit'-lijst: *http://www.forumstandaardisatie.nl/ptolu*

[3] Kennissessies SAML: *https://www.ictu.nl/archief/wiki.noiv.nl/xwiki/bin/view/OpenStandaarden/SAML.html#HKennissessiesSAML*

[4] Toetsing eHerkenning Overheidskoppelvlak: *https://lijsten.forumstandaardisatie.nl/open-standaarden/eherkenning-overheidskoppelvlak*

[5] Reactie van Forum Standaardisatie op 'Ontwerp op hoofdlijnen van de werking van het eID Stelsel NL', *http://www.forumstandaardisatie.nl/fileadmin/os/Vergaderstukken/FS_45-09-07C_20130822_Notitie_reactie_eID_v09.pdf*

1.3 Proces adoptie-evaluatie

De adoptie-evaluatie is uitgevoerd door Dennis Krukkert (TNO) Martijn Oostdijk (InnoValor, voorheen: Novay). Zij hebben daarvoor gebruikgemaakt van het "sjabloon voor een adoptieaanpak per open standaard" [6] zoals is vastgesteld door het Forum Standaardisatie. De invalshoeken uit dit sjabloon zijn gehanteerd in de interviews en komen ook terug in het expertadvies.

Voor het opstellen van dit advies zijn de volgende processtappen doorlopen.

1. Gesprekken met opdrachtgever Bureau Forum Standaardisatie;
2. Deskresearch;
3. Interviews met experts;
4. Opstellen concept-expertadvies;
5. Feedback van experts op concept-expertadvies;
6. Verwerking feedback in definitief expertadvies.

Het Forum Standaardisatie zal op basis van het expertadvies een advies aan het College Standaardisatie opstellen.

1.4 Geïnterviewde experts

Er hebben interviewgesprekken plaatsgevonden met de onderstaande personen.

- Joost van Dijk, SURFnet
- Jelle Jelsma, RDW
- Rainer Hörbe, onafhankelijk adviseur, chair van eGovernment Work Group bij Kantara Initiative
- Joris Joosten, DigiD/Logius
- Peter Groeneveld, eHerkenning/Logius

Daarnaast heeft Bureau Forum Standaardisatie contact gehad met de onderstaande personen over de adoptie van SAML:

- Hans-Rob de Reus, eID stelsel NL/Belastingdienst
- Dick Dekkers, Digidentity
- Benoist Claasen, Digidentity
- Patrick Nelissen, Funatic BV

Het advies is in concept-vorm aan de bovenstaande personen ter review voorgelegd. Het concept is daarnaast voorgelegd aan Guus Bronkhorst (BZK) en Matthijs Claessen (Logius).

Tot slot hebben er gesprekken gevoerd met Bart Knubben en Maarten van der Veen van Bureau Forum Standaardisatie.

[6] Forum-notitie FS 43-04-06B: *https://www.forumstandaardisatie.nl/fileadmin/os/Vergaderstukken/FS_43-04-06B_Conceptversie_standaard_sjabloon_voor_adopt.pdf*

2 Over de standaard SAML

2.1 SAML 2.0

SAML versie 2.0 is ontwikkeld door de Security Services Technical Committee van OASIS dat leden heeft die afkomstig zijn van softwareleveranciers en bedrijven maar ook van onderwijsinstellingen en overheden.[7] De standaard is in 2005 vastgesteld door standaardisatieorganisatie OASIS.[8]

SAML standaardiseert het berichtenverkeer tussen een Identity Provider (IdP) en een Service Provider (SP). Een IdP is een partij die verantwoordelijk is voor authenticatie van gebruikers en die identiteits-attributen van gebruikers kan verschaffen. Een SP is een dienstverlener die een elektronische dienst aanbiedt aan de gebruikers. Een constellatie van bij elkaar horende IdPs en SPs wordt een (SAML-) federatie genoemd.

