



Inventarisatie gebruiksgegevens MOS 2025

1



Inleiding	4
1. Domein veilig internet	5
DKIM, DMARC en SPF	5
DNSSEC	6
HTTPS & HSTS en TLS	8
IPv6 & IPv4	9
NEN-ISO/IEC 27001 en NEN-ISO/IEC 27002	10
NL GOV Assurance profile for OAuth 2.0	12
RPKI	13
Authenticatie-standaarden (OpenID.NLGov en SAML)	14
Security.txt	16
STARTTLS & DANE	17
STIX & TAXII	18
WPA2 Enterprise	19
2. Domein openbaar en toegankelijk	20
Ades Baseline Profiles	20
Digitoegankelijk	21
ODF en PDF	23
SKOS	28
3. Domein uitwisselingsfundament	32
OpenAPI Specification	32
REST_API Design Rules	32
Digikoppeling	33
Geo-Standaarden	36
StUF	39
4. Domein economie en werk	42
NLCIUS	42
SETU	43
WDO Datamodel	45
XBRL	48
5. Domein schoon water en beschermde bodem	50
Aquo-standaard	50
GWSW	52
SIKB0101 en SIKB0102	53

6.	Domein bouwen en wonen	56
	IFC	56
	NLCS	57
	VISI	58
7.	Domein bestuur en recht	61
	BWB	61
	JCDR	61
	ECLI	62
	EML_NL	62
8.	Domein onderwijs en cultuur	64
	E-Portfolio NL NEN 2035	64

Inleiding

Het doel van het open standaardenbeleid is een brede adoptie van de open standaarden van de lijst voor 'pas toe of leg uit', daar waar deze relevant zijn. De verplichting om deze standaarden toe te passen geldt voor gemeenten, provincies, rijk, waterschappen en alle uitvoeringsorganisaties inclusief gemeenschappelijke regelingen. Voor alle andere organisaties in de publieke sector geldt het gebruik van de 'Pas toe of leg uit'-standaarden als een dringend advies.

Het 'pas toe of leg uit'-beleid is gericht op de aanschaf van ICT, en dus op het toepassen van open standaarden bij aanbestedingen die leiden tot doorontwikkeling aan en vernieuwingen van het ICT-systeem. Bij het 'pas toe of leg uit'-regime gaat het om het vragen om open standaarden, en wordt niet gecontroleerd in hoeverre het gevraagde ook (volledig) is geleverd. Tenslotte kunnen overheden open standaarden ook toepassen, mogelijk zelfs zonder zich daarvan bewust te zijn, doordat zij voorzieningen of producten gebruiken waarin deze open standaarden toegepast zijn. Gegevens over het feitelijk gebruik geven een beeld voor het gehele ICT-systeem.

Voor een completer beeld van de adoptie is het feitelijk gebruik dus een interessante indicator. Net als in eerdere jaren is dit deelonderzoek dit jaar uitgevoerd door de accountmanagers van het Bureau Forum Standaardisatie (BFS). De accountmanagers hebben hiervoor contact opgenomen met beheer-organisaties achter de standaarden. Het is niet altijd even makkelijk om voor alle open standaarden vast te stellen in welke mate die feitelijk gebruikt worden.

Voor een aantal standaarden uit het domein Veilig Internet zijn de gebruiksgegevens afkomstig uit het halfjaarlijkse onderzoek naar internet-veiligheids-standaarden. De Meting IV-standaarden begin 2025 is ten tijde van het schrijven van deze monitor-rapportage gepubliceerd en is te vinden op de website van Bureau Forum Standaardisatie, de medio-2025 meting is daar nog niet terug te vinden. Voor deze monitor zijn relevante gegevens uit de begin-2025-meting beschikbaar gesteld

In aanvulling op de informatie afkomstig van accountmanagers en beheerders van open standaarden, is er ook geput uit de 'Quickscan leveranciers', van PBLQ. Dit jaar is ervoor gekozen om binnen het onderzoek naar gebruiksgegevensonderzoek in te zoomen op het leveranciersperspectief. Leveranciers zijn een belangrijke speler met betrekking tot de toepassing van open standaarden, omdat zij de ICT-voorzieningen aan de overheid leveren waar in de (open) standaarden worden toegepast. Het is daarom relevant om te horen hoe leveranciers tegen het beleid en het gebruik van open standaarden aankijken. Ten behoeve van de quickscan is met een beperkt aantal leveranciers en brancheorganisaties over hun opvattingen gesproken. Het onderzoek is ook als zelfstandige rapportage op de site van Forum Standaardisatie te vinden [P.M. link naar het rapport op <https://www.forumstandaardisatie.nl>]. In deze publicatie zijn bij een aantal standaarden relevante bevindingen uit de Quickscan opgenomen (herkenbaar aan de tussenkop: Quickscan Leveranciers). Die teksten betreffen de opvattingen van leveranciers over specifieke standaarden zoals opgetekend door PBLQ.

1. Domein veilig internet

DKIM, DMARC en SPF

Waarom belangrijk?

De hier genoemde drie standaarden voorkomen in onderlinge samenhang e-mailspoofing waardoor phishing uit naam van overheidsorganisaties wordt bemoeilijkt:

- DKIM: dit is een techniek waarmee e-mailberichten kunnen worden gewaarmerkt. Een domeinnaamhouder kan in het DNS-record van de domeinnaam aangeven met welke sleutel e-mail namens de betreffende domeinnaam ondertekend moet worden (op de ‘pas toe of leg uit’ lijst sinds juni 2012 - we vermelden telkens de oorspronkelijke plaatsing op de ‘pas toe of leg uit’-lijst);
- DMARC: maakt het mogelijk om beleid in te stellen over de manier waarop een e-mailprovider om moet gaan met e-mail waarvan niet kan worden vastgesteld dat deze afkomstig is van het vermelde afzenderdomein. Hierdoor kunnen organisaties voorkomen dat anderen e-mails versturen namens het e-maildomein van de organisatie (op de ‘pas toe of leg uit’-lijst sinds mei 2015);
- SPF: dit is een techniek waarmee een domeinhouder de IP-adressen van verzendende mailservers kan publiceren in de DNS. Een ontvangende mailserver kan deze IP-adressen gebruiken om te controleren of een e-mail daadwerkelijk afkomstig is van een verzendende mailserver van de betreffende domeinhouder (op de ‘pas toe of leg uit’-lijst sinds mei 2015).

Feitelijk gebruik

5 Als indicator voor het feitelijk gebruik van deze open standaarden kijken we naar de ondersteuning van DMARC, DKIM en SPF op 2.467 domeinen van de overheid (peildatum medio 2024).

In de meting wordt alleen gekeken naar de toepassing van standaarden op domeinnamen. Er wordt in de meting (nog) niet gekeken naar de validatie op de standaarden. Dat betekent dat validatie van de DMARC-, DKIM- en SPF-kenmerken door ontvangende mailservers van een overheidsorganisatie niet worden gemeten.

Tabel 1. DKIM, DMARC en SPF (2022 – 2025)

	voorjaar 2022	begin 2023	medio 2023 (n = 2.661)	begin 2024 (n = 2.611)	medio 2024 (n = 2.467)	begin 2025 (n = 2.319)
DMARC policy	72 %	79 %	81 %	83 %	83 %	85%
DKIM	82 %	84 %	85 %	86 %	88 %	89%
SPF Policy	87 %	87 %	87 %	86 %	90 %	92%

Het gebruik van anti-phishing standaarden ligt bij de hier gepresenteerde standaarden medio 2025 grofweg rond de 89%. We zien in de loop van de jaren dus **een lichte stijging**. DMARC is net als vorig jaar een relatieve achterblijver. De relatieve winst ten opzichte van vorig jaar bij die standaard is ook het kleinst, ook al zijn de onderlinge verschillen klein. Dat betekent voor nu dat voor 15% van de internetdomeinen nog een strikt DMARC-beleid operationeel moet worden om phishingmails uit naam van overheidsorganisaties te voorkomen. In een volgende monitor-rapportage kunnen deze cijfers verder in perspectief worden geplaatst.

Een uitsplitsing van de cijfers begin 2025 naar type overheid laat een volgend beeld zien (tussen haakjes de score van medio 2024).

Tabel 2 . DKIM, DMARC en SPF (2025)

	Centrale overheid (n=1586)	Provincies (n=23)	Water- schappen (n=27)	Gemeenten (n=357)	Gemeen- schappelijke regelingen (n=326)
DMARC policy	86 % (86%)	87% (88%)	93 % (93%)	96 % (93%)	67 % (61%)
DKIM	87 % (85%)	96 % (92%)	100 % (100%)	99 % (99%)	92 % (90%)
SPF Policy	91 % (89%)	91 % (92%)	96 % (97%)	97 % (96%)	92 % (92%)

In dit overzicht valt op dat vrijwel overal hogere of vergelijkbare percentages worden genoteerd als de meest recente score van om vergelijking met die van medio vorig jaar (uit de monitor 2023). De scores bij de waterschappen en de gemeenten is zo hoog dat daar bijna geen sprake meer is van groeipotentie.

Quickscan Leveranciers

Leveranciers zien dat DMARC vaak wordt uitgevraagd in aanbestedingen, terwijl deze in de ogen van de leverancier niet altijd relevant is voor het product dat door de leverancier wordt geleverd. Of de mailservice wordt door een andere partij geleverd, waardoor een leverancier deze standaarden niet zonder de hulp van de derde partij op een goede manier kan implementeren. Deze constatering doen leveranciers ook met betrekking tot de standaard STARTTLS en DANE.

6

DNSSEC

Waarom belangrijk?

Een domeinnaamhouder kan met DNSSEC een digitale handtekening toevoegen aan DNS-informatie. Met DNSSEC kan de ontvanger vervolgens de echtheid van de domeinnaam-informatie (waaronder IP-adressen) controleren. Dit voorkomt bijvoorbeeld dat een aanvaller het IP-adres ongemerkt manipuleert (DNS-spoofing) en daarmee verstuurde e-mails omleidt naar een eigen mailserver of gebruikers misleidt naar een frauduleuze website (op de ‘pas toe of leg uit’-lijst sinds juni 2012).

Feitelijk gebruik

Als indicator voor het feitelijk gebruik van deze open standaard kijken we wederom naar het gebruik van DNSSEC-handtekeningen op ongeveer 2.400 domeinen van de overheid.

DNSSEC-validatie (controle op handtekeningen) wordt (nog) niet gemeten in de IV-meting.

Tabel 3. DNSSEC (2022-2025)

	voorjaar 2022	begin 2023	medio 2023 (n = 2.600 ¹)	begin 2024 (n = 2.505 resp. 2.611)	medio 2024 (n = 2.332 resp. 2.467)	begin 2025 (n = 2120 web, 2319 e-mail)
DNSSEC						
web-domein	89 %	90 %	91 %	90 %	91 %	92 %
mailserver- domein	57 %	56 %	63 %	61 %	58 %	59 %

Bij webdomeinen is sprake van een hoge score (92%), voor mailserverdomeinen ligt dit beduidend lager (59%). Bij deze laatste variabele is ook sprake van een **geringe daling**, terug naar het niveau van het voorjaar 2022.

In een volgende monitor-rapportage kunnen deze cijfers in een verder-reikend perspectief worden geplaatst.

Een uitsplitsing van deze cijfers naar type overheid laat een volgend beeld zien.

Tabel 4. DNSSEC naar bestuurslaag (2025)

	Centrale overheid (n= 1.455 resp. 1.556)	Provincies (n=19 resp. 24)	Water- schappen (n=25 resp. 30)	Gemeenten (n=357 resp. 370)	Gemeen- schappelijke regelingen (n=264 resp. 352)
web-domein	91 % (91%)	95 % (88%)	100 % (100%)	99 % (99%)	83 % (83%)
mailserver- domein	71 % (76%)	29 % (33%)	67 % (30%)	58 % (53%)	32 % (30%)

Op webdomeinen scoren de verschillende categorieën overheid hoog tot zeer hoog, waarbij de gemeenschappelijke regelingen iets achterblijven (met altijd nog 83%); hetzelfde beeld als vorig jaar.

Bij maildomeinen scoort de centrale overheid enigszins hoger dan de Waterschappen die weer hoger scoren dan de Gemeenten en de rest. Achterliggende reden hierbij is dat cloud-dienstverleners voor email-verkeer deze standaard DNSSEC over het algemeen niet ondersteunen.

Relevante ontwikkeling

Microsoft heeft een start gemaakt om DNSSEC mogelijk te maken in Azure DNS (allereerst voor Microsoft Online Exchange ten behoeve van DANE).

Quickscan Leveranciers

Leveranciers zien DNSSEC - net als IPv4 & IPv6 - als zogenoemde 'no brainers' of 'industry-standards'. Het zijn standaarden die gemeengoed zijn en breed gedragen worden door de markt. Leveranciers erkennen aan de ene kant dat het goed is dat deze standaarden worden gepromoot door hun plek op de PTOLU-lijst, maar vragen zich ook af hoe nodig dit is. Leveranciers die de lijst nu te lang vinden zien deze standaarden als overbodig.

¹ Het exacte aantal varieert. Er zijn twee nieuwe meetmomenten (januari en juli 2023) en soms gaat het om het aantal webdomeinen en soms om het aantal email-domeinen. De preciese range is 2.593 – 2.710.

HTTPS & HSTS en TLS

Waarom belangrijk?

HTTPS & HSTS en ook TLS zorgen samen voor beveiligde verbindingen met websites, met als doel de veilige uitwisseling van gegevens tussen een webserver en client (vaak een webbrowser). Dit maakt het voor cybercriminelen moeilijker om verkeer om te leiden naar valse websites en om de inhoud van webverkeer te onderscheppen.

HTTPS zorgt voor het gebruik van HTTP over een met TLS beveiligde verbinding. Dit betekent dat het webverkeer door middel een certificaat wordt versleuteld.

HSTS zorgt ervoor dat een webbrowser, na het eerste contact over HTTPS, bij vervolfbezoek de website altijd direct over HTTPS opvraagt.

Deze standaarden staan op de 'pas toe of leg uit'-lijst sinds mei 2017.

TLS zorgt door middel van de uitwisseling van certificaten voor de versleuteling van gegevens tijdens het transport tussen internetsystemen. TLS staat op de 'pas toe of leg uit'-lijst sinds september 2014.

Feitelijk gebruik

Als indicator voor het feitelijk gebruik van deze open standaarden kijken we naar het gebruik op 2.319 webdomeinen (begin 2025).

Tabel 5. HTTPS & HSTS en TLS (2022-2025)

	voorjaar 2022	begin 2023 (n = 2.653)	medio 2023 (n = 2.593)	begin 2024 (n = 2.505)	medio 2024 (n = 2.332)	begin 2025 (n = 2.319)
HTTPS (red.)	92 %	93 %	94 %	94 %	91 %	92 %
HSTS	75 %	78 %	80 %	82 %	81 %	83 %
TLS cf. NCSC	75 %	77 %	79 %	81 %	83 %	86 %

Op basis van deze cijfers blijkt dat bij ruim vier van de vijf in het onderzoek betrokken webdomeinen de TLS- en HSTS-configuraties op orde zijn. Voor HTTPS ligt deze score hoger (meer dan negen van de tien). In volgende monitor-rapportages kunnen deze cijfers in een verder perspectief worden geplaatst. Er is sprake van een **lichte stijging** ten opzichte van de eerdere meting. Naarmate de scores hoger komen te liggen, wordt de ruimte om te verbeteren logischerwijs steeds kleiner.

Een uitsplitsing van deze cijfers naar type overheid laat een volgend beeld zien (peildatum: begin 2025, tussen haakjes de cijfers van medio vorig jaar).

Tabel 6. HTTPS & HSTS en TLS naar bestuurslaag (2025)

	Centrale overheid (n=1.455 resp. 1.556)	Provincies (n=19 resp. 24)	Water- schappen (n=25 resp. 30)	Gemeenten (n=357 resp. 370)	Gemeen- schappelijke regelingen (n=264 resp. 352)
HTTPS doorv.	90 % (90%)	100 % (89%)	100% 100%)	99 % (99%)	91 % (91%)
HSTS	81 % (81%)	94% (89%)	100 % (100%)	99 % (97%)	68 % (62%)
TLS cf. NCSC	86 % (83%)	88 % (94%)	91 % (88%)	89 % (89%)	83 % (75%)

De verschillen met de meting medio vorig jaar zijn niet groot. Oplopende en teruglopende percentages houden elkaar daarbij in evenwicht. De centrale overheid – met verreweg de grootste groep webdomeinen – laat een score zien die vrijwel overeenkomt met het overall beeld².

Verder valt op dat met name gemeenten en waterschappen hele hoge scores laten zien, gevolgd door de provincies die ook relatief hoog scoren. De gemeenschappelijke regelingen blijven achter. Als duiding daarvan is in een eerdere IV-meting verondersteld dat “... de streefbeeldafspraken niet doorgesijpeld [zijn] naar deze instanties, hoewel zij in veel gevallen gefinancierd worden vanuit de andere overheden.”

Relevante ontwikkeling

Met de inwerkingtreding van de Wet digitale overheid per 1 juli 2023 zijn overheden ook verplicht hun publiek toegankelijke websites en webapplicaties te beveiligen met de open standaarden HTTPS en HSTS.

9 Verder is NCSC bezig met het vernieuwen van de TLS-richtlijnen.

IPv6 & IPv4

Waarom belangrijk?

De standaard bepaalt dat ieder ICT-systeem binnen het netwerk een uniek nummer (IP-adres) heeft. Hierdoor kunnen ICT-systemen elkaar herkennen en onderling data uitwisselen. IPv6 heeft een veel grotere hoeveelheid beschikbare IP-adressen ten opzichte van de voorganger IPv4. Dit maakt verdere groei en innovatie van het internet mogelijk. IPv6 is niet backwards compatible. Dit wil zeggen dat een IPv4-systeem niet een IPv6-systeem kan bereiken, of andersom. Om die reden moet een organisatie bij de aanschaf van een ICT-product/-dienst beide versies uitvragen. De standaard staat op de ‘pas toe of leg uit’ lijst sinds november 2010.

Feitelijk gebruik

Als indicator voor het feitelijk gebruik van deze open standaard kijken we naar de bereikbaarheid van overheids-websites via de internetstandaard IPv6 voor 2.332 webdomeinen respectievelijk 2.467 domeinen voor e-mailverkeer van de overheid (meting medio 2024).

² De IV-monitor biedt aanvullend inzicht van deze categorie, uitgesplitst naar ministerie.

Tabel 7. IPv6 (2022-2025)

IPv6	voorjaar 2022	begin 2023 (n = 2.653 resp. 2.710)	medio 2023 (n = 2.593 resp. 2.661 ³)	begin 2024 (n = 2.505 resp. 2.611)	medio 2024 (n = 2.332 resp. 2.467 ⁴)	begin 2025 (n = 2.120 resp. 2.319)
Webverkeer	70 %	72 %	75 %	76 %	78 %	83 %
e-mailverkeer	50 %	54 %	56 %	53 %	57 %	83 %

De adoptie van IPv6 voor e-mailverkeer ligt in de meest recente meting op 83% een ruime stijging ten opzichte van vorig jaar. De score voor webverkeer is van vergelijkbaar niveau en ook gestegen ten opzichte van vorig jaar.

Een uitsplitsing van deze cijfers naar type overheid wijst het volgende uit (peildatum: begin 2025, tussen haakjes de cijfers van vorig jaar).

Tabel 8. IPv6 naar bestuurslaag (2025)

	Centrale overheid (n = 1455 web, 1586 e-mail)	Provincies (n = 19 web, 23 e-mail)	Waterschappen (n = 25 web, 27 e-mail)	Gemeenten (n = 357 web, 357 e-mail)	Gemeenschappelijke regelingen (n = 264 web, 326 e-mail)
webverkeer	81 % (76%)	89 % (71%)	100 % (97%)	97 % (96%)	70 % (64%)
Emailverkeer	78 % (61%)	85 % (67%)	85 % (60%)	90 % (67%)	85 % (36%)

10

. In vergelijking met vorig jaar is voor beide variabelen sprake van een flinke stijging. Gemeenten en Waterschappen scoren het best. Met name het verschil met de scores van webverkeer bij de gemeenschappelijke regelingen is groot, de gemeenschappelijke regelingen' hebben een enorme sprong gemaakt ten aanzien van de adoptie van Ipv6 voor het emailverkeer.

Quickscan Leveranciers

Leveranciers zien IPv4 & IPv6 - net als DNSSEC - als zogenoemde 'no brainers' of 'industry-standards'. Het zijn standaarden die gemeengoed zijn en breed gedragen worden door de markt. Leveranciers erkennen aan de ene kant dat het goed is dat deze standaarden worden gepromoot door hun plek op de PTOLU-lijst, maar vragen zich ook af hoe nodig dit is. Leveranciers die de lijst nu te lang vinden zien deze standaarden als overbodig.

NEN-ISO/IEC 27001 en NEN-ISO/IEC 27002

Waarom belangrijk ?

De NEN-ISO/IEC 27001-standaard bevat eisen waar het managementsysteem voor informatiebeveiliging aan dient te voldoen. De standaard werkt uniformerend ten aanzien van het informatiebeveiligingsbeleid. Deze standaard specificeert eisen voor het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van een gedocumenteerd Information Security Management System (ISMS) in het kader van de algemene bedrijfsrisico's van een organisatie.

³ Dit biedt de beste basis voor een vergelijking met vorig jaar..

⁴ Dit biedt de beste basis voor een vergelijking met vorig jaar..

De NEN-ISO/IEC 27002-standaard is een best practice van beveiligingsmaatregelen ('controls') om informatiebeveiligingsrisico's aan te pakken met betrekking tot vertrouwelijkheid, integriteit en beschikbaarheid van de informatievoorziening. De standaard kan gezien worden als een nadere specificatie van NEN-ISO/IEC 27001. ISO 27002 geeft richtlijnen en principes voor het initiëren, implementeren, onderhouden en verbeteren van informatiebeveiliging binnen een organisatie.

Beide standaarden staan op de 'pas toe of leg uit' lijst sinds 18 mei 2015

Burgers en bedrijven moeten ervan uit kunnen gaan dat de overheid zorgvuldig omgaat met hun gegevens. De overheid werkt veel samen met interne en externe partijen. Toepassing van een (inter)nationale beveiligingsnorm waarop partijen zich kunnen certificeren, helpt daarbij. Het hanteren van een internationale beveiligingsnorm helpt in de samenwerking met interne en externe partijen. Je kan hem hanteren als inkoopvoorwaarde, je kan er tegen certificeren, je kan hem hanteren als kennisgebied bij sollicitaties, de norm staat doorgaans niet ter discussie en het onderhoud op de norm is gratis.

Vanaf 1 januari 2019 is de Baseline Informatiebeveiliging Overheid (BIO) van kracht. De BIO vervangt de bestaande baselines voor Rijk, Gemeenten, Waterschappen en Provincies. De BIO is gebaseerd op de actuele, internationale standaard voor informatiebeveiliging (NEN-ISO/IEC 27001 en NEN-ISO/IEC 27002) en heeft risicomanagement als uitgangspunt. Alle overheidslagen hebben zichzelf verplicht de BIO toe te passen. Forum Standaardisatie heeft medio 2018 reeds geadviseerd om actief op adoptie van de BIO in te zetten, en de voortgang te monitoren. In reactie daarop heeft de werkgroep BIO aangegeven dat iedere overheidslaag zelf zal monitoren wat de voortgang is van de implementatie van de BIO.

Verantwoording over de beveiliging vindt in beginsel plaats aan de eigen controlerende organen.

Waterschappen

De waterschappen zijn bezig met de volwaardige implementatie van de BIO; zij gebruiken allen de BIO als normenkader voor informatiebeveiliging en bereiden zich actief voor op BIO2. Deze is aangevuld met de IEC62443, specifiek voor procesautomatisering

Naast de individuele verbeteracties wordt in gezamenlijkheid gewerkt aan het verhogen van de digitale weerbaarheid en veerkracht van zowel de sector, als ook die van ketenpartners. In onderlinge samenwerking wordt onder meer gewerkt aan de ontwikkeling van een sectormethodiek voor risicoanalyses en een CyberSecurity Implementatie Richtlijn (CSIR).

