3A Forumadvies Authenticatie-standaarden (NL GOV AP OIDC en SAML)

Forum Standaardisatie:	Forum Standaardisatie 14 juni 2023
Agendapunt:	3A
Documentnummer:	FS-20230614.3A-Forumadvies-Authenticatie-standaarden-NL-GOV-AP-OIDC-en-SAML
Aan:	Forum Standaardisatie
Van:	Stuurgroep Open Standaarden
Bijlagen:	20220125-Expertadvies-NL-GOV-AP-OpenID-Connect-profiel Reacties uit de openbare consultatie van NL GOV AP OIDC 20230323-Aanvullend-onderzoek-NL-GOV-AP-OpenID-Connect
Rechten	CC0 publieke domein verklaring

1 Advies

Het Forum Standaardisatie adviseert om de standaard NL GOV Assurance profile for OpenID Connect 1.0 (hierna: NL GOV AP OIDC) op te nemen op de 'pas toe of leg uit'-lijst van het Forum Standaardisatie. Met het verplichten van NL GOV AP OIDC (het Nederlandse profiel voor OIDC) wordt ook de achterliggende internationale standaard OIDC verplicht.

Daarnaast adviseert het Forum Standaardisatie om de opname van NL GOV AP OIDC te clusteren met de reeds opgenomen standaard SAML en zo te komen tot een geclusterde registratie (beschrijving) op de 'pas toe of leg uit'-lijst. Deze geclusterde registratie heeft de naam **Authenticatie-standaarden (NL GOV AP OIDC en SAML)**. Het gebruik van een geclusterde registratie sluit aan bij de praktijk van eerdere geclusterde registraties op de lijst voor open standaarden zoals Geo-standaarden of Digikoppeling.

Het voorgestelde functioneel toepassingsgebied voor Authenticatie-standaarden (NL GOV AP OIDC en SAML) is:

> 'Authenticatie-standaarden NL GOV AP OIDC en SAML moeten worden toegepast door aanbieders van identitydiensten, onder wie identity providers en identity brokers/gateways, op hun externe koppelvlak aan serviceproviders

(d.w.z. overheden met digitale diensten) voor federatieve toegang en voor de uitwisseling van attributen, waaronder identiteitsgegevens, zodat serviceproviders de keuze hebben tussen beide standaarden.'

Het voorgestelde organisatorische werkingsgebied voor Authenticatie-standaarden (NL GOV AP OIDC en SAML) is:

'Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector.'

1.1 Samenvatting

De intentie voor de indiener Logius voor het verplichten van NL GOV AP OIDC is mede om een transitie te bewerkstellingen van SAML naar OIDC (incl. het bijbehorende Nederlandse profiel). OpenID Connect heeft de toekomst: het is voor developers beter werkbaar om aan te sluiten op OIDC dan op SAML; OIDC kent een brede ondersteuning in moderne ontwikkelingen rond cloud en mobiele toepassingen; OIDC is toekomstvast vanwege doorontwikkeling en marktondersteuning. Deze transitie van SAML naar OIDC komt niet (of niet voldoende) van de grond, zolang alleen SAML als verplicht op de 'pas toe of leg uit'-lijst blijft staan.

Geclusterde registratie Authenticatie-standaarden met een transitiestrategie draagt bij aan het realiseren van de transitie. Centrale voorziening DigiD, afsprakenstelsel eHerkenning en Logius als beheerorganisatie van het profiel zijn hierin bepalend en zijn eigenaar van de transitiestrategie. De door het Forum Standaardisatie geadviseerde transitiestrategie met roadmap en duidelijk communicatieplan zorgt voor voorspelbaarheid voor aangesloten partijen zodat partijen een afgewogen keuze kunnen maken bij investeringen. Op basis van de roadmap informeert Logius per fase actief de (aangesloten) partijen en Forum Standaardisatie zodra er wijzigingen zijn in de mate van ondersteuning van de standaarden. Logius heeft aangegeven een transitiestrategie op te stellen en te beheren. Forum Standaardisatie stimuleert de transitie via de inzet van instrumentatrium van het Forum. Dit zijn het verplichten (via 'pas toe of leg uit'-beleid) van standaarden aan de overheid, adoptieadviezen bij plaatsing van standaarden op de lijst open standaarden, en tijdige evaluatie van standaarden.

De verplichting van de Authenticatie-standaarden bestaat eruit dat aanbieders van identitydiensten, onder wie identityproviders en identity brokers/gateways, op hun externe koppelvlak aan serviceproviders zowel NL GOV AP OIDC als SAML dienen te ondersteunen. Het voorgestelde functioneel toepassingsgebied zorgt ervoor dat serviceproviders (aanbieders van digitale overheidsdiensten aan burgers, bedrijven en overheden onderling) voor hun aansluiting kunnen kiezen tussen NL GOV AP OIDC of SAML. Dit zorgt ervoor dat de voordelen van OIDC kunnen worden benut, zonder dat gedane investeringen in SAML aan de zijde van serviceproviders in een keer niet meer van waarde zijn.

