notitie

FORUM STANDAARDISATIE 9 DECEMBER 2020

Agendapunt 3B - Intakeadvies NL GOV Assurance Profile for OIDC

Nummer:	FS-20201209.3B
Aan:	Forum Standaardisatie
Van:	Stuurgroep Open Standaarden
Datum:	20 november 2020
Versie:	2.0
Bijlagen:	geen

Advies

Het Forum Standaardisatie wordt geadviseerd om *NL GOV Assurance Profile for Open ID Connect 1.0* in procedure te nemen, maar het resulterende advies niet ter besluit aan het Forum Standaardisatie voor te leggen 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. In het expertonderzoek verdient de relatie met SAML speciale aandacht.

Toelichting

1. Korte beschrijving van de standaard

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.

Het *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.

Het *NL GOV Assurance profile for OIDC 1.0* 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.

Het *NL GOV Assurance profile for OIDC 1.0* maakt het mogelijk dat gebruikers zelf een keuze kunnen maken voor een (goedgekeurde) authenticatievoorziening, zoals DigiD, en niet steeds opnieuw in hoeven te loggen, bijvoorbeeld wanneer er gebruik wordt gemaakt van een routeringsvoorziening.

2. Betrokkenen en proces

Op 15 oktober 2020 heeft Frank van Es (Logius) de standaard *NL GOV Assurance profile for OIDC 1.0* aangemeld voor opname de pas-toe-of-leg-uit lijst. Op 2 november 2020 heeft een intakegesprek plaatsgevonden met de indiener en met Remco Schaar (Logius), Ruud de Jong (Visma), Han Zuidweg (Forum Standaardisatie), Robin Gelhard (Forum Standaardisatie), Jeroen de Ruig (Lost Lemon) en Arjen Brienen (Lost Lemon). In dit gesprek is onderzocht of de standaard

voldoet aan de criteria om in procedure genomen te worden. Daarnaast is vooruitgeblikt op de procedure. Dit intakeadvies is tot stand gekomen op basis van het intakeonderzoek

3. Voldoet de standaard aan de criteria om in procedure genomen te worden?

NL GOV Assurance profile for OIDC 1.0 voldoet aan de vier criteria om in behandeling genomen te worden voor opname op de pas-toe-of-leg-uit lijst. Hoe de standaard is getoetst op de vier criteria wordt hieronder toegelicht in paragrafen 3.1-3.4.

3.1. Is de standaard toepasbaar voor elektronische gegevensuitwisseling tussen (semi-)overheidsorganisaties en bedrijven, tussen (semi-)overheidsorganisaties en burgers of tussen (semi-)overheidsorganisaties onderling?

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.

3.2. Is het beoogde functioneel toepassingsgebied en het organisatorisch werkingsgebied van de standaard, voldoende breed om substantieel bij te dragen aan de interoperabiliteit van de (semi-)overheid?

Ja, het organisatorische toepassingsgebied gaat zelfs verder dan (semi)overheidspartijen. Het betreft organisaties die publieke diensten verlenen, zoals omschreven in de wet digitale overheid. Denk hierbij bijvoorbeeld ook aan pensioenfondsen.

3.3. Is het zinvol de standaard op te nemen, gezien het feit dat deze niet al wettelijk verplicht is voor het beoogde functioneel toepassingsgebied en organisatorisch werkingsgebied?

Ja. Toepassing van het *NL GOV Assurance profile for OIDC 1.0* is niet wettelijk verplicht. In de wet digitale overheid wordt wel omschreven waaraan digitale publieke diensten en authenticatie voorzieningen moeten voldoen.

Aangezien het aantal mobiele en browser-gebaseerde applicaties vanuit de overheid steeds meer toeneemt, ligt het voor de hand om het *NL GOV Assurance profile for OIDC 1.0* voor te schrijven, aangezien de standaard SAML (dat al op de 'pas toe of leg uit' lijst staat) niet geschikt is voor dergelijke toepassingen. Tevens zorgt het opnemen van het *NL GOV Assurance profile for OIDC 1.0* voor en snellere en bredere adoptie hiervan.

3.4. Draagt de standaard bij aan de oplossing van een bestaand, relevant (interoperabiliteits)probleem en het voorkomen van leveranciersafhankelijkheid?

Ja, de momenteel toegepaste standaard SAML biedt geen/beperkte ondersteuning voor gebruik in omgevingen met API’s, mobiele/web applicaties en steeds meer applicatie platformen ondersteunen standaard REST/JSON in plaats van XML. Hierdoor is de verwachting dat de compatibiliteit met OpenID Connect van die platformen zal groeien ten koste de ondersteuning van SAML.

De OpenID Connect-standaard biedt veel ruimte op het gebied van configuratie, waardoor bij gebruik interoperabiliteit niet is gegarandeerd. Hierom is er behoefte aan lokale Nederlandse afspraken. Deze afspraken worden door *NL GOV Assurance profile for OIDC 1.0* ingevuld.