Door TNO is in opdracht van het ministerie van Infrastructuur en Waterstaat, in samenwerking met RWS een landelijke ketenanalyse uitgevoerd op de organisatie-overstijgende ketenrisico's. Ter beoordeling van de individuele en sectorale voortgang is in 2021 en 2023 door een onafhankelijke partij het volwassenheidsniveau van de waterschappen op informatieveiligheid (PA en KA) beoordeeld. De resultaten van deze audit zijn zowel op individueel, als ook op sectoraal niveau, door de auditor voorzien van aanbevelingen. Waterschappen werken zowel sectoraal als individueel aan het verhogen van de digitale weerbaarheid. In 2026 zal opnieuw een sector brede audit uitgevoerd worden. Hierbij is sprake van een accentverschuiving. Waar eerdere audits veel aandacht besteden aan de te implementeren maatregelen (uit ISO27002 en IEC62443) zal de aanstaande audit veel meer nadruk leggen op het managementsysteem conform ISO27001. Hier volgt de sector de ontwikkeling van BIO 1.04 naar BIO2.

In navolging van de vernieuwde ISO normering zal de BIO van versie 1.0.4zv naar 2 gaan. Er wordt op dit moment gewerkt aan de BIO2, deze wordt naar verwachting 2025 van kracht. Op 1 juni 2023 is een BIO2.0-opmaat handreiking gepubliceerd, deze is ingedeeld in lijn met ISO/IEC 27002:2022 en bevat actualisaties van een aantal maatregelen en meer nadruk op het managementsysteem. Dit past bij de ontwikkelingsfase van de waterschappen naar risicogestuurd werken en het sluiten van de PDCA, zoals ISO27001 beoogt. Certificering is daarbij op dit moment geen ambitie.

Waarom belangrijk?

NL GOV Assurance profile for OAuth 2.0 is een open standaard voor de beveiliging van overheidsapplicaties die gegevens uitwisselen met behulp van APIs. Met OAuth 2.0 kunnen gebruikers een website of webapplicatie autoriseren om hun (persoonlijke) gegevens via een API op te halen bij een ander systeem, zonder daarbij hun gebruikersnaam en wachtwoord uit handen te geven. OAuth 2.0 definieert hiervoor een aantal mechanismen. Zo heb je bijvoorbeeld "grants" (algemeen bekend als "flows"). Met behulp van verschillende flows kan het framework worden afgestemd op de beperkingen en beveiligingseisen van elk type applicatie. Webapplicaties zouden gebruik moeten maken van de authorization code flow. Mobiele applicaties moeten dezelfde authorization code flow gebruiken maar dan in combinatie met Proof Key for Code Exchange (PKCE); services kunnen gebruikmaken van client credentials, ondertekende "tokens" (JWT's) of mutual TLS (mTLS) flows. Als we die 'tokens' als voorbeeld nemen, zien we dat ze ingezet kunnen worden om toegang geven tot specifieke gegevens van één gebruikersaccount voor een bepaalde duur. De essentie van het Profiel op de OAuth 2.0 standaard is een aanscherping van de generieke invulling door het iGov profiel in de eindeloze mogelijkheden die OAuth 2.0 biedt. Dit profiel is dan ook van groot belang bij het correct en veilig inrichten en toepassen van OAuth. OAuth biedt de basis functionaliteit voor het realiseren van single Sign On (SSO) en het scheiden van applicaties en autorisaties. Het maakt het mogelijk om op een veilige manier mobiele apps en autonome apparaten te autoriseren om gegevens uit te wisselen. Vrijwel alle IOT, Social Media en Bancaire apps werken veilig op basis van OAuth. Maatschappelijk helpt dit de aanbieders en afnemers van APIs om op een eenduidige en veilige manier zich te authenticeren en autoriseren. Door deze standaard op de 'pas toe of leg uit'-lijst besparen we collectief veel tijd en middelen die anders nodig zijn om dergelijke API autorisatie keuzes voor iedere toepassing opnieuw te maken. Deze standaard staat op de 'Pas toe of leg uit' lijst sinds juli 2020.

Feitelijk gebruik

Het aantal vragen over deze standaard blijft redelijk constant en er is met name interesse in de toepassing van deze standaard in combinatie met de andere API standaarden zoals OAS, de API Design Rules en het Digikoppeling REST profiel. Binnen dat laatste is recent ook door het MIDO besloten om het gebruik van FSC standaard te verplichten. FSC is op een aantal vlakken geïnspireerd door OAuth maar focust zich met name op M2M API verkeer en toegang. Ook binnen het notificerenvraagstuk (FDS) is OAuth in het vizier.

Exacte gebruikscijfers zijn moeilijk te achterhalen aangezien Logius nog niks met compliance doet. Het is daarom nog niet mogelijk om aan te tonen hoeveel organisaties aan deze standaard voldoen. Vanuit de implementatieondersteuning en developer.overheid.nl weten we dat er vanuit Kadaster, 12 Rijkswaterstaat, Justitie, politie, KOOP, Logius, VNG en SSC-ICT met de standaard gewerkt wordt. Ook binnen de iGov werkgroep is het opgemerkt dat de adoptie bevorderd is, zeker binnen de EU.

Om dit om te buigen hebben wij contact opgenomen met developer.overheid.nl om samen een aantal pilots op basis van de specificatie te implementeren en vervolgens te beschrijven in blogs en dit mee te geven aan developers binnen de overheid als steunmiddel.

Relevante ontwikkeling

Afgelopen jaar is de standaard verder doorontwikkeld, denk bijvoorbeeld aan de "client credentials flow". Dit sluit aan bij de wens om PKI-overheid-certificaten te gebruiken voor het verifiëren van clientidentiteiten met beperkte API-rechten.

Ook zijn er een aantal RFC's verwerkt in het profiel: denk aan betere beschrijving rondom JWT's (RFC 9068, in lijn met opname in het upstream iGov profiel), maar ook een stuk over Token Exchange (RFC 8693), met name door de interesse van Geonovum.

Verder zijn er advanced security praktijken zoals PAR (RFC 9126), RAR(), DPOP (RFC 9449), Mutual-TLS Client Authentication and Certificate-Bound Access Tokens (RFC 8705).

In het inleidend document en zijn opaque tokens benoemd en een aantal use-cases geüpdatet of toegevoegd met oog op de nieuwe security features.

Ten slotte is er ook een verbeterslag gemaakt in de opmaak (incl. alle referenties) die we verder gaan trekken in een nieuwe release.

In 2025 wordt er een nieuwe versie van het profiel opgeleverd volgens de gebruikelijke procedures. Na goedkeuring door het MIDO zal deze versie worden aangemeld bij het Forum Standaardisatie. Op dit moment loopt de vaststelling van versie 1.1 bij het Forum, die in 2024 is aangemeld. De standaard heeft een sterke relatie met de OIDC standaard, ook van OpenID Foundation, welke wij ook onder de loep zullen nemen in 2025. Verder zien wij veel verbanden tussen OAuth en de ontwikkelingen op het gebied van stelsel toegang (EU en NL digital wallet incl. verifiable credentials, eDelivery, EIDAS en eHerkenning) en willen onze standaarden daar graag prominent positioneren.

Qua Expertadvies was het belangrijk om contact te houden met de deelnemers van de expertgroep. Dit omwille van het voorkomen van implementatieproblemen maar ook het op de hoogte te blijven van het gebruik van de standaard.

Hier hebben wij op ingespeeld en besloten met KP-API om de expertbijeenkomsten voorafgaand aan onze Technisch Overleggen te plannen.

RPKI

Feitelijk gebruik

Om een beeld te krijgen van het gebruik van RPKI zijn de afgelopen jaren in de vorm van een korte enquête enkele vragen voorgelegd aan deelnemers van Overheidsbrede Verdiepingssessies Connectiviteit, georganiseerd door Logius. De opbrengst van deze enquête was vorig jaar erg beperkt.

Dit jaar is voor een andere aanpak gekozen. Inmiddels kan immers worden beschikt over gemeten data omdat Internet.nl sinds vorig jaar een RPKI-testonderdeel heeft.

De vraagstelling is grotendeels wél hetzelfde als vorig jaar:

Zijn de IP-adressen die uw organisatie zelf beheert ondertekend met RPKI?

Zijn de IP-adressen van uw leveranciers ondertekend met RPKI?

Valideert uw organisatie RPKI-ondertekende IP-adressen?

De eerste twee vragen kunnen deels beantwoord worden met de resultaten uit die meting Informatieveiligheidsstandaarden.

Tabel 9. RPKI (2023-2025)

	begin 2023 (n = 2.653 resp. 2.710)	medio 2023 (n = 2.593 resp. 2.661)	begin 2024 (n = 2.505 resp. 2.611)	medio 2024 (n = 2.332 resp. 2.467)	begin 2025 (n = 2.120 web, 2.319 e-mail)
webverkeer	78 %	86 %	91 %	94 %	96 %
e-mailverkeer	75 %	87 %	90 %	93 %	95 %

De cijfers wijzen uit dat sprake is van een gestage groei.

Een uitsplitsing van deze cijfers naar type overheid wijst het volgende uit (peildatum: begin 2025, tussen haakjes de cijfers van de voorgaande meting).

Tabel 10. RPKI per bestuurslaag (2025)

	Centrale overheid (n = 1455 web, 1586 e- mail)	Provincies (n = 19 web, 23 e-mail)	Water- schappen (n = 25 web, 27 e-mail)	Gemeenten (n = 357 web, 357 e-mail)	Gemeen- schappelijke regelingen (n = 264 web, 326 e-mail)
webverkeer	97 % (94 %)	89 % (88 %)	96 % (93 %)	99 % (97%)	90 % (89 %)
e-mailverkeer	93 % (90 %)	95 % (95 %)	96 % (97 %)	97 % (96%)	96 % (94 %)

14

Wanneer we ons beperken tot bovenstaande uitkomsten van de IV-meting, kan worden vastgesteld dat over de gehele breedte van de overheid sprake is van **een duidelijke stijging** in de ondertekening van de gebruikte routes voor web- en e-mailverkeer. Het aantal netwerkleveranciers en IP adres aankondigingen is beperkt, waardoor het inregelen van ondertekening hiervan door één leverancier een groot effect kan hebben.

Voor de beantwoording van de derde vraag met betrekking tot validatie heeft dit jaar geen aanvullend onderzoek plaatsgevonden en is derhalve geen informatie beschikbaar.

Relevante ontwikkeling

In mei 2023 is er een streefbeeld voor RPKI vastgesteld dat deze voor het einde van 2024 moet worden geïmplementeerd. In de drie Rijksbrede connectiviteitsaanbestedingen CDR2023 van Rijkswaterstaat is RPKI meegenomen als vereiste.

Authenticatie-standaarden (OpenID.NLGov en SAML)

Waarom belangrijk?

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 is randvoorwaardelijk voor integrale dienstverlening binnen de digitale overheid en zorgt voor vertrouwde en veilige authenticatie voor burgers.

Bij SAML spelen drie partijen een rol: de ‘gebruiker’, de ‘Identity Provider (IdP)’ en de ‘Service Provider (SP)’. De IdP regelt het authenticatieproces van de gebruiker en kan na succesvolle authenticatie aan de SP-gegevens verstrekken over de identiteit, attributen en rechten van een gebruiker. SAML wordt gebruikt bij onder andere DigiD machtigen en eHerkenning. SAML is een internationale standaard die is ontwikkeld door de standaardorganisatie OASIS, en in een veelheid aan toepassingen kan worden geïmplementeerd. Er is geen centraal overzicht van toepassingen die op SAML gebaseerd zouden moeten zijn. Het is ook niet doelmatig om een dergelijk overzicht te creëren en actueel te houden. De standaard staat op de ‘pas toe of leg uit’ lijst sinds mei 2009.

Feitelijk gebruik

SAML is de standaard geworden voor (nieuwe) aansluitingen waarbij burgers of bedrijven inloggen bij de overheid. Twee belangrijke toepassingen van SAML in Nederland zijn eHerkenning en DigiD, waarmee bedrijven respectievelijk burgers zich kunnen authenticeren en identificeren bij overheden. Het aantal aansluitingen op deze voorzieningen is dan ook net als in voorgaande jaren als indicator genomen om het gebruik van SAML te meten.

Tabel 11. SAML (2018-2025)

	2018	2019	2020	2021	2022	2023	2024	2025
eHerkenning: SAML	359	439	458	493	n.b.	559	627 ⁵	651
DigiD: SAML	398	429	558	n.b.	n.b.	1.167	1.225	n.n.b.
eHerkenning + DigiD	757	868	1.016	n.b.	n.b.	1.726	1.876	n.n.b.

Bron: navraag bij de beheerders van eHerkenning en DigiD bij Logius (peildatum: zomer 2024).

Uit bovenstaand overzicht kan worden opgemaakt dat sprake is van een continue toename van het aantal aansluitingen en daarmee een gestage toename van het gebruik van SAML. eHerkenning blijft groeien, vooral in het ‘grijze’ gebied van de semi-overheid, maar ook bij Business-to-Business. De exacte reden van de groei bij DigiD is niet bekend maar wellicht speelt mee dat organisaties overstappen van CGI naar SAML en dat het opheffen van DigiD groepsaansluitingen een factor van betekenis is.

Gegevens met betrekking tot OIDC ontbreken nog voor deze monitor. De hoop is erop gevestigd dat hierover bij een volgende monitor meer valt te melden.

Relevante ontwikkeling

Sinds de introductie van DigiD 4.x koppelvlakken lijken de SAML-aansluitingen van DigiD- en eHerkenning heel veel op elkaar. Dat maakt het veel makkelijker voor dienstverleners om op allebei aan te sluiten. Buiten de Nederlandse overheid wordt steeds vaker OIDC gebruikt als protocol voor toegangsdiens ten. En op diverse plaatsen wordt binnen de Nederlandse overheid ook al met OIDC geëxperimenteerd.

Onlangs is een nieuw CombiConnect koppelvlak geïntroduceerd op basis van DigiD4.x SAML. Via dit koppelvlak kunnen zowel authenticaties bij DigiD alsook machtigen vanuit Machtigen worden opgehaald, zodat ook daar de operabiliteit kan worden vergroot. Daarnaast loopt momenteel bij DigiD een pilot voor het vervangen van SAML door OIDC voor het app2app koppelvlak, waarbij een 3rd party app met de DigiD app interacteert om te authenticeren. Beiden zijn nog niet op grote schaal uitgerold en hebben daarom nog geen effect op de gebruikscijfers.

⁵ Mei 2024

Waarom belangrijk?

Elke dag vinden beveiligingsonderzoekers (ook wel goedwillende of ethische hackers) digitale kwetsbaarheden in websites of IT-systemen. Vaak is het niet duidelijk wáár een beveiligingsonderzoeker een gevonden kwetsbaarheid kan melden. Er gaat daardoor mogelijk kostbare tijd verloren aan het bereiken van de juiste afdeling of persoon binnen de verantwoordelijke organisatie. Het gebruik van de security.txt-standaard kan helpen om dit te voorkomen. De standaard beschrijft hoe een organisatie onder meer contactinformatie kan publiceren die een beveiligingsonderzoeker vervolgens kan gebruiken om een gevonden kwetsbaarheid aan de betreffende organisatie te melden.

Met een security.txt-bestand kan een organisatie security-contactinformatie op haar webserver publiceren. Beveiligingsonderzoekers kunnen deze informatie gebruiken om direct contact met de juiste afdeling of persoon binnen de organisatie op te nemen over kwetsbaarheden die zij in de website of IT-systemen van de organisatie hebben gevonden.

Het formaat van het bestand is bedoeld om machinaal en menselijk leesbaar te zijn. De contactinformatie kan een e-mailadres, een telefoonnummer en/of een webpagina (bijvoorbeeld een webformulier) zijn. Merk op dat gepubliceerde contactinformatie openbaar is en ook kan worden misbruikt, bijvoorbeeld om spam te sturen naar een gepubliceerd e-mailadres.

Naast contactinformatie moet het security.txt bestand ook een vervaldatum bevatten. Het is optioneel om ook andere relevante informatie voor beveiligingsonderzoekers op te nemen, zoals een link naar het beleid voor het omgaan met meldingen van beveiligingskwetsbaarheden (meestal Coordinated Vulnerability Disclosure policy genoemd).

Feitelijk gebruik

Op dit moment is er geen informatie over het feitelijk gebruik van Security.txt.

Relevante ontwikkeling

In 2026 wordt naar verwachting de Cyberbeveiligingswet aangenomen in het parlement. Dit is de Nederlandse implementatie van de NIS2-richtlijn. In de richtlijn is ook een artikel overgenomen over het melden van kwetsbaarheden. In de concept wettekst van de Cyberbeveiligingswet is dit artikel opgenomen:

Artikel 17 (aanwijzing en taken coördinator bekendmaking kwetsbaarheden)

1. Bij of krachtens algemene maatregel van bestuur wordt een CSIRT aangewezen als de coördinator met het oog op een gecoördineerde bekendmaking van kwetsbaarheden.
2. De coördinator met het oog op een gecoördineerde bekendmaking van kwetsbaarheden heeft de volgende taken:
 - a) het optreden als tussenpersoon en het waar nodig vergemakkelijken van de interactie tussen de natuurlijke persoon of rechtspersoon die een kwetsbaarheid op grond van artikel 34 meldt en de fabrikant of aanbieder van de mogelijk kwetsbare ICT-producten of -diensten, op verzoek van een van beide partijen;
 - b) het identificeren van en contact opnemen met de betrokken entiteiten;
 - c) het bijstaan van de natuurlijke persoon of rechtspersoon die een kwetsbaarheid meldt;
 - d) het onderhandelen over tijdschema's voor de bekendmaking en het beheren van kwetsbaarheden die van invloed zijn op meerdere entiteiten; en
 - e) wanneer een gemelde kwetsbaarheid significante gevolgen kan hebben voor entiteiten in meer dan één lidstaat van de Europese Unie: het binnen het CSIRT-netwerk samenwerken met de door andere

lidstaten van de Europese Unie aangewezen coördinatoren met het oog op een gecoördineerde bekendmaking van kwetsbaarheden.

De security.txt-standaard kan ook een rol spelen in de uitoefening van deze verplichtingen, bijvoorbeeld als uitwerking van lid 2 sublid a en b.

STARTTLS & DANE

Waarom belangrijk?

STARTTLS maakt het mogelijk om SMTP-verkeer tussen mailservers over een met TLS versleutelde verbinding te laten lopen.

DANE, dat voortbouwt op DNSSEC, geeft zekerheid over de identiteit van de ontvangende mailserver. Dit voorkomt dat een aanvaller zich kan uitgeven als ontvangende-mailserver, waardoor hij het mailverkeer kan onderscheppen. Daarnaast dwingt DANE het gebruik van TLS af. Dit voorkomt dat een aanvaller de opzet van STARTTLS kan blokkeren, om zo toegang tot de onversleutelde berichten te krijgen.

STARTTLS & DANE staan op de ‘pas toe of leg uit’ lijst sinds september 2016.

Feitelijk gebruik

Als indicator voor het feitelijk gebruik van deze open standaarden kijken we naar de ondersteuning van STARTTLS en DANE op 1.405 (medio 2024) e-mailservers van de overheid. Voor wat betreft STARTTLS is getest of bij de mailservers STARTTLS is geconfigureerd zoals door het NCSC is aanbevolen. De test op DANE bestaat eruit dat wordt nagegaan of de nameservers van de mailservers één of meer TLSA-records voor DANE bevatten.

Tabel 12. STARTTLS & DANE (2022-2025)

	voorjaar 2022	begin 2023 (n = 1.502)	medio 2023 (n = 1.470)	begin 2024 (n = 1.438)	medio 2024 (n = 1.405)	begin 2025 (n = 1333)
STARTTLS cf. NCSC	81 %	84 %	89 %	88 %	93 %	93 %
DANE	46 %	46 %	44 %	43 %	40 %	51 %

Bij ruim negen op de tien e-mailservers (93%) is de STARTTLS-configuratie conform de richtlijnen van NCSC geconfigureerd; bij iets minder dan één op de tien moet dat nog gebeuren. De score blijft oplopen. DANE scoort met 51% laag in vergelijking met de andere standaarden die in de IV-meting zijn meegenomen. Er is in vergelijking met voorgaande metingen van enige groei sprake

Een uitsplitsing van deze cijfers naar type overheid levert het volgende beeld op (peildatum: begin 2025, tussen haakjes de cijfers van medio vorig jaar).

Tabel 13. STARTTLS & DANE per bestuurslaag (2025)

	Centrale overheid (n = 625)	Provincies (n=20)	Water- schappen (n=27)	Gemeenten (n=348)	Gemeen- schappelijke regelingen (n=313)
STARTTLS cf. NCSC	92 % (93%)	94 % (100%)	93 % (97%)	95 % (93%)	93 % (91%)
DANE	62 % (59%)	41 % (11%)	63 % (31%)	55 % (33%)	25 % (15%)

De verschillende categorieën overheden ontlopen elkaar weinig waar het gaat om de toepassing van STARTTLS. Bij de meeste overheidslagen is sprake van een stijging van het percentage. Bij DANE ligt dat anders. Terwijl de centrale overheid, waterschappen en gemeenten met een percentage ruim boven de 50% relatief goed scoren, blijven de provincies en vooral de gemeenschappelijke regelingen duidelijk achter; het beeld van vorig jaar herhaalt zich op dit punt.

Relevante ontwikkeling

Microsoft heeft een start gemaakt om DANE mogelijk te maken op Microsoft Online Exchange (Office 365).

Quickscan Leveranciers

Leveranciers zien dat STARTTLS en DANE vaak worden uitgevraagd in aanbestedingen, terwijl deze in de ogen van de leverancier niet altijd relevant zijn voor het product dat door de leverancier wordt geleverd. Of de mailservice wordt door een andere partij geleverd, waardoor een leverancier deze standaarden niet zonder de hulp van de derde partij op een goede manier kan implementeren. Deze constatering doen leveranciers ook met betrekking tot DMARC.

STIX & TAXII

Waarom belangrijk?

STIX en TAXII zijn standaarden voor partijen die cybersecurity informatie verwerken voor het beveiligen van hun informatiesystemen. Het is daarbij van belang om aan te sluiten op actuele bronnen van cybersecurity informatie en om onderling informatie uit te wisselen. Zodoende kunnen organisaties tijdig de juiste maatregelen nemen om hun systemen tegen actuele cyberdreigingen te beschermen.

Daarbij is STIX een gegevensopslagformaat dat gebruikt wordt voor het beschrijven van kwetsbaarheden en incidenten. TAXII is een protocol voor de uitwisseling van deze gegevens. Het gebruik van deze standaarden is een belangrijke stimulans voor de versterking van de weerbaarheid tegen cyberdreigingen. Met plaatsing van de standaarden op de pas-toe-of-leg-uit lijst worden organisaties gestimuleerd om bij de verwerving van cybersecurity producten en -diensten de standaarden op te nemen in het programma van eisen. De standaarden STIX en TAXII staan op de 'pas toe of leg uit' lijst sinds november 2017.

Feitelijk gebruik

Het NCSC heeft geen zicht op het feitelijke gebruik van de standaarden. Als indicator voor het gebruik van de standaarden binnen de Rijksoverheid gebruiken we het aantal aansluitingen op het Nationaal Detectienetwerk (NDN). Bij de uitwisseling van cybersecurity-informatie binnen het NDN worden de standaarden in ieder geval gebruikt. Binnen de Rijksoverheid is een groot deel van de organisaties (166 van de 209) aangesloten bij het NDN waarvan 99 organisaties zijn aangesloten via de sensor van een shared service organisatie. Dat geeft een dekkingsgraad van 79%.

Zowel in absolute aantallen als in dekkingsgraad zijn de aantallen ten opzichte van de vorige rapportage niet noemenswaardig veranderd. Dit is een teken dat de inzet van sensoren bij de bescherming tegen cyberdreigingen een grote mate van dekking bereikt heeft. De aansluitingen zijn het afgelopen jaar echter wel bijna allemaal vernieuwd en overgezet naar de nieuwe versie van de standaarden.

Relevante ontwikkelingen

Bij de vorige rapportage is al gemeld dat sinds 2021 nieuwe versies van de standaarden beschikbaar ter vervanging van STIX 1.2.1 en TAXII 1.1.1 die nu nog op de pas-toe-of-leg-uit lijst staan. De actuele versies zijn STIX 2.1 en TAXII 2.1 die dus ook door het NCSC worden gebruikt en aanbevolen. Het Forum voor

Standaardisatie is samen met het NCSC een procedure gestart om de pas-toe-of-leg-uit lijst met deze nieuwe standaarden aan te passen.

Een andere belangrijke ontwikkeling is dat naar verwachting dit najaar de nieuwe Cyberbeveiligingswet (Cbw) in werking treedt als Nederlandse implementatie van de Europese NIS2 richtlijn. Deze wet omvat een registratieplicht voor een groot aantal (essentiële en belangrijke) organisaties en bedrijven. Voor deze entiteiten geldt tevens een zorgplicht voor het nemen van beveiligingsmaatregelen en een meldplicht voor cybersecurity-incidenten. De standaarden STIX en TAXI zullen een belangrijke rol spelen bij het inrichten van alle kanalen en voorzieningen om deze Cbw-verplichtingen uit te voeren.