Breder kader voor verplichten van Authenticatie-standaarden is de aankomende Wet digitale overheid die regelt dat Nederlandse burgers en bedrijven veilig en betrouwbaar kunnen inloggen bij de (semi-)overheid.

1.2 Betekenis voor lijst open standaarden

De nieuwe geclusterde registratie bevat een overkoepelende beschrijving voor SAML en NL GOV AP OIDC. De verplichting van NL GOV AP OIDC (het Nederlandse profiel) betekent dat de internationale standaard OIDC-standaard verplicht is volgens een aantal aanscherpende (of: inperkende) eisen van het Nederlandse profiel. In de registratie wordt expliciet de onderliggende standaard OIDC vermeld. De registratie vervangt de al bestaande registratie van SAML (en van NL GOV AP OIDC – in behandeling) op de 'pas toe of leg uit'-lijst en maakt de plaatsing van OIDC op de lijst aanbevolen standaarden overbodig. Deze clustering biedt ruimte om een actueel functioneel toepassingsgebied op te stellen.

Geclusterde registratie Authenticatie-standaarden (NL GOV AP OIDC en SAML) betekent het volgende voor de Lijst Open Standaarden.

Huidige situatie	**Voorgestelde situatie**
Aanmelding van NL GOV AP OIDC voor 'pas toe of leg uit'-lijst	Geclusterde registratie van Authenticatie-standaarden op 'pas toe of leg uit'-lijst (SAML en NL GOV AP OIDC) met één functioneel toepassingsgebied
SAML op 'pas toe of leg uit'-lijst	Geclusterde registratie van Authenticatie-standaarden op 'pas toe of leg uit'-lijst (SAML en NL GOV AP OIDC) met één functioneel toepassingsgebied
OIDC op lijst aanbevolen standaarden	OIDC verwijderen van lijst aanbevolen standaarden

Uit de tabel komt naar voren dat dit advies een grotere impact heeft dan het toevoegen van alleen NL GOV AP OIDC aan de 'pas toe of leg uit'-lijst.

Het niet meer separaat aanbevelen van OIDC (via een verwijdering van de lijst aanbevolen standaarden) is in lijn met de aanbeveling uit het onderzoek Doorontwikkeling Lijsten over de verhouding tussen profiel en generieke standaard op lijst open standaarden: "verplichting van een profiel (OIDC profiel) impliceert het verplichte gebruik van de achterliggende generieke standaard (OIDC) en maakt daarmee een aparte plaatsing van de generieke standaard (OIDC) op de lijst aanbevolen standaarden overbodig".

In de rest van dit document wordt dit advies nader toegelicht en onderbouwd. Hoofdstuk 2 geeft een korte uitleg van het belang van de standaarden. Hoofdstuk 3 beschrijft het proces waarmee dit advies tot stand kwam en de experts die daarbij betrokken waren. Hoofdstuk 4 beschrijft de resultaten van de toetsing van NL GOV AP OIDC tegen de criteria voor opname op de lijst en geeft antwoord op aanvullende vraagstukken. Tenslotte geeft hoofdstuk 5

aanvullende adviezen om de adoptie van de standaarden te stimuleren en de te nemen vervolgstappen.

2 Korte beschrijving van de standaard

2.1 Over de standaard

De geclusterde registratie Authenticatie-standaarden op de lijst open standaarden omvat NL GOV AP OIDC en SAML. In de registratie wordt expliciet de onderliggende (en daarmee ook verplichte) standaard OIDC vermeld. Voor de volledigheid is hieronder een korte beschrijving van OpenID Connect en SAML toegevoegd.

2.1.1 NL GOV Assurance profile for OpenID Connect

NL GOV AP OIDC versie 1.0 vult de internationale standaard OpenID Connect aan met richtlijnen zodat de standaard binnen de Nederlandse context eenduidig kan worden toegepast. Deze invulling zorgt 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) OpenID Connect (profiel) 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.

2.1.2 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.

OIDC is een generieke standaard die meestal nog profielen (aanvullende afspraken) vereist voor toepassing in specifieke domeinen.

2.1.3 Security Assertion Markup Language

Security Assertion Markup Language (SAML) Security Assertion Markup Language (SAML) is een standaard voor het veilig uitwisselen van authenticatie- en autorisatiegegevens van gebruikers tussen verschillende organisaties. SAML maakt het mogelijk om op een veilige

manier via het internet toegang te krijgen tot diensten van verschillende organisaties, zonder dat je per dienst eigen inloggegevens nodig hebt, of bij elke dienst apart moet inloggen.

