Expertadvies NL GOV OpenID Connect profiel versie 1.0

Datum:	25 januari 2022
Versienummer:	1.2
Opdrachtgever:	Forum Standaardisatie Postbus 96810 2509 JE Den Haag 070-8887776 info@forumstandaardisatie.nl
Procedurebegeleiding:	Lost Lemon
Voorzitter expertgroep:	Bas van Luxemburg
Auteurs:	Arjen Brienen en Jeroen de Ruig

Inhoud

1 Samenvatting en advies

Op basis van het expertonderzoek adviseren experts om NL GOV OpenID Connect profiel versie 1.0 op te nemen op de 'pas toe of leg uit'-lijst van het Forum Standaardisatie. Tegelijkertijd constateren zij een aantal zorgpunten en doen zij verschillende adviezen ter bevordering van de adoptie.

Als functioneel toepassingsgebied wordt geadviseerd:

Het NL GOV OpenID Connect profiel moet worden toegepast bij het beschikbaar stellen en het gebruik van federatieve authenticatiediensten, inclusief vertegenwoordiging- en attribuut-verstrekking.

Als organisatorisch werkingsgebied wordt geadviseerd:

Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector en organisaties die namens deze organisaties authenticatie voorzieningen aanbieden.

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.

De experts maken zich zorgen over het ontstaan van een mogelijke wildgroei van niet-compatible implementaties van OpenID Connect, zolang er geen afgesproken en gedeeld Nederlands profiel is. Er is belang bij gebruik van NL GOV OpenID Connect profiel versie 1.0 vanwege ondersteuning van het profiel op een toenemend aantal mobiele toepassingen. Vanuit oogpunt van security en privacy is dit een belangrijke standaard. Het belang van de standaard is hiermee groot en de urgentie is hoog.

Tijdens de expertbijeenkomst is duidelijk geworden dat het NL GOV OpenID Connect profiel 1.0 niet aan alle criteria voor toetsing van een standaard voldoet. Het beheer van de standaard is op dit moment nog onvoldoende geregeld. Voor de criteria op het gebied van draagvlak geldt dat de standaard op dit moment in de praktijk nog niet wordt toegepast; er is geen referentie-implementatie.

Vanuit de criteria van toegevoegde waarde is de samenhang met SAML een aandachtspunt. SAML heeft een deels overlappend functioneel toepassingsgebied met OpenID Connect. OpenID Connect staat als standaard op de lijst van aanbevolen standaarden. Dit expertadvies heeft betrekking op het gebruik van het NL GOV profiel. Dit betekent dat als deze standaard op de 'pas toe of leg uit'-lijst staat en je gebruik maakt van OpenID Connect, het NL GOV profiel moet worden toegepast. Zodra OpenID Connect als standaard wordt aangeboden voor de 'pas toe of leg uit'-lijst, moet een duidelijk functioneel onderscheid gemaakt worden tussen het toepassingsgebied van SAML en OpenID Connect.

De experts geven, ondanks bovenstaande punten, een positief advies om het Nederlandse profiel NL GOV OpenID Connect profiel versie 1.0 te plaatsen op de ‘pas toe of leg uit’-lijst.

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 NL GOV OpenID Connect profiel gericht aan het OBDO en Forum Standaardisatie. NL GOV OpenID Connect profiel is aangemeld voor opname op de lijst met open standaarden door Frank van Es werkzaam bij Logius.

Doel van dit document is om het OBDO te adviseren of NL GOV OpenID Connect profiel in aanmerking komt voor opname op de 'pas toe of leg uit' lijst, al dan niet onder voorwaarden.