WPA2 Enterprise

Geen gegevens aangeleverd.

2. Domein openbaar en toegankelijk

Ades Baseline Profiles

Waarom belangrijk?

Een elektronische handtekening wordt gebruikt voor het ondertekenen van digitale berichten en documenten. Voor de ontvanger is het een bewijs dat een bericht afkomstig is van de ondertekenaar. De Ades Baseline Profiles beschrijven de minimale gegevens die uitgewisseld moeten worden om aan de eisen van een geavanceerde elektronische handtekening te voldoen. Dat zijn rechtsgeldige handtekeningen van een hoog betrouwbaarheidsniveau.

Door elektronische ondertekeningen met toepassing van de AdES Baseline Profiles weet een verzender zeker dat de ontvanger de elektronische handtekening kan valideren. Een valideerbare handtekening is voor de ontvanger het bewijs dat een elektronisch document inderdaad afkomstig is van de ondertekenaar (authenticiteit), dat de ondertekenaar de inhoud van het document onderschrijft (onweerlegbaarheid) en dat er niet met de ondertekening gerommeld is (integriteit).

De AdES Baseline Profiles leggen vast hoe de onderliggende AdES standaarden worden gebruikt. Ze worden toegepast bij het ondertekenen van XML-documenten (XAdES), PDF-documenten (PAdES), CMS-documenten (CAdES) en documentcontainers/ZIP (ASiC) en tegenwoordig ook voor het machine-leesbare JSON-formaat (JAdES).

20

AdES Baseline Profiles zijn sinds 9 mei 2017 verplicht aan de overheid ('Pas toe of leg uit'-verplichting). Opname van AdES Baseline Profiles op de 'Pas toe of leg uit'-lijst verplicht verzenders om AdES Baseline Profiles te gebruiken als zij documenten voorzien van een geavanceerde of gekwalificeerde digitale handtekening. Zo draagt de verplichting van AdES Baseline Profiles bij aan betrouwbare overheid door een eenduidige manier te bieden om digitale documenten elektronisch te ondertekenen.

Feitelijk gebruik

Over feitelijk gebruik van deze standaard is helaas net als in achterliggende jaren geen informatie beschikbaar.

Relevante ontwikkelingen

De verplichting aan de overheid van AdES Baseline Profiles volgens het 'Pas toe of leg uit'-regime is in 2023 geëvalueerd via een extern evaluatie-onderzoek. Uit het evaluatieonderzoek kwam naar voren dat de verplichting van AdES Baseline Profiles aan de overheid niet ter discussie staat. Het gebruik van elektronische geavanceerde en gekwalificeerde handtekeningen neemt toe en zal ook verder toenemen. De AdES Baseline Profiles hebben daarbij als volwassen standaard een stevige plek ingenomen. Wel is signaleerd dat de Nederlandse overheid een sturende rol (regierol) moet hebben voor het stimuleren van het gebruik van de standaard om een 'community' vorm te geven van partijen die kennis hebben over dit onderwerp.

De wereld van geavanceerde en gekwalificeerde elektronische ondertekening is volop in ontwikkeling. De belangrijkste ontwikkelingen zijn:

- Toename van het system-to-system (berichten-)verkeer

De toename van het system-to-system (berichten-)verkeer met een steeds breder palet aan content (naast documenten, rapporten ook streaming en rich content) en de steeds hogere betrouwbaarheidseisen daaraan. Binnen dit system-to-system verkeer is er behoefte om langjarig rechtsgeldigheid van overeenkomsten, machtigingen en afspraken te borgen. Eenduidige toepassing van de standaard is nodig om

te borgen dat dit verkeer inderdaad met de gewenste interoperabiliteit kan plaatsvinden. De grote uitdaging in Nederland is het system-to-system berichtenverkeer op een gestandaardiseerde manier in te richten.

- Invoering van EDI-wallet

Onder het European Digital Identity (EUDI) amendement op de eIDAS verordening wordt de Europese Digitale Identiteit (EDI) wallet ingevoerd. De gekwalificeerde elektronische handtekening heeft daar een plek in; dit zal de dynamiek rond elektronisch ondertekenen beïnvloeden en het gebruik er van doen toenemen. De vraag in hoeverre verplichtingen met betrekking tot AdES Baseline Profiles worden gespecificeerd in de Europese verordening, kan van invloed zijn voor het blijven verplichten van de standaard aan de overheid ('Pas toe of leg uit'-verplichting).

- Inwerkingtreding Wet modernisering elektronisch bestuurlijk verkeer

De inwerkingtreding van de Wet modernisering elektronisch bestuurlijk verkeer (Wmebv) in 2024 schrijft voor dat burgers voor een aantal producten en diensten digitaal zaken moeten kunnen doen met de overheid. Voor een aantal diensten en producten geldt een eIDAS 'substantieel' of 'hoog' betrouwbaarheidsniveau. Toepassing van AdES Baseline Profiles is daarbij relevant.

Digitoegankelijk

Waarom belangrijk?

Digitoegankelijk is de Nederlandse naam voor de Europese norm 301 549 die voorziet in toegankelijkheidsrichtlijnen voor overheidswebsites en de documenten die daarop gepubliceerd zijn. EN 301 549 verwijst naar de technische standaard WCAG 2.1 van W3C die specificeert hoe content op websites, in webapplicaties en in documenten toegankelijk kan worden gemaakt. Daarnaast beschrijft EN 301 549 instructies voor het inkopen van toegankelijke producten en diensten. Door toepassing van Digitoegankelijk worden websites, webapplicaties en documenten voor iedereen toegankelijk, ook voor ouderen en mensen met functiebeperkingen. Bij dit laatste kan het gaan om een permanente (bijvoorbeeld dyslexie, kleurenblind, slechthorend, slechtziend, motorisch beperkt), een tijdelijke (bijvoorbeeld een gebroken pols) of een situationele functiebeperking (bijvoorbeeld in de zon, in de trein of met een baby op de arm). Zo krijgt iedereen altijd dezelfde toegang tot overheidsinformatie. Vanaf 23 september 2020 is toepassing van deze standaard wettelijk verplicht. De standaard staat op de 'pas toe of leg uit' lijst sinds oktober 2016.

Feitelijk gebruik

Voor 2023 is voor zicht op het feitelijk gebruik van de standaard gebruik gemaakt van metingen door de Stichting Accessibility (inmiddels onderdeel van Bartiméus): een nulmeting uit 2019 en een tweede meting in 2021.

Inmiddels biedt Logius een Dashboard (dashboard.digitoegankelijk.nl) aan. Het dashboard, gelanceerd in maart 2023, geeft een totaalbeeld van alle websites en apps van overheidsorganisaties.

Bij de vorige monitor open standaarden is gebruik gemaakt van informatie uit dit dashboard.

Op de peildatum 22 augustus 2024 was de Nederlandse overheid verantwoordelijk voor 9.017 websites en mobiele apps. Op 11 juni 2025 staan er 8.849 websites en apps in het dashboard.

Een volgende stap in het monitoren van de digitale toegankelijkheid is gezet met het verschijnen van de jaarmonitor Digitale Toegankelijkheid. Deze monitor biedt inzicht in de ontwikkelingen bij de overheid over opeenvolgende jaren. Onderstaand beeld is ontleend aan deze Jaarmonitor Digitale Toegankelijkheid.

Tabel 14. Dlgitoegankelijk (2021 - 2024)

		A	B	C	D	E	Totaal A-D
Rijk	2021	56	494	357	134		1.041
	2022	84	603	324	143		1.154
	2023	94	606	301	327	537	1328
	2024	94	791	234	447	209	1566
	'23 > '24	0%	31%	-22%	37%	-61%	18%
Provincies	2021	11	25	28	77		141
	2022	11	43	64	84		202
	2023	13	88	79	80	257	260
	2024	13	176	75	101	123	365
	'23 > '24	0%	100%	-5%	26%	-52%	40%
Waterschappen	2021	3	31	15	4		53
	2022	1	42	12	5		60
	2023	3	44	12	18	122	77
	2024	5	77	45	38	14	165
	'23 > '24	67%	75%	275%	111%	-89%	114%
Gemeenten	2021	141	429	520	470		1.560
	2022	210	572	504	518		1.804
	2023	279	735	791	1.122	2.573	2927
	2024	433	1.346	583	1.756	1.370	4118
	'23 > '24	55%	83%	-26%	57%	-47%	41%
Totaal (álle overheidswebsites en apps)	2021	241	979	920	685		2.825
	2022	306	1.260	904	750		3.220
	2023	464	1894	1419	1850	4187	5627
	2024	672	2897	1066	2884	2133	7519
	'23 > '24	45%	53%	-25%	56%	-49%	34%

22

Let op:

- Met een status A, B of C wordt voldaan aan de wettelijke verplichting;
- De scope van DigiToegankelijk is anders dan de pas-toe-of-leg-uitlijst. De wettelijke verplichting rond digitale toegankelijkheid geldt voor alle overheidsorganisaties en niet alleen voor de medeoverheden.

Naar aanleiding van een inventarisatiecampagne in juni 2023 zijn in de tweede helft van dat jaar veel websites en apps zonder toegankelijkheidsverklaring toegevoegd aan het dashboard met status E. In 2024 is het aantal E-statussen met 49% afgenomen. Veel van de websites en apps met status E zijn in 2024 voorzien van een toegankelijkheidsverklaring, opgeheven of verwijderd uit het register omdat er geen overheidsinstantie voor verantwoordelijk is.

Met betrekking tot de websites en apps met Status A tot en met D kan naar aanleiding van bovenstaand overzicht het volgende worden geconcludeerd:

- Voor status A, B en D geldt dat in 2024 sprake is van een stijging;
- Het aantal websites met status C is met 25% gedaald. Sinds 1 april 2024 worden verklaringen die langer dan een half jaar een C-status automatisch teruggezet naar een D-status;

- Het aantal websites en apps dat voldoet aan de wettelijke verplichting (status A, B of C) is in 2024 gegroeid met 23%;
- Het aantal websites dat volledig voldoet aan de toegankelijkheidseisen (status A) is in 2024 met 45% gestegen;
- Deze positieve ontwikkelingen zijn met name bij gemeenten terug te vinden.

Uiteindelijk doel is dat aan alle websites en apps status A kan worden toegekend, maar dat kan in stappen worden bereikt. Met status A, B of C wordt al aan de wet voldaan (met status D nog niet). In de wet (Besluit digitale toegankelijkheid overheid) is onder andere ook geregeld dat er waar dat nodig is ook voortgang wordt geboekt:

- De afgegeven toegankelijkheidsverklaring moet minstens 1 keer per jaar worden geüpdatet;
- Als er tussendoor iets verandert, moet dat direct worden verwerkt in de afgegeven verklaring;
- Aan de updates moet kunnen worden afgelezen dat sprake is van verbetering.

Relevante ontwikkeling

De belangrijkste ontwikkelingen (ambities) op dit moment zijn:

- Er wordt gewerkt aan een mijn-omgeving. Het dashboard en de invulassistent van de toegankelijkheidsverklaring worden dan met elkaar verweven tot één omgeving waar een organisatie centraal toegang heeft tot haar verklaringen en waarin we ook notificaties kunnen sturen. Deze omgeving zal in de tweede helft van 2025 live gaan;
- NLdoc (een publicatietool om ontoegankelijke documenten te converteren naar toegankelijke HTML) zal ook in de tweede helft van 2025 live gaan.

ODF en PDF

Waarom belangrijk ?

PDF is een format voor de uitwisseling van documenten die bedoeld zijn om op te slaan of af te drukken, en waarvan de pagina opmaak vastligt. Het uitgangspunt van PDF is dat gebruikers documenten kunnen uitwisselen, opslaan en afdrukken, onafhankelijk van de omgeving waarin ze zijn aangemaakt. Een PDF-document ziet er op alle apparaten en in alle omgevingen hetzelfde uit. PDF is minder geschikt voor het publiceren van online informatie die veel op mobiele apparaten wordt bekeken. De door ISO gestandaardiseerde PDF/A-1 en A-2 (hierna: PDF/A) en PDF 1.7 varianten staan op de 'Pas toe of leg uit'-lijst sinds resp. 2008, 2012 en 2009. Het verplichtende karakter van een plaats op de 'Pas toe of leg uit'-lijst draagt eraan bij dat het aandeel bestanden op overheidswebsites dat voldoet aan de PDF-standaarden langzaam maar zeker toeneemt.

ODF is een applicatie- en leveranciersafhankelijke open standaard voor de uitwisseling van bewerkbare documenten. ODF is duurzaam toegankelijk: in de toekomst blijven ODF-bestanden leesbaar en bewerkbaar, ongeacht de kantoorapplicaties die op dat moment al dan niet worden ondersteund. Dankzij deze structuur kunnen zoekmachines ODF-bestanden goed indexeren en vinden. Alle gangbare kantoorapplicaties kunnen ODF-bestanden lezen en schrijven: het gebruik van het standaardformat ODF staat los van het al dan niet gebruiken van open source kantoorapplicaties. ODF staat op de 'Pas toe of leg uit'-lijst sinds 15 juni 2012. Het blijft zinvol om ODF op de 'Pas toe of leg uit'-lijst te handhaven. Als ODF van de 'Pas toe of leg uit'-lijst zou verdwijnen, dan hebben organisaties geen dwingende reden meer om ODF uit te vragen in hun aanbestedingen. Daarmee kan de leveranciersafhankelijkheid toenemen, ook voor burgers en bedrijven die met de overheid willen communiceren.

Feitelijk gebruik

De resultaten van de meting voor gebruiksgegevens van PDF en ODF door Bureau Forum Standaardisatie van mei en juni 2025 laten zien dat de trends ten opzichte van voorgaande jaren een lichte verschuiving tonen. Ook in 2025 zijn nog steeds veruit de meeste documenten op overheidswebsites van het type PDF, voldoet ruim de helft van deze PDF bestanden aan open ISO-standaarden en is slechts een klein percentage ervan digitaal toegankelijk. Voor de publicatie van bewerkbare documenten wordt nog altijd overweldigend veel vaker een Microsoft Office format gebruikt dan het open format ODF ondanks een lichte stijging. In deze paragraaf worden deze trends onderbouwd met de resultaten van de meting die in mei en juni 2025 werd uitgevoerd.

De meting is gedaan op basis van een steekproef bij overheidsorganisaties die vallen binnen het organisatorisch werkingsgebied van de ‘Pas toe of leg uit’-lijst. De steekproef bestaat uit een totaal van 93 organisaties uit verschillende delen van de overheid:

- 30 veel bezochte websites van de Rijksoverheid (volgens Communicatie Rijk);
- de 30 grootste gemeenten;
- de 12 provincies;
- de 21 waterschappen.

Voor deze meting zijn op elke onderzochte website de gepubliceerde documenten gezocht en is bepaald van welk type de documenten zijn. Daarbij wordt onderscheiden tussen PDF, ODF (.odt, .ods, .odp) en Microsoft Office (.docx, .xlsx, .pptx, .doc, .xls, .ppt) bestanden. Verder wordt op elke website één willekeurig PDF-document van na 2018 gekozen en wordt vastgesteld of de PDF voldoet aan de standaarden (PDF/A (A-1 en A-2), PDF 1.7) die op de ‘Pas toe of leg uit’-lijst staan. Ook wordt vastgesteld of het willekeurig gekozen bestand PDF bestand digitaal toegankelijk is.

De meting is dit jaar door dezelfde organisatie en op dezelfde manier uitgevoerd als in 2021, 2022 en 2023 (in 2024 heeft er geen meting plaatsgevonden). Voor het tellen van documenten op websites gebruiken wij net als in de voorgaande jaren [Google search \(https://www.google.com\)](https://www.google.com) vanwege continuïteit in de onderzoeksmethoden. Door de aard van commerciële zoekmachines moet rekening worden gehouden met een zekere meetfout. Zoekmachines vinden niet noodzakelijk alle documenten op een website. Anderzijds kunnen de zoekresultaten door *caching* (lokale kopieën) op de zoekmachine referenties bevatten naar documenten die al niet meer geldig zijn. Dit is een nadeel van de huidige meetmethode maar vooralsnog is er nog geen werkbaar alternatief voor. De inzet van een eigen ‘crawler’ bleek in voorgaande jaren nog grotere problemen met zich mee te brengen.

Uit de meting van 2025 die hieronder wordt gepresenteerd, kunnen slechts trends worden opgemaakt, gebaseerd op een steekproef (tussen haakjes de gegevens uit respectievelijk 2023, 2022 en 2021).

Tabel 15. PDF en ODF (2021-2025)

		Top 30 overheid	G30 gemeenten	Provincies	Waterschappen
Aantal gevonden PDF	2025	419.321	137.072	171.707	17.024
	2023	299.141	184.663	143.945	15.885
	2022	396.552	220.320	135.457	19.126
	2021	312.540	183370	150451	19.711

Aantal gevonden ODF	2025	6.403	31	20	2
	2023	839	54	164	1
	2022	876	5	127	0
	2021	952	15	181	3
Aantal gevonden MS Office	2025	17.261	6064	27.630	232
	2023	14.649	9.324	13.155	165
	2022	16.060	10.241	9.150	278
	2021	14.523	17928	10886	348
Percentage PDF van alle gevonden documenten	2025	94,66%	95,74%	86,13%	98,64%
	2023	95,08%	95,17%	91,53%	98,97%
	2022	95,90%	95,56%	93,59%	98,57%
	2021	95.28%	91.09%	93,15%	98.25%
Percentage ODF van de gevonden bewerkbare documenten	2025	27%	<1%	<1%	<1%
	2023	5%	<1%	1%	1%
	2022	5%	<1%	1%	0%
	2021	6%	<1%	2%	1%
Percentage ISO PDF	2025	63%	46%	82%	63%
	2023	54%	55%	31%	61%
	2022	33%	55%	31%	52%
	2021	35%	45%	33%	67%
Percentage digitaal toegankelijke PDF	2025	17%	11%	9%	0%
	2023	8%	4%	8%	0%
	2022	0%	7%	0%	0%
	2021	23%	7%	17%	0%

De belangrijkste observaties naar aanleiding van dit overzicht:

In 2025 was er over het geheel genomen sprake van een stijging van 18% aan documenten op websites van overheden. Bij het Rijk nam het aantal PDF-bestanden het meeste toe. Alleen bij de gemeentes nam het aantal documenten juist flink af.

PDF blijft veruit het meest gebruikte format voor de publicatie van documenten. Over alle gemeten websites heeft 93% van de documenten een PDF-format. Dat is vergelijkbaar met de percentages die wij in voorgaande jaren vonden.

De aantallen PDF-bestanden die wij op Rijksoverheidswebsites vinden, verschillen enorm. Op twee websites staan veruit de meeste PDF bestanden in vergelijking met de andere onderzochte Rijksoverheidswebsites. De

eerste website is overheid.nl. Dit is geen verrassing omdat overheid.nl alle wetten en veel openbare overheidsinformatie publiceert. Overheid.nl biedt dezelfde wetteksten overigens ook in andere formats aan, waaronder HTML, zodat de gebruiker zelf het meest geschikte format kan kiezen. De andere website is werk.nl, met net iets meer PDF-bestanden dan overheid.nl. Werk.nl kent daarmee een grote toename ten opzichte van 2023. Mogelijk dat werk.nl in de tussentijd een ander beheer- en publicatieapplicatie in gebruik heeft genomen. Aan de andere kan van de schaal zijn er ook Rijksoverheidswebsites waar nauwelijks PDF-bestanden op te vinden zijn, zoals kvk.nl, svb.nl, kadaster.nl, werkenbijdefensie.nl en rijkshuisstijl.nl

Van de steekproef van 93 PDF-bestanden (1 per onderzochte organisatie) voldeed 60% aan de ISO-standaard PDF 1.7 of PDF/A op de 'Pas toe of leg uit'-lijst. Dat is meer dan in 2023 (toen 54%). Van alle overheden doen de waterschappen het het beste.

Van de steekproef van 93 PDF-bestanden van na 2018 is slechts 10% in voldoende mate digitaal toegankelijk. Dit is meer dan de 5% in 2023. Wel moeten wij hierbij aantekenen dat de steekproef de uitkomst bepaalt. De steekproef heeft ieder jaar nagenoeg dezelfde omvang maar bestaat ieder jaar uit een verschillende verzameling willekeurig gekozen documenten. Het kan dus zijn dat we per toeval meer, dan wel minder, digitaal toegankelijke documenten treffen. Desondanks laat het resultaat duidelijk zien dat het aantal digitaal toegankelijke PDF bestanden op overheidswebsites erg laag is.

Ongeveer 10% van de onderzochte Rijksoverheidswebsites publiceert geen of vrijwel geen informatie meer in PDF. Dit aantal is iets minder dan in 2023. Het vermijden van PDF-bestanden heeft vaak een positief effect voor de digitale toegankelijkheid van de website. De Rijksoverheid blijft hierin een voorloper: 23% van 30 veel geraadpleegde websites van de Rijksoverheid hebben (vrijwel) geen PDF's meer. Een aantal organisaties hanteert een HTML-first beleid, wat de digitale toegankelijkheid ten goede komt. Voorbeelden hiervan zijn de Geonovum of de gemeente Tilburg.

26

ODF vormt 11% van de bewerkbare documenten op alle onderzochte websites. Dat is stijging ten opzichte van 2023, met dit voorbehoud dat deze stijging het directe gevolg is van een significante toename van het aantal publicaties in ODF format op *alleen* de website overheid.nl.

We zien dat er partijen zijn die hun informatie via nevenschikking in open standaard formats aanbieden, in andere woorden, de gebruiker kan kiezen in welke standaard format (PDF, OOXML (.docx, .xlsx) of ODF (.odt, .ods)) de gebruiker de informatie wil raadplegen ('exporteren'), in plaats van in de alleen door de partij aangeboden standaard format (meestal PDF). Dit is een goede ontwikkeling. Deze nevenschikking is wel van invloed op de gebruikte meetmethode: zo telde de zoekmachine in deze gevallen niet per definitie informatie in *alle* aangeboden standaard formats maar slechts in een *aantal* aangeboden standaard formats; dat zorgt voor een incompleet totaalbeeld. Zodoende is ervoor gekozen de resultaten van de meting van in ieder geval één gemeentelijke website niet mee te nemen in de totaalverwerking van deze onderzoeksresultaten.

Op basis van de meetresultaten en observaties kan een aantal trends worden onderscheiden in het gebruik van open documentstandaarden:

Het **aantal documenten** op websites van de overheid lijkt **toegenomen** ten opzichte van vorig jaar, zelfs als we de (aanzienlijke) meetfout in aanmerking nemen die zoekmachines veroorzaken. De meting toont aan dat de daling van het aantal documenten op websites in 2023 niet heeft doorgezet. In het geval van PDF-bestanden lijkt er sprake van een krachterspel van twee wetten: [Wet digitale overheid](#) die digitale toegankelijkheid verplicht (waaronder ook voor PDF bestanden) waardoor overheden steeds meer inzetten op publiceren via HTML in plaats van via PDF-bestanden, en [Wet open overheid](#) die overheden juist aanzet tot proactief publiceren van documenten.

Ruim meer dan de helft (60%) van de PDF-bestanden uit de steekproef op overheidswebsites voldoet aan de **open standaarden PDF 1.7 en PDF/A** op de 'Pas toe of leg uit' lijst. Dat is een stijging ten opzichte van het percentage van vorige jaren.

Digitale toegankelijkheid van PDF-bestanden op overheidswebsites blijft een knelpunt. Slechts 10% van de recente (van 2019 of jonger) PDF-bestanden uit de steekproef bleek digitaal toegankelijk. Ook al is het percentage van het aantal digitaal toegankelijke bestanden in de steekproef verdubbeld, de **trend blijft dat dit percentage veel te laag** is. De stijging is vooral toe te schrijven aan toenemend aantal digitaal toegankelijke PDF- bestanden op websites van Rijksoverheidsorganisaties. Wel zien wij dat steeds meer organisaties kiezen voor HTML-first publicatiebeleid, waarbij er geen nieuwe PDF-bestanden meer op de website hoeven te komen. Dit komt de digitale toegankelijkheid van de websites meestal ten goede.

Ook dit jaar moeten we concluderen dat **ODF** veel te weinig wordt toegepast waar dat verplicht is. Dit is een **voortzetting van de trend van eerdere jaren**. De stijging in gebruik van ODF uit de meting van dit jaar is toe te schrijven aan één website en geeft zodoende een vertekend beeld voor het gebruik van ODF bij de hele overheid. Voor alle andere gemeten websites van Rijksoverheid, gemeenten, provincies en waterschappen blijft het zeer lage gebruik van <1% dat in lijn is met de metingen van voorgaande jaren.

