3 Oplegnotitie Open Standaarden, lijsten

Vergadering:	Forum Standaardisatie woensdag 14 juni 2023
Agendapunt:	3
Documentnummer:	FS-20230614.3
Aan:	Forum Standaardisatie
Van:	Stuurgroep Open Standaarden
Datum:	Woensdag 14 juni 2023
Versie:	1.0
Bijlage:	FS-20230614.3A-Forumadvies-Authenticatie-standaarden-NL-GOV-AP-OIDC-en-SAML
Opstellers:	Hans Laagland Han Zuidweg (3D. Acties voor doorontwikkeling van de lijst open standaarden)
Rechten:	CC0 publieke domein verklaring

Samenvatting

Ter besluitvorming

Vraag aan Forum Standaardisatie om in te stemmen met het volgende advies:

A. standaard **NL GOV Assurance profile for OpenID Connect 1.0** te verplichten aan de overheid (‘pas toe of leg uit’-verplichting) (veiliger internet) en via een geclusterde registratie **Authenticatie-standaarden (NL GOV AP OIDC en SAML)** te plaatsen op de ‘pas toe of leg uit’-lijst

Ter toelichting

B. Voortgang lopende procedures
   1. Veiliger internet
      a. security.txt (security- en policy-contactinformatie) aanpassing functioneel toepassingsgebied
   2. Betere gegevensuitwisseling:

b. OAS (beschrijven van REST APIs)
   verplichten aan de overheid (‘pas toe of leg uit’-verplichting) in nieuwe versie
c. NEN 3610 (onderdeel van Geo-standaarden; basismodel voor geo-informatie)
   verplichten aan de overheid (‘pas toe of leg uit’-verplichting) in nieuwe versie

3. Verwijderen elf standaarden lijst aanbevolen standaarden
   niet meer aanbevelen aan de overheid (batch-procedure)

C. Onderzoek lifecyclemanagement en prioritering van standaarden (Architectuurraad)
D. Acties voor de doorontwikkeling van de lijst open standaarden
E. Europese Aanbesteding Toetsingsprocedures (Bureau Forum Standaardisatie)

Ter besluitvorming

Ad A. Forumadvies Authenticatie-standaarden (NL GOV AP OIDC en SAML) (veiliger internet)

[Bijlage: FS-20230614.3A-Forumadvies-Authenticatie-standaarden-NL-GOV-AP-OIDC-en-SAML]

Vraag aan Forum Standaardisatie om in te stemmen met de volgende adviezen:

a. standaard **NL GOV Assurance profile for OpenID Connect 1.0** te verplichten aan de overheid ('pas toe of leg uit'-verplichting) (veilig internet)

b. standaard NL GOV Assurance profile for OpenID Connect 1.0 via de geclusterde registratie **Authenticatie-standaarden (NL GOV AP OIDC en SAML)** te plaatsen op de 'pas toe of leg uit'-lijst

Advies

De Stuurgroep Open Standaarden adviseert het Forum Standaardisatie om de standaard **NL GOV Assurance profile for OpenID Connect 1.0** te verplichten aan de overheid ('pas toe of leg uit'-verplichting) (veilig internet).

Daarnaast adviseert de Stuurgroep Open Standaarden om de standaard NL GOV Assurance profile for OpenID Connect 1.0 via de geclusterde registratie **Authenticatie-standaarden (NL GOV AP OIDC en SAML)** te plaatsen op de 'pas toe of leg uit'-lijst.

NL GOV Assurance Profile for OIDC 1.0 draagt bij aan veiliger internet doordat authenticatieservices (zoals DigiD) de identiteit van een eindgebruiker controleren op een gestandaardiseerde wijze.

Samenvatting

Het gebruik van NL GOV AP OIDC (inclusief achterliggende standaard OIDC) zet de weg open naar nieuwe toepassingen, in het bijzonder voor mobiele toepassingen. 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). Een transitie komt niet (of niet voldoende) van de grond, zolang alleen SAML als verplicht op de lijst blijft staan. Daarnaast is het nog te vroeg SAML niet te verplichten. Daarom is het advies NL GOV AP OIDC (inclusief achterliggende standaard OIDC) en SAML te verplichten via een geclusterde registratie 'Authenticatie-standaarden' op de Lijst Open Standaarden. Met het verplichten van NL GOV AP OIDC (het Nederlandse profiel voor OIDC) wordt ook de achterliggende internationale standaard OIDC verplicht.