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.

2.2 Waarom zijn deze standaarden belangrijk?

Authenticatie-standaarden dragen bij aan veiliger internet doordat authenticatieservices (zoals DigiD) de identiteit van een eindgebruiker controleren op een gestandaardiseerde wijze. Authenticatie zorgt ervoor om met een bepaalde zekerheid te weten dat de eindgebruiker ook echt degene is die de eindgebruiker op het internet zegt te zijn.

Inzet van authenticatiestandaarden geeft de mogelijkheid om eenvoudig en veilig toegang te verkrijgen tot digitale (semi-)overheidsdienstverlening zonder steeds opnieuw te moeten inloggen. Dit bespoedigt het gemak van digitale dienstverlening voor burgers en bedrijven. Het verminderen van het aantal afzonderlijke plekken van inloggen met ieder eigen gebruikersnaam en wachtwoord zorgt ervoor dat de kans kleiner wordt dat gebruikers via frauduleuze websites hun inloggegevens worden buitgemaakt.

NL GOV AP OIDC voorkomt het ontstaan van een mogelijke wildgroei van niet-compatible implementaties van OpenID Connect. Er is belang bij gebruik van NL GOV AP OIDC vanwege ondersteuning op een toenemend aantal mobiele toepassingen via apps. Ook vanuit oogpunt van security en privacy is dit een belangrijke standaard.

2.3 Standaarden in relatie tot de Wdo

Het verplichten van Authenticatie-standaarden kent een doorwerking in de Wet digitale overheid (Wdo) (per 1 juli 2023 in werking). Het verplichten van NL GOV AP OIDC en SAML aan de overheid (via opname op de 'pas toe of leg uit'-lijst van Forum Standaardisatie) en de aanpalende transitiestrategie hebben een richtinggevende werking op een beoogde, wettelijke verplichting via ministeriële regeling (Wdo) van de routeringsvoorzieningen.

De Wdo treedt gefaseerd in werking en gaat pas gelden als een instantie technisch en organisatorisch klaar is om aan te sluiten. Er wordt een plan van aanpak opgesteld wanneer en in welke volgorde specifieke onderdelen van de wet voor welke instantie van kracht worden.

Een van deze onderdelen zijn de routeringsvoorzieningen. De Wdo vereist het gebruik van een specifiek koppelvlak. De invulling van dat koppelvlak is op basis van SAML en OIDC. Via een ministeriële regeling kan een verplichting doorwerken naar aangewezen standaarden

(beoogd: OIDC en SAML) doordat beide standaarden deel gaan uitmaken van de uitwerking van specifiek koppelvlak dat Wdo gaat voorschrijven. Ook voor de uitwerking van dit koppelvlak bestaat de wens voor de transitie van SAML naar OIDC. De beoogde toepassing van beide standaarden in het koppelvalk is op moment van opstellen van dit Forumadvies overeenkomstig aan de 'pas toe of leg uit'-verplichting (incl. het functioneel toepassingsgebied) van de Authenticatie-standaarden op de lijst open standaarden van het Forum Standaardisatie.

3 Betrokkenen en proces

3.1 Gevolgde procedure en aanvullende vraagstukken

Op 15 oktober 2020 heeft Logius 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).

De procesbegeleider heeft op 2 november 2020 een intakegesprek gevoerd met de indiener. De procesbegeleider heeft een intakeadvies opgesteld dat de resultaten van het intakeonderzoek documenteert.

Op basis van het intakeadvies heeft het Forum Standaardisatie op 9 december 2020 besloten de aanmelding in procedure te nemen. Voorwaarde was de procedure pas te starten wanneer er minimaal voldaan is aan de criteria voor open beheer en draagvlak.

Na een gesprek tussen het Bureau en de indieners is gezamenlijk afgesproken dat de expertbijeenkomst kan worden ingepland. Vervolgens heeft de procedurebegeleider in overleg met de indiener en Bureau Forum Standaardisatie een expertgroep samengesteld en een voorzitter aangesteld. Paragraaf 3.2 geeft de samenstelling van de expertgroep.

De expertgroep is op 7 oktober 2021 bijeengekomen om de standaard te toetsen tegen de criteria en om geïdentificeerde aandachtspunten te bespreken. Tijdens deze bijeenkomst zijn ook het functioneel toepassingsgebied en organisatorisch werkingsgebied voorgesteld. De uitkomst van het expertonderzoek is vastgelegd in een expertadvies.