2.3 Doorlopen proces

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

1. De procesbegeleider hebben op 2 november 2020 een intakegesprek gesprek gehad met de indiener Frank van Es (Logius) en met Remco Schaar (Logius), Ruud de Jong (Visma), Han Zuidweg (Bureau Forum Standaardisatie) en Robin Gelhard (Bureau Forum Standaardisatie). In dit gesprek is onderzocht of de standaard voldoet aan de criteria om in procedure genomen te worden. Daarnaast is vooruitgeblikt op de procedure.
2. Vervolgens is een intakeadvies geschreven en dit is aangeboden aan het Forum Standaardisatie.
3. Het Forum Standaardisatie heeft geconcludeerd dat het resulterende advies uit de procedure niet ter besluitvorming aan het Forum Standaardisatie wordt voorgelegd totdat het (tijdelijk) beheer van de standaard voldoet aan de criteria voor 'open beheer' en er meer zicht is op praktijkervaring met de standaard en marktaanbod voldoende draagvlak en marktaanbod.
4. Han Zuidweg (Bureau Forum Standaardisatie) heeft in augustus een gesprek gehad met de indieners van de standaard en gezamenlijk afgesproken dat de expertbijeenkomst kan worden ingepland.
5. De expertgroep is op donderdag 7 oktober 2021 bijeengekomen om de standaard te toetsen aan de daaraan gestelde criteria. Tijdens

deze bijeenkomst heeft de expertgroep ook een voorstel gedaan voor het toepassings- en werkingsgebied.

Dit expertadvies geeft de uitkomst van de expertbijeenkomst 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 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 27 januari tot en met 24 februari 2022. 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 Bas van Luxemburg, Hoofd R&D bij Lost Lemon.

Arjen Brienen senior 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 EID (indiener)
- Frank van Es — Logius (indiener)
- Anouschka Biekman — Logius EID
- Arjan van Krimpen — VZVZ
- Bart Geesink — SURF
- Dennis Reumer — RVO
- Edward Hardam — CHvV
- Marcel Molenaar — UWV
- Frans de Kok — Logius eHerkenning
- Frank Zwart — Logius DigiD/DigiD machtigen
- Martin van der Plas — Logius Centrum voor Standaarden
- Gemma Gahan — KPN
- Jan Geert Koops — DICTU
- Peter Haasnoot — Logius Centrum voor Standaarden
- Paul Lemmers — DevCon
- Menno Pleijster — ABN AMRO
- Martin Borgman — Kadaster

Hans Laagland en Han Zuidweg van het Bureau Forum Standaardisatie waren als toehoorder bij de expertbijeenkomst aanwezig.

De aanwezige experts hebben voorafgaand aan de expertbijeenkomst een concept expertadvies opgestuurd gekregen.

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 NL GOV OpenID Connect profiel versie 1.0

OpenID Connect is een open en gedistribueerde manier om authenticatiediensten naar keuze te kunnen hergebruiken bij meerdere dienstverleners, bij gebruik vanuit onder andere webapplicaties en mobiele toepassingen. OpenID Connect is reeds opgenomen op de lijst aanbevolen standaarden. Advies bij de opname van OpenID Connect op de lijst van aanbevolen standaarden, was het gezamenlijk ontwikkelen van een Nederlands profiel van de standaard.

Het **NL GOV OpenID Connect profiel versie 1.0** (NL GOV Assurance profile for OpenID Connect 1.0) vult de standaard OpenID Connect aan met additionele eisen en richtlijnen, welke zorgen voor toepasbaarheid en interoperabiliteit specifiek binnen de Nederlandse (semi-)overheid. Het wordt gezien als een noodzakelijke aanvulling bij OpenID Connect om deze in de Nederlandse context te kunnen toepassen.

Doelen zijn het bespoedigen van interoperabiliteit en voorkomen van dialecten. Het neerzetten van een fatsoenlijke baseline voor privacy en security. Generiek voor gebruik binnen de Nederlandse overheid. Doel is onder andere toepassing van eID (elektronische identiteit)-middelen voor gebruik binnen de Nederlandse overheid. Maar de standaard moet ook toepasbaar zijn voor bi- en multilaterale afspraken tussen partijen, zelfs intern een organisatie. Het moet ook schaalbaar zijn.

