Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Aanbiedingsformulier
Overheidsbreed Beleidsoverleg Digitale Overheid

Agendapunt **Onderwerp**	4c Authenticatie-standaarden (NL GOV AP OIDC en SAML) verplichten aan de overheid via plaatsing op de 'pas toe of leg uit'-lijst (veilig internet
Datum behandeling	21 september 2023
Sponsors **Betrokken partijen**	Forum Standaardisatie
Contactgegevens	Organisatie : Forum Standaardisatie Contactpersoon : Hans Laagland Telefoonnummer : 06-21820789 E-mailadres : hans.laagland@forumstandaardisatie.nl
Doel van de behandeling (dubbelklikken op vakje en 'ingeschakeld' aanvinken)	☐ Ter discussie/meningvormend ☒ Ter besluitvorming ☐ Hamerstuk ☐ Ter advies naar eigenaar/OBDO/staatssecretaris/… ☐ Ter informatie, agendapunt wordt toegelicht ☐ Ter kennisname, agendapunt wordt niet behandeld
Eerder behandeld in Datum behandeling: Uitkomst behandeling: Resultaat toets: Gemaakte afspraken:	☐ DOD ☐ IDO ☐ PGDI ☒ Anders: Forum Standaardisatie ☐ MT DO|DS|CIO RIJK ☐ Overeenstemming ☐ Geen overeenstemming
Discussiepunten **Beslispunten**	Het OBDO stemt in met: Authenticatie-standaarden (NL GOV AP OIDC en SAML) te verplichten aan de overheid via plaatsing op de 'pas toe of leg uit'-lijst (veilig internet)
Financiële consequenties Kosten: Dekking:	 Eenmalige kosten : nvt Jaarlijks terugkerende kosten : nvt ☐ Ja ☐ Nee ☐ Gedeeltelijk
Leeswijzer	In de bijlage vindt u een uitgebreidere toelichting op het proces en onderbouwing van het gevraagde besluit.
Toelichting Ruimte voor aanleiding, voorgeschiedenis, samenvatting, relevante context, zoals betrokken	[bijlagen 4c. Authenticatie-standaarden] Authenticatie-standaarden (NL GOV AP OIDC en SAML) dragen bij aan een veiliger internet doordat authenticatieservices (zoals DigiD) de identiteit van een eindgebruiker controleren op een

(inter)nationale wet- en regelgeving, vervolgproces.	gestandaardiseerde wijze. Dit leidt tot een betrouwbare digitale dienstverlening van de overheid aan burgers en bedrijven. Indiener Logius wil authenticatieservices inrichten met een nieuwe generatie standaard (OpenID Connect). Experts geven aan dat het gebruik van OIDC en het bijbehorende Nederlandse profiel (NL GOV AP OIDC) de weg openzet naar nieuwe toepassingen, in het bijzonder voor mobiele toepassingen zoals apps. Ook vanuit oogpunt van security en privacy is OIDC een belangrijke standaard. Het is nog te vroeg de huidige gangbare standaard voor authenticatie op de 'pas toe of leg uit'-lijst (SAML) in te wisselen voor de nieuwe generatie. Daarom adviseren betrokken experts bij de toetsingsprocedure en reacties uit de openbare consultatie om NL GOV AP OIDC (inclusief achterliggende standaard OIDC) *samen met* SAML (huidige standaard op de 'pas toe of leg uit'-lijst) te verplichten aan de overheid via een **geclusterde registratie 'Authenticatie-standaarden'** op de 'pas toe of leg uit'-lijst. Dit betekent dat de voordelen van OIDC kunnen worden benut en dat huidige ondersteuning en gebruik van SAML in tact blijft. De geclusterde registratie 'Authenticatie-standaarden' betekent: • aanbieders van identitydiensten (bv. DigiD of eHerkenning) ondersteunen zowel het huidige SAML op de 'pas toe of leg uit'-lijst als ook de nieuwe generatie standaard OIDC; • aanbieders van digitale overheidsdiensten aan burgers, bedrijven en overheden onderling (bv. Belastingdienst of UWV) (serviceproviders) *kunnen kiezen* tussen OIDC of SAML voor hun aansluiting op een identitydienst (zoals DigiD). De 'pas toe of leg uit'-verplichting geldt alleen voor de aanbieders van identitydiensten. Met deze gecombineerde verplichting van OIDC en SAML wil Logius een transitie in gang zetten met afbouw van SAML en opbouw naar OIDC. Het is nu te voorbarig om een einddatum te noemen voor uitfaseringstraject van SAML (in ieder geval niet op korte termijn omdat te veel partijen nog gebruik maken van SAML). Bij het verplichten van Authenticatie-standaarden komt ook een door het Forum Standaardisatie geadviseerde transitiestrategie met roadmap en communicatieplan. Logius informeert hiermee actief de (aangesloten) partijen zodra er wijzigingen zijn in de mate van ondersteuning van de standaarden. Dit zorgt voor voorspelbaarheid voor aangesloten partijen zodat zij een afgewogen keuze kunnen maken voor relevante ICT-diensten en -producten. Logius heeft aangegeven deze transitiestrategie op te stellen en te beheren. De transitiestrategie is voorwaardelijk bij het verplichten van de Authenticatie-standaarden aan de overheid. Breder kader voor verplichten van Authenticatie-standaarden is de Wet digitale overheid die regelt dat Nederlandse burgers en bedrijven veilig en betrouwbaar kunnen inloggen bij de (semi-)overheid.