Het Bureau Forum Standaardisatie publiceerde het expertadvies ter openbare consultatie op internetconsultatie.nl van 28 januari 2022 tot 26 februari 2022. Uit expertadvies en uit de zes reacties uit de openbare consultatie kwamen aandachtspunten naar voren, waaronder 'toegevoegde waarde (overlap met SAML) (samenhang met het internationale iGOV-profiel voor OIDC)' en 'draagvlak (marktondersteuning) (voorbeeldimplementatie)'.

Na vervolggesprekken met de indiener Logius en met inhoudsdeskundigen (SURF) heeft op 29 maart 2022 een Extra Stuurgroep Open Standaarden plaatsgevonden. Op basis van de uitkomsten van de Extra Stuurgroep Open Standaarden is in overleg met de indiener Logius (7 april 2022) besloten om een aanvullend onderzoek uit te voeren. 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). Paragraaf 3.5 geeft de samenstelling van de experts.

Het Bureau heeft de uitkomsten van het aanvullend onderzoek vertaald naar de toetsingsprocedure. Dit betreft de plaatsing van NL GOV AP OIDC op de 'pas toe of leg uit'-lijst via de geclusterde registratie Authenticatie-standaarden. Deze vertaling is besproken op Stuurgroep Open Standaarden van 23 maart en een daarna met de indiener Logius op 9 mei 2023.

Dit Forumadvies is opgesteld op basis van het expertadvies, reacties uit de openbare consultatie, het aanvullend onderzoek en inzichten van de leden van het Forum Standaardisatie zelf. Indien het Forum Standaardisatie instemt met dit advies, wordt het aan het OBDO ter besluitvorming voorgelegd.

3.2 Samenstelling van de expertgroep

Forum Standaardisatie streeft naar een representatieve expertgroep met een evenwichtige publiek-private vertegenwoordiging van (toekomstige) gebruikers, leveranciers, wetenschappers en andere belanghebbenden. De expertgroep heeft een onafhankelijk voorzitter die de expertbijeenkomst leidt. De expertbijeenkomst heeft plaatsgevonden op donderdag 7 oktober 2021.

Aan de expertbijeenkomst hebben deelgenomen:

- Remco Schaar (Logius EID) **(indiener)**
- Frank van Es (Logius) **(indiener)**
- Anouschka Biekman (Logius EID)
- Martin Borgman (Kadaster)
- Gemma Gahan (KPN)
- Bart Geesink (SURF)
- Peter Haasnoot (Logius Afdeling Standaarden)
- Edward Hardam (CHvV)
- Frans de Kok (Logius eHerkenning)
- Jan Geert Koops (DICTU)
- Arjan van Krimpen (VZVZ)
- Paul Lemmers (DevCon)
- Marcel Molenaar (UWV)
- Martin van der Plas (Logius Afdeling Standaarden)
- Menno Pleijster (ABN AMRO)
- Dennis Reumer (RVO)
- Frank Zwart (Logius DigiD/ DigiD machtigen)

Als onafhankelijk voorzitter is opgetreden Bas van Luxemburg, hoofd R&D bij Lost Lemon. Arjen Brienen, senior consultant bij Lost Lemon, en Jeroen de Ruig, senior consultant bij Lost Lemon, hebben de procedure in opdracht van het Bureau Forum Standaardisatie begeleid.

Hans Laagland en Han Zuidweg van het Bureau Forum Standaardisatie waren als toehoorder bij de expertbijeenkomst aanwezig.

3.3 Resultaat van het expertonderzoek

De geconsulteerde experts hebben geadviseerd om de standaard NL GOV AP OIDC op te nemen op 'pas toe of leg uit'-lijst. 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. 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 via apps. 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 expertbijeenkomst is duidelijk geworden dat het NL GOV OpenID Connect profiel 1.0 niet aan alle criteria voor toetsing van een standaard voldoet. Het beheer van de standaard is op moment van de expertbijeenkomst nog onvoldoende geregeld. Voor het criterium draagvlak geldt dat de standaard op dat moment in de praktijk nog niet wordt toegepast (er is geen referentie-implementatie). Vanuit het criterium toegevoegde waarde is de samenhang van OIDC-profiel met SAML een aandachtspunt. SAML heeft een deels overlappend functioneel toepassingsgebied met OpenID Connect. Een duidelijk transitiestrategie of –roadmap op authenticatievoorzieningen kan dit verhelpen, bovenop het advies van de experts aan het Forum Standaardisatie om binnen een jaar het onderzoek te starten of het mogelijk is om SAML niet meer te verplichten aan de overheid.

