notitie

FORUM STANDAARDISATIE 12 juni 2019
Agendapunt 4D Intakeadvies OpenID Connect

Nummer:	FS 190612.4D
Aan:	Forum Standaardisatie
Van:	Stuurgroep Open Standaarden
Datum:	27 mei 2019
Versie:	1
Bijlagen:	geen bijlage

Advies
Het Forum Standaardisatie wordt geadviseerd om OpenID Connect (OIDC) in procedure te nemen voor opname op de 'pas toe of leg uit'-lijst. Een volledig expertonderzoek is aangewezen om de standaard te toetsen aan de criteria voor opname op de lijst. In de toelichting hieronder wordt dit advies nader onderbouwd.

Toelichting
1. Korte beschrijving van de 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. Het is een op JSON gebaseerde standaard en bouwt voort op de open standaard OAuth 2.0 welke gebruikt wordt voor autorisatie. OIDC heeft dan ook een grote overeenkomst met OAuth 2.0, een belangrijke toevoeging is het 'ID token' waardoor identificatie van de geauthenticeerde gebruiker mogelijk wordt gemaakt. OIDC is functioneel ook vergelijkbaar met de standaard Security Assertion Markup Language (SAML), een XML gebaseerde standaard op autorisatie en authenticatie.

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

In dit gesprek is onderzocht of de standaard voldoet aan de criteria om in procedure genomen te worden. Daarnaast is vooruitgeblikt op de procedure. Dit intake advies is tot stand gekomen op basis van de inhoud van het aanmeldformulier, de aanvullende informatie die is verkregen tijdens het intakegesprek en op basis van informatie op de website van de OpenID Foundation en andere documentatie.

Voor OIDC is een Nederlands profiel ontwikkeld. Dit profiel is aanvankelijk ingediend als onderdeel van de standaard. Na consultatie van de stuurgroep Open Standaarden van het Forum standaardisatie is besloten OIDC zonder profiel in te dienen. De eerste versie van het profiel is in april 2019 beschikbaar gekomen. Het profiel is daarmee nog onvoldoende gedragen door alle overheidspartijen, bovendien moet een beheer organisatie van het profiel nog benoemd worden. Met de indieners van de standaard is afgesproken dat het profiel nu geen onderdeel is van de

aanmelding van OIDC. In de expertfase wordt wel aandacht besteed aan het profiel, zonder het profiel vooralsnog te toetsen voor plaatsing op de 'pas toe of leg uit' lijst.

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

OIDC 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[1] wordt hieronder toegelicht in paragrafen 3.1 tot en met 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. Het is een open standaard die gebruikt kan worden bij het veilig toegang verlenen met diverse authenticatiediensten tot (systemen van) meerdere dienstverleners, bij gebruik vanuit o.a. webapplicaties en mobiele applicaties. Deze toepassing is mogelijk voor burgers, 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[2]. 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. OIDC is niet wettelijk verplicht, dat wil zeggen het staat niet met naam en toenaam opgenomen in de wet digitale overheid. In de wet wordt omschreven waaraan digitale publieke diensten en authenticatie voorzieningen moeten voldoen. Aangezien het aantal mobiele applicaties vanuit de overheid steeds meer toeneemt, licht het voor de hand om OIDC voor te schrijven, aangezien de standaard SAML (die al op de 'pas toe of leg uit' lijst staat) minder geschikt is voor mobiele toepassingen.

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

Ja. Het interoperabiliteitsprobleem ligt zoals eerder beschreven bij de mobiele apps en machtigen van anderen om in te loggen op digitale publieke diensten en websites. OIDC maakt het mogelijk om andere authenticatievoorzieningen middels een routeringsvoorziening te ontsluiten. Bovendien geeft het de mogelijkheid om meerdere attributen of andere type identifiers mee te geven. Het huidige DigiD-SAML koppelvlak, biedt alleen de mogelijkheid om BSN mee te geven in het authenticatieprotocol.

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[3] 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.

Het intake onderzoek heeft vooralsnog geen inhoudelijke criteria gevonden die een positief expertadvies voor plaatsing van OIDC op de 'pas toe of leg uit'-lijst in de weg zou kunnen staan.

---

[1] Meer informatie over de criteria voor het in procedure nemen van een standaard op de website van het Forum Standaardisatie, https://www.forumstandaardisatie.nl

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

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

Wel zijn er een paar aandachtspunten die tijdens het expertonderzoek nader moeten worden onderzocht.

4.1. Toegevoegde waarde

Op dit moment staat SAML, een XML gebaseerde standaard voor authenticatie en autorisatie, al op de 'pas toe of leg uit'-lijst. SAML wordt nog door verschillende overheidsorganisaties gebruikt. De verwachting is dat SAML nog een tijd naast OIDC gebruikt zal worden. Belangrijkste redenen om op OIDC in te zetten zijn de beperkte mogelijkheden om de SAML door te ontwikkelen. Daartegenover staan de actieve ontwikkelingen binnen de OIDC standaard. Verder ondersteunt OIDC de 'mobile-first' strategie van digitale overheidsdiensten beter dan SAML. SAML voorziet hier minder in en doorontwikkelen op de standaard SAML is dan mogelijk een desinvestering.