	Na afronding van deze toetsingsprocedure verandert de naam NL GOV AP OIDC in **OpenID.NLGov** om aan te sluiten bij de internationale conventie van namen voor profielen bij OIDC. N.B.: in dit aanbiedingsformulier en in de bijlage zijn verduidelijkingen verwerkt naar aanleiding van de vragen van minOCW en minEZK tijdens de bespreking van dit agendapunt in SO OBDO.

Xa Authenticatie-standaarden verplichten aan overheid (veilig internet)

Met opmerkingen [LH1]: LET WEL: nummering aanpassen

Vergadering:	Overheidsbreed Beleidsoverleg Digitale Overheid donderdag 21 september 2023
Documentnummer:	Xa
Aan:	Overheidsbreed Beleidsoverleg Digitale Overheid
Van:	Forum Standaardisatie
Datum:	donderdag 21 september 2023
Versie:	1.0
Bijlagen:	FS-20230614-Forumadvies-Authenticatie-standaarden-NL-GOV-AP-OIDC-en-SAML

Met opmerkingen [LH2]: LET WEL: nummering aanpassen

Ter besluitvorming

Forumadvies: Authenticatie-standaarden (NL GOV AP OIDC en SAML) verplichten aan overheid (‘pas toe of leg uit’-verplichting) (veilig internet)

Het OBDO stemt in om:

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

Het Forum Standaardisatie adviseert 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 het Forum Standaardisatie 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.

Het Forumadvies geeft een nadere onderbouwing.

Samenvatting

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

Indiener Logius wil authenticatieservices inrichten met een nieuwe generatie standaard OpenID Connect. OpenID Connect (OIDC) 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; er is doorontwikkeling en marktondersteuning. Ook vanuit oogpunt van security en privacy is OIDC een belangrijke standaard.

Het is echter nog te vroeg de huidige gangbare standaard voor authenticatie (SAML op de 'pas toe of leg uit'-lijst) in te wisselen voor de nieuwe generatie. Daarom is het advies NL GOV AP OIDC (inclusief achterliggende standaard OIDC) samen met SAML te verplichten aan de overheid via een **geclusterde registratie 'Authenticatie-standaarden'** op de lijst open standaarden. Met deze gecombineerde verplichting van OIDC en SAML wil Logius een transitie in gang zetten met afbouw van SAML en opbouw naar OIDC (en het Nederlandse profiel). Zo kunnen de voordelen van OIDC worden benut en blijft huidige ondersteuning en gebruik van SAML in tact.

