Aanvullend onderzoek NL GOV AP OpenID Connect

Datum:	23 maart 2023
Versienummer:	1.0
Opdrachtgever:	Forum Standaardisatie
Procedurebegeleiding:	Lost Lemon
Auteurs:	Arjen Brienen, Jeroen de Ruig

1. Aanleiding, vraagstelling en proces

Forum Standaardisatie toetst of de standaard van Logius NL GOV Assurance Profile for OpenID Connect 1.0 (hierna: NL GOV AP OIDC) geschikt is om te verplichten aan de overheid via plaatsing op de 'pas toe of leg uit'-lijst. NL GOV Assurance Profile for OIDC 1.0 draagt bij aan veiliger internet doordat authenticatieservices (zoals DigiD) de identiteit van een eindgebruiker controleren op een gestandaardiseerde wijze.

Dit aanvullend onderzoek is onderdeel van de toetsingsprocedure van het Forum Standaardisatie. Het is een aanvullend onderzoek in de toetsingsprocedure van verplichting van NL GOV AP OIDC na de expertbijeenkomst en openbare consultatie.

Dit aanvullend onderzoek behandelt aandachtspunten die naar voren kwamen tijdens het expertonderzoek en de bijbehorende openbare consultatie. Het onderzoek schetst de aanleiding en de achtergrond en stelt op basis daarvan vijf onderzoeksvragen. Onderdeel van het aanvullend onderzoek was het houden van hackathons (juli 2022 en 14 en 15 september 2022) en het consulteren van experts (6 oktober 2022). Hoofdstuk drie geeft een verslag van de bespreking van de vijf vragen incl. de hackathon en consultatie van de experts in najaar 2022. Een conclusie sluit elke bespreking van een vraag af. Het onderzoek sluit af met additionele adviezen.

1.1. Aanleiding en achtergrond

De internationale standaard OpenID Connect (OIDC) is een open en gedistribueerde manier om één authenticatiedienst naar keuze te kunnen hergebruiken bij meerdere (semi-

)overheidsdienstverleners, bij gebruik vanuit onder andere webapplicaties en mobiele apps. Belangrijkste redenen om op OIDC in te zetten is de actieve ontwikkelingen en de mobile-first strategie ondersteuning van digitale overheidsdiensten.

Op dinsdag 25 juni 2019 heeft een grote expertgroep bijeenkomst plaatsgevonden over de standaard OpenID Connect. De expertgroep concludeerde dat de standaard OpenID Connect niet op de 'pas toe of leg uit'-lijst kon worden opgenomen. Belangrijkste reden hiervoor was het ontbreken van een Nederlands profiel voor deze standaard. Bij de functioneel vergelijkbare standaard was in het verleden geen Nederlands profiel gedefinieerd en dit heeft geleid tot meerdere profielen voor deze standaard, waardoor de implementatie en vooral beheer complex werd. Een verplicht Nederlands profiel voor OpenID Connect zou dit moeten voorkomen. Aan het Forum Standaardisatie werd geadviseerd om OpenID Connect op te nemen op de lijst van aanbevolen standaarden. OIDC staat per 23 maart 2020 op de lijst aanbevolen standaarden.

Vervolgens is een werkgroep met daarin vertegenwoordiging van verschillende (overheids)organisaties een Nederlands profiel gaan definiëren. De eerste versie van het profiel werd op 18 februari 2021 gepubliceerd.

Logius heeft NL GOV Assurance Profile for OIDC 1.0 aangemeld bij het Bureau Forum Standaardisatie om te toetsen of dit profiel geschikt is te verplichten aan de overheid ('pas toe of leg uit'-verplichting). Op donderdag 7 oktober 2021 heeft de expertgroep als onderdeel van de toetsingsprocedure van NL GOV AP OIDC geadviseerd (220125-Expertadvies-NL-GOV-AP-OpenID-Connect-profiel) om de standaard op te nemen op de 'pas toe of leg uit'-lijst, ondanks dat aan drie belangrijke criteria niet volledig werd voldaan. De criteria waren:

- toegevoegde waarde, en dan met name de samenhang met SAML is een aandachtspunt. SAML heeft een deels overlappend functioneel toepassingsgebied met OpenID Connect en dat raakt daarmee ook de verplichting van het NL GOV AP OIDC op OIDC;
- open standaardisatie proces en dan met name beheer van de standaard. De beheerorganisatie was wel benoemd, maar zou pas actief worden als ook daadwerkelijk de standaard op de 'pas toe of leg uit'-lijst zou worden geplaatst;
- draagvlak, en dan met name het al toegepast hebben van de standaard door verschillende organisaties. De standaard bestond feitelijk alleen nog op papier, geen organisatie had de standaard daadwerkelijk geïmplementeerd of beproefd.

Vanuit de daaropvolgende openbare consultatie en ook vanuit experts van het Bureau Forum Standaardisatie zijn diverse vragen en opmerkingen geplaatst. De vragen en opmerkingen hadden deels betrekking op de drie criteria waar nog niet geheel aan werd voldaan. Daarnaast werd door een paar respondenten getwijfeld aan het nut van een Nederlands profiel.

In het verlengde van de overlap in het functioneel toepassingsgebied van SAML en OpenID Connect (criterium 'toegevoegde waarde': beide standaarden zijn functioneel vergelijkbaar)

was de vraag hoe eventueel een overgang van de SAML standaard naar de OpenID Connect standaard moet worden vormgegeven.