In een notitie van het programma eID aan het Ministerie van Binnenlandse Zaken en Koninkrijkrelaties wordt aangegeven dat OIDC en SAML naast elkaar kunnen functioneren en dat bij voldoende implementaties van OIDC, SAML kan worden 'uitgezet'[4]. Uitdaging wordt wel om bij het definiëren van het (functioneel) toepassingsgebied van OIDC rekening te houden met het toepassingsgebied van SAML. Aangezien SAML en OIDC standaarden zijn met een bijna gelijk functioneel toepassingsgebied.

4.2. Open standaardisatieproces

Ontwikkeling gebeurt openlijk toegankelijk (https://bitbucket.org/openid/) en het proces is beschreven (zie https://openid.net/foundation/policies/). Het besluitvormingsproces is dus voor alle belanghebbenden toegankelijk en inzichtelijk. Nederlandse overheidspartijen kunnen deelnemen aan het standaardisatie proces voor 100,- dollar per jaar. Daarnaast wordt er ook gewerkt aan kleine updates en enkele uitbreidingen. De uitbreidingen lijken voornamelijk als losse documenten/aanvullende specificaties gepositioneerd te worden. Verder vindt doorontwikkeling ook grotendeels plaats als onderdeel van de onderliggende OAuth 2.0 standaard.

OIDC bevat veel informatie, waardoor er een aantal 'profiles' zijn gemaakt en in ontwikkeling blijven. Het iGOV / internationale profiel voor overheidstoepassingen en het publieke domein wordt door de Open ID Foundation beheerd. Het Nederlandse iGov-NL profiel voor OIDC (met review van werkgroep) bouwt voort op iGov-NL profiel van OAuth 2.0, dat door een werkgroep onder leiding van Geonovum is ontwikkeld. Vanuit het Ministerie van Binnenlandse Zaken wordt geadviseerd om beide profielen over te nemen als één stelsel van standaarden. Het voornemen is het beheer van beide iGov-NL profielen te beleggen bij Logius. Hier wordt binnenkort een besluit over genomen.

Zoals al eerder aangegeven is met de indieners afgesproken om het Nederlandse profiel iGov-NL nog geen onderdeel te maken van de aanmelding van OIDC. De eerste versie van het profiel is in april beschikbaar gekomen. Het profiel is daarmee nog onvoldoende gedragen door alle overheidspartijen, bovendien moet een beheer organisatie van het profiel nog benoemd worden. In de expertfase wordt wel aandacht besteed aan het profiel.

4.3. Draagvlak

Door de indieners wordt aangegeven dat de diverse betrokken overheidspartijen enthousiast zijn over de mogelijkheden van de standaard OIDC. Het is opgenomen in de Project Startarchitectuur (PSA) van eID en deze is goedgekeurd door de programma governance met daarin diverse dienstverleners. Of het enthousiasme ook daadwerkelijk wordt gedeeld door veel overheidspartijen zal worden getoetst bij de totstandkoming van het expertadvies.

4.4. Opname op de lijst bevordert adoptie

De opname op de lijst is een geschikt middel om de adoptie van de standaard te bevorderen. Wel moet er nagedacht worden over de co-existentie van OIDC en SAML en een duidelijke afbakening van het functionele toepassingsgebied. Het expertonderzoek zal veel aandacht moeten besteden aan het scherp stellen van het functionele toepassingsgebied van OIDC en het adviseren over de situaties waarin OIDC dan wel SAML gebruikt kunnen en mogen worden.

[4] Zie hiervoor https://www.forumstandaardisatie.nl/sites/bfs/files/proceedings/FS%20181212.4E%20Notitie%20eID%20over%20OIDC.pdf

Het plaatsen van de standaard op de ‘pas toe of leg uit’-lijst is naar verwachting de beste optie om de adoptie van de standaard te versnellen (zie ook 4.3). Het is sowieso andersom: als het geen verplichte open standaard wordt dan belemmert dat de adoptie.

5. Samenhang met andere standaarden op de lijst

OIDC bouwt voort op OAuth 2.0. Daarmee op o.a. de standaarden voor HTTP, JSON, TLS en andere gangbare internet standaarden van IETF, ISO en W3C.

6. Welke organisaties ondersteunen deze aanmelding?

De volgende overheidsorganisaties ondersteunen de aanmelding:

- De werkgroep Autorisatie / Authenticatie binnen Kennisplatform API’s.
- De governance eID, met daarin VWS, SZW, I&M, RDW, VNG, DUO, UWV/SVB, Belastingdienst, MinBZK, Logius, RVIG, V&J, Politie.
- DigiD en het Programma Machtigen hebben OIDC op hun roadmap staan.

De authenticatie en autorisatievoorziening van SURF ondersteunt reeds OIDC naast SAML richting Service Providers (nog niet richting Identity Providers). Er wordt geen gebruik gemaakt van het iGov-NL profiel.

7. Use case

De use case is federatieve authenticatie en autorisatie. Meerwaarde ten opzichte van het huidige SAML is met name het gebruik van mobiele applicaties op mobiele apparaten. Dus: de gebruiker logt in bij de overheidsdienstverlener, gebruikmakend van een inlogmiddel (bijvoorbeeld een mobiele inlog-applicatie) naar keuze. De gebruiker kan de dienst(en) van de overheidsdienstverlener zowel vanuit de webapplicatie als een (mobiele) applicatie afnemen. Dit naar keus van de gebruiker en afhankelijk van het aanbod van de dienstverlener, maar onafhankelijk van het gebruikte inlogmiddel.