Relevante ontwikkelingen

ODF wordt beheerd door OASIS. Deze internationale organisatie heeft geen specifieke ambities om het gebruik van ODF bij de Nederlandse overheid te stimuleren. In Nederland werd het gebruik van ODF gestimuleerd door de OpenDoc Society (<http://www.opendocsociety.org/>) en NLnet (<https://nlnet.nl/project/odfautotests/>). Zo hebben deze organisaties het ODF Plugfest enkele malen (in 2011 en 2015) in Nederland georganiseerd en stellen ze open source toolondersteuning beschikbaar voor ODF. In de laatste jaren zijn deze organisaties echter niet actief geweest met het stimuleren van het gebruik van ODF. In Nederland is er geen organisatie die optreedt als 'intermediair' voor ODF tussen de internationale beheerorganisatie OASIS en Nederlandse overheidsorganisaties.

Als gevolg van geopolitieke ontwikkelingen is er zowel op bestuurlijk als operationeel niveau steeds meer aandacht voor digitale autonomie. Het bewustzijn groeit om minder afhankelijk te zijn van grote leveranciers, de zogenoemde *hyperscalers*, die ook vaak worden aangeduid onder de noemer 'BigTech'. Op het gebied van kantoor- en samenwerkingsformats komt zodoende ODF (en aanpalende open source software) in beeld als open alternatief voor de leveranciersgebonden ('BigTech') formats die nu overheersend in gebruik zijn. Dit uit zich in diverse projecten en *proofs-of-concept* op alle overheidslagen. Deze ontwikkeling van gebruik van open kantoor- en samenwerkingsformats in plaats van leveranciersgebonden formats is ook internationaal zichtbaar.

PDF/A en PDF 1.7 worden beheerd door ISO. Deze internationale organisatie heeft geen specifieke ambities om het gebruik van PDF bij de Nederlandse overheid te stimuleren. Dit geldt ook voor de NEN die de ISO-specificaties beschikbaar stelt. De PDF Association stimuleert via het delen van kennis en van technieken het gebruik van PDF/A en PDF 1.7 (en de aanbevolen standaard PDF/UA; een PDF/UA-document is een PDF-document dat voldoet aan aanvullende eisen op gebied van digitale toegankelijkheid). De PDF Association wordt gedragen door leveranciers van producten gerelateerd aan PDF. De stimulering en ondersteuning van PDF/A en PDF 1.7 vanuit de PDF Association is daarom nauw verweven met het commerciële aanbod. In Nederland is er geen organisatie die optreedt als 'intermediair' voor PDF tussen de internationale beheerorganisatie ISO en Nederlandse overheidsorganisaties (toegankelijkheidsrichtlijnen in het algemeen (DigiToegankelijk) worden beheerd door [Logius](#)).

Het Nationaal Archief stimuleert het gebruik van PDF/A voor duurzame toegankelijke toepassingen. PDF/A en PDF 1.7 zijn opgenomen in de [Norm Voorkeursformaten](#) van Nationaal Archief. Bij het Nationaal Archief kunnen overheidsorganisaties terecht voor advies over voorkeursformaten. Voorkeursformaten zijn

bestandsformaten die op dit moment het meest geschikt zijn om digitale overheidsinformatie zo duurzaam toegankelijk mogelijk te bewaren.

Er bestaat inmiddels een nieuwe standaard PDF 2.0, die gratis beschikbaar is via de PDF Association. Hiermee onderscheidt PDF 2.0 zich van PDF 1.7 en PDF/A, waarvoor nog betaald moet worden bij NEN-ISO. Geen enkele organisatie heeft PDF 2.0 echter nog aangemeld voor de 'Pas toe of leg uit'-lijst. Dit kan komen omdat het nog te vroeg is om PDF 2.0 te verplichten aan de overheid.

Quickscan Leveranciers

ODF kwam in drie van de negen gesprekken terug. In algemene zin gaven leveranciers aan het vreemd te vinden dat de ODF standaard regelmatig wordt uitgevraagd in aanbestedingen, terwijl de standaard niet tot nauwelijks gebruikt wordt door de aanbestedende dienst. Leveranciers geven aan dat zij ODF in hun producten kunnen leveren, maar zien dat ODF-bestandstypen in de praktijk nauwelijks gebruikt worden. Dit levert de scheve situatie op waarin de overheid de standaard wel verplicht stelt, maar zelf geen opvolging aan het beleid geeft.

Twee leveranciers hebben hun mening over de PDF-standaard gegeven. Zij gaven aan dat het toepassingsgebied van PDF in de aanbesteding vaak te algemeen geformuleerd is. In de aanbesteding wordt gesteld dat een leverancier PDF moet ondersteunen. De leveranciers gaven aan dat niet duidelijk wordt wat ondersteunen in dit geval betekend, bijvoorbeeld of een leverancier een PDF moet kunnen inlezen of zelf moet kunnen genereren.

SKOS

28

Waarom belangrijk?

Het publiceren van gegevensbestanden in de vorm van begrippenlijsten, digitale woordenboeken en taxonomieën door overheidsorganisaties gebeurt vaak in de vorm van documenten die niet bruikbaar zijn voor computerprogramma's. SKOS zorgt ervoor dat deze kennisrepresentaties via het internet aan elkaar kunnen worden gekoppeld en maakt het mogelijk dat zij makkelijker als open data kunnen worden hergebruikt. Dit vindt plaats via linked data principes. Zo draagt SKOS bij aan het eenduidig vastleggen van betekenis van begrippen en maakt SKOS de relatie tussen begrippen inzichtelijk. Daarnaast zijn er ook standaarden op 'Pas toe of leg uit'-lijst die op hun beurt weer gebruik maken van SKOS en aanpalende linked data standaarden, zoals GWSW voor stedelijk waterbeheer of Aquo-standaard voor watermanagement. SKOS staat op de 'Pas toe of leg uit'-lijst sinds 18 mei 2015.

Feitelijk gebruik

Er is (nog) geen objectieve meetmethode voorhanden om het gebruik van SKOS op internet inzichtelijk te maken. In principe kan het gebruik van SKOS vrijwel automatisch worden gemeten op aggregatoren van begrippenlijsten, zoals het internationale [Linked Open Vocabularies](#) (LOV) of het leveranciersgebonden thesaurusplatform [BegrippenXL](#). Op het [Dataregister van de Nederlandse overheid](#) is op het moment van deze meting één dataset aangemeld die gebruik maakt van SKOS. In de markt zijn leveranciers actief die platforms bieden voor het verzamelen van linked data sets. Het al eerder genoemde BegrippenXL biedt een overzicht van een kleine 60 begrippenlijsten van bijna alleen overheden. Het thesaurusplatform is volledig gebaseerd op de SKOS (en linked data standaarden). Een overheidsbreed initiatief is het Nationaal Semantisch Vlak (NSV) van de Nederlandse Overheid Referentie Architectuur (NORA) dat o.a. een [lijst publiceert met 32 gegevenswoordenboeken](#); niet alle 32 gegevenswoordenboeken maken gebruik van SKOS (en linked data standaarden). Verschillende overheidsdomeinen hebben eigen initiatieven zoals het Termennetwerk van het Netwerk Digitaal Erfgoed dat een hulpmiddel is om bestaande definities van erfgoedobjecten uit diverse (inter)nationale begrippenlijsten eenvoudig te kunnen vinden. Organisaties zetten SKOS ook in voor begrippenlijsten ten behoeve van interne bedrijfsprocessen. Begrippenlijsten voor

gebruik intern binnen een organisatie zullen niet altijd gepubliceerd worden op internet en zijn daardoor niet zichtbaar en meetbaar via bovengenoemde aggregatoren.

Net als in voorgaande jaren is o.a. een enquête uitgezet onder ruim 50 overheden en semi-overheden om gebruiksgegevens van SKOS te achterhalen. Deze groep bestaat voornamelijk uit gebruikers van de LOD Nederland groep op LinkedIn en is licht uitgebreid t.o.v. de steekproef bij de metingen van 2019 - 2024. De inhoud en opzet van de enquête in 2025 is onveranderd. Daarmee zijn de antwoorden te vergelijken met de uitkomsten van de enquêtes van voorgaande jaren.

In totaal is de enquête 36 keer ingevuld waaruit 28 unieke organisaties zijn af te leiden. In vergelijking met vorig jaar is er sprake van een lagere respons. Van de 28 unieke organisaties geeft 50% (14 organisaties) aan een begrippenlijst, woordenboek of taxonomie op het internet te publiceren. Dit is minder ten opzichte van 2024 (toen 62%). Dit zijn in principe organisaties die in aanmerking komen voor de verplichting van SKOS. Als wordt ingezoomd op deze 14 organisaties die kwalificeren voor een verplichting van SKOS, dan zien we het volgende:

11 daarvan gebruiken SKOS (79%). Dat is gelijk aan het gebruik van vorig jaar (toen 79%).

Over deze 11 gebruikers van SKOS nog het volgende:

- er zijn geen organisaties die alleen van SKOS gebruik maken
- 6 organisaties geven aan zowel SKOS als Web Ontology Language (OWL) te gebruiken. OWL is een open standaard op de lijst aanbevolen standaarden van het Forum Standaardisatie, met een soortgelijk functioneel toepassingsgebied als SKOS maar wel complexer in het toepassen ervan.
- 6 van de 11 organisaties (55%) gebruiken naast SKOS ook de open standaard Shapes Constraint Language (SHACL). Dit is een aanbevelenswaardige combinatie omdat SHACL de kwaliteit van datasets borgt. SHACL staat (net als OWL) op de lijst aanbevolen standaarden.

29

De basis om een uitspraak te doen over de ontwikkeling van het gebruik van SKOS is smal. Met inachtneming van die constatering is het mogelijk te zeggen dat er sprake is van een **daling in het gebruik** van SKOS t.o.v. vorig jaar. Een belangrijke bijbehorende conclusie is ook: daar waar deze open standaarden gebruikt moeten worden, gebeurt dat ook. De groeipotentie voor het gebruik van SKOS zit er vooral in dat meer overheidsorganisaties hun data (meer) als linked data gaan publiceren en dat overheidsorganisaties toenemende aandacht hebben voor het vastleggen en het harmoniseren van begrippen om de overheid als één te benaderen en overheden een integrale aanpak en dienstverlening kunnen aanbieden.

Enkele aanvullende observaties:

- waar de overheid linked data toepast en publiceert, gebeurt dit vrijwel altijd met open standaarden. De resultaten bevestigen het beeld dat SKOS meestal gebruikt wordt waar het 'Pas toe of leg uit'-beleid dat verplicht. De resultaten zijn in lijn met de resultaten van eerdere jaren.
- we zien dat vooral uitvoeringsorganisaties, koepel- of domeinorganisaties en waterschappen SKOS en linked data toepassen. Uit de respons van decentrale overheden komt een beeld naar voren dat zij meestal geen begrippenlijst, woordenboek of taxonomie op internet publiceren. Meeste gemeentes zijn klein om een eigen SKOS model te ontwikkelen; gemeente-overstijgende modellen liggen meer voor de hand. Provincies geven aan in interprovinciaal verband te werken aan provincie-overstijgend modellen.
- het feit dat een organisatie SKOS gebruikt, zegt minder over de kwaliteit van de datasets. De kwaliteit van de kennisrepresentatie met SKOS is minstens even belangrijk als de inzet van de standaard op zich, maar is veel moeilijker objectief te beoordelen zonder gedetailleerde kennis van het domein. SHACL helpt met verhogen van kwaliteit van datasets..

- de enquête lijkt de ‘alles of niets’ trend van vorige jaren te bevestigen: óf een organisatie doet helemaal niet aan linked data, óf een organisatie gebruikt het palet aan open standaarden in onderlinge samenhang.
- In tegenstelling tot de meting van 2024 noemen respondenten de nieuwe Nederlandse ‘Standaard voor Beschrijven van Begrippen’ (NL-SBB) niet als andere standaard voor begrippenlijsten. Dit is opvallend omdat NL-SBB tractie heeft binnen de Nederlandse overheid. NL-SBB heeft een nauwe relatie met SKOS.

SKOS heeft een ‘Pas toe of leg uit’-verplichting voor publiceren van begrippenlijst **op internet**. De enquête van 2025 heeft na 2024 en 2023 voor de derde keer gevraagd naar het gebruik van begrippenlijsten en linked data standaarden ten behoeve van interne bedrijfsprocessen (dat wil zeggen, zonder begrippenlijst, woordenboek of taxonomie op internet te publiceren). Hiervoor is gekozen omdat uit gesprekken met de community naar voren is gekomen dat meer organisaties SKOS breder toepassen dan alleen voor publicatie op internet. Van de 28 unieke organisaties of programma’s geeft 61% (17 organisaties) aan een begrippenlijst, woordenboek of taxonomie te gebruiken voor interne bedrijfsprocessen. Dat zijn voor een deel andere organisaties dan organisaties die een begrippenlijst op internet publiceren. 8 organisaties gebruiken hierbij linked data standaarden, waarvan 7 organisaties ook SKOS (41%). Organisaties die linked data standaarden gebruiken voor interne bedrijfsprocessen, gebruiken meestal meerdere standaarden in onderlinge samenhang.

Relevante ontwikkeling

SKOS wordt beheerd door W3C. Deze internationale organisatie heeft geen specifieke ambities om het gebruik van SKOS bij de Nederlandse overheid te stimuleren. In Nederland kunnen overheidsorganisaties terecht bij het Platform Linked Data Nederland (PLDN) voor informatie. In Nederland is er geen organisatie die optreedt als ‘intermediair’ voor SKOS tussen de internationale beheerorganisatie W3C en Nederlandse overheidsorganisaties.

Vanuit PLDN heeft een werkgroep de Nederlandse ‘Standaard voor Beschrijven van Begrippen’ (NL-SBB) opgesteld. NL-SBB biedt een kader voor het vastleggen van begrippen. NL-SBB heeft een mapping naar SKOS en is met of zonder SKOS toe te passen. NL-SBB (in beheer bij Geonovum) is in procedure bij Forum Standaardisatie om te verplichten aan de overheid via plaatsing op de ‘Pas toe of leg uit’-lijst. Inmiddels is er een [NL-SBB Community](#) opgestart.

Het publiceren van linked data, en van (SKOS) kennissystemen in het bijzonder, vereist specialistische kennis over semantiek en standaarden. Diverse domeinen bieden in toenemende mate trainingen aan over linked data. De trend lijkt te zijn dat overheden meer linked data in productie in gebruik hebben of voornemens zijn linked data te gebruiken. Organisaties kiezen er steeds vaker voor om eerst een begrippenkader vast te stellen voordat een informatiemodel wordt ontwikkeld. Hiermee ontstaat er een eenduidige basis voor de verdere uitwerking en toepassing van linked data.

Kadaster ([Kadaster Knowledge Graph \(KGG\)](#)), Logius KOOP (o.a. [Linked Data Overheid \(LiDO\)](#)), Ministerie van Financiën, Belastingdienst, DUO, RWS, RCE, waterschappen, de erfgoedsector en de onderwijssector zijn voorbeelden van adoptie van linked data bij de Nederlandse overheid. Ook programma’s zoals Federatief Datastelsel omarmen SKOS en linked data standaarden. De opkomst van Artificial Intelligence en incidenten zoals de Toeslagenaffaire zorgt voor een roep om een transparantere overheid. Met recente ontwikkelingen zoals generatieve Artificial Intelligence (AI) via *large language models* (LLM’s) is het beter dat de overheid zelf begrippen vastlegt in plaats van dat AI (via LLM’s) definities samenstelt (‘verzint’). Dit leidt tot meer betrouwbare overheidsinformatie en betere informatievoorziening. “Er is een grotere behoefte in alle lagen van bestuur om grip te krijgen op de informatiestromen. Harmonisatie van taal draagt bij aan deze grip. Bestuurders spreken niet over standaarden zoals SKOS maar wel over semantiek en harmonisatie van taal. Door deze omslag neemt het aantal overheidsorganisaties dat inzet op het opzetten van begrippenlijsten toe en zodoende wordt daar steeds vaker SKOS voor ingezet.”, aldus [“Evaluatie SKOS en Linked Data](#)

[Standaarden](#)” (2023) in opdracht van Forum Standaardisatie. De opkomende standaard NL-SBB lijkt dit proces te versnellen en als katalysator te dienen voor overheden en programma’s om begrippenlijsten op te stellen.

3. Domein uitwisselingsfundament

OpenAPI Specification

Waarom belangrijk?

Open API Specification (OAS) is een standaard voor de documentatie van Application Programming Interfaces (API's) die beheerd wordt door Open API Initiative. Een API is een koppelvlak waarmee applicaties over het Internet toegang kunnen krijgen tot gegevens en diensten. Zo'n API is in de praktijk zo effectief als z'n documentatie. De documentatie van een API moet voor machines leesbaar en voor mensen begrijpelijk zijn. Daar ligt de essentie van de OPEN API standaard: het is een semantische structuur voor het gestandaardiseerd documenteren van een API die zowel door gebruikers als systemen kan worden gelezen.

Maatschappelijk gezien helpt deze standaard de aanbieders en afnemers van APIs, die samen met of in opdracht van de publieke sector werken, om op een eenduidige manier, de functionaliteit van APIs te begrijpen. OAS 3.0 zorgt voor gemakkelijker (her)gebruik van APIs en minder leveranciersafhankelijkheid. Door deze standaard op de 'pas toe of leg uit'-lijst besparen we collectief veel tijd en middelen die anders nodig zijn om dergelijke API beschrijvingen te maken en toe te lichten aan de gebruikers ervan. Ook besparen we op de lange termijn met deze open standaard door de vermindering van "vendor lock-in" en het stimuleren van open standaarden en open source.

De standaard OpenAPI Specification staat op de 'pas toe of leg uit' lijst sinds mei 2018.

Feitelijk gebruik

Overheidsorganisaties bouwen en gebruiken steeds meer API's. In het API Register van developer.overheid.nl kunnen overheidsorganisaties vrijwillig API's publiekelijk documenteren. Hier staan nu 168 API's in het register, ten opzichte van 92 API's vorig jaar.

Tevens is de nieuwste versie van het API register OpenAPI-first. Dit betekent dat voorheen API's handmatig konden worden toegevoegd, dit nu volledig geautomatiseerd gebeurt op basis van de gepubliceerde 'openapi.json'. Het API register ondersteunt zowel 3.0 als 3.1 versies en kan deze converteren naar elkaar. Alle API's in het API register zijn momenteel vooralsnog 3.0.

Relevante ontwikkeling

Versie 3.1 was enkele jaren geleden aangemeld voor opname op de PTOLU-lijst, maar na expertadvies over het gemis van support van tooling is dat traject stopgezet. Dit jaar is deze versie ingediend ter heroverweging, aangezien de tooling ondertussen 3.1 wel ondersteund. Ondertussen is versie 3.2 gepubliceerd door het Open API Initiative en zijn ze aan het werk aan versie 4.0.

REST_API Design Rules

Waarom belangrijk?

REST-API design rules is een lijst afspraken die ontwikkelaars volgen tijdens het bouwen van een REST-API voor de publieke sector. Door deze regels te hanteren hebben alle verschillende API's van de overheden een eenduidige structuur, werking en documentatie. Hierdoor wordt de API voorspelbaar en dat is wel zo prettig voor andere ontwikkelaars die er gebruik van willen maken. Dankzij deze regels blijft het makkelijk voor organisaties om gegevens met elkaar uit te wisselen.

Maatschappelijk gezien helpt deze standaard de bedrijven, ontwikkelaars en data scientists die samen met of in opdracht van de publieke sector werken om op een eenduidige manier, snel en efficiënt, gegevens uit te wisselen met de overheden. Door deze standaard op de 'pas toe of leg uit'-lijst besparen we collectief veel tijd en middelen die anders nodig zijn om dergelijke API ontwerp keuzes voor iedere toepassing opnieuw te maken. Ook besparen we op de lange termijn met deze standaard door herbruikbaarheid van API designs en het stimuleren van open

Feitelijk gebruik

Overheidsorganisaties bouwen en gebruiken steeds meer API's. In het API Register van developer.overheid.nl kunnen overheidsorganisaties vrijwillig API's publiekelijk documenteren. Hier staan nu 168 API's in het register, ten opzichte van 92 API's vorig jaar.

Tevens is de samenwerking met developer.overheid.nl uitgebreid, waar REST API Design Rules een prominente plek hebben in de kennisbank en in ondersteunende tooling. De standaard verwijst ook naar de website voor extra documentatie en concrete handvaten voor developers. Door gerichtere informatie te verstrekken zien we dat developers sneller API's compliant kunnen maken aan de REST API Design Rules.

Het API register laat voor elke API een score in percentages zien hoeveel van de design rules de API aan voldoet. 50% score voor een API betekent dat die API aan precies de helft van de design rules voldoet. Op dit moment (Oktober 2025) scoren alle API's minimaal 67%. 10 API's behalen een perfecte score en 8 API's tussen de 80 en 100 procent.

Relevante ontwikkeling

Versie 2.0 wordt eind dit jaar voorgedragen aan OBDO voor opname op de PTOLU-lijst, inclusief uitstekend beheer voor Logius. Versie 2.1 is vastgesteld bij MIDO en zal begin volgend jaar worden voorgedragen aan het Forum.

De API's in het register worden sinds dit jaar gebruikt bij het analyseren van impact van wijzigingen op de standaard. Dit resulteert in extra motivatie voor overheidsorganisaties om hun API's aan te melden, zodat ook hun aanpak wordt meegenomen tijdens beslismomenten. Dit vergroot het draagvlak voor wijzigingen, omdat er concrete data is over hoeveel API's al voldoen.

In recente versies is de samenhang van modules en de core standaard verscherpt en is er ingezet op het automatisch testen van compliance op de standaard. Dit levert developers concrete issues op om op te lezen en op deze laagdrempelige manier zien we compliance significant toenemen. Hier zal de komende tijd verder op worden doorgebouwd in samenwerking met Kennisplatform API's om deze automatisering onderdeel te maken van het publicatie proces van API's bij overheidsorganisaties.

Quickscan Leveranciers

De Rest-API Design Rules standaard kwam in vier van de negen gesprekken aan bod. De door PBLQ gesproken leveranciers vinden deze standaard te algemeen geformuleerd voor de producten die zij ontwikkelen voor overheden. Op de PTOLU-lijst staan de ontwerpregels voor Rest-API's, maar er wordt niet voorgeschreven hoe en/of welke API's in welke situatie gebruikt moeten worden. Dat maakt dat de manier waar Rest-API nu op de PTOLU-lijst staat soms verwarrend kan zijn.

Digikoppeling

Algemeen

Digikoppeling bestaat uit een set standaarden voor elektronisch berichtenverkeer tussen systemen van overheidsorganisaties. Digikoppeling onderkent twee hoofdvormen van berichtenverkeer:

- Synchron berichtenverkeer: een verzoek waarbij het vragende informatiesysteem wacht op een antwoord. Snelheid van afleveren is belangrijk. Als een antwoord uitblijft kan de vrager de vraag opnieuw stellen.
- Asynchroon berichtenverkeer: het meldende systeem stuurt een bericht en –eventueel- volgt op een later tijdstip een antwoord. Bij meldingen is de betrouwbare aflevering van het bericht essentieel. De melder moet zekerheid hebben dat zijn melding is ontvangen.

Digikoppeling staat op de 'pas toe of leg uit' lijst sinds mei 2009. De Digikoppeling standaard betreft op interoperabiliteit gerichte afspraken voor gegevensuitwisseling tussen overheidsorganisaties. In verband met het belang van standaardisatie op dit gebied binnen de GDI moet Digikoppeling op de lijst blijven staan.

Tabel 16. Digikoppeling (2013-2025)

	Rijk + Uitvoerings- Organisaties/ ZBO's + OOV + eOverheid	Ministeries + BR's + GR's ZBO's + HCS + AC's + RO's	Gemeenten	Provincies	Waterschappen	Totaal
Voorjaar 2013	3 %		31 %	8 %	14 %	22 %
Zomer 2013	4 %		42 %	15 %	14 %	29 %
Zomer 2014	5 % ⁶		57 %	23 %	14 %	40 %
Zomer 2015	64 %		63 %	42 %	24 %	58 %
Zomer 2016	40 %		75 %	67 %	46 %	64 %
Zomer 2017	67%		92%	67%	50%	76%
Zomer 2018	x ⁷		98%	75%	59%	95% ⁸
Zomer 2019 Najaar 2020		60%	100%	100%	100%	90% ²
Najaar 2020		65%	100%	100%	100%	91%
Zomer 2021		65% ⁹	100%	100%	100%	91%
Zomer 2022		65%	100%	100%	100%	91%
Zomer 2023		69% ¹⁰	100%	100%	100%	92%
Zomer 2024		69%	100%	100%	100%	92%
Zomer 2025		69%	100%	100%	100%	92%

Bron: opgave beheerorganisatie Logius

Het overzicht wijst uit dat na een reeks van jaren van gestage groei het **gebruik** van Digikoppeling lijkt te **stabiliseren**.