Naar aanleiding hiervan is besloten om een aanvullend onderzoek te laten uitvoeren door Lost Lemon.

1.2. De vraagstelling

OpenID Connect heeft een aantal voordelen ten opzichte van SAML. Eén van die voordelen is de betere toepasbaarheid van OpenID Connect voor mobiele toepassingen via apps. Ook vanuit oogpunt van security en privacy is OpenID Connect een belangrijke standaard. Het belang van de toepassing van de standaard OpenID Connect en het daarbij behorende Nederlands profiel, is hiermee groot en de urgentie is hoog.

Tijdens de expertbijeenkomst op 7 oktober 2021 bleek dat de geraadpleegde experts zich zorgen maken over het ontstaan van wildgroei van niet-compatible implementaties van OpenID Connect, zolang er geen afgesproken en gedeeld Nederlands profiel is. Deze zorgen zijn niet onterecht omdat bij de introductie van SAML er geen gedeeld Nederlands profiel was en daardoor verschillende profielen zijn ontstaan, met alle compatibiliteitsproblemen van dien. Ook is tijdens deze bijeenkomst duidelijk geworden dat de standaard NL GOV AP OIDC niet volledig aan alle criteria voor plaatsing op de lijst van open standaarden voldoet. Het beheer van de standaard was nog onvoldoende geregeld, en ook aan het criteria draagvlak en toegevoegde waarde werd niet volledig voldaan. De standaard was bijvoorbeeld nog niet in de praktijk toegepast, er was ook geen referentie-implementatie.

Tijdens de consultatie van experts voor dit aanvullend onderzoek is onderscheid gemaakt tussen standaard en profiel. Experts gaven aan dat zij OIDC standaard willen verplichten, in een geclusterde registratie met SAML; voor profiel bestond er voldoende consensus om profiel te verplichten. Er is in die consulktatie geen uitspraak gedaan hoe profiel (NL GOV AP OIDC) en hoe standaard (OIDC) zich tot elkaar verhouden in de geclusterde registratie Authenticatie-standaarden.

Vanuit het criterium toegevoegde waarde is de samenhang met SAML een aandachtspunt. SAML heeft een deels overlappend functioneel toepassingsgebied met OpenID Connect. Gezien de eerdergenoemde voordelen van de standaard OpenID Connect ten opzichte van SAML bestaat bij veel experts de wens om OpenID Connect zo spoedig mogelijk op te nemen op de ‘Pas toe of leg uit’-lijst.

Hoewel de verplichting voor NL GOV AP OIDC alleen geldt indien gebruik wordt gemaakt van de standaard OpenID Connect (lijst aanbevolen standaarden), is niet voldoende duidelijk wanneer SAML en wanneer OpenID Connect en het bijbehorende NL GOV AP OIDC moet worden toegepast. Een duidelijk transitiestrategie of –roadmap op authenticatievoorzieningen ontbreekt op dit moment.

De hierboven toegelichte knelpunten leiden tot de volgende zaken die verder zijn uitgewerkt en waar mogelijk beantwoord:

1. **Toegevoegde waarde: samenhang met het internationale iGOV-profiel voor OIDC**: is NL GOV AP OpenID Connect noodzakelijk? Zijn er mogelijk alternatieven voor deze standaard denkbaar? Kan er bijvoorbeeld niet gebruik gemaakt worden van een internationaal profiel i.p.v. zelf een Nederlands profiel te ontwikkelen en te gebruiken?
2. **Toegevoegde waarde i.c.m. relatie SAML en OpenID Connect**: met name de opname op de lijst open standaarden van zowel SAML als OpenID Connect leidt tot onduidelijkheid. SAML heeft het volgende functioneel toepassingsgebied: ’SAML moet worden toegepast op de uitwisseling van authenticatie- en autorisatiegegevens om gebruikers na eenmalig inloggen toegang te geven tot meerdere diensten.’ OpenID Connect heeft het volgende functioneel toepassingsgebied: ‘OpenID Connect kan toegepast worden bij het beschikbaar stellen van federatieve authenticatiediensten’. Deze functioneel toepassingsgebieden hebben de nodige overlap.
   Hierom is in het expertadvies OpenID Connect aanbevolen om SAML op de 'pas toe of leg uit'-lijst te houden en om OpenID Connect te plaatsen op de lijst aanbevolen standaarden. Inmiddels is wel voldoende duidelijk dat de standaard OpenID Connect de toekomst heeft. De vraag is wel hoe de transitie moet plaatsvinden van SAML naar OIDC? Moet er bijvoorbeeld een transitie-strategie van SAML naar OIDC en het bijbehorende Nederlandse profiel worden geformuleerd? Zo ja, hoe moet deze transitie-strategie er dan uitzien? Zijn er andere standaarden (zoals Oauth2) om in deze transitie te betrekken?
   De intentie voor de indiener Logius voor het verplichten van NL GOV AP OpenID Connect is mede om een transitie te bewerkstelligen van SAML naar OpenID Connect en het bijbehorende Nederlandse profiel. Deze transitie komt niet (of niet voldoende) van de grond, zolang alleen SAML als verplicht op de lijst blijft staan.
   Vanuit deze intentie bezien is een overlappend functioneel toepassingsgebied niet wenselijk. De kans is groot dat dit gaat leiden tot continuering van gebruik van SAML i.p.v. het stimuleren van een transitie naar OpenID Connect.
   Met de plaatsing van NL GOV AP OIDC op de ‘pas toe of leg uit’-lijst wordt mogelijk de indruk gewekt dat leveranciers/identityproviders al kunnen aansluiten op OpenID Connect via het Nederlandse profiel. In de praktijk is dit niet het geval, omdat er tot op heden weinig aanbod is van NL GOV AP OpenID Connect. Daarnaast wekt de plaatsing van NL GOV AP OpenID Connect op de ‘pas toe of leg uit’-lijst de indruk dat het gebruik van de generieke standaard OpenID Connect (lijst aanbevolen standaarden) verplicht is en dat de aansluitende partij zodoende een keuze dient te maken tussen SAML of OpenID Connect. Het is van belang hier duidelijkheid te scheppen.
3. **Open standaardisatieproces**: op moment van opstellen van dit verslag is Afdeling Standaarden van Logius niet formeel de beheerder van het Nederlandse profiel. Zodoende heeft NL GOV AP OIDC geen beheer. Daarmee voldoet NL GOV AP OIDC niet aan criterium voor open standaardisatieproces. Het beheer van NL GOV AP OIDC wordt pas actief als de daadwerkelijk NL GOV AP OIDC op de ‘pas toe of leg uit’-lijst is