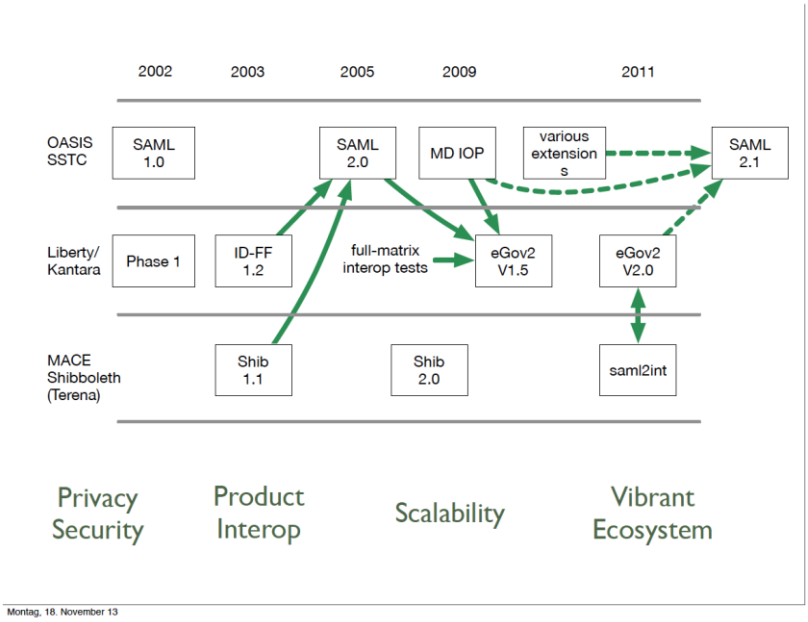
De SAML-specificatie schrijft met name voor:
- het XML gebaseerde berichtformaat voor de identiteitsattributen (assertions);
- welke protocollen er gebruikt worden (welke berichten, in welke volgorde, tussen welke partijen worden uitgewisseld);
- en hoe deze berichten getransporteerd worden (de zogenaamde binding).

SAML wordt ingezet bij webgebaseerde diensten. Identiteiten kunnen, dankzij SAML, herbruikbaar gemaakt worden doordat de IdP en de SP niet dezelfde partij hoeven te zijn en zodat meerdere SP's van één en dezelfde IdP gebruik kunnen maken. Daarbij wordt SAML vaak ook ingezet om Single Sign On voor web-diensten te realiseren. Een gebruiker hoeft dan eenmalig in te loggen om van meerdere diensten binnen de federatie gebruik te kunnen maken. Voor dit toepassingsgebied is de standaard opgenomen op de 'pas toe of leg uit'-lijst, maar de standaard is breder inzetbaar zoals bijvoorbeeld voor het uitwisselen van autorisatie-informatie.

Na de vaststelling in 2005 heeft OASIS vijf errata voor SAML gepubliceerd. De laatste aanvulling dateert van mei 2012 [SAML v2.0 Errata 05].[9] Daarnaast heeft OASIS verschillende aanvullende Committee Specifications gepubliceerd zoals "SAML V2.0 Channel Binding Extensions Version 1.0" (2012) en "SAML V2.0 Asynchronous Single Logout Protocol Extension Version 1.0" (2013).[10] Ondertussen wordt door OASIS gewerkt aan SAML 2.1. De ontwikkelingen daaraan verkeren echter in een pril stadium.

[7] Security Services Technical Committee van OASIS, *https://www.oasis-open.org/committees/security*
[8] Specificatie van OASIS Security Assertion Markup Language (SAML) V2.0, *http://docs.oasis-open.org/security/saml/v2.0/*
[9] SAML Version 2.0 Errata 05. 01 May 2012. OASIS Approved Errata. *http://docs.oasis-open.org/security/saml/v2.0/errata05/os/saml-v2.0-errata05-os.html*
[10] Overzicht van SAML-documentatie: *https://wiki.oasis-open.org/security*

In 2012 kwam een kwetsbaarheid in diverse SAML-implementaties aan het licht ("signature exclusion attack").[11] Met enige regelmaat worden er ook andere kwetsbaarheden gevonden in SAML-software.[12] Voor alle duidelijkheid: het gaat hier dus om kwetsbaarheden in implementaties van de standaard en niet om kwetsbaarheden in de standaard zelf.



Figuur 1: Historie van SAML-standaard (bron: Kantara Initiative)

2.2 Profielen voor SAML

De SAML 2.0 specificatie biedt ruimte voor invulling. Binnen een federatie zijn daarom nadere technische afspraken in de vorm van deployment profielen nodig om SPs en IdPs op elkaar aan te kunnen sluiten.

