Expertadvies OpenID Connect

Datum:	18 juli 2019
Versienummer:	1.0
Opdrachtgever:	Forum Standaardisatie Postbus 96810 2509 JE Den Haag 070-8887776 info@forumstandaardisatie.nl
Procedurebegeleiding:	Lost Lemon
Voorzitter expertgroep:	Diana Koppenol
Auteurs:	Pieter Verkaik en Jeroen de Ruig

Inhoud

1 Samenvatting en advies

Op basis van het expertonderzoek wordt geadviseerd om OpenID Connect (OIDC) op te nemen op de lijst van aanbevolen standaarden van het Forum Standaardisatie.

Als functioneel toepassingsgebied wordt geadviseerd:

OpenID Connect moet worden toegepast bij het beschikbaar stellen van federatieve authenticatiediensten, waarbij sprake is van mobiele toepassingen.

Als organisatorisch werkingsgebied wordt geadviseerd:

Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector.

Paragraaf 5.5 van dit document beschrijft aanbevelingen van de expertgroep aan het Forum Standaardisatie en het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) ten aanzien van de stimulering van adoptie van de standaard.

2 Doelstelling expertadvies

2.1 Achtergrond

De Nederlandse overheid streeft naar betrouwbare gegevensuitwisseling door het gebruik van open standaarden en het voorkomen van vendor lock-in. Het actieplan "Open Overheid", de Digitale Agenda 2017 en de kabinetsreactie op het Rapport Elias benadrukken dit beleid. Om dit doel te bereiken, onderstrepen het instellingsbesluit van het Forum Standaardisatie, de Generieke Digitale Infrastructuur en de verschillende architectuurkaders het gebruik van open standaarden bij het ontwerpen of inkopen van informatiesystemen.

Een van de maatregelen om de adoptie van open standaarden te bevorderen is de publicatie en het beheer van een lijst met open standaarden waarvoor een pas-toe-of-leg-uit verplichting geldt of waarvan het gebruik 'aanbevolen' is. Het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) besluit welke standaarden op deze lijst worden opgenomen. Het OBDO baseert zich hierbij op expertadviezen, openbare consultaties en adviezen van het Forum Standaardisatie.

2.2 Doelstelling expertadvies

Dit document is een expertadvies voor OIDC gericht aan het OBDO en Forum Standaardisatie. OIDC is aangemeld voor opname op de lijst met open standaarden door Coen Glasbergen en Remco Schaar van Logius, programma eID.

Doel van dit document is om het OBDO te adviseren of OIDC in aanmerking komt voor opname op de lijst van aanbevolen standaarden, al dan niet onder voorwaarden.

2.3 Doorlopen proces

Voor het opstellen van dit proces is de volgende procedure doorlopen:

1. De procesbegeleider heeft op 7 mei 2019 een intakegesprek gevoerd met de indieners. Tijdens de intake is de standaard getoetst op criteria voor inbehandelname en is een eerste inschatting gemaakt van de kansrijkheid van de procedure.
2. Op basis van de intake heeft het Forum Standaardisatie op 12 juni 2019 besloten de aanmelding in procedure te nemen. Hierop volgend is een expertgroep samengesteld en een voorzitter aangesteld.
3. De leden van de expertgroep hebben een voorbereidingsdossier gekregen dat is samengesteld met informatie uit de aanmelding en het intake onderzoek. Voorafgaand aan de expertbijeenkomst heeft de expertgroep dit voorbereidingsdossier doorgenomen en aandachtspunten geïdentificeerd.
4. De expertgroep is op dinsdag 25 juni bijeengekomen om de bevindingen in het algemeen en de geïdentificeerde aandachtspunten in het bijzonder te bespreken. Tijdens deze bijeenkomst zijn ook het toepassings- en werkingsgebied vastgesteld.

Dit expertadvies geeft de uitkomst van de expertgroep weer. De procesbegeleider heeft een concept van dit expertadvies aan de leden van de expertgroep gestuurd met verzoek om commentaar. Na verwerking van reacties uit de expertgroep is het rapport nogmaals

toegestuurd aan de experts, afgerond en ingediend bij het Bureau Forum Standaardisatie (het secretariaat van het Forum Standaardisatie) ten behoeve van de publieke consultatieronde.

2.4 Vervolg

Het Bureau Forum Standaardisatie zal dit expertadvies openbaar maken ten behoeve van een publieke consultatie die plaatsvindt van 19 augustus tot 16 september 2019. Dit is op verzoek van de experts tijdens de expertbijeenkomst twee weken later dan de andere standaarden in deze ronde. Gevolg is dat het expertadvies pas zal worden voorgelegd aan het Forum Standaardisatie in de vergadering van december 2019 en niet van oktober. Eenieder kan gedurende de consultatieperiode een reactie geven op dit expertadvies. Na afsluiting van de openbare consultatie koppelt het Bureau Forum Standaardisatie de reacties terug aan de expertgroep.

Het Forum Standaardisatie stelt met het expertadvies en de relevante inzichten uit de openbare consultatie een advies aan het OBDO op. Het OBDO besluit met dit advies om de standaard wel of niet op de lijst open standaarden te plaatsen.

2.5 Samenstelling expertgroep

Het Forum Standaardisatie streeft naar een representatieve expertgroep met een evenwichtige vertegenwoordiging van (toekomstige) gebruikers (zowel publiek als privaat), leveranciers, wetenschappers en andere belanghebbenden. De expertgroep heeft een onafhankelijk voorzitter die de expertgroep leidt en de verantwoordelijkheid neemt voor het expertadvies.