Dit is niet per definitie slecht nieuws. In de categorieën gemeenten, provincies en waterschappen is de dekking sinds 2019 volledig te noemen. Voor de categorie Rijk en uitvoeringsorganisaties geldt dat niet voor alle onderdelen Digikoppeling relevant is zoals bv voor Gemeenschappelijke regelingen en Adviescolleges.

⁶ In 2013 en 2014 is het aantal aansluitingen gedeeld op het aantal overheidsinstellingen. In 2015 en 2016 is aansluiting gezocht bij de rekenwijze van Logius waarbij alleen de overheidsorganisaties zijn betrokken waar uitwisseling via Digikoppeling aan de orde zou moeten zijn.

⁷ In deze berekening in 2018 konden de overheidsorganisaties die zijn betrokken waar uitwisseling via Digikoppeling niet worden achterhaald. Als enkel naar de combinatie ZBO's, Uitvoeringsorganisaties en samenwerkingsverbanden wordt gekeken, dus zonder noodzakelijke betrekking op uitwisseling via Digikoppeling is dit percentage 36%

⁸ Hierin zijn voor 2018 alleen de aantallen voor gemeenten, provincies en waterschappen opgenomen

⁹ Hoewel in 2021 het aantal OIN's is toegenomen in de groep Rijksoverheid + Uitvoeringsorganisaties, is de groep zelf ook gegroeid (met name de groep gemeenschappelijke regelingen) waardoor het percentage niet is veranderd.

¹⁰ Relatieve dekking binnen de groep gemeenschappelijke regelingen is toegenomen.

Over de verantwoording van bovenstaande cijfers nog het volgende. Het meten van de toepassing van de Digikoppeling standaard is lastig omdat het gebruik van dit transportprotocol buiten het zicht van de beheerder – Logius- omgaat. Digikoppeling kent geen centrale component waarlangs berichten worden gevoerd en inzicht in het gebruik kan dus niet op basis van kwantitatieve metingen worden gedaan. Verder zet de trend steeds meer door dat overheidsorganisaties gebruikmaken van Cloudoplossingen aangeboden door zowel publieke als private dienstverleners waardoor de vraag “organisatie gebruikt Digikoppeling” een complex antwoord kan hebben.

Er bestaat echter een objectief meetinstrument om te bepalen of een organisatie Digikoppeling toepast in een van haar ketens van elektronische gegevensuitwisseling. Digikoppeling vereist namelijk een OIN – het Organisatie Identificatienummer. Het OIN-register is onderdeel van de Digikoppeling standaard en wordt beheerd door Logius. Dit register is voor dit peilmoment als primaire bron gebruikt om te bepalen of een organisatie gebruik maakt van Digikoppeling.

Relevante ontwikkeling

De Digikoppeling standaard is een levende standaard en wordt continue doorontwikkeld Twee ontwikkelingen hebben een aanzienlijk impact op de standaard:

1. Het REST API-profiel is doorontwikkeld in lijn met de NL GOV API Design Rules (ADR) 2.0 standaard. Ook is het profiel uitgebreid met afspraken met betrekking tot Signing en Encryptie.
2. Het Digikoppeling ebMS2 profiel zal worden uitgefaseerd en naar verwachting worden vervangen door een Digikoppeling ebMS3/AS4 profiel direct gebaseerd op eDelivery. Dit profiel en het bijbehorend migratie traject wordt de komende tijd verder onderzocht/ontwikkeld (en besluitvorming hierover zal plaatsvinden binnen de MIDO governance).

36

Geo-Standaarden

Waarom belangrijk?

Het geheel van Geo-standaarden behoort tot het domein ‘Uitwisselingsfundament’ op de ‘Pas toe of leg uit’-lijst. In Nederland zijn organisaties in verschillende domeinen betrokken bij het registreren en uitwisselen van informatie met een geografische component. Dat wil zeggen: informatie over objecten die gerelateerd zijn aan een locatie op het aardoppervlak. Voorbeelden hiervan zijn kadastrale informatie en informatie over waterhuishouding. Om ervoor te zorgen dat de geo-informatiehuishouding van deze domeinen op elkaar aansluit zodat informatie tussen domeinen uitgewisseld kan worden, zijn afspraken nodig over de te gebruiken standaarden. De Geo-standaarden voorzien hierin. Of, om met de woorden van de beheerorganisatie achter de Geo-standaarden (Geonovum) te spreken: de set Geo-standaarden maakt geo-informatie FAIR:

- Findable: Nederlandse metadataprofielen stellen gebruikers in staat om datasets en dataservices te vinden en vervolgens te beoordelen op geschiktheid voor gebruik (dankzij implementatie in het [Nationaal Georegister](#));
- Accessible, dankzij de OGC API standaarden die ook zonder geo-kennis goed te implementeren zijn;
- Interoperable, dankzij de semantische standaardisatie conform NEN3610;
- Re-usable doordat de belangrijkste basisgegevens in de geo-basisregistraties (BGT, BAG, BRT, BRO, BRK, WOZ) allemaal als open data beschikbaar gemaakt worden.

De Geo-standaarden staan op de ‘Pas toe of leg uit’-lijst sinds 9 december 2014. In 2024 zijn de OGC API standaarden toegevoegd aan de Geo-standaarden, met het doel de adoptie hiervan te monitoren en stimuleren. De opname van de OGC API standaarden op de ‘Pas toe of leg uit’-lijst prikkelt

overheidsorganisaties om met implementatie ervan aan de slag te gaan en meer informatie met een geografische component te publiceren.

Feitelijk gebruik

Als indicator voor het feitelijk gebruik van deze open standaarden kijken we in eerste instantie naar de gebruikscijfers van [Publieke Dienstverlening Op de Kaart \(PDOK\)](#), het platform voor het ontsluiten van geo-datasets van Nederlandse overheden. Het beheer van PDOK is belegd bij het Kadaster. Dit zijn actuele en betrouwbare gegevens voor zowel de publieke als private sector. PDOK stelt digitale geo-informatie als dataservices en bestanden beschikbaar. De PDOK diensten zijn gebaseerd op open data en zijn daarom voor iedereen vrij beschikbaar. De datasets zijn benaderbaar via geo-webservices, RESTful API's en beschikbaar als downloads en linked data. Deze voorziening vormt samen met de geobasisregistraties die via PDOK worden ontsloten, de kern van de Nederlandse geo-informatie infrastructuur. De set Geo-standaarden fungeert als ruggengraat van die infrastructuur.

Het aantal hits via PDOK is de beste indicator van het gebruik van de standaarden aan de afnamekant, het aantal datasets (en daaraan gekoppeld het aantal services) dat ervoor kiest om ontsloten te worden via PDOK, als indicator voor het gebruik van de standaarden aan de aanbodzijde.

Tabel 17. Gebruikscijfers per platform (2023, 2024, per aantal hits, uitgedrukt in miljoenen)

	2023	2024
PDOK	22.200	28.800
Nationaal Georegister	26,6	33

37

Tabel 18. Gebruikscijfers per standaard (2023, 2024, per aantal hits op PDOK, uitgedrukt in miljoen)

	2023	2024
WMS	2.100	10.200
WFS	212	1.100
WMTS	3.000	13.700
OGC API	xxx	231
OGC API Features	9,4	(geen specifieke cijfers aangeleverd)
OGC API Tiles	140	(geen specifieke cijfers aangeleverd)

In de Monitors Open Standaarden van 2020, 2021 en 2022 is te zien dat PDOK elk jaar aanzienlijke groeicijfers laat zien. In 2023 en 2024 was er een dalende trend, veroorzaakt door de overgang bij PDOK naar de cloud. Deze overgang ging gepaard met een nieuwe rekenmethodiek, waarbij foutieve bevestigingen en uitgefaseerde hits niet meer werden meegeteld. Dit maakte vergelijken met eerdere jaren lastig. De overgang bij PDOK naar de cloud is in 2025 afgerond waardoor de cijfers vanaf 2025 weer beter vergelijkbaar zijn met de voorgaande jaren 2021, 2021 en 2022.

Het aantal datasets is gestegen ten opzichte van het voorgaande jaar, van 214 naar 222, en het aantal services is gestegen van 642 naar 677.

Er zijn flinke stappen gezet in de adoptie van OGC API Tiles en OGC API Features. Er zijn nu 7 datasets via deze nieuwe standaarden ontsloten, tegenover 1 dataset vorig jaar. De OGC API Features verwerking is opgenomen als product binnen PDOK. Naast de 7 datasets die Kadaster zelf via PDOK als OGC API is gaan aanbieden, heeft PDOK een WFS naar OGC API campagne opgestart waarbij inmiddels voor 50 bestaande

Web Feature Services nieuwe OGC API Features aan de data-aanbieders zijn aangeboden voor akkoord. Wij zien dat de nieuwe OGC API's in gebruik genomen worden en wij zien het aantal hits via deze OGC API's stijgen. Daarnaast laat WFS een grote stijging zien: vervijfvoudiging in 2024 t.o.v. 2023. Dit komt vooral doordat meer toepassingen WFS gebruiken i.p.v. downloads van datasets.

Samenvattend: het aantal hits op PDOK 2024 is gestegen van 22,2 miljard naar 28,8 miljard waarvan 10.2 miljard WMS, 1,1 miljard WFS, 13,7 miljard WMTS, en 231 miljoen OGC API Features en Tiles. Het gebruik van de OGC APIs blijft hard stijgen, in de eerste helft van 2025 zijn er al ruim 372 miljoen hits, en dat is ruim 1,5 keer zoveel als het gebruik in volledig 2024.

Het aantal hits op het Nationaal Georegister (NGR) laat nog steeds een stijgende lijn zien: van 26,6 miljoen in 2023 naar bijna 33 miljoen in 2024 en 19 miljoen in de eerste helft van 2025. Het Nationaal Georegister is dé vindplaats van geo-informatie van Nederland. Met de eenvoudige zoekopties en presentatie van resultaten kunnen de datasets in de kaartviewer worden bekeken of worden gedownload.

Relevante ontwikkeling

In 2024 is de procedure bij het Forum Standaardisatie om de profielen voor WMS en WFS te vervangen door de OGC API standaarden, te weten OGC API Features part 1 en 2 en OGC API Tiles, plus het vernieuwen van de versie van GeoPackage, positief afgerond. Hiermee zijn de OGC API Features part 1 en 2 en OGC API Tiles verplicht aan de overheid ('Pas toe of leg uit'-verplichting); de profielen voor WMS en WFS zijn aanbevolen aan de overheid.

Vanuit Logius loopt de procedure bij het Forum Standaardisatie voor het bijwerken van de 'Pas toe of leg uit'-lijst met versie 2.0.2 van de REST-API Design Rules (ADR) waarin de Geo-module binnen de REST-API Design Rules verplicht wordt. Deze module beschrijft hoe je geo-functionaliteit kunt opnemen in een API, en is gebaseerd op OGC API Features. Op deze manier wordt de OGC standaard bij een groter publiek van API-ontwikkelaars onder de aandacht gebracht.

Daarnaast is door Geonovum een [Handreiking OGC API Features](#) gepubliceerd; een eerste versie in mei 2024 en een recente update in mei 2025. Geonovum werkt daarnaast aan een OGC API keuzehulp, die globaal inzicht biedt in alle OGC API standaarden, en aan een update van de Praktijkrichtlijn Vector Tiling, waarin de actuele informatie over OGC API Tiles is opgenomen.

Implementatie van OGC API's wordt ook gestimuleerd in het door Geonovum georganiseerde Testbed Digital Twin as a Service dat loopt van mei tot en met november 2025. Verder heeft PDOK net als vorig jaar een innovatiesubsidie aangevraagd waarvan PDOK, indien gehonoreerd, verdere implementatie van OGC API standaarden gaat bekostigen. Samen met de gemeente Rotterdam organiseert Geonovum een plugfest waarin de *client*-ondersteuning van OGC API's getoetst zal worden.

Geonovum organiseert meerdere keren per jaar [workshops](#), voor iedereen die daar in geïnteresseerd is, over het toepassen van OGC API standaarden.

De vraag wat de relatie is tussen API's en Linked Data onderzoekt Geonovum in een activiteit rond de samenhang van metadata standaarden MIM, NL-SBB, DCAT, en API's. Deze activiteit is nog in de opstartfase.

Waarom belangrijk?

De StUF-standaard is één van de drie stelselstandaarden van de 'pas toe of leg uit' lijst. Het betreft een familie van samenhangende gegevens- en berichtenstandaarden, bedoeld voor de uitwisseling van administratieve overheidsgegevens. StUF richt zich op de standaardisatie van de inhoud van informatie, berichten en services. StUF is als open standaard vastgesteld voor uitwisseling van basisgegevens zoals Personen (GBA), Adressen (BRA), Gebouwen (BAG), Kadaster (BRK), Bedrijven (NHR) en Waarde Onroerende Zaken (WOZ), zaakgegevens van gemeenten en ketens waarin gemeenten participeren en waarvoor geen andere (inter)nationale (XML-gebaseerde) berichtenstandaard is vastgesteld. De standaard staat op de 'pas toe of leg uit' lijst sinds november 2008.

Het beheer van de StUF-standaard wordt uitgevoerd door meerdere overheidsorganisaties. VNG Realisatie beheert de overkoepelende delen van de familie. De StUF-standaarden worden breed ingezet en dat blijkt ook bij inzet in diverse ketens (GGK, Jeugdzorg, Omgevingswet, etc.). Juist in ketens waar gemeenten een rol spelen, zien we hergebruik van de uitgangspunten over de gegevensuitwisseling. Bij diverse ontwikkelingen in de digitale overheid zien we dit terug.

Rondom deze familie van standaarden zijn de afgelopen jaren naast de doorontwikkeling van standaarden zelf veel uitbreidingen gerealiseerd in de processen, kaders en bijbehorende instrumenten, zoals:

- zwaardere inbedding van standaarden in architectuur en binnen grootschalige (landelijke) ontwikkelingen;
- leveranciersmanagement;
- instrumentarium voor preventief testen;
- landelijke softwarecatalogus voor markttransparantie en applicatiemanagement;
- periodieke monitoring over digitalisering en compliance van softwareproducten;
- uniforme inkoopvoorwaarden en contractgenerator;
- bestekteksten, opleidingen en communicatie, enz.

De gegevens die m.b.v. StUF berichten worden uitgewisseld zijn onontbeerlijk voor het goed verlopen van vele processen binnen de gemeenten en dus voor een optimale dienstverlening aan burgers en bedrijven. Zonder de StUF standaard moeten gegevens meervoudig opgevraagd en geregistreerd worden wat tot veel administratieve lasten bij bedrijven en ergernis bij burgers leidt en dus tot een negatiever beeld van de dichtstbijzijnde overheid. Daarnaast wordt het daarmee voor gemeenten lastiger te voldoen aan wettelijke voorschriften m.b.t. de tijdige afhandeling van verzoeken.

De aanwezigheid van StUF op de 'pas toe of leg uit'-lijst bevordert de implementatie daarvan in de vele softwareproducten die door leveranciers aan gemeenten worden geleverd. Bij de aanschaf van nieuwe software staan gemeenten sterker in hun eis dat de relevante StUF standaard moet worden ingebouwd.

Feitelijk gebruik

StUF berichten wordt voornamelijk door applicaties gegenereerd, verstuurd, ontvangen en verwerkt. Berichten gaan dus heen en weer tussen diverse systemen/applicaties. Het gaat daarbij om grote aantallen. Alleen al het GGK (Gemeentelijk Gegevens Knooppunt) verwerkt miljoenen berichten per jaar met een StUF envelop. Maar ook mutaties op BAG, Kadaster, BRP en vele andere registraties worden via StUF berichten uitgewisseld. Dit gaat dus over vele miljoenen berichten per jaar.

Uit de cijfers blijkt dat gemeenten, ketenpartners en hun leveranciers StUF breed gebruiken. Er is een grote diversiteit aan pakketsoftware op de markt waarin de StUF standaard is geïmplementeerd. De adoptie voor StUF ZKN en StUF BG neemt nog steeds toe in oplossingen al lijkt die stijging t.o.v. de voorgaande jaren wel

af te vlakken. Voor beide geldt dat het aantal leveranciers dat deze twee StUF standaarden meeneemt in haar softwareproducten zichzelf lijkt te stabiliseren of zelfs licht daalt.

Tabel 19. Adoptie van de twee StUF onderdelen (StUF-BG en StUF-ZKN) door de ICT-markt

Onderdelen	Totaal	Totaal	StUF-BG	StUF-BG	StUF-ZKN	StUF-ZKN
Aantal leveranciers	336	(312)	80	(81)	70	(74)
Aantal softwareproducten (incl. versies)	4007	(3883)	1510	(1464)	905	(899)
wv. beschikbaar/in gebruik	1694	(1733)	403	(413)	255	(268)
wv. gepland/in ontwikkeling	96	(105)	40	(46)	21	(22)

Peildatum juni 2024 (tussen haakjes de cijfers van de vorige monitor)

(bron VNG-Realisatie: www.softwarecatalogus.nl)

Uit het overzicht valt af te lezen dat het aantal leveranciers het afgelopen jaar is gestegen (overall een stijging van 7,6%). Vanaf 2018 bekeken zien we een gestage stijging van 62%. Het aantal leveranciers dat StUF-BG heeft ingebouwd is over diezelfde periode met slechts 8% toegenomen. Voor StUF-ZKN is dat 35%.

Daarnaast is er een toename te zien van het aantal pakketten ten opzichte van 2024. Die toename is, berekend over de periode vanaf 2018, 45% (52% voor StUF-BG en 21% voor StUF-ZKN)

40

Als aanvulling op de cijfers uit de tabel: het gebruik van de softwarecatalogus door gemeenten is gelijk aan het gebruik bij de vorige meting in 2024.

Er is sprake van enkele toetreders en er is ook sprake van een beweging van samenvoeging door samenwerking tussen partijen of overname van pakketten door een leveranciersgroep.

Begin augustus is een nieuwe patch gepubliceerd op StUF-BG.

Bij de beheerorganisatie zijn geen bijzonderheden bekend over specifieke organisaties die de standaarden wel zouden moeten gebruiken, maar deze niet gebruiken. Feitelijk gebruiken alle gemeenten StUF.

Relevante ontwikkeling

Begin 2025 is door Forum Standaardisatie een evaluatie van de StUF standaard gepubliceerd. Daarin werd onderzocht of StUF nog steeds voldoet aan de criteria voor opname op de 'Pas toe of leg uit'-lijst, gezien de technologische ontwikkelingen en de opkomst van alternatieven zoals API's.

Uit deze evaluatie kwamen de volgende conclusies naar voren:

- Het huidige toepassingsgebied van StUF is niet meer passend. Alternatieven zoals API's zijn in veel gevallen meer geschikt voor eenvoudige bevestigingen van basisgegevens.
- De toegevoegde waarde van StUF staat ter discussie. Hoewel StUF functionaliteit biedt waarvoor nog geen alternatieven bestaan, zoals complexe bevestigingen met historie, geven experts in veel gevallen de voorkeur aan API's voor nieuwe voorzieningen.
- Het draagvlak voor StUF neemt af. Experts verwachten dat het gebruik van StUF in de komende jaren significant zal afnemen door de opkomst van alternatieven.
- Het beheer van StUF is een aandachtspunt. De doorontwikkeling van StUF is stopgezet en experts uiten zorgen over de continuïteit van het beheer.
- De opname van StUF op de 'Pas toe of leg uit'-lijst staat ter discussie: Experts hebben uiteenlopende meningen over de wenselijkheid van het verplicht stellen van StUF.

Vanuit de analyse van de interviews die in het kader van de evaluatie zijn afgenomen en de bovenstaande conclusies zijn de volgende aanbevelingen opgesteld:

- Het is aan VNG Realisatie om een strategie en roadmap op te stellen voor de transitie van StUF naar alternatieven, waaronder API's. Onderdeel hiervan is het creëren van een overzicht van alternatieven en nog te ontwikkelen alternatieven voor de verschillende onderdelen in de StUF familie.
- Het is aan VNG Realisatie om samen met gemeenten en leveranciers te onderzoeken hoe het functioneel toepassingsgebied het beste herzien kan worden aan de hand van domeinspecifieke gesprekken. Dit kan onderdeel zijn voor de strategie en roadmap voor de transitie van StUF naar alternatieven, waaronder API's.
- Het is aan VNG Realisatie om een toetsingsprocedure aan te vragen bij het Forum Standaardisatie, om:
 - Het toepassingsgebied te herformuleren zodat dit reflecteert waar StUF meerwaarde heeft en verplicht toegepast moet worden.
 - Aan de hand van het nieuw geformuleerde toepassingsgebied te bepalen of (delen van) StUF in zijn geheel verplicht moet worden gesteld middels opname op de 'Pas toe of leg uit'-lijst.
 - Aan de hand van het nieuw geformuleerde toepassingsgebied te bepalen of (delen van) StUF moet worden aanbevolen middels opname op de lijst aanbevolen standaarden.
- Het is aan VNG Realisatie en het Forum Standaardisatie om te achterhalen hoe de transitie en het al dan niet gebruik van de bijbehorende standaarden duidelijk gecommuniceerd kan worden aan gebruikers.

Uit de evaluatie blijkt de noodzaak van een zorgvuldige transitie naar een nieuwe informatiearchitectuur, waarbij de voordelen van API's worden benut zonder de functionaliteit te verliezen die StUF op dit moment nog biedt.

Die transitie is ook al ingezet. VNG Realisatie zet in het kader van Common Ground in op het gebruik van API-standaarden. In verband daarmee is er een begin gemaakt met de ontwikkeling van API standaarden die de StUF standaarden uiteindelijk overbodig zullen maken. Met name bij Zaakgericht Werken worden daar resultaten geboekt.

Een ander initiatief in dat kader zijn de Haal Centraal API's waarmee gegevens direct bij een aantal basis registraties opgevraagd kunnen worden. Op de lange termijn zal dit in ieder geval leiden tot een afname van het gebruik van de StUF standaard en zo mogelijk zelfs tot het verdwijnen van de StUF standaarden.

Tenslotte wordt er op het moment bekeken hoe de transitie naar API standaarden vormgegeven kan worden voor die delen van de StUF standaard waarvoor nog geen API alternatieven bestaan. Daartoe is begin 2025 een enquête uitgestuurd naar leveranciers. In fase 1 van dit traject is, op basis van een landelijke inventarisatie onder leveranciers en gemeenten, vastgesteld welke StUF-standaarden en bijbehorende onderdelen zoals StUF-interactiepatronen in aanmerking komen voor de transitie naar moderne API-standaarden.

Met de afronding van de landelijke inventarisatie is fase 1 van de door het MT van VNG Realisatie eerder gegeven opdracht om de route naar de doorontwikkeling van StUF naar API-standaarden afgerond.

Momenteel is er toestemming gevraagd voor het opstarten van fase 2. In deze fase wordt als pilot de StUF BAG-koppeling omgezet naar een nieuwe API-standaard. Op basis van de resultaten van deze transitie zal het plan voor de verdere omzetting naar API's worden opgesteld (fase 3).

Quickscan Leveranciers

De StUF standaard is ter sprake gekomen in het kader van de toekomstbestendigheid van standaarden op de PTOLU-lijst. Het voornaamste punt dat leveranciers maakten ten aanzien van StUF is dat zij vinden dat het een verouderde standaard is waar duurzamere alternatieven voor beschikbaar zijn, zoals REST API's. StUF is daarnaast een voorbeeld van een Nederlandse standaard, die niet samenhangt met een bredere Europese of andere internationale standaard.

4. Domein economie en werk

NLCIUS

Waarom belangrijk?

NLCIUS is een nieuwe versie van de oude standaard Semantisch Model e-Factureren (SMeF) en is een aanvullende specificatie voor facturatie naar de Nederlandse overheid op de Europese Norm EN16931. NLCIUS heeft net als de oude standaard tot doel om op semantisch niveau te komen tot één model voor elektronische facturen. In combinatie met de Europese Norm (EN)16931 beschrijft NLCIUS welke gegevenselementen er in een elektronische factuur opgenomen dienen en kunnen worden, wat de samenhang is tussen deze elementen en wat de betekenis is van deze elementen. Hierdoor wordt het eenvoudiger om meerdere standaarden te ondersteunen omdat een dergelijk model overheid en bedrijfsleven duidelijkheid biedt over welke elementen er op een elektronische factuur opgenomen dienen te worden ongeacht de onderliggende techniek van uitwisseling. De standaard staat op de 'pas toe of leg uit'-lijst sinds mei 2018.