geplaatst. Dit leidt tot het vraagstuk, aangezien het criterium 'Open Standaardisatieproces' vraagt om een onafhankelijk en duurzame standaardisatieorganisatie waarvan financiering voor ontwikkeling en beheer van een standaard voor in ieder geval drie jaar moet zijn geborgd, vóórdat een standaard op de lijst wordt geplaatst. Wel is er opdrachtbrief van Ministerie van Binnenlandse Zaken waarin voorgaande staat benoemd. Is deze opdrachtbrief voldoende om te voldoen aan de criteria voor het 'Open Standaardisatieproces'?

4. **Draagvlak**: de standaard NL GOV AP OpenID Connect voldoet nog onvoldoende aan dit criterium, met name omdat de standaard nog niet wordt toegepast en er geen werkende referentie-implementatie is. Vraag is wanneer de standaard voldoende is toegepast om te kunnen spreken van voldoende draagvlak om de standaard NL GOV AP OpenID Connect versie 1.0 te verplichten aan de overheid via plaatsing op de 'Pas toe of leg uit'-lijst?
   Tijdens de looptijd van het onderzoek in 2022 liep een pilot en er hebben inmiddels twee hackathons in juli en september 2022 plaatsgevonden. Hebben de pilot en de beide hackathons aangetoond dat er inmiddels wel voldoende draagvlak is of is er meer nodig?
5. **Geclusterde beschrijving federatieve authenticatie-standaarden**: de complexiteit van het opnemen van de standaard NL GOV AP OpenID Connect versie 1.0 op de lijst van open standaarden ontstaat ook doordat er twee overlappende standaarden zijn op het vlak van federatieve authenticatie: SAML en OpenID Connect. Een eventueel nieuwe geclusterde registratie van open authenticatiestandaarden kan een overkoepelende beschrijving voor SAML en OpenID Connect bevatten en vervangt dan de huidige, afzonderlijke beschrijvingen van SAML en OpenID Connect. Deze clustering biedt ook ruimte om een differentiatie aan te brengen in het functioneel toepassingsgebied. Deze geclusterde registratie biedt ruimte om NL GOV AP OIDC hierin op te nemen. Er kan in deze geclusterde registratie worden beschreven dat NL GOV AP OIDC alleen verplicht is bij de toepassing van OpenID Connect. Ook kan er gedacht worden aan differentiatie in het functioneel toepassingsgebied voor verplichting van standaarden tussen serviceproviders en identityproviders
   Vraag is of een geclusterde beschrijving van federatieve authenticatiestandaarden, vergelijkbaar met de geclusterde registratie op de lijst open standaarden van geo-georiënteerde standaarden onder de noemer Geo-standaarden, kan leiden tot een heldere uiteenzetting van de verschillende standaarden en de verhouding tot elkaar duidelijk maakt?

1.3. Gevolgd proces

Besloten is een beperkte groep experts te consulteren tijdens een sessie op 6 oktober 2022 op vooraf gedefinieerde onderzoeksvragen. Met een beperkte groep kunnen in korte tijd ingewikkelde vraagtukken worden besproken. Daarbij is besloten om ook de experts die uitgebreid hebben gereageerd tijdens de openbare consultatie, uit te nodigen voor deze expertbijeenkomst.

Aangezien de beide hackathons belangrijke input leveren voor met name criterium ‘Draagvlak’, is gewacht met het consulteren van experts totdat de hackathons afgerond waren en de uitkomsten ervan verwerkt konden worden in het onderzoek. De procesbegeleiders van Lost Lemon hebben de sessie voorbereid en begeleid.

De sessie heeft plaatsgevonden op donderdag 6 oktober. De volgende experts waren daarbij aanwezig:

- Allard Keuter (Signicat)
- André Koot (Sonic Bee)
- Jeroen de Beer (Anoigo)
- Bernard Stibbe (VZVZ)
- Bart Geesink (Surf)
- Remco Schaar (Logius)
- Frank van Es (Logius)

Marcel Molenaar van het UWV was verhinderd wegens ziekte. Namens het Forum Standaardisatie waren aanwezig Hans Laagland en Bart Knubben als toehoorders.

Dit aanvullend onderzoek is vervolgens voorgelegd aan de bovengenoemde experts. De opmerkingen en aanvullingen van de experts zijn vervolgens verwerkt.