Geclusterde registratie Authenticatie-standaarden met een transitiestrategie van Logius draagt bij aan het realiseren van de transitie. 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. Centrale voorziening DigiD, afsprakenstelsel eHerkenning en Logius als beheerorganisatie van het profiel zijn hierin bepalend en zijn eigenaar van de transitiestrategie. Logius heeft aangegeven een transitiestrategie op te stellen en te beheren. Forum Standaardisatie stimuleert de transitie via de inzet van instrumentatrium dat Forum tot zijn beschikking heeft (plaatsen op de lijst, adoptieadviezen en evalueren van standaarden). De transitiestrategie met roadmap en duidelijk communicatieplan is voorwaardelijk bij het verplichten van de Authenticatie-standaarden aan de overheid.

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. Het verplichten van Authenticatie-standaarden (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 (Wdo) van routeringsvoorzieningen waarin OIDC en SAML een onderdeel zijn.

Betekenis nieuwe geclusterde registratie Authenticatie-standaarden 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.

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

Huidige situatie	**Voorgestelde situatie**
SAML op 'pas toe of leg uit'-lijst	Geclusterde registratie van authenticatiestandaarden op 'pas toe of leg uit'-lijst (SAML en NL GOV AP OIDC) met één functioneel toepassingsgebied
Aanmelding van NL GOV AP OIDC voor 'pas toe of leg uit'-lijst	Geclusterde registratie van authenticatiestandaarden 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 de inhoudelijke vertaling een grotere impact heeft dan de initieel aanmelding van NL GOV AP OIDC voor de 'pas toe of leg uit'-lijst.

Met het verplichten van NL GOV AP OIDC (het Nederlandse profiel voor OIDC) wordt ook de achterliggende internationale standaard OIDC verplicht. Dit maakt daarmee een aparte plaatsing van de internationale standaard OIDC op de lijst aanbevolen standaarden overbodig.

Belang van de standaard: veiliger internet

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 degene is die de eindgebruiker op het internet zegt te zijn.

Inzet van Authenticatie-standaarden 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.

Hoe is het proces verlopen?

Logius heeft op 15 oktober 2020 NL GOV Assurance Profile for OIDC 1.0 aangemeld bij het Bureau Forum Standaardisatie om te verplichten aan de overheid via plaatsing op de 'pas toe of leg uit'-lijst. 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 was voldaan aan de criteria voor open beheer en draagvlak.

De expertgroep is op 7 oktober 2021 bijeengekomen om de standaard te toetsen tegen de criteria en om geïdentificeerde aandachtspunten te bespreken. Aan dit expertonderzoek namen vertegenwoordigers deel uit een brede coalitie van overheid, bedrijfsleven en koepelorganisaties.

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; ontbreken van voorbeeldimplementatie)'.

Op basis van bespreking met inhoudsdeskundigen (SURF) en met 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). Het aanvullend onderzoek is vervolgens voorgelegd aan de bovengenoemde experts ter review. Er heeft geen openbare consultatie plaatsgevonden op de uitkomsten van het aanvullend onderzoek.

Het Bureau heeft de uitkomsten van het expertadvies en het aanvullend onderzoek vertaald naar de toetsingsprocedure. Deze vertaling is besproken op Stuurgroep Open Standaarden van 23 maart en daarna met de indiener Logius op 9 mei 2023.

Het 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.

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.

NL GOV Assurance profile for OpenID Connect

NL GOV Assurance profile for OpenID Connect versie 1.0 vult de standaard OpenID Connect aan met richtlijnen zodat OIDC binnen de Nederlandse context eenduidig wordt toegepast. 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.

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.

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 per dienst eigen inloggegevens nodig zijn, of bij elke dienst apart moet worden ingelogd.

Ter toelichting

Ad B. Voortgang lopende procedures

[Bijlage: geen]

1. Veiliger internet

a. security.txt (security- en policy-contactinformatie)

Op basis van nadere inzichten heeft het Bureau Forum Standaardisatie gemeend dat het functioneel toepassingsgebied van security.txt zoals het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) heeft vastgesteld op 25 mei 2023, kan leiden tot onduidelijkheid. Het Bureau heeft daarom een kleine aanpassing doorgevoerd in het functioneel toepassingsgebied om deze onduidelijkheid weg te nemen. security.txt is een standaard voor security- en policy-contactinformatie en draagt bij aan een veiliger internet.

Aangepaste functioneel toepassingsgebied:

> *'security.txt moet worden toegepast op alle systemen die via HTTPS publiek benaderbaar zijn, zodat securitycontactinformatie duidelijk is.'*

De inschatting is dat de aanpassing van het functioneel toepassingsgebied niet extra partijen raakt of uitsluit die security.txt moeten toepassen na plaatsing op de 'pas toe of leg uit'-lijst.