In de originele SAML 2.0 specificatie uit 2005 is een aantal profielenpgenomen (o.a. het veelgebruikte Web-SSO profiel), maar in een concrete federatie moet een profiel nog nader ingevuld worden. Men spreekt dan over een deployment profiel. Een deployment profiel is meestal specifiek voor één federatie. De specificaties van DigiD en eHerkenning zijn bijvoorbeeld deployment profielen.

Daarnaast bestaat het "SAML 2.0 eGov Implementation Profile" van Kantara Initiative (de opvolger van de Liberty Alliance die aan de basis stond van de SAML-standaard).[13] Versie 2.0 van dit profiel dateert van 2010. Dit betreft een interoperabiliteitsprofiel[14] dat algemenere keuzes voor interoperabiliteit bevat en toepasbaar is op meerdere federaties. Het is oorspronkelijk ontwikkeld door overheden maar is zeker ook bruikbaar voor federaties buiten de overheid. Het Kantara interoperabiliteitsprofiel

[11] "On Breaking SAML: Be Whoever You Want to Be", *http://www.nds.rub.de/research/publications/BreakingSAML/*

[12] Overzicht van kwetsbaarheden in SAML-software: *http://web.nvd.nist.gov/view/vuln/search-results?query=saml*

[13] "SAML 2.0 eGov Implementation Profile" van Kantara Inititiative: *https://kantarainitiative.org/confluence/display/fiwg/SAML+Interoperability+and+Deployment+Profiles*

[14] De term 'implementation profile' suggereert dat dit profiel geen implementatiekeuzes meer open laat. Het gaat hier echter om een profiel dat qua abstractie boven concrete deployment profielen staat.

wordt beschouwd als een 'industry best practice', ook door Nederlandse experts. De eerste definitieve versie van dit profiel werd in 2008 gepubliceerd. Tijdens de SAML-kennissessies, die door Forum Standaardisatie in 2010, 2011 en 2013 zijn georganiseerd met betrokkenheid van o.a. eHerkenning en DigiD, is gewezen op dit profiel.

In recentere jaren zijn ook in andere landen deployment profielen gedefinieerd. Een aantal landen, te weten Oostenrijk, Canada, Denemarken, Finland, de VS, en Nieuw Zeeland baseert z'n nationale deployment profiel op het Kantara interoperabiliteitsprofiel (zie figuur 2).

SAML2INT heeft het "Interoperable SAML 2.0 Profile" ontwikkeld.[15] Dit is een deployment profile dat veel wordt gebuikt in de onderwijswereld, zoals door SURFnet in haar dienst SURFconext. Er loopt een initiatief om het SAML2INT deployment profiel meer in overeenstemming te brengen met het Kantara interoperabiliteitsprofiel.

De ideeën uit het Kantara interoperabiliteitsprofiel en het SAML2INT deloyment profile neemt OASIS bij de ontwikkeling nieuwe versie van SAML waarvan het nog niet duidelijk wanneer deze gereed zal zijn.

Binnen het Europese project STORK wordt gekeken naar grensoverstijgend gebruik van nationale identiteitsoplossingen. Binnen STORK is ook een koppelvlakspecificatie op basis van SAML ontwikkeld.[16] Het gebruikte profiel sluit niet goed aan bij het Kantara interoperabiliteitsprofiel. Er is een initiatief gestart om de twee meer in overeenstemming met elkaar te brengen.[17]

2.3 Relatie met andere standaarden

XACML is een aan SAML 2.0 gerelateerde, complementaire standaard, waarbij niet authenticatie en attribuutbeheer herbruikbaar gemaakt worden, maar autorisatieregels. Net als bij SAML 2.0 is XACML 2.0 zeer uitgebreid en beschrijft de standaard: berichten syntax, protocollen, en transportmechanismen. eHerkenning maakt gebruikt van XACML voor het machtigingenregister. XACML is in 2011 getoetst voor de 'pas toe of leg uit'-lijst. Het Forum Standaardisatie is destijds tot de conclusie gekomen dat XACML veelbelovend was maar dat een 'pas toe of leg uit'-status op dat moment, met name gezien de beperkte ervaring binnen de overheid, nog niet opportuun was. Ondertussen is versie 3.0 van de standaard gepubliceerd.