Verdere detaillering zijn onder andere:

- Authenticatie van de OpenID Client bij de OpenID Provider, zodat laatstgenoemde kan vaststellen dat een authenticatieverzoek van een geregistreerde OpenID Client afkomstig is;
- Het verpakken van authenticatievragen in request objects zodat deze ondertekend en versleuteld kunnen worden, indien gewenst;
- Wanneer autorisaties als claims (bv “de eindgebruiker is een beheerder”) of scopes (bv “de eindgebruiker mag de beheerfunctionaliteit gebruiken”) worden gecommuniceerd;
- Afstemming met internationale afspraken, bijvoorbeeld het gebruik van OIDC binnen eIDAS;
- Welke authenticatieniveaus (Levels of Assurance) van belang zijn voor authenticatie.

Het NL GOV OpenID Connect profiel geeft door dienstverleners aangeboden diensten 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 diensten.

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 werkingsgebied* (welke organisaties moeten de standaard gebruiken) beschreven.

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

4.1 Functioneel toepassingsgebied

De expertgroep adviseert als functioneel toepassingsgebied voor NL GOV OpenID Connect profiel:

Het NL GOV OpenID Connect profiel moet worden toegepast bij het beschikbaar stellen en het gebruik van federatieve authenticatiediensten, inclusief vertegenwoordiging- en attribuutverstrekking.

4.2 Organisatorisch werkingsgebied

De expertgroep adviseert om het organisatorisch werkingsgebied van de standaard voor een groot deel 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 en organisaties die namens deze organisaties authenticatie voorzieningen aanbieden.

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

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

Definitie: 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. Na lange discussie is vastgesteld dat het functioneel toepassingsgebied met de aanvulling vanuit de experts voldoende onderscheidend is. OpenID Connect staat op de lijst van aanbevolen standaarden. Dit betekent feitelijk dat als OpenID Connect wordt toegepast het NL GOV OpenID Connect profiel moet worden toegepast.

Aangezien het functioneel toepassingsgebied van NL GOV OpenID Connect profiel afwijkt van het functioneel toepassingsgebied van OpenID Connect adviseert de expertgroep om het functioneel toepassingsgebied van OpenID Connect in overeenstemming te brengen met het functioneel toepassingsgebied van NL GOV OpenID Connect profiel.

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 en organisaties die namens deze organisaties authenticatie voorzieningen aanbieden.

Belangrijk daarbij is dat aanbiedende partijen die werken onder de verantwoordelijkheid of erkenning van de overheid, zoals bijvoorbeeld

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

KPN, ook gehouden zijn aan de standaard. In dit geval betekent dit dat ook niet overheidspartijen de standaard moeten implementeren.

In de Memorie van Toelichting van het wetsvoorstel Wet digitale overheid staat het volgende: 'Bij de aan te wijzen organisaties gaat het om (categorieën van) instanties die elektronische diensten verlenen ter uitvoering van een publieke taak, in het algemeen belang of waarbij het burgerservicenummer (bsn) wordt verwerkt, waarvoor, gelet op de aard en kenmerken van deze diensten, veilige en betrouwbare authenticatie noodzakelijk is.'

De expertgroep geeft het advies aan het Forum om het standaard organisatorisch werkingsgebied te herformuleren en aan te vullen met zowel aanbiedende als afnemende organisaties en organisaties die namens de overheid diensten aanbieden die betrekking hebben op het functioneel toepassingsgebied.

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, omdat het een profiel op een universele authenticatiestandaard specifiek voor gebruik binnen (semi-)overheidsorganisaties is, welke 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 OpenID Connect 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)?

Ja, hoewel de functionele toepassingsgebied en organisatorische werkingsgebieden deels overlappen met die van SAML, kunnen beiden naast elkaar worden toegepast. De verwachting is dat SAML nog enige tijd naast OpenID Connect zal blijven bestaan in omgevingen waar een overstap op OpenID Connect op basis van het NL GOV OpenID Connect profiel nog niet haalbaar is.