De geclusterde registratie 'Authenticatie-standaarden' betekent:

- aanbieders van identitydiensten (bv. DigiD of eHerkenning) ondersteunen zowel het huidige SAML op de 'pas toe of leg uit'-lijst als ook de nieuwe generatie standaard OIDC;
- aanbieders van digitale overheidsdiensten aan burgers, bedrijven en overheden onderling (bv. Belastingdienst of UWV) (serviceproviders) *kunnen kiezen* tussen OIDC of SAML voor hun aansluiting op een identitydienst (zoals DigiD).

De 'pas toe of leg uit'-verplichting geldt voor de aanbieders van identitydiensten. Geclusterde registratie Authenticatie-standaarden met een transitiestrategie van Logius draagt bij aan het realiseren van de transitie naar de nieuwe generatie standaard. De door het Forum Standaardisatie geadviseerde transitiestrategie met roadmap en duidelijk communicatieplan zorgt voor voorspelbaarheid voor aangesloten partijen op authenticatieservices partijen (zoals Belastingdienst of UWV) zodat zij een afgewogen keuze kunnen maken bij relevante ICT-diensten en -producten.

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 NL GOV AP OIDC en SAML. Het is nu te voorbarig om een einddatum te noemen voor uitfaseren van SAML (in ieder geval niet op korte termijn omdat te veel partijen nog gebruik maken van SAML). 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 van het Forum (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 Wet digitale overheid (Wdo) die regelt dat Nederlandse burgers en bedrijven veilig en betrouwbaar kunnen inloggen bij de (semi-)overheid. Het verplichten van Authenticatie-standaarden via de 'pas toe of leg uit'-lijst geldt breed, ook voor zaken buiten scope van Wdo. In kader van Wdo kan de opname van Authenticatie-standaarden op de 'pas toe of leg uit'-lijst richtinggevend zijn voor eventuele verplichtingen die mogelijk via Wdo ingevoerd zullen worden.

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 het gebruik van de internationale standaard OIDC verplicht is volgens een aantal aanscherpende eisen van het Nederlandse profiel. Het gebruik van een geclusterde registratie sluit aan bij de praktijk van eerdere geclusterde registraties op de lijst open standaarden zoals Geo-standaarden of Digikoppeling.

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

Nieuwe naam voor het Nederlandse profiel (NL GOV AP OIDC)

Het Forum Standaardisatie adviseerde bij de bespreking van het Forumadvies op 14 juni 2023 om aan te sluiten bij de internationale conventie van namen voor profielen bij OIDC. De nieuwe naam voor het Nederlandse profiel wordt **'OpenID.NLGov'**. De beherende organisatie Logius heeft aangegeven na afloop van deze toetsingsprocedure de nieuwe naam door te voeren. Er is zodoende gekozen de naam 'NL GOV AP OIDC' te handhaven tot aan de afronding van deze toetsingsprocedure (incl. in dit document).

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. Dit leidt tot een betrouwbare digitale dienstverlening van de overheid voor burgers en bedrijven.

Inzet van Authenticatie-standaarden geeft de mogelijkheid om eenvoudig en veilig toegang te verkrijgen tot digitale (semi-)overheidsdienstverlening via een beperkt aantal authenticatieservices. 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.

Op basis van bespreking met inhoudsdeskundigen (SURF) en met Stuurgroep Open Standaarden is in overleg met de indiener Logius (7 april 2022) besloten 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 leden van het Forum Standaardisatie.

Het Forum Standaardisatie heeft op 14 juni 2023 ingestemd met het Forumadvies.

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 OIDC 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 authenticatieservices 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 bij afzonderlijke dienstverleners.

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 internet toegang te krijgen tot diensten van verschillende organisaties, zonder dat per dienst eigen inloggegevens nodig zijn of dat bij elke dienst apart moet worden ingelogd.