2. Over de standaarden

2.1. OpenID Connect

OpenID Connect 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 de 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.

2.2. Security Assertion Markup Language (SAML)

SAML standaardiseert het berichtenverkeer tussen een Identity Provider (IdP) en een Service Provider (SP). Een IdP is een partij die verantwoordelijk is voor authenticatie van gebruikers en die identiteits-attributen van gebruikers kan verschaffen. Een SP is een dienstverlener die

een elektronische dienst aanbiedt aan de gebruikers. Een constellatie van bij elkaar horende IdPs en SPs wordt een (SAML-) federatie genoemd.

De SAML-specificatie schrijft met name voor:

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

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

2.3. NL GOV AP OpenID Connect

Het Nederlandse profiel NL GOV Assurance profile for OpenID Connect 1.0 vult de standaard OpenID Connect aan met additionele eisen en richtlijnen, die 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, het voorkomen van dialecten en het neerzetten van een baseline voor privacy en security. NL GOV AP is 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.

NL GOV AP OpenID Connect 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.

3. Onderzoeksresultaat

Hieronder per paragraaf de uitwerking van de verschillende vraagstukken. Per vraagstuk een conclusie en eventueel aanvullend advies.

3.1. Toegevoegde waarde: samenhang met het internationale iGOV-profiel voor OIDC

In de expertsessie op 7 oktober 2021 waren de toen aanwezige experts voldoende overtuigd van het nut en noodzakelijkheid van een Nederlands profiel voor de standaard OpenID Connect. Dit is als volgt in het bijbehorende expertadvies opgenomen:

"De experts maken zich zorgen over het ontstaan van een mogelijke wildgroei van niet-compatible implementaties van de 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 openbare consultatie is echter gewezen op internationale standaarden die als alternatief zouden kunnen dienen. Aan de geconsulteerde experts zijn de volgende vragen voorgelegd:

1. is NL GOV AP OIDC noodzakelijk;
2. zijn er mogelijk alternatieven voor deze standaard denkbaar;
3. kan er bijvoorbeeld gebruik gemaakt worden van een internationaal profiel i.p.v. zelf een Nederlands profiel te ontwikkelen en te gebruiken?

In het verleden hebben de toepassingen eHerkenning en DigiD bij de toepassing van SAML verschillende profielen gekozen. Daarna zijn er nog meer profielen in omloop gekomen, waardoor identityproviders in sommige gevallen wel vijf verschillende varianten moesten gaan ondersteunen. Om dezelfde wildgroei bij de implementatie van OpenID Connect te voorkomen is in 2019 geadviseerd om een Nederlands profiel te ontwikkelen voor de toepassing van OpenID Connect in Nederland.

Het Nederlands profiel is gebaseerd op het Amerikaanse I-Gov profiel. Bij het toetsen van het I-Gov profiel op de Nederlandse situatie zijn bij verschillende onderdelen van de standaard andere keuzes gemaakt of nadere invullingen gegeven. Denk hierbij aan de specifieke toepassing van eIDAS en de Nederlandse privacybescherming.

Ondanks de voordelen van een Nederlands profiel wordt door sommige aanwezige experts aangegeven dat het ook mogelijk moet zijn om een al bestaand internationaal profiel te gebruiken, waarbij het uitgangspunt moet zijn dat zo'n internationaal profiel heel erg lijkt op het huidige Nederlandse profiel. Het gebruik van een toenemend aantal nationale profielen kan leiden tot complexiteit in de interoperabiliteit op Europees niveau. FAPI is een goed voorbeeld van zo'n profiel, maar dan voor de financiële sector. Bij gebruik van FAPI moeten toch een aanvullend aantal afspraken gemaakt worden die niet in de FAPI-standaard opgenomen zijn en wel in het Nederlands profiel, zoals bijvoorbeeld vertegenwoordiging.

Dus ook bij de toepassing van een buitenlands profiel is het toch nodig om nationale afspraken te maken over bepaalde onderdelen van de standaard. Deze onderdelen van de standaard zijn ingevuld in het Nederlands profiel. Aangezien het Nederlands profiel inmiddels is gerealiseerd hebben de eerdergenoemde experts geen moeite met de verplichtstelling van een Nederlands profiel op OIDC. Dit voorkomt met name een nieuw traject waarin gezocht moet worden naar een buitenlandse standaard die voor een groot deel lijkt op de Nederlandse standaard en dan moeten alsnog aanvullende afspraken worden gemaakt voor Nederlandse toepassing.

Twee experts blijven moeite houden met de toepassing van een Nederlands profiel en hebben liever dat wordt gezocht naar een buitenlands profiel met aanvullende afspraken op nationaal niveau.

3.1.1. Conclusie

De experts staan niet afwijzend tegenover de standaard NL GOV AP OIDC. De consensus is de standaard voldoet en het tijd wordt om deze toe te passen. De experts roepen wel op om zo dicht mogelijk bij andere internationale Europese profielen te blijven en alleen af te wijken als het niet anders kan.

3.2. Toegevoegde waarde i.c.m. relatie SAML en OpenID Connect

SAML en OIDC hebben een vergelijkbaar functioneel toepassingsprofiel. Dit betekent dat beide standaarden niet tegelijkertijd op de 'pas toe of leg uit'-lijst kunnen worden geplaatst. Dit zou immers tot grote verwarring leiden bij inkopers van overheidsorganisaties die bij inkooptraject moeten vermelden aan welke standaarden het in te kopen pakket/toepassing moet voldoen.