Als onafhankelijk voorzitter is opgetreden Diana Koppenol, Algemeen Directeur bij Lost Lemon.

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

2.6 Leeswijzer

Hoofdstuk 3 geeft een korte toelichting op de standaard, met name het nut en de werking ervan.

Hoofdstuk 4 beschrijft het voorgestelde functioneel toepassingsgebied (situaties waarin de standaard functioneel gebruikt moet worden) en organisatorisch werkingsgebied (organisaties die de standaard moeten toepassen).

Hoofdstuk 5 beschrijft de resultaten van de toetsing van de standaard aan de hand van de criteria voor opname op de lijst open standaarden.

3 Toelichting OpenID Connect

OpenID Connect (OIDC) is een open en gedistribueerde manier om authenticatiediensten naar keuze te kunnen hergebruiken bij meerdere ((semi-)overheids)dienstverleners, 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. Gebruiker kan zelf een keuze maken voor een authenticatievoorziening en gebruiker hoeft niet steeds opnieuw in te loggen.

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 apps. OIDC kent een brede ondersteuning in moderne ontwikkelingen rond cloud en mobiele toepassingen.

4 Toepassings– en werkingsgebied

De *instructie rijksdienst inzake de aanschaf van ICT producten en ICT diensten* verplicht overheidsorganisaties om relevante standaarden op de pas-toe-of-leg-uit lijst uit te vragen en toe te passen bij aanbestedingstrajecten.

Afhankelijk van de aan te schaffen functionaliteit moet een overheidsorganisatie bepalen welke standaarden op de pas-toe-of-leg-uit lijst relevant zijn. Hiervoor is voor iedere standaard een *functioneel toepassingsgebied* (in welke situaties is de standaard functioneel van toepassing) en een *organisatorisch toepassingsgebied* (welke organisaties moeten de standaard gebruiken) beschreven.

Secties 4.1 en 4.2 geven het advies van de expertgroep voor het functioneel en organisatorisch toepassingsgebied van OpenID Connect.

4.1 Functioneel toepassingsgebied

De expertgroep adviseert als functioneel toepassingsgebied voor OpenID Connect:

OpenID Connect moet worden toegepast bij het beschikbaar stellen van federatieve authenticatiediensten, *waarbij sprake is van mobiele toepassingen.*

4.2 Organisatorisch werkingsgebied

De expertgroep adviseert om het organisatorisch werkingsgebied van de standaard overeen te laten komen met het werkingsgebied waarop de ‘pas toe of leg uit’ verplichting van toepassing is, te weten:

Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector.

5 Toetsing van standaard aan criteria

Het Forum Standaardisatie hanteert vier hoofdcriteria om te bepalen of een standaard in aanmerking komt voor opname op de lijst:
1. Heeft de standaard toegevoegde waarde?
2. Zijn de standaard en het standaardisatieproces voldoende open?
3. Heeft de standaard voldoende draagvlak?
4. Is opname op de lijst nodig om de adoptie te bevorderen?[1]

Ieder van deze hoofdcriteria heeft deelcriteria die beschreven staan in het document *'Toetsingsprocedure en criteria voor lijst met open standaarden voor indieners en experts',* te vinden op de website van het Forum Standaardisatie https://www.forumstandaardisatie.nl/content/toetsen-van-standaarden.

Dit hoofdstuk beschrijft per criterium het resultaat van de toetsing. Voor de volledigheid is tevens de beschrijving van elk criterium opgenomen.

5.1 Toegevoegde waarde

De interoperabiliteitswinst en andere voordelen van adoptie van de standaard wegen overheidsbreed en maatschappelijk op tegen de risico's en nadelen.

5.1.1 Is het toepassings- en werkingsgebied van de aanmelding goed gedefinieerd?

5.1.1.1 Is het functioneel toepassingsgebied goed gedefinieerd?

Ja, dat is in de expertgroep als volgt gedefinieerd: OpenID Connect moet worden toegepast bij het beschikbaar stellen van federatieve authenticatiediensten, waarbij sprake is van mobiele toepassingen.

Bij federatieve authenticatie wordt een vertrouwde partij gebruikt om authenticatie af te handelen voor toegang tot de eigen dienstverlening. Hierdoor kan eenvoudig en veilig worden ingelogd (geauthentiseerd) op eigen services door bijvoorbeeld klanten, leveranciers, partners waarmee wordt samengewerkt. Ook SAML en OAuth2 bieden vergelijkbare functionaliteit als het gaat om authenticatie en autorisatie.

Aangezien sprake is van een vergelijkbaar functioneel toepassingsgebied voor de standaarden OIDC (authenticatie), OAuth2 (autorisatie) en SAML (authenticatie en autorisatie) is het plaatsten van de drie standaarden op 'pas toe of leg uit'-lijst niet mogelijk. Overheidsorganisaties moeten immers bij een aanbesteding een keuze kunnen maken voor één standaard bij vergelijkbare functionaliteit. De verwachting is dat deze drie standaarden nog enige tijd zullen blijven bestaan[2].

Om dit probleem op te lossen adviseert de expertgroep het Forum Standaardisatie om OIDC op de lijst van aanbevolen standaarden te

1 Dit criterium is voornamelijk van toepassing op standaarden op de 'pas toe of leg uit' lijst, niet voor aanbevolen standaarden.