De expertgroep geeft het advies aan het Forum om binnen een jaar het onderzoek te starten of het mogelijk is om SAML van de lijst te halen. Het eventueel verwijderen van SAML van de lijst betekent overigens niet dat SAML niet meer gebruikt mag worden, maar dat bij de inkoop van nieuwe voorzieningen niet langer SAML hoeft te worden vereist.

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. OpenID Connect is meer geschikt dan SAML voor mobiele, browser-gebaseerde en IoT toepassingen dan SAML en is beter toepasbaar in API-ecosystemen. De trend van steeds meer mobiele- en browser-gebaseerde apps en grote adoptie van API-architecturen, zal een toename betekenen in de behoefte aan OpenID Connect.

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

Tenslotte biedt dit profiel meerwaarde boven de OpenID Connect standaard, welke momenteel als aanbevolen standaard is opgenomen binnen de lijst van open standaarden. Dit betekent feitelijk dat als OpenID Connect wordt toegepast het NL GOV OpenID Connect profiel moet worden toegepast. Daarnaast spitst het NL GOV OpenID Connect profiel specifiek zich toe op de context van (semi-)overheidsorganisaties in Nederland. Bovendien voorziet de standaard in een aantal best-practices op het gebied van beveiliging bij gebruik van mobiele en browser-gebaseerde applicaties. Tot slot voorkomt het hanteren van het profiel het ontstaan van verschillende, mogelijk niet-interoperabele, “dialecten”.

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

Er zijn eigenlijk geen concurrerende standaarden die in aanmerking zouden kunnen komen voor opname. Het NL GOV OpenID Connect profiel bouwt voort op het NL GOV OAuth 2.0 profiel en voegt daar de mogelijkheid aan toe om authenticatie- en identiteitsgegevens uit te wisselen.

OAuth2 is een open standaard welke bedoeld is voor autorisatie. Het faciliteert toegang tot bijv. apps met 'delegated authorization'. OpenID Connect biedt deze federatieve authenticatie. De OpenID Connect-flow maakt gebruik van de OAuth 2.0 authorization code flow, waarbij een belangrijke toevoeging het 'ID-token' is, dat identificatie van de geauthentiseerde gebruiker mogelijk maakt.

OAuth 2.0 en OpenID Connect liggen meer in elkaars verlengde. Voor de eenduidigheid in de toepassing van authenticatie en autorisatie te realiseren binnen de Nederlandse overheid en publieke diensten is een Nederlands profiel ontwikkeld voor OpenID Connect in afstemming met het ontwikkelde Nederlandse OAuth 2.0 profiel.

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

Ja, de standaard betreft een Nederlands profiel voor de internationale standaard OpenID Connect, die wordt beheerd door de OpenID Foundation.

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, omdat het NL GOV OpenID Connect profiel compatibel is met de OpenID Connect standaard en voornamelijk keuzes maakt waar de OpenID Connect standaard meerdere mogelijkheden openlaat. Hierdoor zullen de kosten van implementatie niet enorm afwijken van die van een reguliere OpenID Connect implementatie.

Wel biedt het profiel een aantal optionele uitbreidingen, bijvoorbeeld het gebruik van vertegenwoordiging, waarvoor kosten apart moeten worden ingeschat wanneer een implementatie deze aan wil bieden.

De expertgroep geeft aan de beheerders het advies om conformerende configuraties van gangbare implementaties van het profiel beschikbaar te stellen, deze zouden door partijen kunnen worden gebruikt bij de implementatie van de standaard.

In vergelijking met een SAML-implementatie is het zeker goedkoper. Deze vereist veel inspanning onder andere vanwege de vele dialecten. Met de introductie van een standaard NL GOV profiel wordt de inspanning van de implementatie van Open ID Connect beperkt.

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

Het profiel leidt juist tot eenduidigheid en dat bevordert de interoperabiliteit, verhoogt de security en privacy en de werkbaarheid van de toepassing. Het profiel is daardoor een belangrijkere enabler van een eenduidige toepassing van OpenID Connect.

