notitie

FORUM STANDAARDISATIE 11 december 2019
Agendapunt 4B – Forumadvies OIDC

Nummer:	FS-191211.4B
Aan:	Forum Standaardisatie
Van:	Stuurgroep Open Standaarden
Datum:	11 december 2019
Versie:	1.1
Bijlagen:	Expertadvies OpenID Connect (OIDC) Commentaar op de openbare consultatie OpenID Connect

1. Aanleiding en achtergrond

De Wet digitale overheid beschrijft waaraan digitale publieke diensten en authenticatie voorzieningen moeten voldoen. Deze wet maakt het voor publieke dienstverleners verplicht authenticatie voor hun elektronische diensten aan te bieden middels DigiD en een privaat alternatief voor DigiD, zoals bijvoorbeeld iDIN. Daarnaast legt de eIDAS-verordening diezelfde partijen de verplichting op om authenticatiemiddelen uit het buitenland (onder voorwaarden) te accepteren.

Vanuit het eID programma is voorgesteld om een routeringsvoorziening te realiseren waar alle (semi)overheidspartijen en publieke diensten gebruik van kunnen maken. Dienstverleners in de eID-governance hebben aangedrongen op het in eerste instantie aanbieden van het DigiD-SAML koppelvlak. Via de Routeringsvoorziening worden de oudere DigiD-koppelvlakken (CGI/a-select) niet meer aangeboden omdat de wens al langer bestond deze uit te faseren.

Het DigiD-SAML koppelvlak volstaat echter niet om de gehele set aan technische en functionele wensen van de dienstverleners in de eID-governance te kunnen bieden op langere termijn. Een nieuw koppelvlak op basis van een andere standaard is dus (op termijn) noodzakelijk. Hiervoor heeft de eID governance (waarin dienstverleners breed vertegenwoordigd zijn) opgeroepen om niet een nieuw koppelvlak te baseren op SAML, maar op OpenID Connect (vanaf nu OIDC). Belangrijkste redenen zijn de beperkte doorontwikkeling van de SAML standaard en juist de actieve ontwikkelingen binnen de OIDC standaard. Verder vormen de eenvoud en de ondersteuning van de mobile-first strategie van diverse dienstverleners belangrijke redenen hiervoor. SAML voorziet hier minder in.

Vertegenwoordigers van het programma eID hebben vervolgens het initiatief genomen om OIDC aan te melden bij het Bureau Forum Standaardisatie.

2. Toelichting op de standaard

OIDC is een open en gedistribueerde manier om authenticatiediensten naar keuze te kunnen hergebruiken bij meerdere (semi-)overheidsdienstverleners, bij gebruik vanuit onder andere webapplicaties en mobiele toepassingen.

OIDC geeft apparaten en programma's de mogelijkheid om de identiteit van een eindgebruiker te controleren gebaseerd op verschillende authenticatieservices (zoals DigiD), waarbij profielinformatie van de eindgebruiker volgens een gestandaardiseerde wijze beschikbaar wordt gesteld aan de daarvoor geautoriseerde apparaten en programma's. Bovendien geeft het de mogelijkheid om meerdere attributen of andere type identifiers mee te geven.

De authenticatie vindt plaats op basis van moderne standaarden, zoals REST en JSON. REST en JSON wordt steeds vaker toegepast in de realisatie van met name mobiele apps. OIDC kent een brede ondersteuning in moderne ontwikkelingen rond cloud en mobiele toepassingen.

3. Betrokkenen en proces

Op 17 april 2019 hebben Coen Glasbergen en Remco Schaar (Logius, programma eID) de standaard aangemeld voor opname op de 'pas toe of leg uit'-lijst. Op 7 mei 2019 heeft een intakegesprek plaatsgevonden met de indieners. Bij het intakegesprek waren aanwezig Coen Glasbergen (Logius, Programma eID), Remco Schaar (Logius, Progamma eID) Redouan Ahaloui (Bureau Forum Standaardisatie), Robin Gelhard (Bureau Forum Standaardisatie), Pieter Verkaik (Lost Lemon) en Jeroen de Ruig (Lost Lemon).

In dit gesprek is onderzocht of de standaard voldoet aan de criteria om in procedure genomen te worden en vervolgens is een intakeadvies geschreven. In het intakeadvies is aandacht besteed aan de overlap met de reeds verplichte standaard SAML. Op basis van het intakeadvies heeft het Forum standaardisatie opdracht gegeven om te komen tot een expertadvies.

Aangezien SAML en OIDC vergelijkbare standaarden zijn met een bijna gelijk functioneel toepassingsgebied is het niet mogelijk om beide standaarden op de 'pas toe of leg uit'-lijst te plaatsen. Om beide standaarden op de 'pas toe of leg uit'-lijst te plaatsen is een duidelijk onderscheid in de functionele toepassingsgebied voorwaardelijk. Overheidspartijen kunnen immers niet aan twee gelijksoortige standaarden voldoen voor hetzelfde functionele toepassingsgebied.