Tevens is het *NL GOV Assurance profile for OIDC 1.0* gebaseerd op volledig open standaarden welke door elke leverancier te implementeren is, waardoor leveranciersafhankelijkheid wordt uitgesloten.

4. Is er zicht op een positief expertadvies?

Wanneer het Forum Standaardisatie de standaard in procedure neemt, zal een groep experts de standaard gaan toetsen op de vier inhoudelijke criteria[1] voor opname op de lijst. Het Forum Standaardisatie neemt geen standaarden in procedure waarvan al vaststaat dat deze in het expertonderzoek op tenminste één van de criteria zal stranden. Daarom wordt in dit intakeadvies vooruitgeblikt op de vier inhoudelijke criteria.

Ten tijde van het intake onderzoek voldeed *NL GOV Assurance profile for OIDC 1.0* niet volledig aan de vier criteria voor plaatsing op de 'pas toe of leg uit lijst'. Wel bestaat er voldoende vertrouwen dat *NL GOV Assurance profile for OIDC 1.0* volledig aan de vier inhoudelijke criteria kan voldoen voordat het uiteindelijke Forumadvies wordt opgesteld.

De indiener en andere belanghebbenden wijzen op de urgentie om het profiel op afzienbare termijn verplicht te stellen. Hiermee wordt voorkomen dat verschillende overheidsorganisaties Open ID Connect op hun eigen manier gaan inzetten waarmee de compatibiliteit van authenticatiediensten van de overheid gevaar loopt.

Bovenstaande wordt hieronder toegelicht in paragrafen 4.1-4.4.

4.1. Toegevoegde waarde

Het profiel NL GOV OIDC biedt meerwaarde als toepassingsprofiel bij de OpenID Connect standaard, welke momenteel als aanbevolen standaard is opgenomen binnen de Lijst open standaarden. Het spitst zich specifiek toe op de context van (semi-)overheidsorganisaties in Nederland en de standaard vult de OpenID Connect standaard aan met een aantal best-practices op het gebied van beveiliging bij gebruik van mobiele en browser-gebaseerde applicaties.

Het NL GOV OIDC biedt betreft 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.

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. Bovendien is OpenID Connect 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. Hierom is er ook behoefte aan een Nederlands profiel voor het gebruik van OpenID Connect. In het expertonderzoek zal bijzondere aandacht besteed moeten worden aan de relatie van SAML en OpenID Connect op de 'pas toe of leg uit'-lijst. SAML is nog altijd in gebruik bij de overheid en het is niet realistisch om te veronderstellen dat de gehele overheid op korte termijn kan migreren naar Open ID Connect.

Er zijn geen onoverkomelijke beveiligings- en privacyrisico's gevonden. De standaard OpenID Connect biedt op dit vlak juist een meerwaarde: aanbieders van onlinediensten hoeven geen (gevoelige) inloggegevens van gebruikers te kennen om ze wel te kunnen authenticeren en profielinformatie van de gebruiker op te kunnen vragen. Daarmee nemen privacy risico's en risico's op identiteitsdiefstal en misbruik van identiteitsgegevens af.

Gegeven het belang van OpenID Connect en de verwachting van snelle groei van OpenID Connect wordt de toegevoegde waarde van *NL GOV Assurance profile for OIDC 1.0* gezien als groot, en noodzakelijk om tegen te gaan dat overheidspartijen eigen, niet met elkaar compatibel, profielen ontwikkelen.

4.2. Open standaardisatieproces

NL GOV Assurance profile for OIDC 1.0 is ontwikkeld door een werkgroep onder leiding van Logius, waar ook andere belanghebbende overheidsorganisaties in deelnamen. Er is echter geen sprake van een gedocumenteerd open specificatieproces met bijvoorbeeld goed gedocumenteerde deelnamevoorwaarden, besluitvorming, open consultatie en bezwaarprocedure. De specificatie van

[1] Meer informatie over de inhoudelijke toetsingscriteria op de website van het Forum Standaardisatie, https://www.forumstandaardisatie.nl

het profiel is niet overheidsbreed ter openbare consultatie aangeboden. Wel is de resulterende specificatie vrij beschikbaar op Gitlab (https://gitlab.com/logius/oidc).

Centrum voor Standaarden van Logius is beoogd beheerder van *NL GOV Assurance profile for OIDC 1.0*. De Programmeringsraad van Logius stelt echter als voorwaarde dat *NL GOV Assurance profile for OIDC 1.0* eerst op de 'pas toe of leg uit' lijst moet staan voordat het Centrum voor Standaarden van Logius het beheer van dit profiel mag aanvaarden. Hiermee ontstaat een 'kip-ei' probleem omdat het Forum Standaardisatie een open beheerproces als criterium vereist voor plaatsing op de 'pas toe of leg uit' lijst.