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?

Zie 5.1.3.2.

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

Ja, omdat het profiel juist mitigerende maatregelen voor implementatie van OpenID Connect treft. Hierbij is ook specifiek aandacht voor mobiele en web-gebaseerde applicaties. Hiermee brengt dit profiel meer veiligheid, dan standaard OpenID Connect implementatie.

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

Ja, omdat het profiel juist privacy verhogende maatregelen ondersteunt, zoals dataminimalisatie bij uitvraag van attributen (claims) en gebruik van *pairwise* identifiers. En waar mogelijk in de vorm van (polymorf) versleutelde identiteiten en pseudoniemen te communiceren.

5.1.4 Conclusie criteria 'Toegevoegde waarde'
De experts geven aan dat de standaard een grote toegevoegde waarde heeft. De standaard zorgt voor eenduidigheid van implementaties, dit leidt tot interoperabiliteit. Bij SAML zijn in de loop der jaren meerdere dialecten ontstaan dit heeft geleid tot veel extra inspanning om het stelsel interoperabel te houden. Dit wordt voor OpenID Connect voorkomen, dankzij NL GOV OpenID Connect profiel.

5.2 Open standaardisatieproces

Definitie: 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 eenieder drempelvrij beschikbaar?

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

Ja, het is vrij beschikbaar via de Gitlab repository.

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. Alle versies van het specificatiedocument zijn beschikbaar via het internet op de Gitlab repository. In de Gitlab repository van de standaard zijn alle review commentaren met daarbij behorende discussies en genomen besluiten alsook de notulen van de werkgroepsessies .

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. Het profiel is onder de licentie "Creative Commons Attribution 4.0 International Public License (CC-BY)" gepubliceerd. Deze licentie legt geen beperkingen aan het gebruik anders dan naamsvermelding en het niet mogen toevoegen van aanvullende juridische restricties.

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. Dit betreft een open standaard. Zie vorige vraag.

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, in de Gitlab repository van de standaard zijn alle review commentaren met daarbij behorende discussies en genomen besluiten alsook de notulen van de werkgroepsessies .

Overheidspartijen en afnemende partijen zijn betrokken bij het besluitvormingsproces. Centrum voor Standaarden gaat de standaard beheren en zal daar de BOMOS-methodiek toepassen. De toepassing van de BOMOS-methodiek garandeert dat de standaard voldoet aan de criteria van een open standaardisatieproces.

Toegezegd is dat het beheer kan starten als de standaard op de lijst van open standaarden van het Forum Standaardisatie staat. Dit is ook zo gegaan bij het NL GOV Oauth 2.0 profiel. Vergelijkbare procedure.

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

Ja. De besluiten zijn op basis van consensus gemaakt tijdens de werkgroepsessies. In die gevallen dat besluiten dienden te worden genomen tijdens het proces van opstellen van de profielspecificatie zijn besluiten altijd voorgelegd aan de werkgroep. Tevens hebben alle werkgroepleden de mogelijkheid gehad om het profiel tijdens het specificatieproces te reviewen en ook al het review commentaar is met de werkgroep besproken en tevens openbaar in te zien in het Issues overzicht van het Gitlab project van het profiel.

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

Het is voor iedereen en zonder belemmeringen mogelijk om issues aan te maken in het Gitlab project van het profiel, welke vervolgens voor iedereen inzichtelijk zijn. Tevens wordt, wanneer het profiel in beheer wordt genomen door het Centrum voor Standaarden, een vaste klachtenprocedure voor het beheer van open standaarden van het Centrum voor Standaarden gehanteerd.

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

Op het moment dat deze standaard in beheer komt van het Centrum voor Standaarden van Logius zal de governance worden ingevuld conform BOMOS met periodiek overleggen met belanghebbenden (naast de online community).