3.4 Resultaat van de openbare consultatie

In de openbare consultatie werden zes reacties ontvangen (waarvan vijf reacties zijn gepubliceerd), waaronder van de volgende personen en organisaties:

- A.Z.N. van Pelt
- P.A.A. Keuter (Signicat)
- B. Stibbe (VZVZ)
- A. Koot (SonicBee BV)

In de volgende paragraaf worden deze reacties op hoofdlijnen weergegeven.

De reacties gaan in op detail(technisch)niveau van het OIDC-profiel. Er worden vragen gesteld over nut en noodzaak van een apart Nederlands profiel bij OIDC en over de aansluiting van een Nederlands profiel bij internationale standaarden. Er worden vragen gesteld over de samenhang en onderscheid van het OIDC-profiel met SAML en met andere authenticatiestandaarden. Stimuleren van adoptie van het profiel wordt gezien als hoofdreden voor opname op de lijst. De geraadpleegde experts lijken eenzijdig te zijn samengesteld. Er ontbreekt een referentie-implementatie en de vooropgestelde wildgroei aan dialecten wordt niet onderbouwd.

3.5 Aanvullend onderzoek

Er is besloten de aandachtspunten expertadvies en uit de openbare consultatie nader te onderzoeken via een aanvullend onderzoek. 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). Bij het consulteren van experts is een aantal experts uitgenodigd die hebben gereageerd tijdens de openbare consultatie van de standaard NL GOV OpenID Connect profiel.

Aan de expertbijeenkomst hebben deelgenomen:

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

Marcel Molenaar (UWV) was verhinderd. Namens het Forum Standaardisatie waren aanwezig Hans Laagland en Bart Knubben. Onafhankelijke begeleiding van de consultatie is verzorgd door Jeroen de Ruig en Arjen Brienen, senior consultants bij Lost Lemon.

Het aanvullend onderzoek is vervolgens voorgelegd aan de bovengenoemde experts. De opmerkingen en aanvullingen van de experts zijn vervolgens verwerkt in dit Forumadvies. Er heeft geen openbare consultatie plaatsgevonden op de uitkomsten van het aanvullend onderzoek; de experts vertegenwoordigden zowel de expertbijeenkomst (2021) als de openbare consultatie.

In het onderzoek stonden volgende vraagstukken centraal:

- toegevoegde waarde: overlap met SAML; samenhang met het internationale iGOV-profiel voor OIDC
- draagvlak: marktondersteuning; voorbeeldimplementatie
- open standaardisatieproces: toewijzen en inrichten van beheerorganisatie
- geclusterde registratie Authenticatie-standaarden

4 Toetsing op inhoudelijke criteria en aanvullend vraagstuk

Het Forum Standaardisatie hanteert vier criteria om te bepalen of een standaard in aanmerking komt voor opname op de lijst:

1. Heeft de standaard toegevoegde waarde?
2. Zijn de standaard en het standaardisatieproces voldoende open?
3. Heeft de standaard voldoende draagvlak?
4. Is opname op de lijst een passend middel om de adoptie te bevorderen?

Vanuit het aanvullend onderzoek is een vijfde onderzoekpunt toegevoegd aan de toetsing: geclusterde registratie Authenticatie-standaarden.

Op de website van het Forum Standaardisatie is informatie te vinden over de vier criteria en de toetsingsprocedure.

Dit hoofdstuk beoordeelt in hoeverre NL GOV AP OIDC versie 1.0 voldoet aan deze vier criteria op basis van het expertadvies, de reacties uit de openbare consultatie, de resultaten van het aanvullend onderzoek, en de inzichten van de leden van het Forum Standaardisatie.

4.1 Toegevoegde waarde

De toetsingsprocedure wijst uit dat NL GOV OpenID Connect profiel **voldoet** aan het criterium 'toegevoegde waarde'.

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 OpenID Connect of andere niet gestandaardiseerde authenticatie protocollen bij mobiele applicaties, 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. Het belang van de standaard is hiermee groot en de urgentie is hoog."

Wel bestonden er vragen over de samenhang met het internationale iGOV-profiel voor OIDC en de overlap met SAML. Beide vraagstukken zijn in het aanvullend onderzoek nader uitgezocht.

4.1.1 Samenhang met het internationale iGOV-profiel voor OIDC

Tijdens de openbare consultatie is gewezen op internationale standaarden die als alternatief zouden kunnen dienen voor een Nederlands profiel. In het verleden hebben DigiD en eHerkenning voor 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 al 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 geven sommige geconsulteerde experts aan dat het ook mogelijk moet zijn om een al bestaand profiel in het buitenland te gebruiken,

waarbij het uitgangspunt moet zijn dat zo'n buitenlands profiel erg overeenkomt met het huidige Nederlandse profiel.

