Inventarisatie gebruiksgegevens 2024 door BFS

Inhoudsopgave

Inleiding

Het uiteindelijke 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 van toepassing zijn. De verplichting om deze standaarden toe te passen geldt voor gemeenten, provincies, rijk, waterschappen en alle uitvoeringsorganisaties. 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'-regime is gericht op de aanschaf van ICT, en dus op het toepassen van open standaarden bij aanbestedingen die leiden tot toevoegingen 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 gemeten 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 vorig jaar is dit onderzoek uitgevoerd door de accountmanagers van het Bureau Forum Standaardisatie (BFS). De accountmanagers hebben hiervoor contact opgenomen met beheer-organisaties achter de standaarden. Helaas is het lang niet altijd even eenvoudig gebleken om (voor alle open standaarden) vast te stellen in welke mate die feitelijk gebruikt worden. Dat is bij eerdere versies van de monitor overigens niet anders geweest.

In vergelijking met vorig jaar is één wijziging doorgevoerd op de 'pas toe of leg uit'-lijst. SAML maakt sinds kort onderdeel uit van de gecombineerde authenticatie-standaarden OpenID.NLGov en SAML (datum besluit: 21 september 2023). Ten tijde van de vorige monitor-rapportage liep de toetsingsprocedure voor een geclusterde opname van NL GOV AP OIDC en SAML nog.

Voor een aantal standaarden uit het domein Veilig Internet zijn de gebruiksgegevens afkomstig uit het halfjaarlijkse onderzoek naar internet-veiligheids-standaarden. De Meting Internet-veiligheids-standaarden begin 2024 is ten tijde van het schrijven van deze monitor-rapportage gepubliceerd en is te vinden op de website van Bureau Forum Standaardisatie, de medio-2024 meting is daar nog niet terug te vinden. Wel zijn de voor deze monitor relevante gegevens uit de medio-2024-meting beschikbaar gesteld

Over het gebruik van de volgende 7 standaarden is dit jaar geen (actuele) informatie beschikbaar: NEN-ISO/IEC 27001, NEN-ISO/IEC 27002, WPA2 Enterprise, Ades Baseline Profiles, ODF, PDF en NL LOM.

Domein veilig internet

Voor een aantal standaarden binnen dit domein is zoals gezegd gebruik gemaakt van de opbrengst van de meting IV-standaarden door Forum Standaardisatie. Het betreft de volgende standaarden: DKIM, DMARC, SPF, DNSSEC, HTTPS & HSTS, TLS, IPv6 en IPv4, RPKI ,security.txt en STARTTLS & DANE. Over de relatief nieuwe standaard security.txt is overigens geen informatie te vinden in de rapportage 'Meting informatieveiligheidsstandaarden overheid begin 2024'. Reden daarvan is dat met betrekking tot deze standaard nog geen streefbeeldafspraak is gemaakt.

In de meest recente meting (medio 2024) zijn weer meer domeinnamen getoetst dan daarvoor. De verwachting is dat deze groei de komende tijd verder gaat doorzetten. De groei komt voornamelijk door het toevoegen van alle domeinnamen met en zonder 'www'. Daarnaast is er een stijging van nieuw geregistreerde domeinnamen en oudere domeinnamen die pas later aan de domeinnaamportfolio's zijn toegevoegd.

Een wijziging van de steekproefomvang maakt het lastig om meerdere peilmomenten op een verantwoorde manier met elkaar te vergelijken. Om toch aan die behoefte tegemoet te komen, voorziet de rapportage van de medio-2024--meting in een 'afgeleide' meting die is gebaseerd op de steekproef die in begin 2024 is gebruikt. Zodoende is er een goede basis om de beide peilmomenten uit 2024 met elkaar te vergelijken. De steekproef die afgelopen januari is gehanteerd, verschilt niet veel van de steekproef uit 2022 en 2023. Om die reden wordt ook de meting uit 2022 en 2023 in het gepresenteerde tijdsperspectief meegenomen. Een geringe terugloop van het aantal testbare domeinen is evenwel niet te voorkomen als gevolg van het tussentijds uitfaseren van oude domeinnamen.

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

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.

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

Het gebruik van anti-phishing standaarden ligt bij de hier gepresenteerde standaarden medio 2024 grofweg rond de 87% (voorjaar vorig jaar: ongeveer 85%). We zien dus **een geringe stijging** ten opzichte van de monitor-rapportage van vorig jaar. DMARC is net als vorig jaar een relatieve achterblijver (83%). 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 17% 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 medio 2024 naar type overheid laat een volgend beeld zien (tussen haakjes de score van medio 2023).