De toegevoegde waarde voor de NLCIUS-standaard van een plaats op de 'pas toe of leg uit'-lijst, is dat de NLCIUS belangrijk is voor het economisch verkeer in Nederland en daarbuiten. Met een plaats op de lijst wordt het verplichte karakter van NLCIUS voor het versturen van elektronische facturen aan Nederlandse overheden en instellingen uit de (semi-)publieke sector nogmaals benadrukt.

Feitelijk gebruik

42

Beheer van NLCIUS is sinds 1 januari 2024 belegd bij de normcommissie e-Facturatie van NEN. De normcommissie wordt ondersteund door het Ministerie van Economische Zaken en Klimaat vanwege het maatschappelijke belang. De belangrijkste gebruikersgroepen zijn aangesloten bij de normcommissie: softwareleveranciers van financiële pakketten, PEPPOL-service providers, leveranciers van telecommunicatie en IT, en overheden.

De normcommissie maakt gebruik van data van de Nederlands Peppolautoriteit (NPa), Logius en leverancier Ionite B.V. (e-facturatie specialist) voor een observatie van de ontwikkeling van het gebruik van NLCIUS. Deze observaties betreffen de NLCIUS-adoptie op het PEPPOL-netwerk. Dit laat buiten beschouwing de graad van adoptie via andere kanalen, zoals bilaterale koppelingen of email. We nemen echter aan dat het grootste deel van NLCIUS-facturen over het PEPPOL-netwerk verzonden wordt, en dus dat NLCIUS-adoptie op dat netwerk indicatief is voor de totale NLCIUS-adoptie.

Uit de gegevens van NPa is het volgende op te maken:

- het aantal verstuurd e-facturen in het NLCIUS-formaat (2.237.927) via het Peppol-netwerk is in 2023 met 14% gestegen t.o.v. 2022 (ter vergelijking: vorig jaar een stijging van 40%);
- het aantal ontvangen e-facturen in het NLCIUS-formaat (2.869.465) via het Peppol-netwerk is in 2023 met 11% gestegen t.o.v. 2022 (ter vergelijking: vorig jaar een stijging met 109%).

Het aantal ontvangen e-facturen in het NLCIUS-formaat heeft derhalve wederom om een duidelijke groei doorgemaakt in 2024. Waar het aantal verstuurd en ontvangen e-facturen in het verleden ver uit elkaar lag, omdat er serviceproviders tussen zitten die vaak facturen omzetten in andere formaten ten behoeve van de ontvanger, is nu te zien dat de adoptie van de NLCIUS als factuurformaat daadwerkelijk is gerealiseerd.

Uit gegevens van Ionite blijkt het volgende:

- het aantal endpoints in Nederland is naar 43.912 in de Peppol Directory gestegen. Dit is een stijging van 14% t.o.v. 2023 (vorig jaar: 17% stijging);

- het aantal endpoints dat documenttype SI-UBL 2.0 invoice ondersteunt, groeide naar 43.010. Een stijging van 14% t.o.v. 2023 (vorig jaar een stijging van 18%);
- het aantal endpoints dat documenttype SI-UBL 2.0 creditnote ondersteunt, groeide naar 42.166. Een stijging van 14% t.o.v. 2023 (vorig jaar een stijging van 18%).
- Ook de gegevens van Ionite wijzen op een verdere stijging van de adoptie van de NLCIUS.

Tot slot blijkt uit gegevens van Logius het volgende:

In 2024 is wederom een stijging te zien in het aantal ontvangen e-facturen. Het totaal aantal e-facturen bedroeg 2.459.928, dat is 83,8% van de totale facturenstroom. Het percentage e-facturen steeg met 1,6% t.o.v. 2023. (bron: Jaarrapportage bedrijfsvoering Rijk 2024).

Ten opzichte van 2023 is er een flinke groei geweest van het aantal e-facturen wat naar de overheid is gestuurd. Het aantal e-facturen in het NLCIUS-formaat in 2024 (1.484.795) is gestegen met 22,8% ten opzichte van het jaar daarvoor.

Ten opzichte van 2023 is een lichte stijging van 26,1% in het aantal ontvangen facturen te zien via het Rijksoverheid Peppol Accesspoint (vorig jaar een stijging van 45%).

Mede op basis van bovenstaande gegevens is de mening van de normcommissie e-Facturatie dat het gebruik van NLCIUS nog steeds toeneemt. De data laten immers niet alleen een groei zien in het aantal NLCIUS endpoints maar ook in het totaal volume van e-facturen, wat het beste verklaard wordt door sterk stijgend gebruik van NLCIUS. Wel wordt zichtbaar, dat de adoptierate verlangzaamd. Dit kan onder andere worden verklaard met het feit, dat een steeds groter onderdeel van de facturenstroom al e-facturen zijn.

Relevante ontwikkeling

43

In 2024 zijn de werkzaamheden met betrekking tot het beheer van de NLCIUS overgedragen aan de normcommissie e-Facturatie van NEN. De verbeterde website van het STPE met semantic treehouse blijft gedurende 2025 behouden voor de gebruikersgemeenschap.

De normcommissie e-Facturatie is actief betrokken bij de herziening van EN 16931-1 naar aanleiding van wetgeving op het gebied van BTW in het digitale tijdperk (ViDA).

SETU

Waarom belangrijk?

De SETU-standaarden worden gebruikt voor het elektronisch berichtenverkeer in de branche voor flexibele arbeid. SETU regelt het uitwisselen van berichten tussen aanbieders en afnemers (inleners) van tijdelijk personeel.

De SETU-standaarden zijn Nederlandse implementaties van internationaal geldende standaarden, namelijk HR-Open en voor de factuur ook UBL. Deze standaarden specificeren voor de Nederlandse markt van flexibele arbeid welke gegevenselementen verplicht en welke optioneel zijn bij de uitwisseling van informatie. Deze gegevenselementen worden vervolgens afgebeeld op de gegevens in de HR-Open standaarden waardoor er toepassingsprofielen ontstaan.

De SETU-standaarden worden ontwikkeld en beheerd door de Stichting SETU waarin alle grote uitzendorganisaties in Nederland betrokken zijn. Ook kleinere uitzendorganisaties en softwareleveranciers voor de branche voor flexibele arbeid kunnen actief participeren in de ontwikkeling.

De SETU-standaarden staan op de 'pas toe of leg uit' lijst sinds 20 mei 2009.

Het gebruik van de SETU-standaarden is nog zeker niet bij alle (semi-)overheden common practice. De SETU-standaarden betreffen verschillende berichten, benodigd op verschillende momenten in het proces rondom tijdelijk personeel. En zeker niet al de berichten in de set van SETU-standaarden zijn breed geadopteerd. Dit bevestigt nog altijd het nut van de SETU-standaarden op de lijst.

Feitelijk gebruik

Belangrijke gebruikers van de SETU-standaarden zijn de participanten en abonnees van SETU: daaronder naast uitzendorganisaties ook uitvoeringsorganisaties (Logius, UWV), softwareleveranciers, CAO partijen, en publiekrechtelijke organisaties als TNO. Overheden zijn als klanten van de uitzendorganisaties gebruikers van de SETU-standaarden.

De SETU beschikt niet over gebruikscijfers, aangezien het berichtenverkeer niet via een centraal platform geregeld wordt. De enige concrete informatie over gebruikscijfers die de SETU heeft is een gebruikerspeiling uit 2020, waarin ook is nagegaan in welke volumes haar achterban berichtuitwisseling doet op basis van de SETU-standaarden. Op jaarbasis kwam dat toen per SETU-bericht per organisatie uit op het volgende (dit beeld is ook al opgenomen in eerdere monitoren):

Tabel 20. SETU (2020)

SETU bericht	volumes op jaarbasis per organisatie
Invoice	range 20.000 – 2.500.000
Timecard	range 350.000- 2.500.000
Assignment	range 40.000 – 800.000
Human Resource	range 40.000 – 800.000
Staffing order	range 0 – 500.000

Deze cijfers betreffen echter ook organisaties die buiten de publieke sector vallen. De nieuwe SETU Planning standaarden zijn niet meegenomen in de peiling van 2020 aangezien die in 2023 zijn ontwikkeld. De SETU beschikt niet over de gebruikscijfers van deze standaarden.

Van de kant van de beheerorganisatie wordt de inschatting gemaakt dat het gebruik van de standaard lichtelijk gestegen is. De beheerorganisatie ziet dat er in de markt steeds meer gebruik wordt gemaakt van geautomiseerd en gestandaardiseerd berichtenverkeer. Ook de introductie van de nieuwe ‘SETU Standards for Planning and Scheduling ’ heeft de scope van de set aan SETU standaarden verbreed en daarmee 25% nieuwe leden geworven, namelijk organisaties die zich bezighouden met planning. De introductie van de inlenersbeloning standaard heeft de scope ook vergroot en veel nieuwe partijen aangetrokken, zoals CAO-partijen. Daarnaast is er een verschuiving naar REST API's als factoren die de adoptie beïnvloeden.

Relevante ontwikkeling

In 2025 is de SETU Standard for Planning and Scheduling versie 2.0 gereleased. De eerste partijen zijn gestart met de implementatie van deze nieuwe standaard. Dit zijn zowel de voor SETU bekende uitzenders en softwareleveranciers alsook partijen die gespecialiseerd zijn in het ontwikkelen van personeelsplanningssoftware.

In 2023 heeft het bestuur van SETU opdracht gegeven voor het ontwikkelen van 2.0 versies van de huidige StaffingOrder, HumanResource, Assignment, Timecard en Vacancies standaarden. Deze ontwikkeling is in 2024 uitgevoerd, met uitzondering van de Vacancies standaard die in 2025 wordt ontwikkeld. Hiermee wordt er naast XML ook JSON-formaat ondersteund in de uitwisseling. Deze nieuwe berichten worden gebaseerd

op de nieuwste versie van de internationale HR Open standaard aangevuld met SETU-eigen eigenschappen. Hierdoor zijn deze berichten in lijn met de nieuwe planningsberichten.

Ter ondersteuning van de adoptie van de standaard is in samenwerking met Forum Standaardisatie een korte [animatievideo](#) ontwikkeld, waarin op toegankelijke wijze wordt uitgelegd wat de SETU-standaard is en welke rol deze speelt bij digitale gegevensuitwisseling. Daarnaast heeft de SETU ook in 2024 en 2025 een aantal webinars georganiseerd over haar standaarden en het gebruik ervan, waaronder een webinar over de 2.0-standaarden. Deze webinars zijn terug te vinden via de SETU-website en vormen een belangrijk middel om adoptie in de praktijk te stimuleren.

In het kader van community management is er een nieuwe SETU-werkgroep opgestart: werkgroep Adoptie & Communicatie. In 2025 is deze werkgroep bezig met het verbeteren van de website en aan te sluiten bij de verschillende doelgroepen van de SETU.

Een belangrijke ontwikkeling in de markt is de Wet toelating terbeschikkingstelling van arbeidskrachten (WTTA) en het correct toepassen van de inlenersbeloning. Om hieraan tegemoet te komen, heeft de SETU in 2025 een nieuwe standaard ontwikkeld voor het uniform uitvragen en vastleggen van de benodigde gegevens voor de inlenersbeloning. Deze standaard faciliteert de gegevensuitwisseling tussen inleners en uitleners, zodat alle ingrediënten aanwezig zijn voor een correcte en gelijkwaardige beloning van flexkrachten. De nieuwe standaard is volledig in lijn met de andere SETU-standaarden. De verwachting is dat deze initiatieven en ontwikkelingen leiden tot toename van de bekendheid, bruikbaarheid en het gebruik van de standaarden.

WDO Datamodel

Waarom belangrijk?

Het WDO Datamodel (WDO: Wereld Douane Organisatie, in het Engels WCO: World Customs Organization) is een wereldwijde gegevens-standaard die als basis dient voor het elektronisch uitwisselen van gegevens en berichten wanneer goederen, personen en/of vervoermiddelen de grens over gaan. De gegevensstroom verloopt tussen bedrijven en overheden en tussen overheden onderling. Het WDO Datamodel voorziet erin om deze uitwisseling van gegevens te simplificeren, te standaardiseren en te harmoniseren, zowel ten faveure van de bedrijven (bij het handel drijven) als de betrokken overheidsinstellingen.

Het doel van het gebruik van de standaard is een vlot en efficiënt verloop van de aankomst, het vertrek, de doorvoer en de vrijgave van goederen, vervoersmiddelen en personen in de internationale handel. In sommige landen wordt de douaneaangifte nog steeds (gedeeltelijk) op papier ingediend. Daarnaast moeten veel gerelateerde documenten, bijvoorbeeld certificaten van oorsprong of landbouwcertificaten, op papier bij andere overheidspartijen worden ingediend. In veel andere landen wordt al elektronisch gecommuniceerd, maar worden lokale standaarden gebruikt. Het betreft hier vaak nog verschillende standaarden omdat overheidsorganisaties in veel gevallen een eigen standaard voorschrijven. Dit vindt ook binnen de EU plaats, i.p.v. gebruik van 1 internationale standaard (WDO datamodel en EUCDM) kiezen de diverse landen toch vaak voor een eigen standaard. Door het gebruik van het WDO Datamodel kunnen de diverse overheidsorganisaties dezelfde taal spreken en eenvoudig informatie uitwisselen. Het WDO Datamodel bevat zogenaamde 'informatiepakketten' met informatie specifiek voor aangiften of vergunningen. Een informatiepakket beschrijft de semantiek van de uitgewisselde informatie: gegevens- en procesmodellen en hiervan afgeleide berichtspecificaties, de zogenaamde *Message Implementation Guidelines*, afgekort tot MIG's.

De standaard staat op de 'pas toe of leg uit' lijst sinds 15 april 2014. In 2023 heeft een evaluatie plaatsgevonden, waarbij voldoende draagvlak is geconstateerd om plaatsing van het WDO datamodel op de 'pas toe of leg uit'-lijst te handhaven. Zie ook; [Evaluatie WDO Datamodel | Forum Standaardisatie](#)

Feitelijk gebruik

Niet alleen de Douane past het WDO Datamodel toe, ook andere overheidsinstellingen die betrokken zijn bij grensoverschrijdend verkeer. Denk aan Rijkswaterstaat, de Havenautoriteiten, de Koninklijke Marechaussee en het Ministerie van I&W. De Douane past de standaard met name toe in berichten voor goederenstromen. Daarnaast biedt het WDO Datamodel zoals eerder al opgemerkt ook ruimte voor informatie over personen (voor bijvoorbeeld de Marechaussee) en informatie over vervoermiddelen (voor bijvoorbeeld Rijkswaterstaat).

De Douane (de beheerder van de standaard) meldt toepassing van het WDO Datamodel in de volgende typen bericht- en aangiftestromen:

- *MIG Single Window*
Dit betreft 20 inkomende berichten en 16 uitgaande berichten, gebaseerd op het WDO datamodel. Het Single Window voor maritiem en lucht is 1 loket waar alle meldingen voor Douane, Koninklijke Marechaussee/Zeehavenpolitie en NCA SafeSeaNet elektronisch dienen te worden doorgegeven. In 2026 wordt i.v.m. de komst van het EMSWe (European Maritime Single Window environment) in NL een NMSW (National Maritime Single Window) ingericht bij Portbase. Er zal uitwisseling van informatie gaan plaatsvinden van dit NMSW naar het huidige SW), dit zal gebeuren met op het WDO Datamodel gebaseerde berichten en betreft G2G (Government to Government) uitwisseling!
- *MIG Declaration Management System (DMS)*
Dit betreft 3 hoofdberichten (aangifte, aanvullende aangifte en response), gebaseerd op het WDO Datamodel. Deze berichten ondersteunen 24 douaneprocedures zoals beschreven in de EU wetgeving (voor inkomende berichten).
- *MIG Douane e-commerce (DECO)*
Dit betreft 3 hoofdberichten (aangifte, aanvullende aangifte en response), gebaseerd op het WDO Datamodel. Deze berichten ondersteunen 3 douaneprocedures zoals beschreven in de EU wetgeving (voor inkomende berichten).
- *MIG Import Control System Presentation Notification Information (ICS2 PNI)*
Dit betreft 2 inkomende berichten, gebaseerd op het WDO Datamodel.

Deze partijen passen het WDO datamodel nog niet toe:

- *De Nederlandse Voedsel- en Warenautoriteit (NVWA) Veterinair en Fytosanitair*
Het gaat om 2 hoofdberichten (aangifte en response), gebaseerd op het WDO datamodel. Deze berichten ondersteunen 6 procedures. De WDO gebaseerde berichten zijn nog niet geïmplementeerd, hiervoor wordt het juiste moment nog gezocht. Op dit moment wordt nog gebruik gemaakt van de zg. Sagitta-standaard in combinatie met een nationale standaard voor EDIFACT.
- *Douane Vervoer Aangifte (DVA)*
Voor deze MIG wordt het WDO datamodel (ondanks dat de gegevens in scope zijn) niet als standaard gehanteerd. Door onvoorziene omstandigheden kon voor het NL douanesysteem DVA de deadline niet gehaald worden als douane vast wilde houden aan zelfbouw. Er is daarom ook gekozen voor het zogenaamde ERMIS pakket, waarin een module voor Transit is opgenomen. Dit pakket werkt echter op basis van de door de EU gedefinieerde bericht(syntax)standaarden, welke niet identiek zijn aan de WDO syntax standaard. Gebruik van het WDO datamodel voor het externe domein (Business to Government en Government to Business) was wel mogelijk maar zou teveel werk (conversies) met zich meebrengen.

In zijn algemeenheid constateert de Douane dat in Nederland de meeste partijen die de standaard zouden moeten toepassen, dit ook doen. De adoptiegraad is hoog, en zal naar verwachting iets toenemen ten opzichte van vorig jaar door de toename in het gebruik van de Single Window voor maritiem en lucht.

Relevante ontwikkelingen

Nederlandse Voedsel en Waren Autoriteit

De Douane heeft met de NVWA een aantal gesprekken gevoerd over de toepassing van het WDO datamodel maar tot nu toe zonder resultaat. Forum Standaardisatie zal in 2025 initiatief nemen om deze gesprekken te hervatten.

Nieuw dataplatform/ datacatalogus bij de Douane

Binnen Douane wordt gewerkt aan een nieuw dataplatform / datacatalogus. Eén van de te gebruiken datastandaarden voor de modellen wordt het WDO datamodel.

Twee Europese ontwikkelingen

Andere relevante ontwikkelingen spelen vooral op Europese schaal:

1. Ontwikkeling European Maritime Single Window Environment

Zo ontwikkelt de EU een European Maritime Single Window Environment (EMSWe)-omgeving die ook is gerelateerd aan het WDO Datamodel, zij het via het International Maritime Organization datamodel (IMO). Daarbij lijkt het EMSWe zich te gaan richten op het Multimodal Transport, dat vooral betrekking heeft op havenprocessen. De IMO en de Wereld Douane Organisatie stemmen ontwikkelingen onderling af, om tegenstrijdigheden te vermijden. Het EMSWe kan gezien worden als een regionale specialisatie van het IMO Datamodel. Het IMO heeft een focus op vrachtverkeer; het EMSWe kijkt ook naar personen en bijvoorbeeld vergunningen. De scope is daarmee dus niet helemaal hetzelfde. Implementatie van het EMSWe heeft naar verwachting vooral impact aan de 'markt-zijde' van het Single Window voor maritiem en lucht. Het hangt af van de keuze die gemaakt wordt bij implementatie, of dit vooral tot aanpassingen leidt voor het centrale Single Window voor maritiem en lucht of voor individuele marktpartijen.

2. Ontwikkeling EUCDM

Verder ontwikkelt de EU een nieuw raamwerk voor douane-informatie, het EUCDM. De EU is lid van de Wereld Douane Organisatie, en stelt daar wijzigingen voor op basis van hun wensen om deze twee modellen op elkaar afgestemd te houden. Net als het WDO datamodel heeft dit model een focus op douane-gegevens die in dit geval gebaseerd zijn op EU wetgeving.

Wat met name deze twee Europese ontwikkelingen te betekenen zullen hebben op het WDO datamodel zoals dat nu op de 'Pas toe of leg uit'-lijst staat, moet nog blijken.

Uit de evaluatie van 2023 blijkt dat de adoptieadviezen die in 2014 gegeven zijn, zijn vervuld of niet meer relevant zijn. Wél geven de onderzoekers in het evaluatierapport drie adviezen aan het Forum Standaardisatie:

- a) Ga in gesprek met de NVWA over de achtergrond van het nog niet adopteren van het WDO Datamodel.
- b) Overweeg of het Forum Standaardisatie een meer aanjagende rol wil nemen in het opnemen van andere standaarden uit dit werkveld op de 'Pas toe of leg uit'-lijst. Dit kan door in enkele gesprekken te verkennen of er andere standaarden zijn in het domein 'Economie en Werk' op het vlak van handel en transport, die interoperabiliteit verbeteren en leveranciersafhankelijkheid binnen de overheid helpen voorkomen, als zij breed geadopteerd zouden worden.
- c) Ga in gesprek met de Douane over een planmatige aanpak om de impact van Europese ontwikkelingen op de standaard op de 'Pas toe of leg uit'-lijst in beeld te krijgen. In het licht van de Europese

ontwikkelingen (EMSWe en EUCDM) is namelijk nog niet duidelijk wat die kunnen betekenen voor het WDO Datamodel op de 'Pas toe of leg uit'-lijst.

In 2025 pakt Forum Standaardisatie het eerste advies op.

XBRL

Waarom belangrijk?

XBRL (eXtensible Business Reporting Language) is een internationale open standaard voor het gestructureerd digitaal delen van bedrijfsmatige informatie. Het is voor digitale informatie-uitwisseling belangrijk dat zowel computersystemen als mensen over alle sectoren en landen heen dezelfde (informatie)taal spreken. XBRL biedt de mogelijkheid om de inhoud en betekenis van gegevens te beschrijven en vast te leggen in een XBRL taxonomie.

Softwareontwikkelaars koppelen de taxonomie bijvoorbeeld aan gegevens uit de financiële administratie, fiscale regelgeving en rapportgenerators zodat de gegevens (her)gebruikt kunnen worden voor het samenstellen van (wettelijk) verplichte rapportages. Doordat XBRL-bestanden direct leesbaar zijn voor softwareapplicaties, betekent dit een enorme kostenbesparing op het vlak van verzamelen en verwerken van bedrijfsinformatie. Door deze wijze van aanlevering van financiële informatie is het mogelijk om in een boekhoudpakket één rapportage aan te maken en te versturen naar zowel bank als overheid.

Deze XBRL-standaard staat op de pas-toe-of-leg-uit-lijst sinds 17 april 2010.

Feitelijk gebruik

Het gebruik van XBRL wordt in de Monitor Open Standaarden gemeten door te kijken naar het gebruik van de nationale standaard SBR (Standard Business Reporting) die gebruikt wordt in de voorziening Digipoort. In onderstaande tabel staat het aantal XBRL-berichten. Deze cijfers zijn in het kader van SBR gerapporteerd t.b.v. de Monitor GDI. Belangrijke voorstanders van deze XBRL-standaard binnen het publiek-private SBR-samenwerkingsverband zijn terug te vinden in de tabel: de Kamer van Koophandel, de Woningcorporatiesector, DUO en de Belastingdienst.

Tabel 21. XBRL (2019-2025)

	Realisatie 2019	Realisatie 2021	Realisatie 2023	Realisatie 2025 t/m september
Belastingdienst				
Aangifte IB + VPB	16.558.025	15.846.758	17.219.117	13.596.686
Aangifte OB + Intercomm.	5.429.106	6.379.104	7.960.681	6.098.904
Toeslagen	1.325.719	1.355.471	1.978.644	1.264.748
Erfbelasting+	4.073	31.496	52.176	39.089
Uitsluitend Zakelijk Gebruik	1.143	854	312	247
KvK – Reporting Services (SBR)				
Jaarrekeningen	1.020.450	889.466	943.625	608.714
DUO – Reporting Services (SBR)				
Jaarrekeningen	1.953	1.963	5.015	3.511
SBR Wonen - Reporting Services (SBR)				
DPI (prognose informatie)	1.112	898	1.163	116
DVI (verantwoordingsinformatie)	1.363	1.745	1.744	1.630
SBR Wonen Jaarrekening	1.364	1.226	1.185	1.140

49

Deze cijfers zijn in lijn met de cijfers over de voorgaande jaren: de adoptie van SBR en daarmee XBRL binnen Nederland is stabiel.