2 Zie notitie "Routeringsvoorziening en OIDC koppelvlak" datum 7 november 2018 van programma eID aan Forum standaardisatie.

plaatsen in plaats van op de 'pas toe of leg uit' lijst. Vervolgens een Nederlands overheidstoepassingsprofiel voor de standaard OIDC op te stellen. Door het programma eID is al een profiel ontwikkeld, dit zal dienen als input om te komen tot een breed gedragen Nederlands profiel. Dit profiel moet afgestemd worden met het bestaande Nederlands profiel voor OAuth2 (zie https://geonovum.github.io/KP-APIs-OAuthNL/#dutch-government-assurance-profile-for-OAuth-2-0).

Het profiel regelt afspraken over veiligheid, interoperabiliteit en nieuwe structurele upgrades voor bepaalde toepassingen in het publieke domein in Nederland. Het eerste profiel richt zich op eenzelfde use case als het OAuth2 profiel, dus een oplossing waarin een client (dienstverlener) om identificatie en authenticatie van een gebruiker aan een vertrouwde partij vraagt, waarbij bepaalde attributen worden meegeleverd.

Dit Nederlandse OIDC profiel zal vervolgens moeten worden opgenomen op de 'pas toe of leg uit'-lijst, verwijzend naar de onderliggende standaarden OIDC en OAuth2. OAuth2 en SAML moeten dan vervolgens (ook) worden opgenomen op de lijst van aanbevolen standaarden. Ook het Nederlands OAuth2 profiel zal opgenomen moeten worden op de 'pas toe of leg uit' lijst. Hiermee worden de opgestelde Nederlandse profielen leidend en niet de daaraan ten grondslag liggende standaarden.

5.1.1.2 Is het organisatorisch werkingsgebied goed gedefinieerd?

Ja. De Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector.

In de Wet digitale overheid komt een opsomming van organisaties die moeten voldoen aan de wet.[3]

5.1.1.3 Is de standaard generiek toepasbaar (en niet alleen bedoeld voor gegevensuitwisseling met één of een beperkt aantal specifieke organisaties)? (toelichtende vraag)

Ja. Het is een open standaard die gebruikt kan worden bij het veilig toegang verlenen met diverse authenticatiediensten tot (systemen van) meerdere dienstverleners van met name mobiele toepassingen. Deze wijze van toepassen van OIDC kan worden ingezet bij authenticatie van burgers en ondernemers en (semi)overheidsorganisaties onderling.

5.1.2 Verhoudt de standaard zich goed tot andere standaarden?

5.1.2.1 Kan de standaard naast of in combinatie met reeds opgenomen standaarden worden toegepast (d.w.z. de standaard conflicteert niet met reeds opgenomen standaarden)?

Nee. Zoals eerder aangegeven zijn de functionele overeenkomsten tussen met name SAML en OIDC te groot om beide standaarden op de 'pas toe of leg uit'-lijst te plaatsen.

De experts adviseren om voor OIDC een gedragen Nederlands profiel te ontwikkelen, afgestemd op het Nederlandse profiel in wording voor

3 https://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?cfg=wetsvoorsteldetails&qry=wetsvoorstel%3A34972

OAuth2 (zie https://geonovum.github.io/KP-APIs-OAuthNL/#dutch-government-assurance-profile-for-OAuth-2-0). OAuth2 zit nog in de procedure om op de 'pas toe of leg uit'- lijst te plaatsen in afwachting van een Nederlands profiel. OIDC is gebaseerd op OAuth2.

Tijdens de expertbijeenkomst is ook de suggestie gedaan om voor SAML een Nederlands profiel, of meerdere gestandaardiseerde profielen te ontwikkelen of bestaande profielen te formaliseren.

5.1.2.2 Biedt de aangemelde standaard meerwaarde boven reeds opgenomen standaarden met een overlappend functioneel toepassings- en organisatorisch werkingsgebied? (Dit kan ook om een nieuwe versie van dezelfde standaard gaan.)

Ja. Op dit moment is SAML de standaard voor federatieve authenticatie die op de 'pas toe of leg uit'-lijst staat. De verwachting is dat SAML nog enige tijd naast OIDC zal blijven bestaan. OIDC is meer geschikt voor mobiele toepassingen dan SAML. De trend van steeds meer mobiele apps, zal een toename betekenen in de behoefte aan OIDC .

Een ander belangrijk argument om op OIDC in te zetten zijn de beperkte doorontwikkelingsmogelijkheden van de SAML standaard. De adoptie en doorontwikkeling van de OIDC standaard is groter dan bij SAML. Kortom OIDC heeft meerwaarde ten opzichte van de huidige verplichte standaard SAML.

5.1.2.3 Biedt de aangemelde standaard meerwaarde boven bestaande concurrerende standaarden die in aanmerking zouden kunnen komen voor opname? (toelichtende vraag)

Ja. OAuth2 is een open standaard welke bedoeld is voor autorisatie. Het faciliteert toegang tot bijv. apps met 'delegated authorization'. OIDC biedt deze federatieve authenticatie. De OIDC flow maakt gebruik van de OAuth2 authorization code flow, waarbij een belangrijke toevoeging het 'ID token' is, dat identificatie van de geauthentiseerde gebruiker mogelijk maakt.