In de formulering van het functioneel toepassingsgebied werd verwezen naar het gebruik van de standaard 'HTTP' en 'HTTPS'. Met name volgende twee punten zijn relevant die tot onduidelijkheid kunnen leiden vanwege de formulering met 'HTTP' in het oorspronkelijke functioneel toepassingsgebied:

1. het specificatiedocument (RFC) van security.txt schrijft het gebruik van HTTPS voor;
2. HTTPS wordt van 1 juli 2023 wettelijk verplicht voor overheden op basis van de Wdo.

2. Betere gegevensuitwisseling

b. OpenAPI Specification (beschrijven van REST APIs)

Forum Standaardisatie toetst of de standaard OpenAPI Specification (OAS) in de nieuwe versie (3.1) geschikt is om te blijven verplichten aan de overheid ('pas toe of leg uit'-verplichting). OAS is een standaard voor het beschrijven van REST API's; een Application Programming Interface (API) draagt bij aan het uitwisselen van informatie tussen applicaties.

Op basis van conclusies uit de expertbijeenkomst van 5 april 2023 is ervoor gekozen de toetsingsprocedure tijdelijk stil te leggen. De experts kwamen gezamenlijk tot de conclusie dat het nu te vroeg is OAS in de nieuwe versie (3.1) te verplichten. Experts adviseren de procedure voort te zetten zodra OAS voldoende voortgang heeft op de geconstateerde aandachtspunten. Deze aandachtspunten zijn:

- OAS 3.1 bevat breaking changes ten opzichte van OAS 3.0. OAS 3.1 is niet backward compatible met OAS 3.0;

- er is onvoldoende (internationale) ondersteunende tooling beschikbaar om OAS 3.1 te implementeren en de transitie van OAS 3.0 naar OAS 3.1 soepel te laten verlopen;
- op basis van bovenstaande twee redenen zijn de kosten voor de migratie van OAS 3.0 naar OAS 3.1 op dit moment nog te hoog;
- er is internationaal nog weinig adoptie van OAS 3.1. Dit lijkt de ontwikkeling van goede ondersteunende tools tegen te werken.

De experts hebben tijdens de expertbijeenkomst adviezen uitgebracht die kunnen bijdragen aan het verplichten in de toekomst van OAS in de nieuwe versie.

Logius heeft OAS in de nieuwe versie 3.1 op 10 augustus 2022 aangemeld bij het Bureau Forum Standaardisatie. Het Forum Standaardisatie heeft op 7 december 2022 besloten om de versiewijziging van OAS in procedure te nemen. De expertbijeenkomst heeft plaatsgevonden op 5 april 2023.

c. NEN 3610 (onderdeel van Geo-standaarden; basismodel voor geo-informatie)

Forum Standaardisatie toetst of de standaard NEN 3610 (onderdeel van Geo-standaarden) in de nieuwe versie (NEN 3610:2022 nl) geschikt is om te blijven verplichten aan de overheid ('pas toe of leg uit'-verplichting). NEN 3610 is een basismodel voor geo-informatie en geeft regels voor het eenduidig beschrijven, uitwisselen en op het web publiceren van geo-informatie.

Geonovum heeft NEN 3610 in de nieuwe versie (NEN 3610:2022 nl) op 30 augustus 2022 aangemeld bij het Bureau Forum Standaardisatie. Het Forum Standaardisatie heeft op 8 februari 2023 besloten om de versiewijziging van NEN 3610 in procedure te nemen. De expertbijeenkomst is in voorbereiding.

3. Verwijderen elf standaarden lijst aanbevolen standaarden

Forum Standaardisatie toetst in een gecombineerde toetsingsprocedure om een groep van elf standaarden van de lijst aanbevolen standaarden niet meer aan te bevelen aan de overheid. Het betreft de standaarden CalDAV, DHCP, DNS, EI Standaarden, http, IMAP, IPP, MTOM, SIP, UDDI, WebDav. Forum Standaardisatie heeft deze elf standaarden vastgesteld op 8 februari 2023.

Het Forum Standaardisatie heeft op 8 februari 2023 besloten om deze groep standaarden in procedure te nemen via een gecombineerde toetsingsprocedure die iedere standaard afzonderlijk op hoofdlijnen beoordeelt tegen de criteria die het Forum Standaardisatie voor de lijst hanteert. De expertbijeenkomst in september is in voorbereiding.

Deze verwijdering maakt deel uit van acties uit het onderzoek van Paul Dam over de doorontwikkeling van de lijsten open standaarden, nl. actiever onderhoud van de lijst aanbevolen standaarden en standaarden verwijderen die op de lijst geen toegevoegde waarde meer hebben.