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

Op dit moment staat de standaard op Gitlab en heeft iedereen dus de mogelijkheid om hierop te reageren. Voordat de standaard is ingediend is deze gereviewed door verschillende (overheids)partijen. Er zijn verschillende sessies geweest om commentaar te bespreken en te verwerken in de standaard.

Op het moment dat deze standaard in beheer komt van het Centrum voor Standaarden van Logius zal de governance worden ingevuld conform

BOMOS met publieke consultaties bij voorgenomen wijzigingen aan de standaard.

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. Het beheer wordt belegd bij het Centrum voor Standaarden (CvS) van Logius. CvS werkt conform BOMOS een heeft verschillende andere standaarden in beheer.

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

Ja. De financiering voor deze standaard is samen met twee andere API-standaarden (ADR en OAuth profiel) geborgd door ministerie van Binnenlandse Zaken. Op verzoek kan het CvS het Forum de opdrachtbrief van Ministerie van Binnenlandse Zaken sturen.

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)

Nog niet. Op het moment dat deze standaard bij CvS in beheer komt, wordt er als eerst een beheermodel beschreven waarin dit terug komt (wederom conform BOMOS).

5.2.5.2 Is de beheerdocumentatie goed vindbaar en verkrijgbaar?

Zie 5.2.5.1. De specificatie zelf is openlijk beschikbaar via Gitlab.

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

Ja, omdat het profiel is gebaseerd op het NL GOV OAuth profiel en de standaard tot stand is gekomen in nauwe samenwerking tussen verschillende (overheids)organisaties. Beheer ook bij overheidsorganisatie.

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?
Ja, want alle belanghebbenden mogen aanhaken bij de werkgroep en meebeslissen aan de toekomstige richting van het NL GOV OpenID Connect profiel.

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?

Bij deze eerste 1.0 versie nog niet, omdat CvS nog niet formeel de beheerder is. Op het moment dat CvS wel die rol heeft zal het bij de volgende versie van de standaard het predicaat 'uitstekend beheer' aanvragen.

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?

Ja, dit betreft (binnenkort) het Centrum voor Standaarden. Vragen worden nu actief in behandeling genomen.

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

Ja, ondersteuning in de adoptie en implementatie van het profiel wordt niet hands-on gegeven, maar wel op basis van documentatie en voorbeelden. Bovendien is het advies dat Logius (de beheerder) een compliance tool beschikbaar stelt.

5.2.7 Conclusie criteria 'Open standaardisatieproces'
De experts geven aan dat er voldoende vertrouwen is dat de standaard door CvS op een goede wijze beheerd wordt (BOMOS), zodat sprake is van een open standaardisatieproces.

5.3 Draagvlak

Definitie: 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?

Aangezien de standaard een nieuw profiel betreft, wordt deze nog niet ondersteund door leveranciers. Echter biedt het profiel een invulling van openstaande keuzes in het OpenID Connect profiel en wijkt het profiel niet enorm af van de standaard, waardoor de verwachting is dat het merendeel van de leveranciers die OpenID Connect aanbieden met acceptabele inspanning ook aan kunnen sluiten op het profiel.

In februari heeft een Hackaton plaatsgevonden waar implementaties deels zijn vormgegeven. Een volledige implementatie op basis van het profiel is er nog niet, maar er is wel ervaring met onderdelen van het profiel.

Experts adviseren aan de beheerders om nog een aantal aspecten van de standaard nader te bekijken met name de representatie van relaties.

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

Nee, op dit moment is dit nog niet mogelijk. Het is wel mogelijk te toetsen op de conformiteit van de OpenID Connect standaard, hier biedt de OpenID Foundation tevens zelf software voor aan.

De expertgroep geeft de beheerders het advies om gereviewde en geauditeerde voorbeeld configuraties van gangbare implementaties beschikbaar te stellen, die je kunt downloaden en importeren. Daarnaast een vorm van een testvoorziening in te richten om compliance aan te tonen op het NL GOV profiel, bij voorkeur door de beheerder van de standaard.