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

4.1.2 Relatie OpenID Connect en SAML: transitiestrategie

OpenID Connect (en het Nederlandse profiel) en SAML hebben overlap in het functioneel toepassingsprofiel. Dit betekent dat beide standaarden niet tegelijkertijd kunnen worden verplicht via plaatsing op de 'pas toe of leg uit'-lijst. Dit zou immers tot grote verwarring leiden bij inkopers van overheidsorganisaties: inkopers moeten bij een inkooptraject vermelden aan welke standaarden het in te kopen pakket/toepassing moet voldoen.

Inmiddels is voldoende duidelijk dat de standaard OpenID Connect de toekomst heeft, onder meer vanwege compatibiliteit met mobiele devices.

Het voorstel is om een verplichting van NL GOV AP OIDC (met de achterliggende standaard OIDC) en SAML te vergezellen van een gedocumenteerde transitiestrategie om de transitie van SAML naar OIDC te realiseren. Transitieperiode (op hoofdlijnen):

1. aanbieders van identitydiensten, onder wie identity providers en identity brokers/gateways, hebben tijd nodig om OIDC te implementeren volgens het Nederlandse profiel NL GOV AP OIDC op hun koppelvlak aan serviceproviders;
2. periode om NL GOV AP OIDC en SAML gelijkwaardig aan te bieden;
3. periode om NL GOV AP OIDC te prefereren (bijv. geen SAML meer voor nieuwe klanten);
4. periode om SAML uit te faseren (bijv. stoppen met SAML aanbieden aan bestaande klanten).

De transitiestrategie met roadmap en duidelijk communicatieplan zorgt voor voorspelbaarheid voor aangesloten partijen zodat partijen een afgewogen keuze kunnen maken bij investeringen. Met de verplichting voor de aanbieders van identitydiensten onder wie identity providers en identity brokers/gateways voor ondersteunen van èn SAML èn OIDC ontvangt OIDC een stimulans in de transitie van SAML naar OIDC. Zo wordt tegemoet gekomen aan de intentie van Logius rond het OIDC-profiel. Het voorgestelde functioneel toepassingsgebied zorgt ervoor dat serviceproviders (aanbieders van digitale overheidsdiensten aan burgers, bedrijven en overheden onderling) voor hun aansluiting kunnen kiezen tussen NL GOV AP OIDC (en onderliggende standaard OIDC) of SAML.

Expert hebben benadrukt dat de communicatie rondom deze mogelijke transitie-strategie belangrijk is. Logius heeft aangegeven de transitiestrategie op te stellen en vervolgens te beheren. De transitiestrategie wordt afgestemd met de beoogde invulling van een wettelijke verplichting (via ministeriële regeling) van de routeringsvoorzieningen via de Wdo.

Kortom, de transitie van SAML naar OIDC wordt bespoedigd door zowel de ondersteuning van SAML en van OIDC in eerste instantie verplicht te maken voor de partijen, onder wie identityproviders en identity broker/gateways, op hun koppelvlak aan serviceproviders. Hiermee wordt een *big bang* vermeden en kunnen dienstverleners gecontroleerd overstappen van SAML naar OIDC. Logius stelt zich verantwoordelijk voor de benodigde transitiestrategie met een roadmap en een communicatieplan waarin bovenstaande wordt vormgegeven.

4.2 Open standaardisatieproces

De toetsingsprocedure wijst uit dat er voldoende vertrouwen is dat de standaard **gaat voldoen** aan het criterium 'open standaardisatieproces'.

Het beheer van NL GOV AP OIDC wordt belegd bij de Afdeling Standaarden van Logius. De Afdeling Standaarden werkt conform BOMOS en heeft verschillende andere standaarden in beheer. Op het moment dat deze standaard in beheer komt van de Afdeling Standaarden van Logius zal de governance worden ingevuld conform BOMOS met periodiek overleggen met belanghebbenden (naast de online community).

De specificatiedocumenten zijn vrij beschikbaar. Ook alle review commentaren met daarbij behorende discussies en genomen besluiten als ook de notulen van de werkgroepsessies zijn vrij te raadplegen.

4.2.1 Toewijzen en inrichten van beheerorganisatie

De financiering voor het beheer en doorontwikkeling van deze standaard is samen met twee andere API-standaarden (ADR en OAuth2 profiel) geborgd door ministerie van Binnenlandse Zaken.

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

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

4.3 Draagvlak

De toetsingsprocedure wijst uit dat de NL GOV AP OIDC **voldoet** aan het criterium 'draagvlak.

De verwachting is dat het merendeel van de leveranciers die OpenID Connect aanbieden met acceptabele inspanning ook aan kunnen sluiten op het profiel. OpenID Connect wordt breed toegepast binnen het bedrijfsleven als moderne toepassing voor federatieve authenticatie.