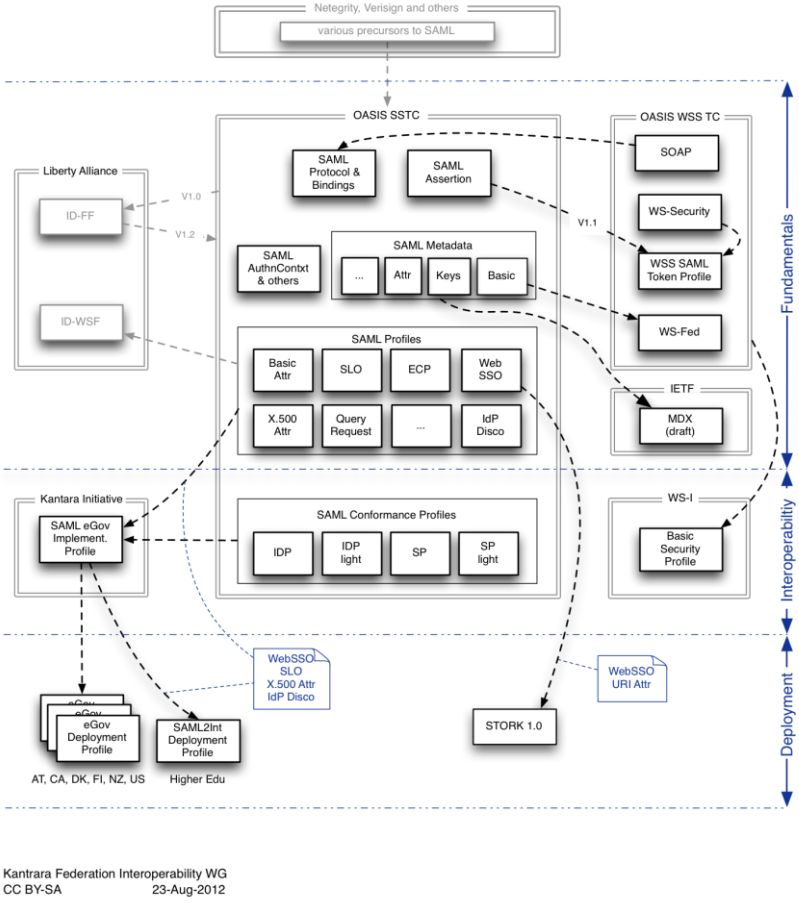
WS-Federation (en de onderliggende WS-* stack) vormt een alternatief voor SAML dat minder wijdverbreid en voornamelijk in Microsoft / .NET omgevingen populair is. De standaarden overlappen maar zijn deels ook complementair. Binnen WS-Federation wordt SAML bijvoorbeeld regelmatig gebruikt als berichtformaat voor de identiteitsattributen (assertions).

OpenID Connect (gebaseerd op OAuth 2.0) is een relatief jonge standaard die vooral in het social network domein populair is. OpenID Connect en OAuth 2.0 worden gebruikt om toegang tot RESTful web-

[15] "Interoperable SAML 2.0 Profile" van SAML2INT, *http://saml2int.org/*
[16] "D5.8.3b Interface Specification" van STORK, *https://www.eid-stork.eu*
[17] STORK/SAML Interoperability WG, *https://refeds.terena.org/index.php/STORK/SAML_Interoperability_WG*

services te reguleren en worden ook veel gebruikt in non-web clients, zoals mobiele applicaties. De nieuwe standaarden komen wat meer uit de internet-hoek, terwijl SAML zijn oorsprong vindt in het bedrijfsmatige domein. OpenID Connect beperkt zich tot Web SSO en mist bijvoorbeeld de mogelijkheid om gestandaardiseerd autorisatie-attributen door te geven. Hoewel OpenID Connect veelbelovend is, lijkt de standaard op dit moment qua focus en volwassenheid geen meerwaarde te bieden ten opzichte van SAML2.0 in grootschalige overheidsfederaties. Begin 2013 is door Novay in opdracht van SURFnet een vergelijking[18] gemaakt tussen OpenID Connect en SAML 2.0.

SAML maakt gebruik van **XML** en kan (als binding) gebruik maken van **SOAP** en **HTTP**. **HTTPS/TLS** en **XMLSig**, **XMLEnc** (beide onderdeel van XML) en onderliggende standaarden (zoals bijvoorbeeld **X.509**) kunnen gebruikt worden binnen SAML 2.0 om de vertrouwelijkheid en integriteit van het berichtenverkeer te beschermen.