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?

Ja. Hoewel er geen (volledige) implementaties zijn, is de verwachting van wel, omdat de standaard een profiel op de OpenID Connect standaard betreft en concrete invulling geeft aan een aantal openstaande keuzes vanuit de OpenID Connect standaard. Wel biedt het profiel vrijheid om implementaties uit te breiden met extra functionaliteiten, waarvoor aanvullende standaardisatieafspraken benodigd zullen zijn.

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

Nee, er zijn er op dit moment nog geen voorbeeldimplementaties van het NL GOV OpenID Connect profiel. Wel is een groot aantal configureerbare implementaties en libraries beschikbaar voor de OpenID Connect standaard. Experts geven aan dat deze implementaties wel wenselijk zijn.

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, want de belangrijkste organisaties hebben meegewerkt aan de werkgroepsessies, te weten - Logius, Gemeente Den Haag, SURF, Ministerie van VWS, RvIG, RVO, Belastingdienst, iShare, Kennisnet, Dictu, CIV, VZVZ, Justid, Kadaster en VNG.

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, want de belangrijkste organisaties hebben meegewerkt aan de werkgroepsessies, te weten - Logius, Gemeente Den Haag, SURF, Ministerie van VWS, RvIG, RVO, Belastingdienst, iShare, Kennisnet, Dictu, CIV, VZVZ, Justid, Kadaster en VNG. UWV staat ook achter de standaard, mits aangetoond dat de standaard ook werkt en haalbaar is. Belangrijk dat er marktondersteuning is voor de standaard.

Belangrijk is dat er een implementatie komt. Voorstel is om een hackaton te organiseren, waarbij één of meerdere implementaties worden vormgegeven. Eén expert geeft aan dat hij bestaande implementaties wil verleiden om het profiel toe te passen. Daarnaast is er haast omdat er anders wildgroei van dialecten dreigt.

Advies van de expertgroep is om zo spoedig mogelijk, uiterlijk binnen een half jaar na plaatsing op de 'pas toe of leg uit' lijst, een implementatie van NL GOV OpenID Connect profiel vorm te geven en te implementeren. De experts willen eigenlijk geen dag vertraging. Door de experts wordt geschat dat een referentie implementatie ongeveer indicatief € 150.000 kost. Dit is inclusief projectorganisatie, ontwikkeling en implementatie.

Naschrift (januari 2022): inmiddels is duidelijk geworden dat er een proof of concept wordt geïnitieerd. BZK en Logius voeren een proof of concept uit voor het vereenvoudigen van de koppelvlakken binnen het domein Toegang. Binnen de proof of concept wordt ook het gebruik van het OIDC koppelvlak met het opgestelde NL-Gov profiel beproefd. In eerste instantie wordt het gebruik van het koppelvlak voor het authentiseren en het verstrekken van attributen onderzocht. Daarbij wordt aan de kant van de dienstverleners met meerdere standaard OIDC producten gewerkt om te onderzoeken hoe dienstverleners hun clients zo veel mogelijk door enkel configureren kunnen gaan inrichten.

Ten behoeve van de implementatie van de concept Wet digitale overheid zullen in de proof of concept ook vervolgstappen worden gezet met vertegenwoordiging en federatie met meerdere authenticatiediensten.

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

Nee, de standaard wordt nog niet bij de Nederlandse overheid gebruikt. Wel wordt de OpenID Connect standaard gebruikt door meerdere Nederlandse (semi-)overheidsorganisaties, waaronder SURF en iShare.

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

N.v.t., aangezien dit de eerste versie van het NL GOV OpenID Connect profiel betreft.

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

N.v.t., aangezien het de eerste versie van het NL GOV OpenID Connect profiel betreft. Het NL GOV OpenID Connect profiel is wel volledig compatible—en gebaseerd op—het Nederlandse OAuth 2.0 profiel.