De standaard wordt nog niet bij de Nederlandse overheid gebruikt. Het is de verwachting dat de standaard op den duur zal worden toegepast bij centrale voorziening DigiD en de stelsels eID en eHerkenning. Wel wordt de OpenID Connect standaard gebruikt door meerdere Nederlandse (semi-)overheidsorganisaties, waaronder SURF en iShare. Overheidsorganisaties

staan wel achter de standaard. Belangrijk is wel dat er marktondersteuning is voor de standaard en dat er referentie-implementaties beschikbaar komen.

Het belang en de urgentie van de standaard hoog is. Vooral uit oogpunt van security en privacy is dit een belangrijke standaard.

4.3.1 Marktondersteuning en voorbeeldimplementatie

Tijdens de expertconsultatie van de standaard op 7 oktober 2021 bleek dat NL GOV AP OIDC nog niet voldoet aan het criterium draagvlak, met name omdat de standaard nog niet wordt toegepast en er geen werkende referentie-implementatie is.

De opstellers van de standaard hebben daarom twee hackathons georganiseerd, één in juli 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. De uitkomsten van de hackathons is gedeeld met de experts tijdens de consultatie op 6 oktober 2022.

De geconsulteerde experts zien op basis van de uitkomsten van de hackathons geen belemmering voor de toepassing van het Nederlands profiel. Tijdens de expertbijeenkomst van 7 oktober 2021 bestond 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.

Kortom, de experts concluderen unaniem dat de uitgevoerde hackathons aantonen dat de technische implementeerbaarheid van de standaard voldoende is, en dat zij 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.

4.4 Geclusterde beschrijving federatieve authenticatie-standaarden

De intentie voor de indiener Logius voor het verplichten van NL GOV AP OIDC is mede om een transitie te bewerkstellingen van SAML naar OIDC 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.

Met de plaatsing van NL GOV AP OIDC op de ‘pas toe of leg uit’-lijst wordt de indruk gewekt dat serviceproviders al kunnen aansluiten op OIDC via het Nederlandse profiel. In de praktijk is er tot op heden geen volledig aanbod van NL GOV AP OIDC.

Daarom is er het voorstel voor een nieuwe, geclusterde beschrijving ‘Authenticatie-standaarden’ op de ‘pas toe of leg uit’-lijst, onder de noemer ‘Authenticatie-standaarden’. Een dergelijke geclusterde beschrijving is vergelijkbaar met de Geo-standaarden of Digikoppeling op de ‘pas toe of leg uit’-lijst. Een nieuwe geclusterde beschrijving bevat een overkoepelende

registratie voor SAML en NL GOV AP OIDC en vervangt de huidige, afzonderlijke registraties van SAML en NL GOV AP OIDC (en OIDC op de Lijst Aanbevolen Standaarden). Deze clustering biedt ook ruimte om het functioneel toepassingsgebied te actualiseren.

De geclusterde registratie Athenticatie-standaarden krijgt een nieuw functioneel toepassingsgebied. De volgende formulering is afgestemd met de experts met betrekking tot het functioneel toepassingsgebied:

> 'Authenticatie-standaarden NL GOV AP OIDC en SAML moeten worden toegepast door aanbieders van identitydiensten, onder wie identity providers en identity brokers/gateways, op hun externe koppelvlak aan serviceproviders (d.w.z. overheden met digitale diensten) voor federatieve toegang en voor de uitwisseling van attributen, waaronder identiteitsgegevens, zodat serviceproviders de keuze hebben tussen beide standaarden.'

Uit het aanvullend onderzoek komt naar voren dat de experts achter het voornemen staan voor een geclusterde beschrijving van de standaarden SAML en NL GOV AP OIDC (met een expliciete melding van achterliggende standaard OpenID Connect). Met het verplichten van NL GOV AP OIDC (het Nederlandse profiel voor OIDC) wordt ook de achterliggende internationale standaard OIDC verplicht. Een geclusterde registratie zorgt ervoor 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 beschrijving moet duidelijk zijn dat het hier om SAML en OpenID Connect gaat.

Kortom, de geconsulteerde experts adviseren een geclusterde registratie voor de standaarden NL GOV AP OIDC en SAML voor plaatsing op de 'pas toe of leg uit'-lijst.

4.5 Opname op de lijst bevordert adoptie

De toetsingsprocedure wijst uit dat de standaard NL GOV AP OIDC **voldoet** aan het criterium 'opname op de lijst bevordert adoptie'.

Plaatsing van NL GOV AP OIDC vindt plaats via een geclusterde registratie (beschrijving) op de lijst open standaarden. Deze registratie heeft de naam **Authenticatie-standaarden (NL GOV AP OIDC en SAML)**. Bij de opname van Authenticatie-standaarden op de 'pas toe of leg uit'-lijst is de ondersteuning van zowel NL GOV AP OIDC en SAML verplicht voor partijen, onder wie aanbieders van identitydiensten (identity providers en identity brokers/gateways), op hun koppelvlak aan serviceproviders.