Figuur 2: Samenhang van SAML met andere standaarden en profielen (bron: Kantara Initiative)

[18] "OpenID Connect for SURFconext, Assessment of the OpenID Connect protocol for Federations of Higher Education and Research", *https://blog.surfnet.nl/wp-content/uploads/2013/04/SURFnet-OpenID-Connect-1.1-.pdf*.

3 Stakeholderanalyse

Er kan, vanuit SAML oogpunt, onderscheid gemaakt worden tussen twee categorieën stakeholders:

(1) Partijen die in het primaire proces van een SAML federatie een rol spelen (actief SAML berichten genereren, doorgeven, interpreteren, …), zoals:
    a. Eindgebruiker;
    b. Identity provider;
    c. Service provider (SP, ook wel dienstverlener of relying party);
    d. Federatie operator (de hub, broker, meta-data repository, …);
(2) Partijen die het primaire proces slechts faciliteren zoals:
    a. Standaardisatieorganisaties;
    b. Trust framework eigenaar (ook beheerder implementatieprofiel);
    c. Softwareleverancies.

Sommige van deze rollen kunnen in de praktijk samenvallen en bij één partij belegd worden. DigiD is bijvoorbeeld de centrale identity provider in een federatie met verder alleen service providers, het is dan logisch om DigiD ook de rollen federatie operator, en trust framework eigenaar te geven. Bij eHerkenning spelen marktpartijen juist de rol van identity provider.

Een SAML-federatie biedt, in principe, voordelen in termen van kosten, beveiliging en gebruiksgemak. De voordelen zijn voornamelijk voor de dienstverlener (die een aantal verantwoordelijkheden uitbesteedt aan de identity provider) en voor de eindgebruiker (die minder identiteitsaccounts hoeft aan te houden).

De federatie operator bepaalt (in samenspraak met stakeholders) het deployment profiel voor SAML. Voor de adoptie is met name van belang in welke mate de producten van softwareleveranciers eenvoudig dit deployment profiel kunnen ondersteunen. De kaders die standaardisatieorganisaties (OASIS en Kantara) stellen bieden daarvoor houvast.

Verschillende stakeholders, met name dienstverleners, hebben in het verleden mogelijk geïnvesteerd in identiteitsinfrastructuur. Deze stakeholders hebben er vervolgens belang bij om de kosten om vanuit die bestaande situatie aan te sluiten bij de SAML-federatie zo laag mogelijk te houden.

Ook bij de identity provider(s) of bij de trust framework eigenaar kan reeds bestaande identiteitsinfrastructuur of andere legacy overwegingen van invloed zijn op toekomstige implementatiekeuzes m.b.t. SAML. Zo heeft DigiD voor zijn SAML-implementatie de eerdere keuzes van DigiD Eenmalig Inloggen voor een belangrijk deel overgenomen.

4 Analyse van de adoptie: kansen en drempels

In dit deel zal aan de hand van de volgende invalshoeken worden ingegaan op de adoptie van de open standaard zelf.

1) Bekendheid van de standaard
2) Kennisdimensie
3) Technische dimensie
4) Financiële dimensie
5) Organisatorische dimensie
6) Maatschappelijke ontwikkelingen
7) Internationale ontwikkelingen

4.1 Bekendheid van de standaard

De bekendheid van de standaard is naar mening van de geïnterviewde experts de afgelopen jaren sterk gegroeid en is ondertussen aanzienlijk. De status van SAML 2.0 als standaard voor gefedereerd identiteitsmanagement en single-sign on lijkt onomstreden.

De standaard is 'proven technology' en wordt ingezet door het verschillende commerciële aanbieders van webdiensten, zoals door Google, Amazon, ING bank. Ook binnen de publieke sector wordt de standaard veel gebruikt, zowel in binnenland als buitenland. DigiD, DigiD Machtigen, eHerkenning, SURFconext, Kennisnet Entree gaan allemaal uit van SAML. Ook voor shared services van het Rijk wordt SAML ingezet (bijv. single sign on voor P-direkt). Het in ontwikkeling zijnde eID-stelsel lijkt eveneens uit te gaan van SAML.

