Inleiding
Het is een prima initiatief om na te denken over ontwikkelingen met betrekking tot de inzet van federatieve toegangstechnieken. Helaas wordt voorbijgegaan aan de doel-middel discussie. OpenID Connect (OIDC) is geen doel op zich, maar een middel om het doel, communicatie, interoperabiliteit en platformonafhankelijk, te bereiken. OIDC is een middel om federatieve toegang te faciliteren.

Verschillende stellingen en uitgangspunten zijn vanuit deze blik opgesteld en daarbij wordt het doel van de toepassing dus miskend. Doel van federatie is communicatie, interoperabiliteit, gebruiksgemak, security en platformonafhankelijkheid. Federatieve protocollen moeten in staat zijn die doelstellingen te ondersteunen.

De volgende principe gelden hierbij ook:
Federatieve toegang vergt overeenstemming tussen de Identity Provider (IdP) en de Serviceprovider (SP, of relying party). Deze overeenstemming wordt bereikt in de vorm van:

- een bilaterale afspraak
- een contract of een convenant
- door gezamenlijke aansluiting (dus zowel IdP als SP) bij een trust framework, zoals eIDAS.

Een belangrijk uitgangspunt daarbij is dat het verlenen van toegang een verantwoordelijkheid is van de SP. De SP bepaalt de condities waaronder een identiteit van een IdP toegang kan krijgen.

Daar waar een bilaterale overeenstemming wordt bereikt, kan een overeenstemming worden bereikt over vorm en inhoud van het token. Daar waar een multilateraal samenwerkingsverband bestaat, in de vorm van een trust framework, worden concessies gedaan. Als meer partijen zjin betrokken, impliceert dit dat er een generiek, dus minder fijnmazig en minder specifiek toegangsprincipe met bestaan.

Omissie
Belangrijke omissie in dit document: Zero Trust Architectuur (conform NIST 800-207) als toepassingsgebied voor OIDC-communicatie wordt niet vermeld.

Reacties per pagina:
P3: NL GOV OpenID Connect profiel versie 1.0 [opnemen] op de ‘pas toe of leg uit’-lijst van het Forum Standaardisatie
Reactie: Als al een GOV-profiel nodig is: Is overwogen om aan te sluiten bij het internationale GOV-profiel? Waarom wordt hier niet aan gerefereerd?

P3: “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.”
Reactie: Hier wordt een aanname gedaan die niet onderbouwd is. Wildgroei is niet aan de orde, aangezien IdP en SP altijd samen overeenstemming bereiken. Overeenstemming bereiken over de vorm en inhoud. Is dat in beeld geweest ?

P8: “welke zorgen voor toepasbaarheid en interoperabiliteit specifiek binnen de Nederlandse (semi-)overheid.”
Reactie: Opnieuw is dit niet te danken aan een overheidsbreed profiel, als wel aan het principe van federatie, waarbij de SP bepaalt. De IdP hoeft toch alleen maar aan te sluiten?

Een tweede bezwaar tegen deze stelling is dat interoperabiliteit met name gaat over het ontsluiten van diensten over en weer, binnen en buiten de overheid. Sterker, de meeste API's worden nu toch al buiten de overheid ontwikkeld en ontsloten? Interoperabiliteit is toch niet het gevolg van een profiel, maar van een afspraak, of inkoopcontract of welk ander contract dan ook?

P8: "Het neerzetten van een fatsoenlijke baseline voor privacy en security."
Reactie: OIDC is een protocol dat door STS-componenten wordt toegepast. OIDC is niet meer en niet minder dan een protocol dat drager is van informatie. Het tot stand komen van de tokens en het transport is alleen mogelijk als er adequate privacy en security baselines worden toegepast. Deze stelling is een dooddoener.

P8: "claims"
Reactie: Claims zijn de afspraken die tussen IdP en SP worden opgesteld. De attribute-value pairs worden binnen het afsprakenstelsel gedefinieerd, maar als die te generiek zijn, zijn ze niet toepasbaar voor fijnmazige toegang, of voor toepassing binnen zero trust netwerken die via Policy Based Access Control worden ontsloten.