Tijdens de expertsessie is besloten om te adviseren OIDC op de lijst van aanbevolen standaarden te plaatsen. Daarnaast is geadviseerd dat zo snel mogelijk een breed gedragen Nederlands profiel moet worden ontwikkeld voor OIDC. Dit Nederlands profiel zal dan moeten worden aangedragen voor plaatsing op de 'pas toe of leg uit'-lijst.

Diana Koppenol Algemeen Directeur bij Lost Lemon was tijdens de expertsessie de onafhankelijk voorzitter. Pieter Verkaik consultant en Jeroen de Ruig senior consultant bij Lost Lemon, hebben de procedure in opdracht van het Bureau Forum Standaardisatie begeleid.

Aan de expertbijeenkomst hebben deelgenomen:

- Remco Schaar Logius (indiener)
- Bart Geesink Surfnet
- Paul Oude Luttighuis Medmij
- Frans de Kok Logius
- Frank Zwart Logius
- Pieter Hering Logius
- Joris Joosten Logius
- Esther Makaay Connectis
- Floris Diemel Digidentity
- Cristian Gonzalez VNG
- Peter Haasnoot Logius
- Rob Post RvIG
- Martin Borgman Kadaster
- Amos Kater Betaalvereniging
- Dennis Reumer RVO
- Jan Geert Koops DICTU
- Mark Nijmeijer Justid
- Yves Fonk DICTU

Redouan Ahaloui van het Bureau Forum Standaardisatie was als toehoorder bij de expertbijeenkomst aanwezig.

De volgende experts hebben voorafgaand aan de expertbijeenkomst schriftelijke input gegeven en/of hebben de conceptversie van het expertadvies ook mede beoordeeld:

- Indra Henneman VNG Realisatie
- Maurice Laarhoven Belastingdienst
- Leon van der Ree Logius
- Kick Willemse Evidos

In de voorbereidende stuurgroep-vergadering van het Forum van 21 november is voorgesteld om het toepassingsgebied van OIDC te verbreden. OIDC omvat meer dan alleen mobiele toepassingen. Bovendien sluit deze verbreding beter aan op aankomende profielen. De indiener is akkoord met dit voorstel.

4. Hoe scoort de standaard op de toetsingscriteria?

Open standaardisatieproces
De beheerder van OIDC is de OpenID Foundation. Voor de standaard OIDC is sprake van een open standaardisatieproces. De doorontwikkeling en het beheer is open en transparant en is vergelijkbaar met IETF, W3C en ISO.

Toegevoegde waarde
De experts zien toegevoegde waarde voor OIDC bij de overheid en wordt breed gedragen binnen de Nederlandse overheid. Belangrijke voorwaarde voor de toepassing van de standaard OIDC is een Nederlands profiel. Dit Nederlands profiel regelt onder andere afspraken over veiligheid, interoperabiliteit en nieuwe structurele upgrades voor bepaalde toepassingen in het publieke domein in Nederland. Dit Nederlands profiel moet snel gerealiseerd worden. De toegevoegde waarde van OIDC ten opzichte van SAML zit in de toepassingsmogelijkheid van deze standaard voor mobiele toepassingen. Aangezien SAML op de 'pas toe of leg uit'-lijst staat en het niet mogelijk is twee standaarden met hetzelfde functionele toepassingsgebied op deze lijst te plaatsen, is besloten om te adviseren OIDC op de lijst van aanbevolen standaarden te plaatsen.

Het nog te ontwikkelen Nederlandse profiel van de standaard OIDC zal worden ingediend als standaard voor de 'pas toe of leg uit'-lijst. Door OIDC op de lijst van aanbevolen standaarden te plaatsen is deze zichtbaar voor overheidspartijen en geeft dit ook ondersteuning om te starten met de ontwikkeling van het Nederlandse profiel.

Draagvlak
De experts van de diverse betrokken overheidspartijen zien draagvlak voor de standaard OIDC, vanwege de noodzakelijke toepassingsmogelijkheden. Het is opgenomen in de Project Startarchitectuur (PSA) van eID en deze is goedgekeurd binnen de programma governance met daarin diverse publieke dienstverleners. Alle betrokken experts zijn unaniem voor het gezamenlijk komen tot een Nederlands profiel voor OIDC en willen daar graag een bijdrage aanleveren. Inmiddels heeft een eerste vergadering van de werkgroep, verantwoordelijk voor de ontwikkeling van een Nederlands profiel, met een brede vertegenwoordiging vanuit diverse (semi) overheidspartijen, plaatsgevonden. Het Nederlands profiel zal na realisatie worden aangedragen voor plaatsing op de 'pas toe of leg uit'-lijst.

