Rotterdam, 22 februari 2022

# Reactie op de consultatie van NL GOV OpenID Connect profiel

## Inleiding

Het is goed te zien dat de overheid in deze consultatie ook andere belanghebbenden vraagt om een reactie op het voorgestelde profiel van OpenID Connect (ook wel OIDC). Als internationale identity broker, waarbij we ‘trust services’ leveren in veel Europese landen, waar we moeten voldoen de Europese richtlijnen ter zake, raakt dit Signicat direct.

We herkennen dat zowel van SAML and OIDC er vele smaken bestaan, die per regio, per sector, per dienstverlener en soms zelfs per toepassing kunnen verschillen. Standaardisatie daarvan heeft zeker voordelen, al moet voorkomen worden dat de introductie van een standaard er alleen maar toe leidt dat er een nieuw ‘smaakje’ bij gekomen is. Aansluiten bij internationale standaarden is dan ook altijd aan te bevelen boven het opstellen van een nieuwe. Dit is dan ook tevens onze belangrijkste aanbeveling. Verder wijzen we op enkele aandachtspunten over het profiel zelf en de relatie tot andere standaarden of profielen.

## Aanbeveling

Bij het introduceren van een Nederlands specifiek profiel is het risico dat er lokale keuzes gemaakt worden, die van invloed zijn in een internationale markt. Voor Authenticatie en identificatie is deze markt sinds de introductie van eIDAS in 2014 Europees, en niet langer nationaal. De keuzes die de Nederlandse overheid nu voorstelt kunnen beperkend werken voor toetreders uit het buitenland, ook wanneer deze voldoen aan Europese regels en standaarden en daarmee de open Europese markt benadelen.

Bij het gebruik van deze OIDC standaard is het daarom goed gebruik om de voorgestelde invulling te toetsen bij de beheer organisatie van de internationale standaard, in dit geval: https://openid.net/certification/. Daar is een certificeringsproces te vinden voor een OpenID Connect invulling. Hiermee wordt zoveel mogelijk gewaarborgd dat er geen specifieke Nederlandse keuzes gemaakt worden die internationaal beperkend kunnen zijn. Die van Signicat voldoet aan deze certificering. Wij adviseren van harte om het voorgestelde profiel op deze manier internationaal te laten certificeren.

## Aandachtspunten

1. Wat we zien is een uitgebreide lijst aan requirements waar de implementatie aan moet voldoen. Vanuit onze ervaring is het vaststellen daarvan een uitdaging. Een referentie implementatie en test-tooling zijn daarom aan te bevelen voor de acceptatie van het profiel.
2. Onder andere in sectie 6.1 van de standaard wordt bewust afgeweken van de OpenID Core standaard. Dat betekend een verlies van internationale interoperabiliteit en een Nederlandse afwijking. Aanbevolen wordt dit niet te doen en de Core standaard te volgen. We denken dat dit oplosbaar is.
3. Nu wordt gebruik gemaakt van enkele RfC's die nog niet afgerond of in de standaard zijn opgenomen. We raden aan dit pas te doen wanneer de RfC's zijn goedgekeurd en opgenomen in de standaard. Er kunnen immers nog aanpassingen op de draft RfC's volgen en voldoen aan toekomstige wijzigingen is niet iets wat thuishoort op een pas-toe-of-leg-uit lijst van (geaccepteerde) standaarden.
4. Naast SAML en OIDC zijn er ook andere technische protocollen, zoals REST, die in sommige technische omgevingen leiden tot een betere gebruikersinteractie of security. REST staat ook al op de pas-toe-of-leg-uit lijst van het forum, maar niet met hetzelfde toepassingsgebied. Het definiëren van de functionele toepassingsgebied zou daarom verduidelijkt moeten worden dat OIDC of SAML niet de enige protocollen zijn die gebruikt mogen worden binnen de context van authenticatie, maar in ieder geval ook REST.
5. Het is belangrijk om de digitale dienstverlening zo veilig mogelijk te maken. Daartoe bestaan er ook de verschillende certificeringen die binnen sectoren of landsgrenzen gehanteerd worden om vast te stellen dat de keten van partijen op een veilige manier met elkaar samenwerken. Dat onderschrijven wij volledig. Een ander OIDC profiel hoeft daarom ook niet slechter te zijn dan de nu voorliggende, en kan ook bijdragen aan dezelfde doelstellingen rondom de veiligheid van de dienstverlening. We verwijzen hierbij onder meer naar het werk van de Financial-grade API Werkgroep (FAPI: https://openid.net/wg/fapi/). We zouden graag zien dat dergelijke reeds bestaande standaarden die ook voldoen aan de bovenliggende doelstellingen van het voorliggende profiel toegestaan worden binnen de publieke sector. Denk bijvoorbeeld aan zorgverzekeraars die ook DigiD gebruiken, maar al voldoen aan het FAPI profiel.

## Tot slot

We hopen dat onze opmerkingen bijdragen aan een zorgvuldige afweging rond het voorgestelde profiel en dat we hiermee van dienst geweest zijn in dit proces.