SAML heeft het volgende functioneel toepassingsgebied:

'SAML moet worden toegepast op de uitwisseling van authenticatie- en autorisatiegegevens om gebruikers na eenmalig inloggen toegang te geven tot meerdere diensten.'

OpenID Connect heeft het volgende functioneel toepassingsgebied:

'OpenID Connect kan toegepast worden bij het beschikbaar stellen van federatieve authenticatiediensten'.

Deze functioneel toepassingsgebieden hebben de nodige overlap.

Hierom is in het expertadvies OpenID Connect aanbevolen SAML op de 'pas toe of leg uit'-lijst te houden en OpenID Connect op de lijst aanbevolen standaarden. Inmiddels is wel voldoende duidelijk dat de standaard OpenID Connect de toekomst heeft vanwege comptabiliteit met mobiele devices. De vraag is wel hoe de transitie moet plaatsvinden van SAML naar OIDC. Het opstellen van een transitie-strategie van SAML naar OIDC en het bijbehorende Nederlandse profiel bevordert de transitie. De vraag is hoe transitie-strategie er dan uit komt te zien. Zijn er andere standaarden (zoals Oauth2) om in deze transitie te betrekken? De plaatsing van NL GOV AP OIDC op de 'pas toe of leg uit'-lijst wekt wellicht de indruk dat het gebruik van de generieke standaard OpenID Connect (nu lijst aanbevolen standaarden) verplicht is en dat de aansluitende partij zodoende een keuze dient te maken tussen SAML en OpenID Connect.

Door vertegenwoordigers van Bureau Forum Standaardisatie en de procesbegeleiders is een voorstel gemaakt voor een mogelijke transitie-strategie van SAML naar OIDC. Dit voorstel ziet er als volgt uit:

Invoering van een differentiatie in het functioneel toepassingsgebied voor verplichting van standaarden tussen serviceproviders en identityproviders:

- verplichting aan identityproviders voor het bieden van ondersteuning voor èn SAML èn OpenID Connect
- verplichting aan serviceproviders (dienstaanbieders/ dienstverleners) voor het gebruiken van òf SAML òf OpenID Connect

Gezien de ervaring tot nu toe is het voor de dienstverleners ondoenlijk om één van de twee standaarden nu uit te sluiten. Op dit moment zijn er dienstverleners die de voorloper van SAML (A-select) toepassen. Het is nog niet gelukt deze te migreren naar SAML. Zowel SAML als OIDC ondersteunen door de identityproviders is vanuit technisch beheer gezien een extra belasting te prefereren boven een big bang transitie waarbij alle dienstaanbieders/dienstverleners in korte tijd overgezet moeten worden naar OIDC. Een *big bang* transitie is niet realistisch. Het voorstel is om het functioneel toepassingsgebied alleen te richten op de identityproviders met de verplichting aan identityproviders voor het bieden van ondersteuning voor èn SAML èn OpenID Connect OIDC en het bijbehorende Nederlandse profiel. De experts geven aan dat het niet nodig is aparte verplichtingen te stellen aan de serviceproviders omdat de serviceproviders de identityproviders volgen. Een verplichting alleen aan IdP's sorteert voor op het in beweging brengen van SP's.

Vraag is wanneer deze verplichting moet worden opgelegd aan de identityproviders? De inschatting van de experts is dat eHerkenning en DigiD als grote identityproviders tijd nodig hebben om zowel SAML als OIDC te kunnen ondersteunen. De suggestie wordt gedaan om in eerste instantie SAML als *technical debt* te verklaren, hiermee wordt duidelijk gemaakt dat de toepassing van SAML als standaard eindig is. Daarnaast moet door de beheerders van eHerkenning en DigiD een realistische tijdsperiode worden gedefinieerd waarbinnen zij OIDC

implementeren en beschikbaar stellen, naast SAML. De experts tijdens de sessie van 6 oktober 2022 schatten in dat identityproviders (waaronder DigiD en eHerkenning) een transitieperiode van twee jaar nodig hebben om in staat te zijn om zowel SAML als OIDC te kunnen ondersteunen.

Experts benadrukken dat de communicatie rondom deze transitie-strategie heel belangrijk is. De communicatie moet onder andere vormgegeven worden door DigiD en eHerkenning middels een duidelijk eenduidige roadmap. Ook andere betrokken organisaties, zoals het Ministerie van Binnenlandse Zaken en (Bureau) Forum Standaardisatie hebben hier een belangrijke rol in.

De experts geven aan dat in principe Oauth geen onderdeel is bij deze transitie. Experts beschouwen Oauth als een afzonderlijke standaard zonder direct overlap in functioneel toepassingsgebied. Overheidsorganisaties kunnen zelf bepalen of en wanneer ze Oauth gaan inzetten. Experts zien toegevoegde waarde in NL GOV AP OIDC in relatie tot OIDC.

In een aantal gevallen koppelen serviceproviders via een gateway met identityproviders. De experts spreken de voorkeur uit de verplichting als eerste wel voor DigiD en eHerkenning te laten gelden maar niet direct voor alle identityproviders.