OAuth2 en OIDC liggen meer in elkaars verlengde. Om begripsverwarring te voorkomen en eenduidigheid in de toepassing van authenticatie en autorisatie te realiseren binnen de Nederlandse overheid en publieke diensten adviseren de experts een gedragen Nederlands profiel te ontwikkelen voor OIDC in afstemming met het inmiddels vergevorderde ontwikkelde Nederlandse OAuth2 profiel.

5.1.2.4 Is de standaard een internationale standaard of sluit de standaard aan bij relevante internationale standaarden? (toelichtende vraag)

OIDC bouwt voort op OAuth2. Daarmee op o.a. de standaarden voor HTTP, JSON, REST, TLS en andere gangbare internet standaarden van IETF, ISO en W3C.

5.1.3 Wegen de kwantitatieve en kwalitatieve voordelen van adoptie van de

standaard, voor de (semi-)overheid als geheel en voor de maatschappij, op tegen de nadelen?

5.1.3.1 Zijn de kosten van implementatie acceptabel en zijn deze kosten bekend en inzichtelijk?

Ja. Voor de toepassing van OIDC zijn er geen kosten voor eindgebruikers. Als OIDC vanuit de overheid ter beschikking wordt gesteld aan publieke diensten, dan zijn er geen kosten verbonden aan het gebruik van OIDC. De Nederlandse overheid betaalt 100 dollar voor participatie in de doorontwikkeling van OIDC. Wanneer een leverancier een certificering wil voor ondersteuning van OIDC, dan zijn hier wel kosten aan verbonden maar deze zijn volgens de experts acceptabel.

Zoals eerder aangegeven is een Nederlands profiel noodzakelijk. Voor het opstellen van een Nederlands profiel en het beheer daarvan moeten kosten worden gemaakt. Hoeveel kosten hiermee gemoeid zijn is op dit moment nog onduidelijk.

De (concept) Wet digitale overheid[4] schrijft voor dat de burger een keuze moet kunnen maken tussen meerdere authenticatie voorzieningen, ook private voorzieningen zoals IDIN. OIDC biedt hiervoor ondersteuning. Kortom OIDC draagt bij aan het tegemoet te komen aan de toekomstige wetgeving.

5.1.3.2 Is er een (kwalitatieve) businesscase van de standaard aanwezig?

In 5.1.3.3. wordt een voorbeeld geschetst van een mogelijke toepassing van OIDC. Met dit voorbeeld wordt tegemoet gekomen aan de eisen in de Wet digitale overheid.

5.1.3.3 Is de meerwaarde van de standaard goed inzichtelijk te maken? Wat betekent de standaard voor de (bedrijfs)processen van een organisatie of keten en wat los je met de standaard op?

Aan de hand van een voorbeeld wordt de meerwaarde van de standaard geschetst. Dit voorbeeld is afkomstig uit een notitie opgesteld door het Programma eID[5].

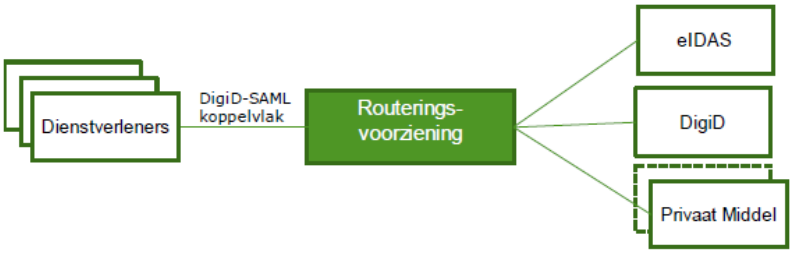
In de Wet digitale overheid wordt omschreven waaraan digitale publieke diensten en authenticatie voorzieningen moeten voldoen. In deze wet worden dienstverleners verplicht authenticatie voor hun elektronische diensten aan te bieden middels DigiD en een privaat alternatief voor DigiD. Daarnaast legt de eIDAS-verordening diezelfde partijen de verplichting op om authenticatiemiddelen uit het buitenland (onder voorwaarden) te accepteren. Vanuit eID programma wordt voorgesteld om een routeringsvoorziening te realiseren waar alle (semi)overheidspartijen en publieke diensten gebruik van kunnen maken.

---

[4] *https://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?cfg=wetsvoorsteldetails&qry=wetsvoorstel%3A34972*

[5] *Notitie vanuit programma eID van Ministerie van Binnenlandse Zaken, datum 17 november 2018; https://www.forumstandaardisatie.nl/sites/bfs/files/proceedings/FS%20181212.4E%20Notitie%20eID%20over%20OIDC.pdf*

Dienstverleners worden voor de aansluitverplichting 'ontzorgd' door het ter beschikking stellen van een routeringsvoorziening, welke als doel heeft de dienstverlener één aanspreekpunt, één contract, één factuur en één koppelvlak te bieden, zie figuur 1.



Figuur 1: Weergave van routeringsvoorziening gebruikmakend van DigiD-SAML koppelvlak

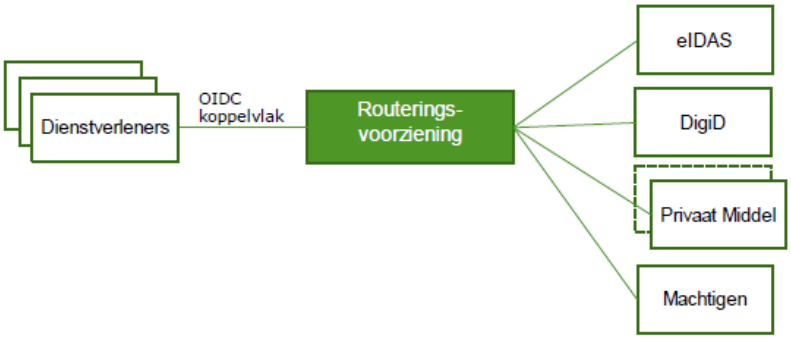
Dienstverleners in de eID-governance hebben aangedrongen op het in eerste instantie aanbieden van het DigiD-SAML koppelvlak. Via de Routeringsvoorziening worden de oudere DigiD-koppelvlakken (CGI/a-select) niet meer aangeboden omdat de wens al langer bestond deze uit te faseren.