Op moment van schrijven van dit intakeadvies voldoet *NL GOV Assurance profile for OIDC 1.0* derhalve niet volledig aan het criterium 'open standaardisatieproces'

4.3. Draagvlak

De volgende organisaties zijn betrokken geweest bij de totstandkoming van de standaard en hebben deelgenomen in de werkgroepsessies: Logius, Gemeente Den Haag, Surfnet, Ministerie van VWS, RvIG, RVO, Belastingdienst, iShare, Kennisnet, Dictu, CIV, VZVZ, Justid, Kadaster en VNG. Dit omdat er behoefte is aan een standaard set afspraken bij het gebruik van OIDC.

NL GOV Assurance profile for OIDC 1.0 is recent gespecificeerd en wordt in de praktijk nog niet toegepast bij de overheid. Daardoor is er ook nog geen praktijkervaring met het gebruik van dit profiel.

De verwachting is dat het profiel binnen afzienbare tijd zal worden toegepast bij DigiD en de stelsels eID en eTD. OIDC (zonder dit profiel) wordt momenteel al toegepast binnen het iShare stelsel en bij onder andere Surfconext, deze zullen naar verwachting ook *NL GOV Assurance profile for OIDC 1.0* gaan toepassen. Verder wordt de generieke standaard OIDC 1.0 toegepast binnen het bedrijfsleven als moderne toepassing voor federatieve authenticatie.

NL GOV Assurance profile for OIDC 1.0 wordt nog niet ondersteund door leveranciers. Wel is de verwachting dat leveranciers die implementaties van Open ID Connect aanbieden, ook eenvoudig *NL GOV Assurance profile for OIDC 1.0* kunnen ondersteunen. Voor zover bekend kan PingFederate een implementatie van OpenID Connect op basis van het *NL GOV Assurance profile for OIDC 1.0* bieden.

Ondanks dat de *NL GOV Assurance profile for OIDC 1.0* tot stand is gekomen in een werkgroep met een brede vertegenwoordiging vanuit de overheid is het niet duidelijk of alle belanghebbenden, voldoende zijn gehoord. Om deze reden moet het expertonderzoek extra aandacht besteden aan het draagvlak bij andere overheidspartijen die door opname van het profiel op de lijst 'pas toe of leg uit' lijst geraakt worden.

Op basis van deze vaststellingen (nog geen toepassing in de praktijk, weinig marktaanbod, en onduidelijk beeld van draagvlak van verplichting voor de hele overheid) voldoet *NL GOV Assurance profile for OIDC 1.0* niet volledig aan het criterium 'draagvlak'.

4.4. Opname op de lijst bevordert adoptie

NL GOV Assurance profile for OIDC 1.0 is aangemeld voor de pas-toe-of-leg-uit lijst. Het betreft een profiel op OIDC 1.0 waar grote behoefte aan is binnen de Nederlandse overheid. Een verplichting is aangewezen om te voorkomen dat organisaties OIDC 1.0 elk op hun eigen manier gaan implementeren, waardoor incompatibiliteit kan ontstaan tussen verschillende authenticatiesystemen van de overheid.

5. Samenhang met andere standaarden op de lijst

NL GOV Assurance profile for OIDC 1.0 is een toepassingsprofiel bij OpenID Connect dat moet worden toegepast bij het beschikbaar stellen van federatieve authenticatiediensten, waarbij sprake is van mobiele toepassingen. OpenID Connect op haar beurt is een authenticatie-extensie op OAuth2.

Verder heeft OpenID Connect een overlappend toepassingsgebied met SAML. 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. In het vervolgtraject verdient de relatie met SAML nog wel speciale aandacht, omdat SAML nog geruime tijd in gebruik zal zijn bij de overheid.

We constateren dat OpenID Connect raakvlakken heeft met andere standaarden op de lijst, maar dat *NL GOV Assurance profile for OIDC 1.0* alleen een raakvlak heeft met OpenID Connect. *NL GOV Assurance profile for OIDC 1.0* kent geen strijdigheden met andere standaarden op een van de lijsten.

6. Welke organisaties ondersteunen deze aanmelding?

De volgende organisaties hebben meegewerkt aan de werkgroepsessies waarbij de standaard is opgesteld en ondersteunen de aanmelding: Logius, Gemeente Den Haag, Surfnet, Ministerie van VWS, RvIG, RVO, Belastingdienst, iShare, Kennisnet, Dictu, CIV, VZVZ, Justid, Kadaster en VNG.

7. Use case

De standaard OIDC wordt gebruikt als een gebruiker een (mobiele) online-dienst van een overheidsdienstverlener wil gebruiken, waarbij authenticatie is vereist. De gebruiker logt in bij de dienst, gebruikmakend van een inlogmiddel (-app) naar keuze. De gebruiker kan de dienst(en) van de overheidsdienstverlener zowel vanuit de webapplicatie als een (mobiele) app afnemen. Dit naar keus van de gebruiker en afhankelijk van het aanbod van de dienstverlener, maar onafhankelijk van het gebruikte inlogmiddel. NL GOV Assurance profile for OIDC 1.0 wordt gebruikt als standaard voor het realiseren van authenticatie op basis van OIDC.

In het expertonderzoek moet nog worden gezocht naar een concreter praktijkvoorbeeld, bijvoorbeeld authenticatie met DigiD.