De verplichting in combinatie met de transitiestrategie zorgt voor het bewerkstelligen van de overgang van SAML naar OIDC en zal leiden tot meer duidelijkheid bij inkopers van (semi)overheidsorganisaties en daarmee tot adoptie van de geclusterde standaarden en de toepassing daarvan. Met het verplichten van NL GOV AP OIDC (het Nederlandse profiel voor OIDC) wordt ook de achterliggende internationale standaard OIDC verplicht. Daarnaast zal het verplichten van het Nederlandse profiel voorkomen dat er verschillende profielen gaan

ontstaan van implementaties van OpenID Connect hetgeen een vermindering van interoperabiliteit als gevolg voorkomt.

Breder kader voor verplichten van Authenticatie-standaarden is de aankomende Wet digitale overheid. Het verplichten van Authenticatie-standaarden heeft een doorwerking in de Wet digitale overheid (Wdo) (per 1 juli 2023 in werking). Het verplichten van NL GOV AP OIDC en SAML aan de overheid (via opname op de 'pas toe of leg uit'-lijst van Forum Standaardisatie) en de aanpalende transitiestrategie hebben een richtinggevende werking op beoogde wettelijke verplichting (via ministeriële regeling) van routeringsvoorzieningen.

5 Adviezen bij opname van de standaard

Het Forum Standaardisatie geeft de volgende adviezen bij plaatsing van Authenticatie-standaarden (NL GOV AP OIDC en SAML) op de 'pas toe of leg uit'-lijst. Een deel van de adviezen uit de expertbijeenkomst van 7 oktober 2021 zijn inmiddels opgevolgd via het aanvullend onderzoek en zijn hieronder niet opgenomen:

1. aan centrale voorziening DigiD, afsprakenstelsel eHerkenning en Logius als beheerorganisatie van het profiel om binnen een jaar een transitiestrategie voor de overgang van SAML naar NL GOV AP OIDC op te stellen. Deze transitiestrategie heeft de volgende onderdelen:
    - publieke roadmap waarin de ondersteuning van de standaarden op de koppelvlakken voor serviceproviders twee jaar vooruit inzichtelijk is. Dit zorgt voor voorspelbaarheid zodat serviceproviders een afgewogen keuze kunnen maken bij investeringen. Op basis van de roadmap informeert Logius per fase actief de (aangesloten) partijen en Forum Standaardisatie zodra er wijzigingen zijn in de mate van ondersteuning van de standaarden;
    - communicatieplan zodat alle geraakte partijen tijdig en duidelijk geïnformeerd zijn. Logius communiceert hiermee hoe de verplichting ten aanzien van beide standaarden wordt opgepakt en hoe dit toegepast kan worden door het veld.
2. aan Logius in de rol van beheerorganisatie van NL GOV AP OIDC om voortaan internationale ontwikkelingen rond OIDC te monitoren op Europees en wereld niveau, en op het moment dat internationaal andere keuzes worden gemaakt, het Nederlandse profiel zo nodig aan te passen;
3. aan Forum Standaardisatie om twee jaar na plaatsing van Authenticatie-standaarden op de 'pas toe of leg uit'-lijst de Authenticatie-standaarden (NL GOV AP OIDC en SAML) te evalueren voor het waarborgen van de kwaliteit van de 'pas toe of leg uit'-lijst. De evaluatie onderzoekt de voortgang van de transitiestrategie en dient als peilstok voor de transitie van SAML naar NL GOV AP OIDC;
4. aan Forum Standaardisatie om de komende twee jaar alle geraakte partijen tijdig en duidelijk te informeren wat de verplichting van Authenticatie-standaarden behelst, wie de doelgroep is voor de verplichting en wat het Forum Standaardisatie beoogt met de verplichting (bevorderen van transitie van SAML naar OIDC zet de weg open naar nieuwe toepassingen);

5. aan Logius als beheerder van en andere betrokken partijen bij NL GOV AP OIDC om gereviewde en geauditeerde voorbeeld configuraties beschikbaar te stellen die je kunt downloaden voor gebruik in gangbare implementaties;
6. aan Logius als beheerder van NL GOV AP OIDC een poging te doen om een kortere versie te maken van de beschrijving van de standaard, een soort easy start guide. Dit moet overigens niet leiden tot vertraging van de eerste implementatie;
7. aan Logius als de beheerder van de standaard, een vorm van een testvoorziening in te richten voor NL GOV AP OIDC, waarmee serviceproviders kunnen testen.