Echter, het DigiD-SAML koppelvlak volstaat niet om de gehele set aan technische en functionele wensen te kunnen bieden op langere termijn. Dit geldt bijvoorbeeld op de volgende gebieden:

- Levering van (polymorfe) pseudoniemen i.p.v. BSN's.
- Machtigingsinformatie – de ambitie bestaat ook de nieuwe machtigingsvoorziening uit het programma Machtigen via de routeringsvoorziening aan te bieden.
- Attribuutlevering, vooral de minimale dataset vanuit eIDAS.

Een nieuw koppelvlak is dus (op termijn) noodzakelijk. Hiervoor heeft de eIDgovernance (waarin dienstverleners breed vertegenwoordigd zijn) opgeroepen om niet een nieuw koppelvlak te baseren op SAML, maar op 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.

Op deze manier ontstaat op termijn (enkele jaren) de volgende situatie, zie figuur 2:



Figuur 2: weergave van routeringsvoorziening gebruikmakend van OIDC koppelvlak

Als uitgangspunt voor de transitie naar deze doelsituatie is bepaald dat eerst beide koppelvlakken naast elkaar worden aangeboden, waarna SAML wordt uitgefaseerd.

5.1.3.4 Zijn de beveiligingsrisico's aan overheidsbrede adoptie van de standaard acceptabel?

Ja. OIDC voorkomt juist beveiligingsrisico's en daarom draagt het eventueel niet opnemen van de standaard bij aan beveiligingsrisico's in de toekomst.

5.1.3.5 Zijn de privacyrisico's aan overheidsbrede adoptie van de standaard acceptabel?

Ja. OIDC schrijft encryptie niet voor, maar ondersteund het wel: dit kan in de profielen voorgeschreven worden. Gepseudonimiseerde informatie verstrekken is wel een van de standaard opties in OIDC (bekend als pairwise identifiers). Hierdoor levert het privacywinst op t.o.v. de bestaande SAML, maar zeker t.o.v. de bestaande legacy koppelvlakken zoals CGI/a-select.

5.1.4 Conclusie criteria 'Toegevoegde waarde'

De experts geven aan dat OIDC toegevoegde waarde heeft, mits er een Nederlands profiel is. De toegevoegde waarde zit in de toepassingsmogelijkheid van deze standaard voor mobiele toepassingen.

5.2 Open standaardisatieproces

De ontwikkeling en het beheer van de standaard zijn op een open, onafhankelijke, toegankelijke, inzichtelijke, zorgvuldige en duurzame wijze ingericht.

5.2.1 Is de documentatie voor een ieder drempelvrij beschikbaar?

5.2.1.1 Is het specificatiedocument beschikbaar zonder dat er sprake is van belemmeringen (zoals hoge kosten of lidmaatschapseisen)?

Ja. Ontwikkeling gebeurt openlijk toegankelijk (https://bitbucket.org/openid/) en het proces is beschreven (zie https://openid.net/foundation/policies/). Het besluitvormingsproces is dus voor alle belanghebbenden toegankelijk en inzichtelijk. Nederlandse overheidspartijen kunnen deelnemen aan het standaardisatieproces voor 100 dollar.

5.2.1.2 Is de documentatie over het ontwikkel- en beheerproces (bijv. het voorlopige specificatiedocument, notulen en beschrijving van de besluitvormingsprocedure) beschikbaar zonder dat er sprake is van belemmeringen (zoals hoge kosten of lidmaatschapseisen)?

Ja. Er wordt gewerkt aan kleine updates en enkele uitbreidingen. De uitbreidingen lijken voornamelijk als losse documenten/aanvullende specificaties gepositioneerd te worden. Verder vindt doorontwikkeling ook grotendeels plaats als onderdeel van de onderliggende OAuth2 standaard. De documentatie en ontwikkeling is openlijk toegankelijk, zie 5.2.1.1.

5.2.2 Is het intellectuele eigendomsrecht voor eenieder beschikbaar, zodat de standaard vrij implementeerbaar en te gebruiken is?

5.2.2.1 *Stelt de standaardisatieorganisatie het intellectueel eigendomsrecht op de standaard (bijvoorbeeld patenten of licenties) onherroepelijk royalty-free voor eenieder beschikbaar?*

Ja. De licentie voorwaarden van de OpenID Foundation en OpenID specificaties zijn zeer open, enkel *attribution* (vermelding van OpenID Foundation) is vereist. Zie https://openid.net/intellectual-property/

5.2.2.2 Garandeert de standaardisatieorganisatie dat partijen die bijdragen aan de ontwikkeling van de standaard hun intellectueel eigendomsrecht voor (onderdelen van) de standaard onherroepelijk royalty-free voor eenieder beschikbaar stellen?

Ja.