In het najaar van 2013 waren er 32 overheidsorganisatie op het SAML-koppelvlak van DigiD aangesloten. De overige aangesloten overheidsorganisaties maakten nog gebruik van het 'oude' Aselect-koppelvlak. In diezelfde periode waren 72 partijen via SAML op de eHerkennings-federatie aangesloten.

Een alternatief voor SAML, WS-Federation, is vooral populair in Microsoft-only omgevingen. Microsoft biedt in zijn producten zelf ook ondersteuning voor SAML.

Aan nieuwere standaarden (OAuth 2.0 en het daarop gebaseerde OpenID Connect) wordt gewerkt. Deze standaarden komen uit de hoek van social media, worden als minder complex ervaren en zijn bij uitstek geschikt voor mobiele apparaten. Deze standaarden zijn op dit moment nog niet volwassen genoeg om de positie van SAML 2.0 te bedreigen.

Hier lijkt geen sprake van een adoptiedrempel. Het is wel aan te bevelen om de ontwikkelingen rondom OpenID Connect in de gaten te houden.

4.2 Kennisdimensie

In de praktijk is o.a. bij DigiD en eHerkenning gebleken dat het niet altijd eenvoudig is voor dienstverleners om bestaande software te configureren conform de deployment profielen van DigiD en eHerkenning. Vaak is een aanzienlijke hoeveelheid specialistische kennis nodig. Door het toegenomen gebruik van SAML is de kennis rondom de standaard weliswaar toegenomen, maar voor interoperabele toepassing is daarnaast

kennis van het implementatieprofiel en ook kennis van de te configureren software nodig.

Het hebben van SAML-compliant software is onvoldoende voor interoperabele gegevensuitwisseling. Aanvullende afspraken in de vorm van een deployment profiel zijn altijd noodzakelijk. De software dient geconfigureerd of aangepast (maatwerk) te worden om dit deployment profiel te ondersteunen. De hoeveelheid maatwerk is met name afhankelijk van of keuzes in het deployment profiel aansluiten bij gangbare implementatiekeuzes van softwareleveranciers die o.a. terugkomen in interoperabiliteitsprofielen zoals "SAML 2.0 eGov Interoperability Profile".

4.3 Technische dimensie

Profielkeuzes

Technische implicaties zijn vooral afhankelijk van keuzes die binnen de SAML-specificatie gemaakt worden (in gekozen profielen). Een product dat SAML-compliant is zal doorgaans nader geconfigureerd moeten worden om met het specifiek gekozen SAML-implementatieprofiel binnen een federatie te kunnen werken.

De grote overheidsimplementaties, DigiD en eHerkenning, hebben ieder eigen keuzes gemaakt. De verschillen blijken soms te maken te hebben met het verschil in opzet (voorziening versus stelsel), waaruit weer verschillen in risico voortkomen, maar in verschillende gevallen lijkt het te gaan om niet-noodzakelijke verschillen. Zo zijn er, mede op basis van risico-afwegingen,verschillende keuze gemaakt rondom de binding (back-channel versus front-channel). Daarnaast zijn er in beide gevallen keuzes gemaakt die niet geheel aansluiten bij wat er intussen in de markt gangbaar is en met name niet bij het Kantara interoperabiliteitsprofiel.

Een en ander heeft ervoor gezorgd dat het niet altijd eenvoudig was voor overheidsorganisaties om aan te sluiten en voor softwareleveranciers om hun software compatibel te maken. In sommige gevallen is configuratie dusdanig ingewikkeld gebleken dat een externe maatwerk 'bridge' tussen de identitymanagment-software bij een overheidsorganisatie en de federatie geschakeld moest worden.

Volgens de geïnterviewde experts is de weg ingeslagen naar betere afstemming tussen de twee deployment profielen. Logius heeft de verschillen tussen de koppelvlakken ten opzichte van het Kantara interoperabiliteitsprofiel in beeld gebracht in het document "Verschillen analyse DigiD – eHerkenning koppelvlakken" van eind 2012. Ook zijn er nieuwe versies van de deployment profielen van DigiD en eHerkenning gepubliceerd die beter met elkaar en met het Kantara interoperabiliteitsprofiel in lijn zijn.

eID biedt duidelijk een kans voor meer uniformiteit. Tegelijkertijd bestaat het risico op nog meer profielen. Van belang is een strategie waarbij ook rekenening wordt gehouden met compatibiliteit en uitfasering van de legacy-profielen.