Er is nog potentie voor verdere groei van het gebruik van XBRL binnen Nederland. Immers, indien er van uit wordt gegaan dat bij financiële verantwoordingsrapportages SBR gebruikt zou moeten worden dan impliceert dat dat alle ministeries, provincies, waterschappen, gemeenten, uitvoeringsinstanties en ZBO's gebruik zouden moeten maken van XBRL. Dit is echter nog niet de praktijk.

[XBRL Nederland](#) zet zich in voor de verbreding van gebruik van XBRL, zowel binnen als buiten de overheidssector, door het organiseren van webinars, schrijven van blogs en nieuwsbrieven.

Relevante ontwikkeling

Grote rechtspersonen moeten vanaf boekjaar 2025 verplicht hun jaarrekeningen in Inline XBRL deponeren. Inline XBRL is gekozen omdat die standaard ook gebruikt wordt voor European Single Electronic Format. Dat is de verplichte standaard voor de manier waarop beursgenoteerde bedrijven in de EU hun financiële jaarverslagen moeten opstellen en indienen. Het grote voordeel van Inline XBRL is dat de informatie zowel leesbaar is voor mensen als dat het geautomatiseerd kan worden verwerkt.

5. Domein schoon water en beschermde bodem

Aquo-standaard

Waarom belangrijk?

De Aquo-standaard is één van de drie stelselstandaarden op de 'pas toe of leg uit' lijst. De Aquo-standaard maakt het mogelijk om op een uniforme manier gegevens uit te wisselen tussen partijen die betrokken zijn bij het waterbeheer. (waterbeheerders maar ook laboratoria en adviesbureaus die gegevens uitwisselen met deze waterbeheerders). Daardoor draagt de Aquo-standaard bij aan een kwaliteitsverbetering van het waterbeheer. De Aquo-standaard is bedoeld voor iedereen die te maken heeft met het vastleggen en gebruiken van gegevens; zowel op zee als binnendijks, in beekdalen en polders, bij grond- en afvalwater, voor waterkwaliteit, -kwantiteit, -systeem en -veiligheid. De Aquo-standaard wordt beheerd door het Informatiehuis Water (IHW). De Aquo-standaard staat op de 'pas toe of leg uit' lijst sinds 17 mei 2016.

Deze status houdt in dat nieuwe versies van de Aquo-standaard automatisch op de 'Pas Toe Of Leg Uit'-lijst van het Forum Standaardisatie komen. Het betekent bovendien dat het beheer van de Aquo-standaard goed geregeld is. Aquo is een verplichte open standaard: alle informatie is vrij toegankelijk en gratis te downloaden. Daarmee zijn overheidsorganisaties verplicht om de Aquo-standaard toe te passen bij de aanschaf van een ICT-dienst of -product met een waarde vanaf € 50.000.

Feitelijk gebruik

De waterbeheerders (waterschappen, de provincies en Rijkswaterstaat) hebben jaarlijks de verplichting om aan bij het ministerie van Infrastructuur & Waterstaat te rapporteren over de waterkwaliteit en waterveiligheid. Hiervoor zijn verschillende informatiestromen ingericht die het Informatiehuis Water organiseert en faciliteert. Door daarbij gebruik te maken van de Aquo-standaard is sprake van uniforme en efficiënte gegevensuitwisseling.

In 2021 is de nieuwe Aquo-omgeving [Aquo Wiki](#), in gebruik genomen. Deze nieuwe geïntegreerde omgeving wordt sindsdien veelvuldig gebruikt. Het onderstaande inzicht van het gebruik in 2023 is gebaseerd op deze bron:

• bezoeken	30.573	(+ 44% t.o.v. 2022)
• paginaweergaven ¹¹	115.433	(+ 14% t.o.v. 2022)
• downloads	4.025	(+ 7% t.o.v. 2022)
• uitgaande links ¹²	1.414	(- 28% t.o.v. 2022)

Deze cijfers wijzen alles bij elkaar genomen op een **toename van het gebruik** in de periode 2023 ten opzichte van 2022. Alleen de laatste variabele valt wat terug, nadat juist daar vorig jaar sprake was van een grote stijging (+ 77%; zie de vorige monitor-rapportage).

Wat mogelijk heeft bijgedragen aan deze toename is dat in 2023 een aantal bijzondere resultaten is behaald en verder dat enkele ontwikkelingen in gang zijn gezet. Zie daarvoor de onderstaande passage 'relevante ontwikkeling'.

¹¹ Geslaagd verzoek om een bepaalde webpagina te tonen.

¹² Links op onze site, die bezoekers sturen naar andere sites (o.a. Aquo-sharepoint, IHW, SIKB).

Gebruikers van de Aquo-standaard zijn ook middels het indienen van wijzigingsvoorstellen en het melden van incidenten (gestelde vragen) betrokken bij de ontwikkeling van de standaard. Een deel van de door het Informatiehuis Water verstrekte gegevens over het gebruik van de Aquo-standaard haakt hierop in:

Instroom op de Aquo-standaard:

aantal ingediende wijzigingsvoorstellen:	122 (vorig jaar: 154)
aantal gemelde incidenten:	136 (vorig jaar: 149)

Aantal waterbeheerders dat een wijzigingsvoorstel indient / een incident meldt:

betrokken instanties bij wijzigingsvoorstellen:	35 (vorig jaar: 29)
betrokken instanties bij melden incident:	49 (vorig jaar: 46)

Relevante ontwikkeling

In 2023 is onder meer gewerkt aan de verbetering en vernieuwing van de Aquo-standaard en de doorontwikkeling van het Waterkwaliteitsportaal en het Waterveiligheidsportaal. Daarnaast hebben we de waterbeheerders ook dit jaar weer maximaal ondersteund om te kunnen voldoen aan de landelijke en Europese verplichtingen. Zowel in werkprocessen, met rapportages als met onze portalen en systemen. We lichten deze activiteiten hierna toe.

Door standaardisatie is het mogelijk om met de data van verschillende waterbeheerders landelijk dekkende informatie te geven. En om die informatie op een uniforme manier uit te wisselen tussen bijvoorbeeld waterbeheerders, laboratoria en adviesbureaus. Het efficiënt delen van informatie levert voordeel op in tijd en geld en draagt daarmee bij aan de kwaliteit van het waterbeheer.

In 2023 is daarnaast ook een aantal bijzondere resultaten behaald en zijn enkele ontwikkelingen in gang gezet:

- Met de opname van de Naam, Code, Symbool (NCS) in de Aquo-standaard is de basis gelegd voor een uniforme naamgeving, codering en symboliek binnen de afvalwatersector. Maandag 27 september zagen meer dan 80 deelnemers in een online presentatie dat vanuit de Aquo-standaard een serieuze stap is gezet in het ondersteunen van Assetmanagement. Minder zichtbaar, maar niet minder belangrijk is dat gelijktijdig een basis is gelegd voor een Linked Data implementatie van de Aquo. Zie ook [NCS - Naam Code \(Symbool\) opgenomen in Aquo-standaard \(ihw.nl\)](#).
- Met de oprichting van een Aquo Linked Data Community is een virtuele plek gecreëerd waar gebruikers van de Aquo-standaard en Aquo-teamleden elkaar kunnen inspireren door kennis te delen. Zie ook [Kick-off Aquo Community: 2+2=.... meer dan 4! \(ihw.nl\)](#)
- De hermodellatie van de Aquo-informatiemodellen is van start gegaan. Het eerste model dat vernieuwd is, is IMWA Kunstwerken. Om optimaal te kunnen aansluiten op de wensen van de gebruikers, wordt per informatiemodel een publieke consultatie gehouden. Zie ook [Aquo-standaard: Publieke consultatie IMWA Kunstwerken \(ihw.nl\)](#)
- In 2023 is in opdracht van de partners die deelnemen in het Centraal College van Deskundigen Datastandaarden (CCvD-D) een onderzoek uitgevoerd naar de toekomstbestendigheid van het CCvD-D. Het eindrapport 'Kansen vergroten voor samenwerking' leverde minder expliciete conclusies op dan vooraf werd verwacht. Samen met Rioned en SIKB heeft het Informatiehuis Water een vervolgopdracht gegeven om een Roadmap Datastandaarden op te stellen¹³.

¹³ Bron: Jaarverslag 2023 Informatiehuis Water

Waarom belangrijk ?

Riolering is een essentiële maatschappelijke voorziening en het beheer ervan een sleutelzaak voor gemeenten. Het doelmatig managen van (afval)watersystemen vraagt om een gemeenschappelijke taal. Ook maatschappelijke opgaven zoals klimaatadaptatie, energietransitie en de bouwopgave vereisen een goede (digitale) integrale aanpak. Het Gegevenswoordenboek Stedelijk Water (GWSW), een speciale datastructuur die systemen en processen op het gebied van stedelijk waterbeheer eenduidig structureert en faciliteert, voorziet hierin. De GWSW-ontologie specificeert het uniform vastleggen, uitwisselen, presenteren en (her)gebruiken van data van objecten (kenmerken, conditie, metingen) en processen.

De GWSW-standaard staat op de 'pas toe of leg uit' lijst sinds 23 maart 2020. Opname op deze lijst draagt bij aan de implementatiegraad; het verplichte karakter is een prikkel voor zowel softwarebouwers als de publieke opdrachtgevers.

Feitelijk gebruik

Eind 2023 hebben 203 gemeenten rioleringsdatasets (die 71% van de inwoners van NL omvatten) op het landelijke dataplatform met rioleringsdatasets geplaatst. Een jaar daarvoor, eind 2021, waren dat nog 185 gemeenten. De **gestage groei** (net als vorig jaar) is toe te schrijven aan het volgende:

- ook in 2023 zijn beheerapplicaties en adviesbureaus het GWSW beter gaan ondersteunen waardoor gemeenten in staat zijn het GWSW zelf toe te passen;
- steeds meer gemeenten (inmiddels 100!) willen hun rioleringsdata open publiceren via Publieke Dienstverlening Op de Kaart (PDOK)¹⁴;
- andere (software-)toepassingen baseren zich (rechtstreeks, via het GWSW-platform van Stichting RIONED en zeker ook via PDOK) op GWSW-conforme rioleringsdata, waardoor meer gemeenten gemotiveerd worden om de voordelen van GWSW-conforme data zelf ook te benutten;
- toenemende regionale samenwerking is voor gemeenten en waterschappen een prikkel om het GWSW te gebruiken als basis voor hun beheer en daarbij benodigde data(uitwisseling);
- in 2024 zal voor de Monitor Gemeentelijke Watertaken een deel van de gegevensverzameling plaatsvinden op basis van de (GWSW-conforme) gemeentelijke datasets op het GWSW-platform <https://apps.gws.nl>. Dat motiveerde een flink aantal gemeenten om hun data voor het eerst of weer geactualiseerd op dat platform te plaatsen;
- de waterschappen hebben in 2023 hun rioleringsdata ook conform de GWSW-standaard op dat platform geplaatst en van daaruit is de doorlevering naar PDOK in een eigen geo-thema gerealiseerd. Bovendien gebruiken de waterschappen sinds kort gemeentelijke rioleringsdata gebaseerd op het GWSW-deelmodel Kengetallen voor afvalwaterprognoses (capaciteits-berekeningen).

Verder mag in het kader van het realiseren van de randvoorwaarden voor het gebruik van GWSW het volgende niet onvermeld blijven:

- alle openbare bestekken voor rioolreiniging en –inspectie schrijven het GWSW.RibX uitwisselformaat voor en uitvoerende partijen gebruiken dat bestandsformaat routinematig;
- uit de periodieke GWSW applicatietoets blijkt dat vrijwel alle integrale en rioleringsbeheer-pakketten, alle inspectiesoftware en alle modelleringsoftware de voorgeschreven GWSW-formaten kunnen uitwisselen;

¹⁴ PDOK is het landelijke platform voor het ontsluiten van geodatasets van Nederlandse overheden.

- in 2024 worden belangrijke stappen gezet in de integratie van het GWSW in het IMBOR (Informatiemodel Beheer Openbare Ruimte) en in het afronden en toepasbaar maken van nieuwe GWSW deelmodellen GWSW Persleidingen, GWSW Gemalenbeheer en GWSW Maatregelen. Die zullen naar verwachting de adoptie en het gebruik verder stimuleren.

Relevante ontwikkeling

Het Overheidsbrede Beleidsoverleg Digitale Overheid (OBDO) heeft op 12 mei 2021 op voorspraak van Forum Standaardisatie een aantal mutaties op de officiële lijsten met open standaarden bekrachtigd. GWSW versie 1.4 is daarmee op de 'Pas toe of leg uit'-lijst vervangen door versie 1.5.1 en eind 2021 is dat vervangen door versie 1.5.2. Per 1 januari 2023 is de vigerende versie 1.6. Medio 2024 wordt versie 1.6.1 gepubliceerd.

Overheden zijn verplicht bij alle relevante software-aanbestedingen de GWSW-standaard inclusief gespecificeerde uitwisselformaten OroX, HydX en/of RibX te eisen. Met name de module GWSW-HYD ten behoeve van hydraulische modellering en de ontsluiting rioleringsdata als open data naar PDOK leiden tot waardevolle gebruiksmogelijkheden voor gemeenten, waterschappen en adviesbureaus.

Voor nog niet alle gemeenten is het vanzelfsprekend dat de vigerende GWSW-standaard en uitwisselformaten als eis gelden voor hun integraal softwarepakket voor beheer van (objecten in) de openbare ruimte. Hoewel het draagvlak bij functioneel beheerders afgelopen twee jaar flink gegroeid is, is de verplichting bij inkoopafdelingen, management en bestuur veelal nog niet bekend en vanzelfsprekend. Omdat implementatie van het GWSW op termijn wel zal leiden tot aanpassingen in werkprocessen, benodigde competenties en inrichting van ICT-systemen, is ook daar wel draagvlak nodig. De PTOLU-status zal daaraan bijdragen.

53

De zeer positieve verhouding van de kosten (voor ontwikkeling en implementatie van de GWSW-standaard) tot de baten (in de vorm van betere inzichten, betere investeringen, betere beheermaatregelen en betere afstemming) zal dat versterken. De samenwerking bij de ontwikkeling en implementatie van informatiestandaarden in andere domeinen in de openbare ruimte zal veel synergie geven. Onder de titel 'BORius', Beheer Openbare Ruimte Informatie- en Uitwisselstandaarden, werken daartoe o.m. Stichting RIONED, CROW, VNG, GeoBusiness Nederland, IPO, Rijkswaterstaat, DigiGO, MijnAansluiting en Centrum Ondergronds Bouwen samen.

SIKB0101 en SIKB0102

Waarom belangrijk?

De standaarden verhogen de efficiëntie van de uitwisseling in de keten van informatie over de milieu-hygiënische kwaliteit van de bodem (SIKB0101) en over archeologische vondsten in de bodem (SIKB0102). De standaarden besparen veel tijd, omdat overtypen van data achterwege kan blijven. Met behulp van de standaarden SIKB0101 en SIKB0102 kunnen bodemgegevens en archeologische gegevens op een eenduidige wijze en foutloos worden uitgewisseld. Ook voor de softwareleveranciers is de standaard erg praktisch: aanpassingen aan de eigen software door wijzigingen bij een andere leverancier kunnen achterwege blijven.

SIKB0101 is een standaard voor de uitwisseling van bodemkwaliteitsgegevens, inclusief geografische en administratieve gegevens. Op basis daarvan kan worden vastgesteld of sprake is van schadelijke gevolgen voor de volksgezondheid en het milieu ten gevolge van bodemvervuiling. Deze inzichten dragen ook bij aan het voorkomen van dergelijke schadelijke effecten. Zo wordt een bijdrage geleverd aan de bescherming van de volksgezondheid en het milieu. Belangrijke gebruikers binnen de overheid zijn Rijkswaterstaat, omgevingsdiensten, provincies, waterschappen en gemeenten.

SIKB0102 voorziet in de optimalisering van de digitale uitwisseling van archeologische gegevens tussen opgravende instanties, vondstendepots en/of archeologische registers. Een opgravende instantie, overheidsorganisatie of een bedrijf dat archeologisch onderzoek en/of vondsten doet heeft namelijk een wettelijke plicht om binnen twee jaar na afronding van de opgraving de verzamelde informatie beschikbaar te stellen aan daartoe ingestelde depots binnen de overheid: op landelijk niveau, provinciaal, en op gemeentelijk niveau.

SIKB 0101 staat op de 'pas toe of leg uit' lijst sinds juni 2012, SIKB0102 sinds februari 2016. Vermelding van beide standaarden op de lijst bevordert het duurzaam gebruik van deze standaarden in de sector.

Feitelijk gebruik

Voor beide standaarden geldt dat informatie over de milieu-hygiënische kwaliteit van de bodem (SIKB0101) respectievelijk over archeologische vondsten in de bodem (SIKB0102) in de regel niet door overheden zelf wordt gegenereerd. Marktpartijen zoals onderzoeksbureaus en opgravende bedrijven voeren het onderzoek uit. Daarna leveren deze marktpartijen de verzamelde informatie aan bij overheden, waarna de overheden deze informatie weer onderling delen. De keten van bodeminformatie bestaat in deze context dus zowel uit private partijen als uit overheidsorganisaties. De beide standaarden worden zowel gebruikt voor de uitwisseling binnen het private domein, de uitwisseling van het private domein met het publieke domein als voor de uitwisseling van overheidsorganisaties onderling. SIKB0101 en SIKB0102 zijn breed geïmplementeerde standaarden binnen de domeinen Bodem en Archeologie.

Specifiek met betrekking tot SIKB0101 is de praktijk dat alle gemeenten, omgevingsdiensten en provincies werken met software die gebruik maakt van de datastandaard SIKB0101. Dit blijkt uit de overeenkomsten die SIKB heeft met de leveranciers van software die SIKB0101 gebruiken. Deze leveranciers zijn lid van de Technische Werkgroep die de wijzigingsverzoeken behandelt voor SIKB0101. Softwareleveranciers als ook de eindgebruikers van data zijn in het Centraal College van Deskundigen (CCvD) Datastandaarden vertegenwoordigd, waar besluitvorming plaatsvindt over de doorontwikkeling van de standaard.

Op jaarbasis worden miljoenen data uitgewisseld via SIKB0101 tussen applicaties die deze standaarden hebben geïmplementeerd. Afgelopen jaar en dit jaar wordt vanuit de beheerorganisatie aangegeven dat het **gebruik van SIKB0101 stabiel** is. Gezien het feit dat alle gemeenten, omgevingsdiensten en provincies werken met software die gebruik maakt van de datastandaard SIKB0101, is de groeipotentie in Nederland voor wat betreft het aantal gebruikers uit de overheidssector niet groot meer bij SIKB0101. Vanuit het buitenland begint de interesse in de datastandaard toe te nemen. SIKB is momenteel met de stakeholders aan het bezien of en hoe dit gefaciliteerd kan worden, bijvoorbeeld door het beschikbaar stellen van een Engelse vertaling van de datastandaard.

Via SIKB0102 is sprake van uitwisseling van tienduizenden data; dit betreft een veel kleinere markt dan die van SIKB0101. Voor deze standaard SIKB0102 is sprake van **toename van het gebruik** gedurende het afgelopen jaar. Bij SIKB0102 is vooral sprake van toename in de keten bij opgravende bedrijven waar digitale uitwisseling steeds meer gemeengoed wordt. De beheerorganisatie achter de standaarden, SIKB, ziet dit aan de toename van het aantal softwareleveranciers en -ontwikkelaars die een deelnameovereenkomst hebben met SIKB voor het gebruik van SIKB0102 (en ondersteuning). Ook wordt een toenemend gebruik van de validatietool waargenomen. Dit geldt zowel voor marktpartijen (opgravende bedrijven) als depots. De volgende partijen gebruiken de datastandaard SIKB0102 in hun software en stellen het gebruik ervan verplicht:

Landelijk registratiesysteem ARCHIS van de Rijksdienst voor het Culturele Erfgoed (RCE);
Data Archiving and Networking Services (DANS). Het E-depot voor de duurzame opslag van digitale data;
BIJ12, beheerder van het provinciaal depot beheer system (Archeodepot). Archeodepot wordt inmiddels door 11 van de 12 provincies gebruikt.

Nagenoeg alle provincies maken gebruik van dit systeem waarvan het beheer is ondergebracht bij GBO-BIJ12. Vanuit Archeodepot worden gegevens volledig geautomatiseerd doorgezet naar het landelijke E-depot van DANS. Aansluiting van Archis op deze landelijke voorziening is in ontwikkeling.

Relevante ontwikkeling

Voor wat betreft SIKB0101 is de uitbreiding van de Basisregistratie Ondergrond met data over de milieuhygiënische kwaliteit van de bodem (BRO fase II) nagenoeg afgerond. Bij de standaardisatie van de milieukwaliteit (inclusief PFAS) is het de datastandaard SIKB0101 als basis genomen voor de ontwikkeling van IMBRO/IMBRO-A standaard. Hiervoor zijn enkele aanpassingen in de standaard doorgevoerd. Vanaf 1 oktober 2024 is het mogelijk om gegevens van het milieuhygiënisch bodemonderzoek (SAD) aan de landelijke voorziening van de BRO aan te leveren. Milieukwaliteit is vanaf 1 juli 2025 een nieuw en verplicht onderdeel van de BRO. Hiernaast is gewerkt aan het uitbreiden van de standaard ten behoeve van uitwisseling van onderzoeksgegevens over asbest in bodem. Hiervoor wordt eind 2025 een grotere update (x-wijziging) verwacht.

Ten aanzien van SIKB0102 werkt de Rijksdienst voor het Culturele Erfgoed aan een grote verbeterslag op het Archeologisch Basis Register (ABR). Begin 2024 is de gewijzigde Artefactentabel vastgesteld en dit was het laatste onderdeel van de verbeterslag. Deze wijziging wordt in 2024 geïmplementeerd in SIKB0102, waardoor optimale harmonisatie wordt bereikt met het ABR.

Voor de herbouw van ArcheoDepot door Bij12 is in oktober 2023 akkoord gegeven door de provincies op de business case met de voorgestelde oplossingsrichting. De herbouw is in volle gang en er is vanuit de TW SIKB 0102 verbinding gelegd met de ontwikkelaars voor het verzorgen van feedback vanuit het perspectief van het gebruik van de datastandaard.

6. Domein bouwen en wonen

IFC

Waarom belangrijk?

De IFC-standaard (Industry Foundation Classes) is een open en neutraal bestandsformaat dat wordt gebruikt voor het uitwisselen van bouw informatie in de bouw- en vastgoedsector, onafhankelijk van leverancier. Door gebruik te maken van dit uitwisselformaat hoef je niet specifieke bestandstypen uit te vragen en is samenwerken tussen partijen eenvoudiger. Ook zijn er voldoende gratis IFC-viewers beschikbaar waarmee je de ontvangen IFC kunt openen. Hierdoor hoef je geen dure programmatuur aan te schaffen om een ontvangen IFC-model te bekijken.

Hiernaast biedt het gebruik van IFC meer voordelen, zoals geautomatiseerde controles door middel van vooraf gestelde eisen aan de IFC (ook wel IDS genoemd), en is het mogelijk om geautomatiseerde rapportages te genereren met afwijkingen (BCF). Zie ook onderstaande afbeelding:

Voorbeeld: Je gebruikt zelf Revit 2018 en je ontvangt een Revit 2025-bestand. Je kunt dit bestand niet openen, aangezien je een oudere versie van het programma hebt. IFC voorkomt dit.

Maatschappelijk nut: Je voorkomt onnodige uitwisselproblemen die voor frustratie en tijdverlies zorgen. Daarnaast hoeft er ook geen specifieke programmatuur aangeschaft te worden om modellen te bekijken/valideren. Bevordert duurzaamheid en circulariteit via digitale informatiestromen. Ondersteuning van beleidsdoelen rond klimaat, energie, woningbouw en infrastructuur.

56

Pas toe of leg uit: IFC vergemakkelijkt (internationaal) samenwerken. Door het op de "pas toe of leg uit"-lijst te plaatsen, is de organisatie voorbereid op de toekomst en kan er zonder dure aanschaf van applicaties toch informatie uitgewisseld worden. Ondersteunt beleidsdoelen van het Bestuursakkoord Digitale Gebouwde Omgeving (Digitaal Stelsel Gebouwde Omgeving) waarin het gebruik van open standaarden als randvoorwaarde is opgenomen. Duidelijk signaal aan publieke opdrachtgevers om IFC structureel op te nemen in aanbestedingen. Creëert een gelijk speelveld voor marktpartijen en versnelt digitale transformatie in de bouwsector.