5.2.3 Is de inspraak van eenieder in voldoende mate geborgd?

5.2.3.1 Is het besluitvormingsproces toegankelijk voor alle belanghebbenden (bijv. gebruikers, leveranciers, adviseurs, wetenschappers)?

Ja. Besluitvorming is openlijk toegankelijk en inspraak is mogelijk. Voor overheidspartijen of individuen is de contributie zeer laag. Voor commerciële organisaties is de contributie wel hoger. Zie https://openid.net/foundation/benefits-members/.

5.2.3.2 Vindt besluitvorming plaats op een wijze die zoveel mogelijk recht doet aan de verschillende belangen?

Ja. OpenID specificaties worden gefaseerd ontwikkeld door werkgroepen. Dit wordt gedaan in drie fases: Drafts, Implementer's Drafts, and Final Specifications. De procedure is open. Iedere partij die een convenant heeft met de OIDC foundation kan participeren in de werkgroepen. Toetreden is nagenoeg kosteloos.

5.2.3.3 Kan een belanghebbende formeel bezwaar aantekenen tegen de gevolgde procedure?

Nee. De besluiten van werkgroepen worden gemaakt op basis van consensus, niet op basis van stemmen. Aanwezigen zitten er niet namens organisaties, maar op persoonlijke titel. Mocht er desondanks geen consensus bereikt worden, dan kan er gestemd worden. Dit is niet gangbaar. Er kan niet formeel bezwaar gemaakt worden tegen genomen besluiten, maar er is voldoende gelegenheid tot inspraak en het proces verloopt open en democratisch. Daarom is het geen bezwaar kunnen maken volgens de experts geen belemmering.

5.2.3.4 Organiseert de standaardisatieorganisatie regelmatig overleggen met belanghebbenden over doorontwikkeling en beheer van de standaard?

Ja. Zie https://openid.net/foundation/calendar-of-events/
Onder https://openid.net/wg/ staan ook de geplande overleggen van verschillende werkgroepen.

5.2.3.5 Organiseert de standaardisatieorganisatie een publieke consultatie voordat (een nieuwe versie van) de standaard wordt vastgesteld?

Er is geen sprake van publieke consultatie. De totstandkoming van de specificatie is wel openlijk te volgen.
https://openid.net/wordpress-content/uploads/2010/01/OpenID_Process_Document_December_2009_Final_Approved.pdf
Voor inspraak op de specificaties hoef je geen lid te zijn van OpenID Foundation maar wel de intellectuel property rights onderschrijven.

5.2.4 Is de standaardisatieorganisatie onafhankelijk en duurzaam?

5.2.4.1 Is de ontwikkeling en het beheer van de standaard belegd bij een onafhankelijke non-profit standaardisatieorganisatie?

Ja, een non-profit gebaseerd in Oregon. Zie
https://openid.net/foundation/policies/

5.2.4.2 Is de financiering van de ontwikkeling en het onderhoud van de standaard voor tenminste drie jaar gegarandeerd?

Het betreft een internationale organisatie met veel grote organisaties als lid van de OpenID Foundation. Bovendien kent de standaard een toenemende belangstelling en is het gebaseerd op standaarden die geschikt zijn voor mobiele toepassingen, zoals, JSON en Restfull API. Daarmee lijkt de ontwikkeling van de standaard de komende drie jaar zeker gegarandeerd.

5.2.5 Is het (versie) beheer van de standaard goed geregeld?

5.2.5.1 Heeft de standaardisatieorganisatie gepubliceerd beleid met betrekking tot (versie)beheer van de standaard? Bij voorkeur is dit beleid ook beschreven in een beheerplan (met o.a. aandacht voor migratie van gebruikers)

Ja,
https://openid.net/wordpress-content/uploads/2010/01/OpenID_Process_Document_December_2009_Final_Approved.pdf

5.2.5.2 Is de beheerdocumentatie goed vindbaar en verkrijgbaar?

Ja, alle documenten en maillinglists moeten openlijk toegankelijk zijn op
https://openid.net/

5.2.5.3 Is het belang van de Nederlandse overheid voldoende geborgd bij de ontwikkeling en het beheer van de standaard?

Ja, mogelijk door deelname aan OpenID Foundation tegen geringe vergoeding. Logius is voornemens hier lid van te worden.

5.2.5.4 Is de vertegenwoordiging van belanghebbenden bij het beheer van de standaard een goede representatie van het werkingsgebied en functioneel toepassingsgebied van de standaard?

Veel grote overheidsorganisaties en bedrijven zijn lid van de OpenID Foundation. Het lidmaatschap vereist onderschrijving van de spelregels van de OpenID Foundation. Daarmee is deze toegankelijk voor alle organisaties.

5.2.5.5 Is het standaardisatieproces van de standaardisatieorganisatie zodanig goed geregeld dat het Forum zich kan onthouden van aanvullende toetsing bij de aanmelding van een nieuwe versie van de standaard?

De Open ID Foundation heeft een policy vergelijkbaar met andere open standaard beheer en doorontwikkel organisaties. Toetsing bij aanmelding van een nieuwe versie is niet nodig.

5.2.6 Is er adoptieondersteuning voor de standaard?

5.2.6.1 Is er een toegankelijk aanspreekpunt of organisatie waar meer informatie over de standaard is te vinden en op te vragen is?