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

Ja, het is de verwachting dat de standaard op den duur zal worden toegepast bij DigiD en de stelsels eID en eHerkenning. De OpenID

Connect standaard wordt momenteel al toegepast binnen het iShare stelsel en bij onder andere SURFconext, deze zullen naar verwachting aansluiten bij het NL GOV OpenID Connect profiel wanneer deze beschikbaar is. Verder wordt OpenID Connect breed toegepast binnen het bedrijfsleven als moderne toepassing voor federatieve authenticatie.

5.3.3 Conclusie criteria 'Draagvlak'
De experts geven aan dat, ondanks dat er geen voorbeeldimplementatie is, het belangrijk is dat deze standaard snel op de 'pas toe of leg uit' lijst komt. Deze conclusie komt tot stand na een discussie waarin de afweging is besproken dat het enerzijds niet wenselijk is een standaard te verplichten als er nog geen voorbeeldimplementatie heeft plaatsgevonden, en anderzijds dat het belang en de urgentie van de standaard hoog is. Vooral uit oogpunt van security en privacy is dit een belangrijke standaard. Er moet met grote spoed een voorbeeld implementatie volgen.

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?

Ja, omdat organisaties wachten met het implementeren van het NL GOV OpenID Connect profiel totdat deze verplicht wordt gesteld. Men maakt zich zorgen over een wildgroei van niet-compatible implementaties van de OpenID Connect standaard.

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?

Nee, omdat de standaard Open ID Connect op de aanbevolen lijst staat en als je deze standaard toepast het verplicht moet zijn om het NL GOV profiel toe te passen, en niet een ander of afwijkend profiel te implementeren.

5.4.3 Conclusie criteria 'Opname bevordert adoptie'
De experts geven aan dat de lijst adoptie bevordert.

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 NL GOV OpenID Connect profiel te doen:

- Advies aan de opstellers en beheerder van de standaard om een gereviewde en geauditeerde voorbeeld configuraties beschikbaar te stellen die je kunt downloaden voor gebruik in gangbare implementaties.
- Oproep aan overheidspartijen om zo spoedig mogelijk, uiterlijk binnen een half jaar na plaatsing op de 'pas- toe-of-leg-uit' lijst, een implementatie van NL GOV OpenID Connect profiel vorm te geven en te implementeren om op deze manier te kunnen beantwoorden aan de criteria rond draagvlak. De experts willen eigenlijk geen dag vertraging. Eventuele beproeving kan nog worden gedaan voordat het Forumadvies wordt aangeboden aan het Forum. In dat geval wordt dit advies geactualiseerd. Inmiddels is vanuit het Ministerie van Binnenlandse Zaken en Logius, het initiatief genomen om een proof of concept te ontwikkelen.
- De expertgroep geeft het advies aan het Forum om binnen een jaar het onderzoek te starten of het mogelijk is om SAML van de lijst te halen. Het eventueel verwijderen van SAML van de lijst betekent overigens niet dat SAML niet meer gebruikt mag worden, maar dat bij de inkoop van nieuwe voorzieningen niet langer SAML hoeft worden vereist.
- Aangezien het functioneel toepassingsgebied van NL GOV OpenID Connect profiel afwijkt van het functioneel toepassingsgebied van OpenID Connect adviseert de expertgroep het Forum om het functioneel toepassingsgebied van OpenID Connect in overeenstemming te brengen met het functioneel toepassingsgebied van NL GOV OpenID Connect profiel.
- Advies aan de opstellers van de standaard een poging te doen om een kortere versie te maken van de beschrijving van de standaard, een soort easy start guide. Dit moet overigens niet leiden tot vertraging voor de eerste implementatie.
- Advies aan het Centrum voor Standaarden het beheer uit te voeren als de standaard op de 'pas- toe-of-leg-uit' lijst staat. Net zoals bij het NL GOV OAuth2.0.
- Advies aan de beheerder van de standaard , een vorm van een testvoorziening in te richten voor het profiel, bij voorkeur door de beheerder van de standaard.