P9: "Het NL GOV OpenID Connect profiel moet worden toegepast bij het beschikbaar stellen en het gebruik van federatieve authenticatiediensten, inclusief vertegenwoordiging- en attribuutverstrekking."
Reactie: Let op het risico van spraakverwarring. OIDC is een authenticatieprotocol. Attributen die iets zeggen over autorisatie zijn alleen relevant voor de SP. De IdP moet met de SP afstemmen over toepassing, syntax en semantiek van attributen. Dat is niet standaard in te richten, aangezien elke SP een eigen autorisatie- en toegangsmodel kan hebben. Alleen daar waar de SP onderdeel is van een IdP-organisatie, is afstemming betrekkelijk eenvoudig.

P10: 5.1.1.1 Is het functioneel toepassingsgebied goed gedefinieerd?
Reactie: Nee: Overheid maakt naast overheidsdiensten ook gebruik van andere diensten. Dat betekent dat elke IdP hoe dan ook al met meerdere partijen te maken heeft.
Nee: Opleggen van een GOV-profiel aan partijen buiten het overheidsdomein zal niet werken. Dat is een van de redenen dat het internationale GOV-profiel nog in ontwikkeling is.

P10: 5.1.1.2 Is het organisatorisch werkingsgebied goed gedefinieerd?
Reactie: Nee: Het is een illusie te veronderstellen dat toepassing van OIDC beperkt blijft tot de partijen die GOV-profielen accepteren. IdP's zullen toch met meer partners moeten samenwerken?

P11: 5.1.1.3 Is de standaard generiek toepasbaar (en niet alleen bedoeld voor gegevensuitwisseling met één of een beperkt aantal specifieke organisaties)?
Reactie: Nee: federatieve toegang is nooit generiek, elke federatie is een één-op-één relatie tussen een IdP en een SP. Binnen een stelsel is de toepassing zo generiek dat fijnmazig gebruik niet aan de orde is.

P11: 5.1.2.2 Biedt de aangemelde standaard meerwaarde boven de reeds opgenomen standaarden met een overlappend functioneel toepassings- en organisatorisch werkingsgebied?
Reactie: Nee, althans de vraag is onjuist beantwoord. De beantwoording gaat over toepassing van OIDC t.o.v. SAML. Daarvoor heeft GOV-profiel toch geen enkele betekenis?
Nee: toepassing van het GOV-profiel beperkt toepassing van OIDC als generiek protocol.

P12: 5.1.2.3 Biedt de aangemelde standaard meerwaarde boven bestaande concurrerende standaarden die in aanmerking zouden kunnen komen voor opname?
Reactie: Nee, er zijn geen concurrerende standaarden. GOV concurreert met een al bestaande open standaard, namelijk OIDC.

P12: 5.1.2.4 Is de standaard een internationale standaard of sluit de standaard aan bij relevante internationale standaarden?
Reactie: Nee: NL-GOV profiel gaat voorbij aan het Internationale GOV-profiel. Van compatibiliteit is niets gebleken.

P13: 5.1.3.1 Zijn de kosten van implementatie acceptabel en zijn deze kosten bekend en inzichtelijk?
Reactie: Nee. Het GOV-profiel vergt aanpassingen aan de open standaardimplementaties. Het profiel zal vermoedelijk (door agile werkwijzen bij SP's en mogelijk ook IdP's) dan ook regelmatig aangepast moeten worden?

P13: 5.1.3.2 Is er een (kwalitatieve) businesscase van de standaard aanwezig?
Reactie: Nee: het GOV-profiel is beslist geen enabler voor eenvoudiger implementatie van OIDC.

P13: 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?
Reactie: Nee. Ten eerste is de vraag niet beantwoord door te wijzen op 5.1.3.2. Maar ten tweede levert de beperking van een GOV-profiel t.o.v. een niet gedefinieerd profiel nadelen op ten aanzien van inzet en schaalbaarheid van de functionaliteit van het profiel.

P13: 5.1.3.4 Zijn de beveiligingsrisico's aan overheid brede adoptie van de standaard acceptabel?
Reactie: Nee. Het OIDC-protocol voldoet toch van nature (rekening houdend met standaard gedefinieerde beveiligingsmaatregelen conform de Baseline Informatiebeveiliging Overheidsdiensten) aan alle te stellen eisen?

Paragraaf 5.2 geen opmerkingen.