Tot nu toe is dat de OpenID Foundation. Deze heeft ook een Europese vertegenwoordiging in Zwitserland en Denemarken. Binnen de Nederlandse overheid zal waarschijnlijk Logius de organisatie worden die kennishouder wordt van OIDC en implementatieondersteuning zal bieden aan overheidspartijen.

5.2.6.2 Wordt er ondersteuning gegeven in de adoptie en de implementatie van de standaard?

Zie 5.2.6.1.

5.2.7 Conclusie criteria 'Open standaardisatieproces'

Er is sprake van een open standaardisatieproces. De doorontwikkeling en het beheer is open en transparant en is vergelijkbaar met IETF, W3C en ISO.

5.3 Draagvlak

Aanbieders en gebruikers moeten voldoende positieve ervaring met de standaard hebben.

5.3.1 Bestaat er voldoende marktondersteuning voor de standaard?

5.3.1.1 Bieden meerdere leveranciers ondersteuning voor de standaard?

Ja. Er zijn diverse leveranciers en producten, zowel commercieel als open source, door de OpenID Foundation gecertificeerd. Zie https://openid.net/developers/certified/. Dit kan overigens per rol en profiel verschillen.

5.3.1.2 Kan een gebruiker de conformiteit van de implementatie van de standaard (laten) toetsen?

Ja, alle organisaties aangesloten bij de OpenID foundation kunnen meedoen bij het toetsen van conformiteit van een nieuwe partij.

5.3.1.3 Draagt de standaard voldoende bij aan interoperabiliteit zonder dat aanvullende standaardisatieafspraken (zoals lokale profielen) noodzakelijk zijn om de standaard te implementeren of te gebruiken?

Nee, een Nederlands profiel is nodig om interoperabiliteit te bespoedigen. Het iGOV / internationale profiel voor overheidstoepassingen en het publieke domein wordt door de OpenID Foundation beheerd. De Nederlandse werkgroep onder leiding van Geonovum ontwikkelt het nationale iGov-NL profiel voor OAuth2. iGov-NL voor OIDC (met review van werkgroep) bouwt voort op iGov-NL profiel van OAuth2. Dit profiel is een beperkte aanvulling op een profiel voor interoperabiliteit in het overheids/publieke domein (iGov).

Aanvankelijk was ook dit iGov-NL profiel, opgesteld door het programma eID, ingediend voor plaatsing op de lijst samen met de standaard OIDC. Op advies van het Forum Standaardisatie is dit iGOV NL profiel uiteindelijk niet als onderdeel van de standaard aangeboden. Het profiel is op dit moment nog onvoldoende breed gedragen om te kunnen spreken van een gedragen Nederlands profiel. Daarnaast is er op dit moment nog geen beheerorganisatie benoemd voor het beheer en doorontwikkeling van het iGov-NL profiel. Waarschijnlijk wordt dit Logius.

5.3.1.4 Zijn er profielen of voorbeeldimplementaties van de standaard aanwezig en zijn deze vrij te gebruiken?

Ja. Voor OIDC is een Nederlands profiel ontwikkelt door het programma eID. Ook SURF heeft een werkende toepassing (richting Service Providers) waarin gebruik is gemaakt van OIDC, daarbij is gebruik gemaakt van het internationale profiel.

Door de experts is aangegeven dat een Nederlandse profiel noodzakelijk is om effectief en efficiënt gebruik te maken van de voordelen die de standaard OIDC biedt. Bij de introductie van SAML zijn in eerste instantie geen profielen ontwikkeld. Deze profielen zijn in de loop der jaren ontstaan en niet landelijk vastgesteld met negatieve gevolgen voor de interoperabiliteit.

Het advies is dan ook om vaart te zetten achter de ontwikkeling van een breed gedragen Nederlands profiel voor OIDC afgestemd op het Nederlandse OAuth2 profiel.

5.3.2 Kan de standaard rekenen op voldoende draagvlak?

5.3.2.1 Staan de belangrijkste stakeholders vanuit de overheid voor deze standaard achter de adoptie van de standaard?

Ja. De experts en belangrijkste stakeholders staan achter adoptie van de standaard, mits er een Nederlands profiel OIDC vastgelegd wordt en de doorontwikkeling en het beheer is belegd.

De standaard is opgenomen in de Project Startarchitectuur (PSA) van eID en deze is goedgekeurd door de programma governance met daarin

diverse dienstverleners. In diezelfde PSA is ook aangegeven dat SAML nog enige tijd gehandhaafd zal worden.

5.3.2.2 Staan de overheidsorganisaties die daadwerkelijk worden geraakt door een mogelijke verplichting van de standaard achter het gebruik van de standaard?

Ja. De overheidsorganisaties staan achter adoptie van de standaard, maar voorwaarde voor brede toepassing van de standaard is een gedragen Nederlands OIDC profiel is. Gedragen middels opname van dit Nederlandse profiel op de 'Pas toe of leg uit' lijst.

5.3.2.3 Wordt de aangemelde versie van de standaard binnen het organisatorische werkingsgebied door meerdere Nederlandse overheidsorganisaties gebruikt?

Nee. Wel is er veel interesse en ontwikkeling op dit gebied. De authenticatie en autorisatievoorziening van SURF ondersteunt reeds OIDC naast SAML richting Service Providers (nog niet richting Identity Providers). Er wordt hierbij geen gebruik gemaakt van het iGov-NL profiel. Ook in de zorgsector is de standaard OpenID Connect wel al in gebruik, maar ook niet gebaseerd op een Nederlands profiel.