Feitelijk gebruik

We zien een toename van het gebruik. In de bijlage, de IFC-mandaten van 2024 en 2025, zien we internationaal een trend dat steeds meer opdrachtgevers dit vereisen. Binnen de Nederlandse sector zien we ook steeds meer gebruik, denk bijvoorbeeld aan Port of Rotterdam of Waterschappen, maar ook aan RVB, gemeenten en provincies. Binnen kleinere gemeenten speelt dit minder, vanwege een tekort aan bekendheid/onwetendheid, terwijl bij grotere gemeenten dit toeneemt (zie ook: <https://www.buildingsmart.nl/nieuws/2024-07-06-nieuwe-sponsor-gemeente-rotterdam-binnen-de-gemeente-rotterdam-zijn-we-volop-bezig-om-data-door-de-keten-te-laten-stromen>). Zeker met de behoefte aan de "digitale tweelingstad", zoals bij Gemeente Den Haag (Spiegelstad), Gemeente Rotterdam, maar ook Gemeente Groningen.

Zie ook presentaties van Digital Friday door digiGo, waar het onderwerp afgelopen jaar onderdeel van de presentatie was (zie afspeellijst:

https://www.youtube.com/watch?v=2XemTltw_9Q&list=PLLFgh1x7aep13lj14s8HEixo4CPUDFFmG).

Zeker met de automatisering die verder ontwikkeld wordt op basis van IFC, zal dit alleen maar toenemen. Denk bijvoorbeeld aan de automatische vergunningchecker (ontwikkeling bij o.a. Gemeente Rotterdam) of de hierboven genoemde werkmethode.

Relevante ontwikkelingen

Momenteel is IFC 5 in ontwikkeling, die op zeer korte termijn verwacht wordt. Hierin wordt adoptie nog makkelijker, aangezien er fundamentele wijzigingen toegevoegd worden. Afgelopen jaar is IDS live gegaan. Hiermee wordt het nog makkelijker om een IFC-model automatisch te toetsen, waarmee de kwaliteit van de modellen toeneemt en de tijdsbesteding afneemt. Hierdoor meer Kostenbesparing door hergebruik van data. Ook is de buildingSMART Foundation Course afgelopen jaar veelvuldig gevolgd, met meer dan 160 ingenieurs die dit binnen de Benelux hebben gevolgd. Deze cursus geeft je als organisatie de handvatten om conform deze werkmethode te werken. Ook is de Practitioner Course dit jaar live gegaan, waarin een hands-on training plaatsvindt over hoe je de bovenstaande werkmethode binnen je organisatie kunt toepassen.

NLCS

Waarom belangrijk?

De Nederlandse CAD Standaard (NLCS) bevat afspraken voor het maken van tweedimensionale ontwerptekeningen in de grond-, weg- en waterbouw (GWW). De standaard omvat onder andere richtlijnen voor metadata in objecten, het tekenblad, lettertypen, maatvoering en de ordening van objecten en lagen. NLCS zorgt voor uniformiteit in het tekenwerk, wat de samenwerking tussen organisaties aanzienlijk vereenvoudigt.

De standaard wordt breed toegepast in zowel de publieke als private sector. NLCS zorgt ervoor dat opdrachtnemers op een eenduidige manier werken, wat meerdere voordelen oplevert: digitale tekeningen zijn makkelijker uit te wisselen, hertekenen is niet nodig, tekeningen blijven 10 tot 15 jaar na oplevering bruikbaar voor onderhoud en reconstructie, opdrachtnemers hoeven niet per opdrachtgever verschillende tekenafspraken te hanteren.

Dankzij plaatsing op de 'pas toe of leg uit'-lijst in 2018 is de adoptie van de standaard sterk toegenomen. De groeiende gebruikersgroep draagt via een vrijwillige bijdrage bij aan beheer en doorontwikkeling van NLCS.

NLCS speelt ook een rol in actuele maatschappelijke opgaven, zoals energietransitie, circulariteit, duurzaamheid en CO₂-reductie.

De NLCS-standaard wordt gebruikt voor ontwerp en revisie van onder andere straten, pleinen, stadsgebieden, ondergrondse infrastructuur (riolering, kabels en leidingen), spoortrajecten, elektriciteitsnetwerken, groenvoorzieningen en natuurgebieden, sportvelden

Feitelijk gebruik

NLCS wordt gebruikt door ±1.340 organisaties, waarvan:

- 1.100 private partijen (zoals advies- en ingenieursbureaus, aannemers, installateurs)
- 230 publieke partijen (waaronder Rijksoverheid, provincies, gemeenten, waterschappen, Schiphol, netbeheerders, Rijksvastgoedbedrijf)
- ±7.000 eindgebruikers, via softwareleveranciers verspreid

Het gebruik van de NLCS standaard is stabiel. Dit heeft te maken met het feit dat de adoptie in de GWW-sector hoog is. Er gaan enkele gebruikers of omdat organisaties het tekenwerk uitbesteden aan en er komen nieuwe gebruikersgroepen bij als gevolg van de uitbreidingen van de standaard.

Overige kengetallen:

- 90% van alle GWW-projecten maakt gebruik van de NLCS-standaard
- Totale projectomvang: > €1-2 miljard

- Jaarlijkse baten voor de sector: €20-40 miljoen
- Voordelen: Hogere efficiëntie, minder faalkosten, verlaging van de Total Cost of Ownership

Relevante ontwikkelingen

- **Energiesector:** heeft een uitbreiding op de NLCS-standaard uitgebracht, die binnenkort wordt geïntegreerd met de NLCS standaard.
- **Drinkwaterbedrijven:** starten een project om hun maatwerkoplossingen te integreren in de landelijke standaard.
- **Verkeersborden:** toegevoegd aan de NLCS-standaard.
- **Ketenbrede doorontwikkeling:** gericht op toepassing van NLCS van ontwerp tot assetmanagement en revisie.
- **2D en 3D integratie:** project gestart om beide tekenvormen beter op elkaar aan te laten sluiten.

Marktontwikkelingen:

- Steeds meer gemeenten beschikken niet meer over een civieltechnische afdeling of vakinhoudelijke medewerkers. Zij besteden tekenwerk conform NLCS volledig uit aan opdrachtnemers.
- Deze gemeenten voldoen wél aan de 'pas toe of leg uit'-verplichting, maar hebben geen eigen software meer nodig.

De professionalisering van de standaard wordt de komende jaren voortgezet. Release- en changemanagement zijn verbeterd; updates worden regelmatig uitgebracht op basis van gebruikerswensen.

58 Organisaties vervangen steeds vaker hun maatwerkoplossingen door standaarden. Een voorbeeld:

“Onze GIS- en CAD-processen zijn strak ingericht met maatwerk, waarmee zelfs aannemers contractueel moeten werken. Maar maatwerk is niet langer houdbaar. Het vraagt te veel van onze beperkte expertcapaciteit en remt innovatie. We willen toe naar een open landschap waarin asset-informatie gestandaardiseerd uitwisselbaar is. Daarom stellen we voor om de NLCS-standaard uit te breiden met de drinkwatersector. Zodra leveranciers deze integreren, kunnen wij afscheid nemen van ons maatwerk.”

Ondanks de trend richting 3D-tekeningen blijft 2D-tekenwerk onmisbaar. Het aantal initiatieven om NLCS te harmoniseren met andere standaarden, én te combineren met zaken als kostenraming en vergunningstrajecten, neemt toe.

De NLCS-standaard is sinds eind jaren '80 in gebruik en vormt een stabiele en onmisbare schakel in de digitale transformatie van de bouw- en infrasector.

VISI

Waarom van belang?

VISI is een standaard workflow-systematiek die zorgt voor gestructureerde uitwisseling van berichten binnen bouw- en beheerprocessen. Hierdoor wordt informatie op een uniforme manier gedeeld tijdens de uitvoering en het beheer van bouwprojecten. De VISI-systematiek beschrijft wanneer iemand in het bouwproces informatie aanlevert aan een ander, en welke informatie dat is. Dit zorgt voor transparantie, duidelijkheid en maakt afspraken juridisch en planmatig traceerbaar.

Het doel van VISI is om de transparantie en traceerbaarheid van het bouwproces te vergroten. Daarmee wordt de kwaliteit en efficiëntie verhoogd en de doorlooptijd verkort. Dit draagt uiteindelijk bij aan lagere

bouwkosten, georganiseerd contractmanagement, betere procesbeheersing en duidelijke juridische afspraken.

Het gebruik van de VISI-standaard wordt voornamelijk geïnitieerd door opdrachtgevers. Zij willen grip houden op hun bouwprojecten. Opdrachtgevers zijn onder andere ministeries, agentschappen, provincies, gemeenten en hoogheemraadschappen.

De totale omvang van lopende VISI-projecten in de sector bedraagt meer dan €2 miljard. De effecten zijn onder andere: hogere efficiëntie, reductie van faalkosten, kortere doorlooptijd en grotere transparantie. De geschatte jaarlijkse besparing in de sector ligt tussen de €20 en €40 miljoen.

Nadere toelichting

VISI digitaliseert contractuele en bedrijfsprocessen in de vorm van workflows, die digitaal uitvoerbaar zijn in gecertificeerde software. Daarmee wordt vastgelegd wanneer (proces), wie (rol), wat (informatie), aan wie (rol) informatie aanlevert of goedkeurt.

Door het uitwisselen van VISI-berichten (digitale formulieren) worden processen stapsgewijs doorlopen. Denk hierbij aan het geven van opdrachten, aanleveren van tijdschema's, ontwerpen of plannen, het opleveren van resultaten en het melden van afwijkingen of wijzigingen.

VISI creëert voor elke deelnemende organisatie een compleet dossier van afspraken en communicatie. Elke organisatie kan werken in eigen software, zonder in andermans systemen te hoeven inloggen. Dit voorkomt gedoe met centrale systemen. Bij geschillen hebben alle partijen toegang tot dezelfde informatie en is direct inzichtelijk hoe de samenwerking is verlopen. VISI zorgt in elke aangesloten applicatie voor een audit trail.

De VISI-standaard staat sinds 9 december 2014 op de pas-toe-of-leg-uit-lijst en wordt toegepast sinds 2003.

59

Feitelijk gebruik

Organisaties kunnen VISI-gecertificeerde software aanschaffen bij een van drie softwareleveranciers, of ervoor kiezen de standaard zelf te implementeren in hun eigen applicaties. In een VISI-project zijn meestal twee of meer organisaties betrokken. Elke organisatie kan een softwareleverancier naar keuze gebruiken.

Om een VISI-applicatie effectief te gebruiken, is een VISI-raamwerk (workflowdefinitie) nodig. Dit raamwerk beschrijft de verantwoordelijkheden, interacties en processtromen tussen de actoren in een project, en kan worden aangepast aan elke samenwerkingsvorm of contracttype. VISI-raamwerken zijn onafhankelijk van softwareleveranciers en worden opgesteld door gespecialiseerde (advies)organisaties. Momenteel zijn er zeven organisaties die deze raamwerken ontwikkelen.

Het gebruik van de VISI-standaard is wijdverspreid in de GWW-sector en de naamsbekendheid is hoog. Steeds meer organisaties nemen VISI op als onderdeel van hun digitale bedrijfsvoering. Bij bouwprojecten vanaf €50.000 en met een langere doorlooptijd is VISI met name relevant. Het gebruik van VISI is conjunctuurgevoelig: meer bouwprojecten betekent meer gebruik, en omgekeerd.

Kentallen:

- 300 opdrachtgevers: Nederlandse overheden (Rijk, provincies, Schiphol, RWS, RVB, ProRail, gemeenten en waterschappen) en instellingen uit de (semi-)publieke sector
- Eindgebruikers: 800 tot 1.000 organisaties, waaronder architecten, adviseurs, aannemers en installateurs
- Aantal eindgebruikers: ongeveer 35.000
- Aantal actuele projecten: circa 5.000

VISI is oorspronkelijk ontwikkeld voor bouwprojecten in de grond-, weg- en waterbouw, maar wordt inmiddels breder toegepast, onder andere in de bouw- en utiliteitssector. De toepassingsmogelijkheden zijn

veelzijdig: van het grootste windmolenpark van Europa tot aanleg van ondergrondse infrastructuur, gemeentelijke groenvoorzieningen, fietspaden, meldingen van burgers en afvalbeheer.

Voorbeelden van recente toepassingen zijn:

- De renovatie van het Binnenhof
- Revisie/renovatie van 300 bruggen
- Beheer van gemalen
- Uitwisseling van personeel tussen twee provincies

Opmerkelijk is dat sinds dit jaar alle provincies de VISI-standaard toepassen.

Relevante ontwikkeling

Momenteel wordt onderzocht of de VISI-systematiek kan worden aangesloten op het afsprakenstelsel binnen de gebouwde omgeving.

7. Domein bestuur en recht

BWB

Waarom belangrijk?

BWB staat voor Basis Wetten Bestand. Het is de Juriconnect-standaard voor identificatie van en verwijzing naar geconsolideerde wet- en regelgeving. Daarvoor is aan elke regeling die is opgenomen in het BWB een uniek identificatienummer (BWB-id) toegekend. BWB beschrijft hoe deze verwijzing wordt vormgegeven. De standaard is een Uniform Resource Identifier (URI), een unieke computer-leesbare identificatiecode voor -in dit geval- wet- en regelgeving. Op de website van Juriconnect wordt de BWB standaard ook wel aangeduid als de standaard "logische links naar wetgeving". BWB staat op de 'pas toe of leg uit'-lijst sinds 2 februari 2016, met als achterliggende gedachte om toepassing van deze standaard te bevorderen.

Feitelijk gebruik

BWB wordt o.a. toegepast in de website wetten.overheid.nl. Conform de wettelijke opdracht bevat wetten.overheid.nl de geldende, geconsolideerde, regelgeving van de Nederlandse Rijksoverheid. Verder wordt BWB toegepast in LiDO, waarover hieronder meer.

Relevante ontwikkeling

De BWB standaard heeft tekortkomingen waarvoor mogelijke alternatieven worden onderzocht. Daarbij wordt in het bijzonder gekeken naar implementatie van de European Legislation Identifier (ELI), alsmede naar bredere inzet van de naming convention van de OASIS-standaard Akoma Ntoso die in de STOP-standaard (Standaard Officiële Publicaties) binnen het Digitaal Stelsel Omgevingswet wordt gebruikt. Op korte termijn wordt geen uitfasering verwacht van de BWB standaard

JCDR

Waarom belangrijk?

JCDR is de Juriconnect standaard voor identificatie van en verwijzing naar decentrale regelgeving en zorgt zo -net als BWB- voor vindbare en betrouwbare data aangaande deze decentrale regelgeving. Decentrale overheden slaan hun regelgeving en wijzigingen op in de voorziening Decentrale Regelgeving en Officiële Publicaties (DROP). JCDR is een afgesproken tekstvolgorde (syntaxis) voor verwijzingen naar die documenten. Zo kunnen computersystemen gemakkelijk de regels citeren, vinden en met elkaar verbinden. De standaard is net als BWB ook een URI, een Uniform Resource Identifier. JCDR staat op de 'pas toe of leg uit'-lijst sinds 28 november 2013, om toepassing van deze standaard te bevorderen.

Feitelijke gebruik

JCDR werd aanvankelijk ontwikkeld binnen de Centrale Voorziening voor Decentrale Regelgeving (CVDR). Die voorziening is in 2018 overgegaan in eerdergenoemd DROP, de voorziening voor Decentrale Regelgeving en Officiële Publicaties. In DROP kunnen decentrale overheidsorganisaties zoals eerder vermeld zorgen voor consolidatie en publicatie van hun regelgeving.

Relevante ontwikkeling

Een nieuwe, in het kader van BWB te ontwikkelen standaard (zoals een ELI-implementatie), zal ook bruikbaar moeten zijn voor de identificatie van en verwijzing naar decentrale regelgeving.

ECLI

Waarom belangrijk?

ECLI is de Europese standaard voor de identificatie van rechterlijke uitspraken en verwijzing daarnaar. In Nederland wordt de ECLI toegepast in de publicatie van alle uitspraken van alle (tucht)rechterlijke instanties. Alle rechterlijke uitspraken zijn met ECLI te vinden op Rechtspraak.nl. De tuchtrechtelijke uitspraken staan op Tuchtrecht.nl. Ook uitspraken die door uitgevers of alleen rechtspraak-intern zijn gepubliceerd hebben een ECLI. Gebruikers van ECLI zijn rechters in vonnissen en arresten, rechtsgeleerden en ambtenaren, maar ook juridische studenten, journalisten en burgers. Ook in Europa is ECLI de leidende standaard voor het identificeren en citeren van rechterlijke uitspraken. De uitspraken van drie Europese gerechten en van nationale gerechten in 20 EU-lidstaten hebben een ECLI.

ECLI staat op de 'pas toe of leg uit'- lijst sinds 28 november 2013, om zo toepassing te bevorderen.

Feitelijk gebruik

Het gebruik van ECLI wordt voorgeschreven in de Aanwijzingen voor de regelgeving en de Leidraad voor juridische auteurs. Het is door brede dekking inmiddels de leidende standaard.

Relevante ontwikkeling

Een nieuwe versie van de standaard is in oktober 2019 gepubliceerd in het Publicatieblad van de Europese Unie. Deze nieuwe versie bevat vooral uitbreidingen; de functionaliteit van de oorspronkelijke standaard blijft ongewijzigd. De nieuwe versie wordt niet nog gebruikt en is ook door de Europese Commissie nog niet geïmplementeerd in de ECLI Search Engine van het Europese e-Justice portaal.

62

Indicatie feitelijk gebruik van de drie standaarden (BWB, JCDR en ECLI) samen

Leidend hierin is nu het door Juriconnect vastgestelde [conformiteitsdocument](#), waarmee bij diverse partijen inzicht kan worden verkregen in de mate waarin aan de drie standaarden van de lijst wordt voldaan. Juriconnect is doende om een eerste monitoring op dit compliancy-document in gang te zetten.

EML_NL

Waarom belangrijk?

EML_NL is het Nederlands toepassingsprofiel op de Election Markup Language standaard. De standaard definieert de gegevens en de uitwisseling van digitale gegevens bij verkiezingen (die vallen onder de Nederlandse Kieswet). Daarbij gaat het om de uitwisseling van gegevens over kandidaten en over uitslagen om zo de verkiezingsuitslag en zetelverdeling vast te kunnen stellen. EML_NL draagt ertoe bij dat het verkiezingsproces transparant plaatsvindt en met minder kans op overname- en optelfouten. De standaard staat op de 'pas toe of leg uit'-lijst sinds 28 november 2013.

Feitelijk gebruik

De EML_NL standaard is opgenomen in de Ondersteunende Software Verkiezingen OSV2020. Het gebruik van de OSV2020 is daarmee een indicator voor het gebruik van de EML_NL standaard. OSV2020 wordt beschikbaar gesteld bij verkiezingen die onder de Kieswet vallen.

Alle bij het verkiezingsproces betrokken overheden maken gebruik van OSV2020 programmatuur bij verkiezingen en passen zo de EML_NL toe. Zo is – sinds de vorige versie van deze monitor – OSV2020 en daarmee de EML_NL standaard toegepast bij de Verkiezingen voor de Provinciale Staten van 15 maart 2023,

de verkiezingen voor de Waterschappen van 15 maart 2023, de Eerste Kamerverkiezing van 30 mei 2023, de Tweede Kamerverkiezing van 22 november 2023 en de Europees Parlementsverkiezing van 6 juli 2024.

De Kiesraad heeft de digitale tellingsbestanden van bovengenoemde verkiezingen in EML_NL formaat ontsloten op data.overheid.nl.

Het gegeven dat alle overheden in geval van verkiezingen gebruik maken van de OSV2020 programmatuur maakt dat met deze standaard in de huidige vorm een stabiel 100% doelbereik wordt gerealiseerd.

Relevante ontwikkeling

In het wetsvoorstel Wet programmatuur verkiezingsuitslagen (WPV) is opgenomen dat het verplicht wordt om de uitslagprogrammatuur, zoals door de Kiesraad ter beschikking gesteld, te gebruiken. Daarnaast is in hetzelfde wetsvoorstel opgenomen dat de uitslagprogrammatuur aan een aantal transparantievereisten moet voldoen, waaronder het toepassen van de EML_NL standaard.

Hiermee wordt de toepassing van de EML_NL standaard de facto verplicht gesteld zodra de WPV in werking treedt. Met ingang van 1 augustus 2025 treedt de WPV in werking. Hiermee is de vraag of daarna de EML_NL nog op de 'pas toe of leg uit'-lijst hoeft te staan.

8. Domein onderwijs en cultuur

E-Portfolio NL NEN 2035

Waarom belangrijk?

E-Portfolio NL (NEN 2035) beschrijft een semantisch, interoperabel model voor het vastleggen, opslaan, uitwisselen en doorgeven van informatie over het individuele leer- en ontwikkelproces van mensen. Het model ondersteunt het registreren van onder andere competenties en leerresultaten van een individu, en maakt deze gegevens uitwisselbaar tussen systemen zoals leeromgevingen en loopbaanondersteunende platforms. Het maatschappelijk belang van E-Portfolio NL ligt in het vergroten van de transparantie en overdraagbaarheid van leer- en loopbaangegevens. Hiermee wordt invulling gegeven aan het principe van een leven lang ontwikkelen. E-Portfolio NL (beheerorganisatie: NEN) is een Nederlands toepassingsprofiel van de internationale IMS ePortfolio-specificatie, bedoeld voor toepassing door studenten en werknemers bij Nederlandse organisaties. De norm staat sinds mei 2010 op de 'Pas toe of leg uit'-lijst.

Feitelijk gebruik

Volgens de gegevens van NEN is de norm in 2024 1 keer aangeschaft via de NEN-website en 5 keer ingezien via NEN Connect, het licentiesysteem van NEN. Eén van de gebruikers van de norm is werkzaam bij een publieke organisatie, terwijl de overige gebruikers niet werkzaam zijn bij een publieke organisatie.

64

De score van 2023 was 6 keer aangeschaft en respectievelijk 2 keer ingezien. Hier gold tevens dat één van de hier bedoelde gebruikers van de norm werkzaam was bij een publieke organisatie.

Relevante ontwikkeling

Er hebben het afgelopen jaar een aantal nieuwe ontwikkelingen plaatsgevonden.

1. De internationale norm ISO/IEC 20013:2020 heeft dezelfde reikwijdte E-Portfolio NL (NEN 2035). In eind 2025 start een systematic review van deze norm. Deze review zou – indien herziening volgt – kunnen leiden tot een geactualiseerde versie van ISO/IEC 20013, met mogelijk consequenties voor NEN 2035 als afgeleide nationale norm. Dit maakt de ontwikkelingen op internationaal niveau relevant voor het toekomstig beleid ten aanzien van E-Portfolio NL.
2. De Stichting ePortfolio Support (StePS), in 2010 opgericht om het gebruik van ePortfolio te stimuleren, heeft aangegeven binnenkort te worden opgeheven. StePS organiseerde in 2023/2024 een reeks landelijke bijeenkomsten. Deze bijeenkomsten richtten zich op de invoering van een skillspaspoort als onderdeel van een meer op vaardigheden gebaseerde arbeidsmarkt.

In de bijbehorende reflectie werd benadrukt dat hoewel veel initiatieven gericht zijn op verbetering van de aansluiting tussen onderwijs en arbeidsmarkt, er beperkt aandacht is voor het belang van standaarden en betrouwbare uitwisseling en uitwisselbaarheid van de persoonlijke en persoonsgegevens die nodig zijn voor een goede aansluiting voor tussen opleiding en beroepspraktijk en tussen school- en beroepsloopbaan. De voorgenomen opheffing van StePS gaat gepaard met het advies om ondersteunende activiteiten voor NEN 2035 te beëindigen. Dit onderstreept het beperkte draagvlak voor verdere implementatie van deze norm.

3. In maart 2025 lanceerde de Europese Commissie het initiatief 'Union of Skills'. Dit initiatief richt zich op het verbeteren van onderwijs en vaardigheden in de hele EU met aandacht voor grensoverschrijdende uitwisseling van digitale skillspaspoorten en focus op een leven lang ontwikkelen. Hoewel het gedachtegoed aansluit bij het doel van NEN 2035, speelt de Nederlandse norm hierin geen rol. Deze beleidsontwikkeling laat wel zien dat het belang van interoperabele vaardighedensystemen groeit, maar dat de technische en beleidsmatige regie steeds meer op Europees niveau wordt gelegd.