Programma eID (Logius) heeft het initiatief genomen om de Werkgroep OpenID Connect te starten om een breed gedragen Nederlandse OIDC-profiel te ontwikkelen. De werkgroep bestaat uit een brede vertegenwoordiging vanuit de publieke sector.

Opname bevordert de adoptie
Adoptie van de standaard is nodig. De toepassingsmogelijkheid van OIDC voor met name mobiele toepassingen is nodig binnen de Nederlandse overheid. De opname op de lijst van aanbevolen standaarden is het hoogst haalbare op dit moment, gezien de functionele overeenkomst met SAML. Opname op de lijst van aanbevolen standaarden maakt de standaard zichtbaar voor overheidspartijen en geeft ondersteuning bij het gezamenlijk komen tot een Nederlands profiel voor de deze standaard.

Van belang is om zo snel mogelijk een breed gedragen Nederlands profiel te ontwikkelen voor OIDC. Het voornemen is om in het tweede kwartaal 2020 het aankomende profiel in te dienen voor de 'pas toe of leg uit'-lijst.

5. Wat is de conclusie van de expertgroep en de openbare consultatie?

Conclusie van het expertonderzoek
Tijdens de expertsessie is duidelijk geworden dat het opnemen van OIDC op de 'pas toe of leg uit'-lijst niet haalbaar is. OIDC en SAML (standaard op de 'pas toe of leg uit'-lijst) hebben hetzelfde functionele toepassingsgebied. Het is onwenselijk om twee standaarden met hetzelfde functionele toepassingsgebied op te nemen op de 'pas toe of leg uit'-lijst. (Semi)-overheidspartijen moeten immers een duidelijke keuze kunnen maken bij het opnemen van standaarden in een bestek. Als er sprake is van twee standaarden met hetzelfde functionele toepassingsgebied leidt dat tot onduidelijkheid.

Bovendien adviseren de experts om een Nederlands profiel te ontwikkelen voor OIDC. Het Nederlands profiel zorgt voor landelijke afspraken over de toepassing van de standaard. Deze afspraken zijn essentieel om interoperabiliteit te waarborgen. Zodra het Nederlands profiel gereed is zal het profiel worden aangedragen voor plaatsing op de 'pas toe of leg uit'-lijst.

Analyse van reacties uit de openbare consultatie
Tijdens de openbare consultatie zijn zes reacties binnengekomen van verschillende (semi) overheidspartijen. De volgende (Semi)-overheidspartijen hebben een inhoudelijke reactie gegeven; Ministerie van Buitenlandse zaken, DUO, Kamer van Koophandel en IND. De reacties vanuit de openbare consultatie onderstrepen het belang van het opnemen van OIDC op de lijst van aanbevolen standaarden en om zo snel mogelijk te komen tot een Nederlands profiel. Daarnaast zijn enkele vragen gesteld over hoe nu verder en wanneer het Nederlands profiel gereed is.

6. Gevraagd besluit
Het Forum Standaardisatie wordt gevraagd om in te stemmen met onderstaand advies.

Het Forum Standaardisatie adviseert het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) om:

1. *Open ID Connect op te nemen op de lijst van aanbevolen standaarden.*
2. *Het functioneel toepassingsgebied voor Open ID Connect als volgt vast te stellen: "*OpenID Connect kan toegepast worden bij het beschikbaar stellen van federatieve authenticatiediensten.*"*
3. *Ten aanzien van de adoptie van OpenID Connect de oproepen te doen die beschreven staan in hoofdstuk 7 hieronder.*

7. Welke additionele adviezen zijn er ten aanzien van de adoptie van de standaard?
De experts doen het Forum Standaardisatie en Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) de aanbeveling om bij de opname op de lijst van aanbevolen standaarden de volgende oproep ten aanzien van de adoptie van OIDC te doen:

- De Nederlandse overheid moet een toekomstige beheerpartij voor het Nederlandse OIDC profiel benoemen, die meedraait in de ontwikkeling van dit profiel en deze in beheer kan nemen na oplevering door de Werkgroep OpenID Connect. De beheerorganisatie moet eigenaarschap uitstralen en ondersteuning bieden bij de implementatie van OIDC en het Nederlandse profiel door (semi)overheidspartijen.

- Een oproep aan alle (semi)overheidspartijen en publieke diensten te melden bij De Werkgroep OpenID Connect om kennis af te vaardigen voor het ontwikkelen van een breed gedragen Nederlands profiel voor OIDC.

8. Referenties

[1] Expertadvies OIDC:
https://www.forumstandaardisatie.nl/sites/bfs/files/Expertadvies%20OpenID%20Connect%201.0.pdf

[2] Reacties uit de consultatieronde OIDC:
https://www.forumstandaardisatie.nl/sites/bfs/files/Commentaar-uit-de-openbare-consultatie-OIDC.pdf