3.2.1. Conclusie

De transitie van SAML naar OIDC wordt geregeld door in eerste instantie zowel de ondersteuning van SAML als van OIDC verplicht te maken voor de identityproviders. De positie van het Nederlandse profiel hierbij wordt nog nader beschouwd. Het moment van verplichting van alleen OIDC is afhankelijk van de tijd die de grote identityproviders (zoals DigiD en eHerkenning) nodig hebben om ook daadwerkelijk OIDC te kunnen ondersteunen. OIDC zal op dat moment als enige verplicht worden aangemerkt en de verplichting van SAML vervalt dan. Identityproviders zullen dan gedurende een ‘Grace-periode’ voor bestaande aansluitingen ook nog SAML moeten ondersteunen. Hiermee wordt een *big bang* vermeden en kunnen dienstverleners gecontroleerd overstappen van SAML naar OIDC. Gateways dienen hierbij als eerste DigiD en eHerkenning te verplichten.

3.3. Open Standaardisatieproces

Het beheer van NL GOV AP OIDC wordt belegd bij de Afdeling Standaarden van Logius. De Afdeling Standaarden van Logius werkt conform BOMOS en heeft verschillende andere standaarden in beheer. De financiering voor het beheer en doorontwikkeling van deze standaard is samen met twee andere API-standaarden (ADR en Oauth-profiel) geborgd door ministerie van Binnenlandse Zaken.

Vertegenwoordiging van het Forum Standaardisatie heeft de opdrachtbrief van Ministerie van Binnenlandse Zaken ingezien, waarin de benodigde garanties zijn vastgelegd.

3.3.1. Conclusie

De opdrachtbrief en de ervaring van de Afdeling Standaarden van Logius geven voldoende garantie dat het beheer en doorontwikkeling van het NL GOV AP OIDC en de financiering ervan voor langere termijn geborgd is.

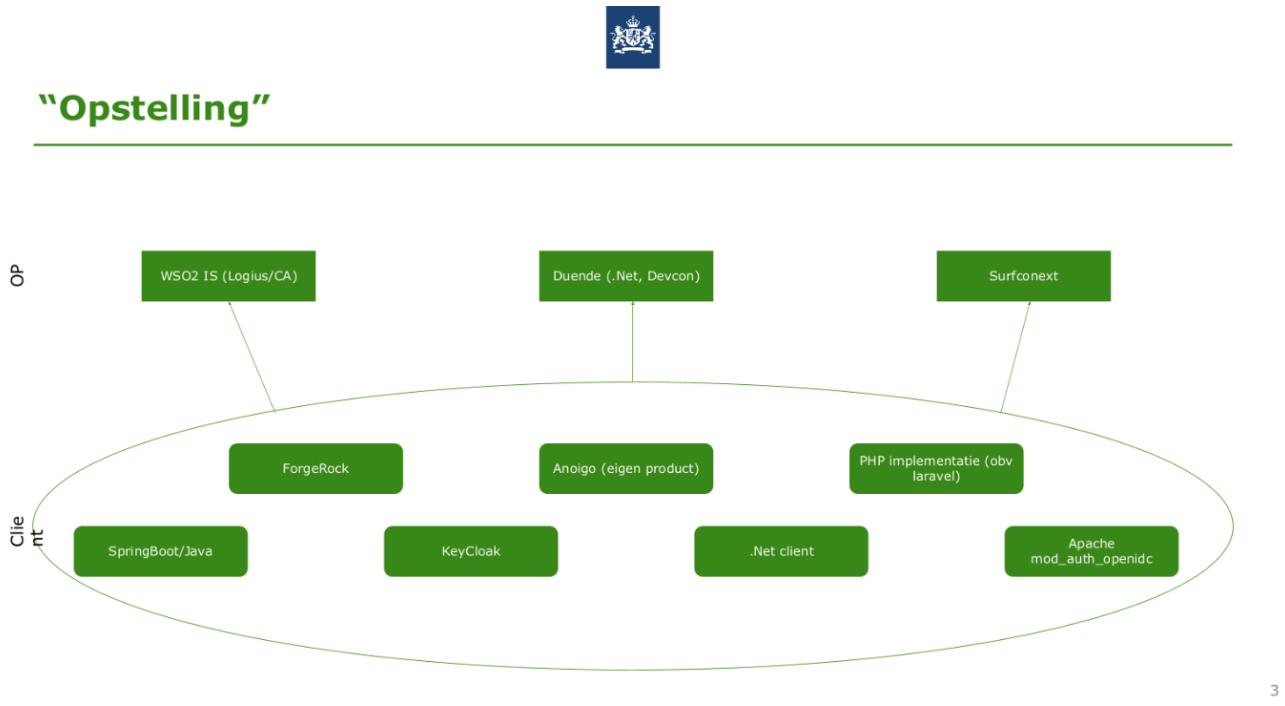
3.4. Draagvlak

Tijdens de expertconsultatie van de standaard op 7 oktober 2021 bleek dat NL GOV AP OpenID Connect nog niet voldoet aan het criterium 'Draagvlak'. De standaard wordt nog niet toegepast en daarmee is er nog geen werkende referentie-implementatie. De vraag is wanneer de standaard voldoende is toegepast om te kunnen spreken van voldoende draagvlak om de standaard NL GOV AP OpenID Connect versie 1.0 op de 'pas toe of leg uit'-lijst te plaatsen?

Om antwoord te kunnen geven op de vraag of er voldoende representatieve producten zijn waarmee de standaard geïmplementeerd kan worden, en eventuele tekortkomingen te constateren, zijn twee hackathons georganiseerd door de opstellers van de standaard, de eerste in juli 2022 en de tweede op 14 en 15 september 2022. Tijdens deze hackathons is de implementeerbaarheid van NL GOV AP OIDC getoetst en is de standaard toegepast op diverse producten en bibliotheken.