Conformiteit
Kantara heeft een certificatieprogramma en heeft in het verleden SAML interoperability events[19] georganiseerd rondom het eGov 2.0 profiel en voor SAML zelf.

Er bestaan tools die helpen om conformiteit aan de standaard te testen, zoals SAML tracer (Firefox plugin) en SAML debugger (online), die terugkomen op de website van het Federation Lab.[20] Deze testen echter alleen deelaspecten en alleen voor de brede SAML 2.0 standaard, niet voor specifieke profielen.

Door een aantal geïnterviewden is aangegeven dat testen of een implementatie aan DigiD voldoet net zo moeilijk is als daadwerkelijk aansluiten. O.a. is het nodig om een PKI-overheidcertificaat aan te schaffen. Een laagdrempelige conformiteitstoets, specifiek voor een gekozen deployment profile, helpt partijen bij het aansluiten en bij selectie van producten. Als voorbeeld kan worden gewezen op de SAML SP Test van het Federation Lab. Van de andere kant heeft eHerkenning de testvoorziening voor service providers juist opgeheven wegens gebrek aan belangstelling.

4.4 Financiële dimensie

De specificatie van de standaard is vrijelijk beschikbaar bij standaardisatieorganisatie OASIS. SAML wordt goed ondersteund in softwareproducten, zowel met open source licentie als met commerciële licentie.

Wel kunnen eerder genoemde problemen bij het configureren er voor zorgen dat derde partijen nodig zijn om configuratie te ondersteunen of om protocol-translatie te doen. Dit brengt extra kosten met zich mee. Des te meer keuzes in het deployment profiel aansluiten bij hetgeen gangbaar is onder softwareleveranciers, des te lager deze kosten zullen zijn. Het Kantara interoperabiliteitsprofiel speelt als best practice hierbij een belangrijke rol.

4.5 Organisatorische dimensie

Dienstverlening door de overheid gebeurt meer en meer online. Hierdoor worden goede beveiliging, in het algemeen, en authenticatievoorzieningen, in het bijzonder, belangrijker. Hergebruik van een centrale identiteit bij meerdere dienstverleners helpt om risico's rondom misbruik met identiteiten te beperken. Tegelijkertijd zorgt de bredere inzetbaarheid van zo'n centrale identiteit ervoor dat deze een aantrekkelijk doelwit wordt voor internetcriminelen. Beveiligingsincidenten bij afnemers kunnen bijvoorbeeld negatief afstralen op de reputatie van de IdP. DigiD heeft daarmee te maken gehad.

Er is een reële mogelijkheid dat het eID stelsel NL, naast de overheidsdienstverleners ook andere, private, dienstverleners toe zal laten. Dit betekent dat een nog grotere groep dienstverleners, met

[19] Interoperability Certification Program van Kantara Initiative, *https://kantarainitiative.org/confluence/display/certification/Interoperability+Certification+Program*.
[20] Federation Lab van Géant en Kantara Initiative, *http://openidtest.uninett.no/*

bestaande identiteitsoplossingen aan zullen gaan sluiten op de identiteitsoplossing van de overheid. Dit stelt hoge eisen aan het gewenste niveau van beveiliging en aan het SAML deployment profiel dat gekozen wordt.

4.6 Maatschappelijke ontwikkelingen

Eindgebruikers raken steeds meer vertrouwd zijn met het hergebruik van identiteiten omdat het federeren van identiteiten ook in het social netwerk en het commerciële domein (de Googles en Facebooks van deze wereld) aan populariteit wint. Ze zullen dit soort gebruiksgemak ook in toenemende mate verwachten van de overheid.

Tegelijkertijd verwachten burgers ook dat een overheid in hoge mate betrouwbaar is, terwijl de dreiging van ICT-criminaliteit lijkt toe nemen. Voldoende aandacht voor de beveiliging van de SAML-federatie is daarom cruciaal.

4.7 Internationale ontwikkelingen

Hieronder volgt een drietal relevante internationale ontwikkelingen. Deze ontwikkelingen zijn uitgebreider behandeld in hoofdstuk 2.