5.3.2.4 Wordt een vorige versie van de standaard binnen het organisatorische werkingsgebied door meerdere Nederlandse overheidsorganisaties gebruikt?

Niet van toepassing.

5.3.2.5 Is de aangemelde versie backwards compatible met eerdere versies van de standaard?

Nee. Er is wel een migratie specificatie, indien van toepassing: https://openid.net/specs/openid-connect-migration-1_0.html

5.3.2.6 Zijn er voldoende positieve signalen over toekomstige gebruik van de standaard door (semi-)overheidsorganisaties, het bedrijfsleven en burgers?

Ja. Zie ook 5.1.3.3 in verband met ontzorging die geboden wordt voor wettelijke verplichting.

5.3.3 Conclusie criteria 'Draagvlak'

5.4 Opname bevordert adoptie

De opname op de lijst is een geschikt middel om de adoptie van de standaard te bevorderen.

Met de lijst wil het OBDO de adoptie van open standaarden bevorderen die voldoen aan de voorgaande criteria (toegevoegde waarde, standaardisatieproces en draagvlak).
- Met de pas-toe-of-leg-uit lijst beoogt het OBDO standaarden te verplichten als:
  a. hun huidige adoptie binnen de (semi-)overheid beperkt is;

b. opname op de lijst bijdraagt aan de adoptie door te stimuleren (functie = stimuleren).

- Met de lijst aanbevolen standaarden beoogt het OBDO standaarden aan te bevelen als :
  a. hun huidige adoptie binnen de (semi-)overheid reeds hoog is;
  b. opname op de lijst bijdraagt aan de adoptie door te informeren en daarmee onbedoelde afwijkende keuzes te voorkomen (functie = informeren).

5.4.1 Is opname op de pas-toe-of-leg-uit lijst het passende middel om de adoptie van de standaard binnen de (semi)overheid te bevorderen?

Dit zou inderdaad een passend middel zijn, ware het niet dat een functioneel vergelijkbare standaard op de 'pas toe of leg uit'-lijst staat; SAML. Aangezien niet twee standaarden op de 'pas toe of leg uit'-lijst kunnen staan met een vergelijkbaar functioneel toepassingsgebied, is het advies van de experts eerst een Nederland profiel te ontwikkelen afgestemd op het Nederlandse OAuth2 profiel. Dit Nederlands profiel moet breed gedragen worden en ook het beheer daarvan moet belegd zijn. Vervolgens kan het Nederlandse OIDC profiel worden ingediend voor plaatsing op de 'pas toe of leg uit'-lijst.

5.4.2 Is opname op de lijst aanbevolen standaarden het passende middel om de adoptie van de standaard binnen de (semi)overheid te bevorderen?

Het plaatsen van OAuth2, OIDC en uiteindelijk ook SAML op de lijst aanbevolen standaarden is naar verwachting de beste optie om de adoptie van de standaard OIDC te versnellen. Het is sowieso andersom: als SAML een verplichte standaard blijft en OIDC heeft aan aanbevolen status, belemmert dat de adoptie.

5.4.3 Conclusie criteria 'Opname bevordert adoptie'

Adoptie van de standaard is nodig en opname op de lijst van aanbevolen standaarden is het hoogst haalbare op dit moment, gezien de functionele overeenkomst met SAML. Van belang is om zo snel mogelijk een breed gedragen Nederlands profiel te ontwikkelen voor OIDC. Dit Nederlands profiel zal moeten worden opgenomen op de 'pas toe of leg uit'-lijst .

Hetzelfde geldt voor het Nederlands profiel van OAuth2. SAML moet gelijktijdig met het op de 'pas toe of leg uit' lijst plaatsen van de Nederlandse OAuth2 en OIDC profielen, worden verplaatst van de 'pas toe of leg uit'-lijst naar de lijst van aanbevolen standaarden.

5.5 Adoptieactiviteiten

Gebruik van de standaard is het uiteindelijke doel van het Forum Standaardisatie en OBDO. Plaatsing op de pas-toe-of-leg-uit lijst of de lijst aanbevolen standaarden is hiervoor een eerste stap, maar voor het daadwerkelijk adopteren (implementeren en gebruiken) van de standaard is vaak aanvullende actie benodigd. Aanvullend kan Forum Standaardisatie dan ook bijdragen aan adoptie van de standaard door het actief inzetten van adoptie-instrumenten of ondersteunende acties. Welke kansen zijn er om de adoptie te versnellen en welke drempels bestaan er die de adoptie van de standaard hinderen?

De expertgroep adviseert het Forum Standaardisatie en OBDO om bij de opname op de lijst voor pas-toe-of-leg-uit de volgende oproepen ten aanzien van de adoptie van OIDC te doen:

- De Nederlandse overheid moet op korte termijn een partij of programma aanwijzen die het initiatief neemt om een breed gedragen Nederlandse OIDC-profiel te ontwikkelen. Het programma eID lijkt hiervoor een geschikte partij.

- 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. De beheerorganisatie moet eigenaarschap uitstralen en ondersteuning bieden bij de implementatie van OIDC en het Nederlandse profiel door (semi)overheidspartijen.

- Oproep aan alle (semi)overheidspartijen en publieke diensten om kennis af te vaardigen voor het ontwikkelen van een Nederlands profiel voor OIDC.

- De expertgroep adviseert om de jaarlijkse evaluatie van de adoptie van de standaard door het Bureau Forum Standaardisatie uit te laten voeren.