P17: 5.3.1.1 Bieden meerdere leveranciers ondersteuning voor de standaard?
"Het profiel wijkt niet enorm af van de standaard."
Reactie: Elke afwijking van de (OIDC) standaard kan resulteren in maatwerk, customization. En kan dus leiden tot incompatibiliteit.
Bovendien wordt voorbijgegaan aan het uitgangspunt dat de SP vorm en inhoud van het protocol voorschrijft.

P17 5.3.1.2 Kan een gebruiker de conformiteit van de implementatie van de standaard (laten) toetsen?
Reactie: Nee. Er is nog geen implementatie Is dan toch ook niet te toetsen?

P18: 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?

Reactie: Nee. De verwachting mag uitgesproken zijn, feit is dat sprake is van een bijzonder, lokale aanpassing van de open standaard. Van interoperabiliteit in internationaal verband, of doorontwikkeling van de open standaard kan dus al helemaal geen sprake zijn.

P18 5.3.1.4 Zijn er profielen of voorbeeldimplementaties van de standaard aanwezig en zijn deze vrij te gebruiken?
Reactie: Nee. Het antwoord op deze vraag ondergraaft ook de stelling die aanleiding was voor ontwikkelen van het GOV-profiel.

P18: 5.3.2 Kan de standaard rekenen op voldoende draagvlak?
Reactie: Als externe partij dragen wij deze standaard vanuit de verwachting dat wij een grote bijdrage aan het inrichten ervan kunnen leveren.
Nee dus, geen goed plan.

P18: 5.3.2.2 Staan de overheidsorganisaties die daadwerkelijk worden geraakt door een mogelijke verplichting van de standaard achter het gebruik van de standaard?
Reactie: Onduidelijk of dat daadwerkelijk het geval is. De vraag is of de behoefte aan functionaliteit niet ook door de open standaard zelf kan worden geleverd als IdP en SP conform het federatieconcept de afstemming voor hun rekening nemen.

P19: 5.3.2.3 Wordt de aangemelde versie van de standaard binnen het organisatorische werkingsgebied door meerdere Nederlandse overheidsorganisaties gebruikt?
Reactie: Extra opmerking: Toepassen van de OIDC-standaard valt al onder proven technology. Ook buiten de overheid. En dat werkt blijkbaar ook.

P19: 5.3.2.4
Reactie: OK

P19: 5.3.2.5
Reactie: OK

5.3.2.6 Zijn er voldoende positieve signalen over toekomstige gebruik van de standaard door (semi-)overheidsorganisaties, het bedrijfsleven en burgers?
Reactie: Het antwoord gaat over OIDC en ja, die open standaard wordt toegepast, ook in de toekomst. Het antwoord zegt niets over het GOV-profiel.

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 voorbeeldimplementatie volgen.”
Reactie: m.i. dekt deze conclusie de eerdere bevindingen niet. Wellicht kan de toepassing van andere elders toegepaste profielen worden beoordeeld.

Vragen aan de commissie

- Waarom is niet verder gebouwd op het concept vanVectors of Trust, als integraal onderdeel van de OIDC specificatie?

- Als borgen van security het uitgansgspunt is, waarom wordt dan niet aangesloten bij het Financial Grade Security Profile, waarbij uitsluitend de technische randvoorwaarden, zoals toepassing van DNSSEC, worden gesteld en wordt niet ruimte geboden om de procesmatige beveiliging in de vorm van PBAC over te laten aan de SP?

Conclusie op grond van mijn analyse:
Het is mij onduidelijk waarom op grond van dit advies het NL-GOV profiel nu als standaard zou moeten worden ingesteld.
Het advies miskent de ontwikkelingen op het gebied van toepassing van federatieve toegang, waarbij ontwikkelingen als Policy Based Access Control, API-access, service meshes en Zero Trust Architectuur niet mee zijn genomen.

Het lijkt erop dat het concept van federatieve toegang uitsluitend met een protocol-technische bril op is bekeken, het protocol verwordt daarmee tot een platform, waar OIDC juist bestemd is om de transitie van platform naar protocol mogelijk te maken.

Met vriendelijke groeten,

André Koot
Adviseur IAM SonicBee BV
andre.koot@sonicbee.nl