- Europa: In verschillende Europese initiatieven en projecten (eIDAS, STORK, mandate M/460) wordt gewerkt aan grensoverstijgend gebruik van nationale identiteitsoplossingen. Het eIDAS-traject omvat Europese regelgeving voor elektronische handtekeningen en authenticatie. Binnen STORK is ook een SAML deployment profiel ontwikkeld. Binnen mandate M/460 van de Europese Commissie wordt gewerkt aan standaardisatie van de elektronische handtekening.[21]
- SAML-standaard: Voor SAML2.0 is er de afgelopen nieuwe relevante documentatie verschenen in de vorm van errata voor de standaard, comittee specifications, en het Kantara interoperabiliteitsprofiel waarop verschillende deployment profielen in het buitenland zijn gebaseerd. Aan de nieuwe versie SAML 2.1 wordt gewerkt, maar dit standaardisatieproces bevindt zich nog in een pril stadium.
- Nieuwe standaarden: OpenID Connect is een veelbelovende nieuwe standaard.

[21] Mandate M/460 door de Europese Commissie: *http://www.e-signatures-standards.eu/*

5 Conclusies en adoptie-adviezen

5.1 Conclusies

Uit de voorgaande analyse volgen de onderstaande conclusies.

1. De adoptie van SAML 2.0, als standaard voor gefedereerde authenticatie, is sinds de opname op de 'pas toe of leg uit'-lijst enorm toegenomen. De standaard wordt veelvuldig gebruikt door de overheid maar ook door het bedrijfsleven.
2. De standaard is 'proven technology' en lijkt daarom voor de komende jaren ook een goede keuze, alhoewel nieuwkomer OpenID Connect veelbelovend is.
3. De SAML-specificatie geeft ruimte voor nadere invulling. Binnen een federatie zijn daarom altijd nadere technische afspraken in de vorm van een deployment profiel nodig. Door bij de invulling keuzes te maken die gangbaar zijn in de markt, kunnen interoperabiliteit en implementatiegemak worden bevorderd.
4. Voor het ontwikkelen van deployment profielen is de afgelopen jaren verschillende relevante documentatie van OASIS en Kantara verschenen, namelijk errata voor de SAML-standaard en 'industry best practrices' in de vorm van committee specifications en het Kantara interoperabiliteitsprofiel.
5. Bij de uitrol van DigiD en eHerkenning is gebleken dat het voor overheden en hun softwareleveranciers niet altijd eenvoudig was om hun software te configureren. DigiD en eHerkenning hebben eigen deployment profielen ontwikkeld en deze zijn niet volledig conform de 'industry best practice'.
6. Voor een softwareleverancier die zijn software wil configureren conform het deployment profiel van DigiD is het niet eenvoudig om te testen of de configuratie voldoet aan het deployment profiel.
7. De afgelopen jaren is een aantal kwetsbaarheden in implementaties van SAML (niet in de standaard zelf) aan het licht gekomen.
8. eID biedt een kans op meer uniformering. Tegelijkertijd vormt het een risico voor nog meer profielen als niet wordt nadacht over migratie en uitfasering van bestaande profielen van met name DigiD en eHerkenning.
9. De opname van SAML op de 'pas toe of leg uit'-lijst is voor verbetering vatbaar. Aanvullend zou een interoperabiliteitsprofiel of deployment profiel opgenomen kunnen worden. Bovendien is het toepassingsgebied smal gedefinieerd. De standaard is breder inzetbaar.

5.2 Adoptie-adviezen

Op basis van de conclusies zijn de onderstaande adviezen ter bevordering van de adoptie opgesteld. Telkens is tussen vierkante haakje [organisatie] de organisatie benoemd die het beste invulling kan geven aan het advies.

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];
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];

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];
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];
5. Beheer het Nederlandse eID deployment profiel als open standaard en betrek stakeholders (leveranciers, overheidsorganisaties en standaardisatie-experts) actief bij de ontwikkeling [eID];
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];
7. Ontwikkel een planning en strategie voor migratie en uitfasering van 'oude' koppelvlakspecificaties [DigiD, eHerkenning, eID];
8. Monitor en waarschuw over kwetsbaarheden in SAML-implementaties [NCSC i.s.m. Logius];
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];
10. Volg de ontwikkelingen rondom OpenID Connect actief [Forum Standaardisatie i.s.m. eID].