3.4.1. Hackathons

Remco Schaar (Logius) heeft tijdens de sessie van 6 oktober 2022 de aanwezige experts een presentatie gegeven over de aanpak, uitvoering en resultaten van de hackhatons.



Figuur 1 geeft de getoetste producten en bibliotheken weer

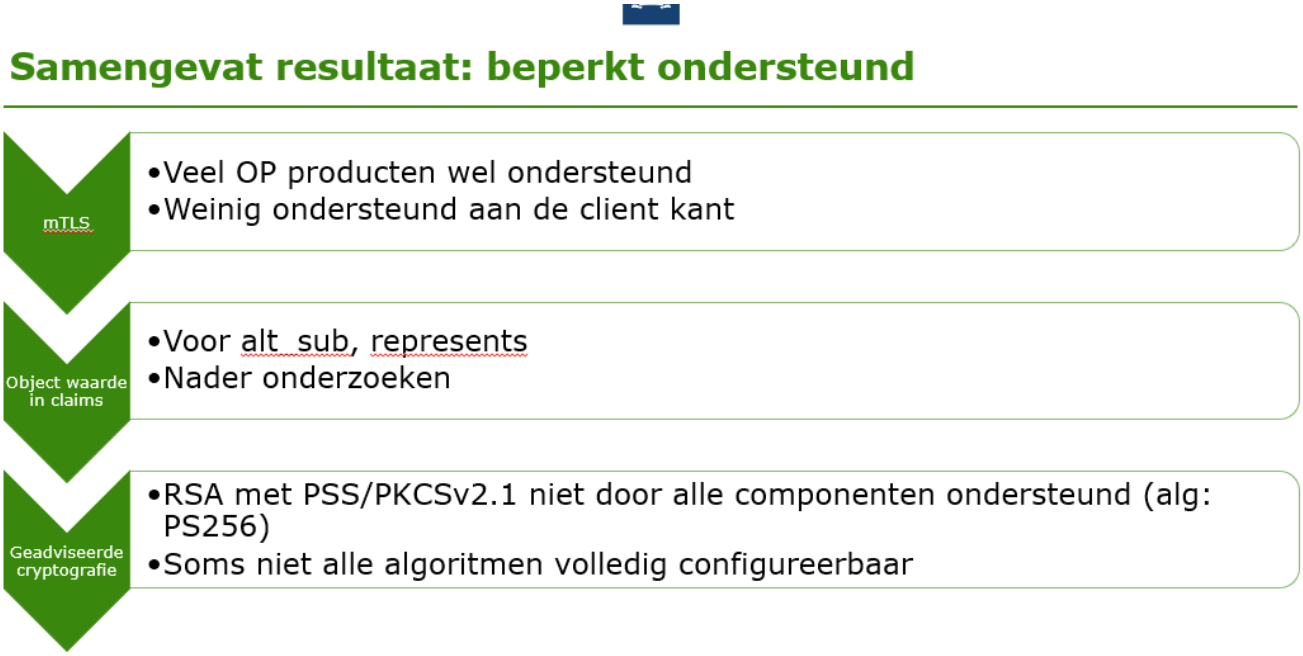
De volgende features van de standaard worden door alle in de hackaton getoetste producten en bibliotheken ondersteund: Authorization Code Flow, PKCE, Strict redirect_uri registratie, Signed & encrypted request objects, Private_key_jwt client authenticatie. Algemeen: claim als key-value pair, OP server metadata, jwks_uri, Security & entropie (128-bit+), jti uniqueness, Access token JWT, UserInfo, AuthnReqeust parameters, Token Request parameters en ID token parameters.

De sheet in figuur twee geeft de features weer die gedeeltelijk ondersteund worden.

Figuur 2 Samengevat resultaat: gedeeltelijk ondersteunde features

In Figuur 2 is te zien dat de volgende features slechts gedeeltelijk ondersteund blijken: claims parameter (diverse componenten en met name voor OP complexe configuratie), encrypted AT/IDT (niet in alle componenten), signed metadata (niet in alle producten opgeleverd/gevalideerd), dynamic client registration (meestal anoniem en/of initial access token, niet vlekkeloos interoperabel), signed/encrypted userinfo (niet door alle componenten).

In Figuur 3 is te zien dat er beperkte ondersteuning is voor: mTLS (veel OP-producten wel ondersteund, weinig ondersteuning aan de client-kant), Objectwaarde in claims (voor alt sub represents, nader te onderzoeken), geadviseerde cryptografie (RSA met PSS/PKCSv2.1 niet door alle componenten ondersteund, soms niet alle algoritmen volledig configureerbaar).



Figuur 3 Samengevat Resultaat: beperkt ondersteund

Door de experts wordt tijdens de sessie van 6 oktober 2022 bevestigd dat de beperkte ondersteuning van deze onderdelen van de standaard geen belemmering is voor de toepassing van het Nederlands profiel. De toepassing van deze onderdelen zijn vaak specifieke implementatie keuzes afhankelijk van het domein waarin de standaard wordt toegepast. Het profiel schrijft hier beperkt of niets voor.

Voor alle producten die zijn gebruikt is de implementatie van de standaard tijdens de hackatons gelukt binnen één dag. De eHerkenningsmakelaars waren niet aanwezig, ook Signicat was voor de hackatons uitgenodigd, maar niet aanwezig. Signicat wil graag alsnog proberen het Nederlands profiel te implementeren. De vertegenwoordiger van Signicat verwacht de standaard eenvoudig te kunnen implementeren.