Ad C. Onderzoek lifecyclemanagement en prioritering van standaarden (Architectuurraad)

[Bijlage: geen]

Het Bureau Forum Standaardisatie gaat Logius met kennis ondersteunen in twee beknopte onderzoeken over standaardenbeheer. Het betreft het onderzoeken of principes voor lifecyclemanagement en voor prioritering van standaarden van toepassing kunnen worden verklaard op verplichte standaarden voor de digitale overheid. De twee onderzoeken komen voort op voorstel van de Architectuurraad.

Logius heeft de Architectuurraad gevraagd om afspraken te bekrachtigen voor lifecyclemanagement en prioritering van standaarden in de GDI. Deze afspraken houden in dat standaarden gebaseerd moeten zijn op actief beheerde onderliggende standaarden (lifecyclemanagement) en dat Europese en mondiale standaarden voorrang hebben boven eigen Nederlandse standaarden (prioritering). Voor beide onderdelen geldt dat na goedkeuring afwijken van de afspraken mogelijk moet zijn.

De Architectuurraad heeft steun uitgesproken voor de intentie van het voorstel van Logius. De Architectuurraad heeft daarbij Logius en Forum Standaardisatie benaderd te onderzoeken dat deze afspraken gaan gelden voor verplichte standaarden voor de digitale overheid buiten de standaarden in de GDI.

Het onderzoek maakt voor Forum Standaardisatie inzichtelijk hoe de toetsingscriteria van het Forum zich verhouden tot door Logius voorgestelde principes. Daarnaast dragen de onderzoeken bij aan verdere kruisbestuiving tussen Forum en Architectuurraad.

Ad D. Acties voor de doorontwikkeling van de lijst open standaarden

[Bijlage: geen]

In de vergadering van 20 april 2022 onderschreef het Forum Standaardisatie de acties die voortkwamen uit het onderzoek van Paul Dam over de doorontwikkeling van de lijsten open standaarden. Hieronder volgt een overzicht van de voortgang.

Opname 'andersoortige standaarden' op de lijst aanbevolen standaarden

Het Forum Standaardisatie nam het advies over uit het onderzoek doorontwikkeling van de lijsten open standaarden om 'andersoortige standaarden' zoals principes, baselines en richtlijnen toe te laten op de lijst aanbevolen standaarden als deze belangrijke meerwaarde hebben voor de interoperabiliteit, online veiligheid of leveranciersonafhankelijkheid van de overheid.

Op advies van de Stuurgroep Open Standaarden en het Forum Standaardisatie toetsen wij in eerste instantie MANRS en NL Design System als *proof of concept* voor plaatsing op de lijst aanbevolen standaarden. Bureau Forum Standaardisatie verwacht het Forum Standaardisatie tegen het einde van 2023 inzichten te hebben vergaard uit de *proof of concept* met MANRS.

Gangbare standaarden minder op de voorgrond op de lijst aanbevolen standaarden

In de vergadering van 20 april 2022 gaf het Forum Standaardisatie opdracht aan BFS om gangbare standaarden op de lijst aanbevolen standaarden minder op de voorgrond te laten treden. Bureau Forum Standaardisatie verwacht het Forum Standaardisatie tegen het einde van 2023 een voorstel voor te leggen van standaarden die als 'gangbaar' op de lijst aangemerkt kunnen worden.

Ad E. Europese Aanbesteding Toetsingsprocedures (Bureau Forum Standaardisatie)

[Bijlage: geen]

Het Bureau Forum Standaardisatie heeft in **InnoValor** een nieuwe partij gevonden om de toetsingsprocedures voor de lijsten open standaarden te begeleiden. Dat is de uitkomst van de Europese Aanbesteding voor de begeleiding van de toetsingsprocedures voor de lijsten open standaarden. Het contract met de vorige partij liep af in 2022.

Dit betekent dat huidige procedures kunnen worden voortgezet en dat nieuwe procedures kunnen starten voor mutaties van standaarden voor de Lijst Open Standaarden. Dit betreft de voortgang van NEN 3610 (onderdeel van Geo-standaarden) ('pas toe of leg uit'-verplichting) en *proof of concept* met MANRS. Procedures die kunnen starten, zijn onder andere versiewijziging van NLRS en versiewijziging Geo-standaarden. De afronding van de procedures voor NL GOV AP OIDC ('pas toe of leg uit'-verplichting) en voor verwijderen elf standaarden lijst aanbevolen standaarden (lijst aanbevolen standaarden) vindt nog plaats via de vorige partij.