Aanwezige experts willen en kunnen geen algemene uitspraak doen over het draagvlak voor de standaard bij overheidspartijen. Tijdens de expertbijeenkomst van 7 oktober 2021 was er voldoende draagvlak bij de experts voor de standaard, zonder dat deze was toegepast. Ook is gebleken dat een aantal overheidspartijen de standaard al toepassen, waaronder het Ministerie van VWS en een aantal lagere overheden. Signicat ondersteunt veel overheidsorganisaties en geeft aan dat de verwachting is dat zij de standaard snel kunnen implementeren als overheidspartijen Signicat benaderen de standaard te implementeren namens hen.

3.4.2. Conclusie NL GOV AP OIDC

De experts concluderen unaniem dat de uitgevoerde hackathons aantonen dat de technische implementeerbaarheid van de standaard NL GOV AP OIDC voldoende is, en dat zij ook voor nog niet getoetste producten het vertrouwen hebben in de implementeerbaarheid van de standaard. Bovendien hebben de experts vertrouwen dat er voldoende technische ondersteuning in de markt beschikbaar is om de standaard bij overheden te implementeren.

Hiermee is aangetoond dat de standaard voldoende toepasbaar is en daarmee is er voldoende draagvlak voor de standaard.

3.5. Geclusterde beschrijving federatieve authenticatie-standaarden

Het verplichten van zowel SAML als OpenID Connect via plaatsing op de 'pas toe of leg uit'-lijst kan gaan leiden tot verwarring bij overheidsorganisaties.

De experts begrijpen dit en geven aan dat ze achter het voornemen staan om te komen tot een geclusterde registratie (beschrijving) van de standaarden SAML en OIDC op de lijst open standaarden. De positie van het Nederlandse profiel hierbij wordt nog nader beschouwd. Een geclusterde registratie draagt eraan bij dat overheidsorganisaties, met name inkopers, duidelijkheid hebben over de te gebruiken teksten bij inkoop of verwerving van nieuwe applicaties of toepassingen.

In de naamgeving van de geclusterde registratie moet duidelijk zijn dat het hier om SAML en OpenID Connect gaat, bijvoorbeeld; Geclusterde registratie SAML en OIDC.

De volgende formulering is afgestemd met de experts met betrekking tot het functioneel toepassingsgebied voor een dergelijke geclusterde registratie:

'Voor federatieve toegang en voor de uitwisseling van attributen, waaronder identiteitsgegevens, moet SAML en OIDC worden toegepast door identityproviders, inclusief gateways via welke deze te benaderen zijn.'

De positie van het Nederlandse profiel in de geclusterde registratie wordt nog nader beschouwd. In de geclusterde registratie moet voldoende aandacht zijn voor het verschil tussen SAML en OIDC en de transitie van SAML naar OIDC. Daarnaast moet ook duidelijk worden gemaakt dat NL GOV AP OIDC leidend is bij de implementatie van OIDC. Ook moet een duidelijke toelichting worden gegeven op identityproviders en waarom deze verplichting voorlopig alleen voor hen geldt. Dit inclusief de verplichting voor gateways via welke deze identityproviders te benaderen zijn.

De experts stellen voor de procedure voor opname van de geclusterde registratie (beschrijving) op de 'pas toe of leg uit'-lijst zo snel mogelijk te starten, zodat overheidsorganisaties rekening kunnen houden met de transitie bij inkoop en implementatie. De ingangsdatum van de verplichting hangt af van de opleverdata van ondersteuning van OIDC door DigiD en eHerkenning. Hiervoor dienen de betreffende beheerders z.s.m. een roadmap uit te werken van de transitie van SAML naar OIDC. De verplichting om OIDC te gebruiken dient te gelden voor de identityproviders, en de koppelvlakken die deze partijen aanbieden. SAML dient tenminste gedurende een nader te bepalen transitieperiode na de genoemde ingangsdatum ondersteund te blijven.

Experts adviseren om Oauth geen deel te laten maken van de geclusterde registratie Authenticatiestandaarden. De experts beschouwen Oauth als een afzonderlijke standaard zonder direct overlap in functioneel toepassingsgebied tussen Oauth en de geclusterde Authenticatiestandaarden.

3.5.1. Conclusie

De experts adviseren om voor de standaarden OIDC en SAML tot een geclusterde registratie te komen en deze ook de procedure van het Forum te laten doorlopen van een standaard voor plaatsing op de 'pas toe of leg uit'-lijst. De positie van het Nederlandse profiel in de geclusterde registratie wordt nog nader beschouwd.

4. Additionele adviezen

Tijdens de expertbijeenkomst zijn diverse additionele adviezen benoemd:

1. aan het Forum Standaardisatie: opvolging van de adviezen (uit pa 3.1 tot en met 3.5) betekent dat het Forum Standaardisatie extra aandacht gaat besteden aan de communicatie van de te ondernemen stappen met betrekking tot plaatsing van (geclusterde) standaarden op de lijst en wat dit betekent voor overheidspartijen.
2. aan de twee belangrijkste identityproviders (DigiD en eHerkenning): per direct een roadmap definiëren voor de implementatie van OIDC, naast SAML. Deze roadmap is voorwaardelijk voor de plaatsing van de geclusterde beschrijving van OIDC en SAML op de 'pas toe of leg uit'-lijst. Vanuit de geclusterde registratie moet verwezen worden naar deze roadmap.