	Centrale overheid (n=1.690)	**Provincies** (n=24)	**Water-schappen** (n=30)	**Gemeenten** (n=368)	**Gemeen-schappelijke regelingen** (n=355)
DMARC policy	86 % (84%)	88 % (71%)	93 % (90%)	93 % (90%)	61 % (57%)
DKIM	85 % (83%)	92 % (92%)	100 % (100%)	99 % (99%)	90 % (85%)
SPF Policy	89 % (85%)	92 % (88%)	97 % (97%)	96 % (96%)	88 % (86%)

In dit overzicht valt op dat vrijwel overal hogere percentages worden genoteerd als de meest recente score van dit jaar (medio 2024) wordt vergeleken 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.

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.

DNSSEC	**voorjaar 2022**	**begin 2023**	**medio 2023** (n = 2.6001)	**begin 2024** (n = 2.505 resp. 2.611)	**medio 2024** (n = 2.332 resp. 2.467)	**begin 2025**
web-domein	89 %	90 %	91 %	90 %	91 %	
mailserver-domein	57 %	56 %	63 %	61 %	58 %	

Bij webdomeinen is sprake van een hoge score (91%), voor mailserverdomeinen ligt dit beduidend lager (58%). 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.

[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.

	Centrale overheid (n=1.556 resp. 1.690)	Provincies (n=24 voor beide)	Water-schappen (n=30 voor beide)	Gemeenten (n=370 resp. 368)	Gemeen-schappelijke regelingen (n=352 resp. 355)
web-domein	90 % (91%)	88 % (92%)	100 % (97%)	99 % (99%)	83 % (83%)
mailserver-domein	76 % (77%)	29 % (33%)	30 % (30%)	43 % (52%)	30 % (38%)

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 met 76% duidelijker hoger dan de rest. Gemeenten komen met een score van 43% nog het dichtst bij, ook al is daar wel sprake van een daling ten opzicht van medio vorig jaar. De andere drie categorieën scoren duidelijk onder-gemiddeld. 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).

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 vervolgbezoek 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 2.332 webdomeinen (medio 2024).

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

Op basis van deze cijfers blijkt dat bij 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 op twee van de drie standaarden sprake van een **lichte stijging** ten opzichte van de meting uit 2023. 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: medio 2024, tussen haakjes de cijfers van medio vorig jaar).

	Centrale overheid (n=1.556)	**Provincies** (n=24)	**Water-schappen** (n=30)	**Gemeenten** (n=370)	**Gemeen-schappelijke regelingen** (n=352)
HTTPS doorv.	90 % (93%)	89 % (92%)	100% 100%)	98 % (99%)	83 % (91%)
HSTS	81 % (81%)	89 % (88%)	100 % (93%)	97 % (97%)	62 % (58%)
TLS cf. NCSC	83 % (78%)	94 % (92%)	88 % (97%)	89 % (90%)	75 % (72%)

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 beeld[2].

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.

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

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).

IPv6	voorjaar 2022	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
Webverkeer	70 %	72 %	75 %	76 %	78 %	
e-mailverkeer	50 %	54 %	56 %	53 %	57 %	

De adoptie van IPv6 voor e-mailverkeer ligt in deze meting met 57% net boven de helft (medio vorig jaar: 56%). De score voor webverkeer is beter, met 78% adoptiegraad (medio vorig jaar: 75%). Voor beide deel-metingen geldt dat over-all sprake is van een **geringe maar continue stijging**.

Een uitsplitsing van deze cijfers naar type overheid wijst het volgende uit (peildatum: medio 2024, tussen haakjes de cijfers van vorig jaar).

	Centrale overheid (n=1.556 resp. 1.690)	**Provincies** (n=24 voor beide)	**Water-schappen** (n=30 voor beide)	**Gemeenten** (n=370 resp. 368)	**Gemeen-schappelijke regelingen** (n=352 resp. 355)
webverkeer	76 % (75%)	71 % (75%)	97 % (93%)	96 % (94%)	64 % (55%)
Emailverkeer	61 % (58%)	67 % (62%)	60 % (53%)	67 % (70%)	36 % (38%)

De centrale overheid scoort het dichtst bij het overall gemiddelde voor beide variabelen. In vergelijking met vorig jaar is voor beide variabelen sprake van een beperkte stijging. Gemeenten scoren op beide variabelen duidelijk het best. Met name het verschil met de

scores van de gemeenschappelijke regelingen is groot. Deze categorie 'gemeenschappelijke regelingen' blijft op beide variabelen duidelijk achter, ook al is daar sprake van een flinke stijging bij 'webverkeer'.

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

Over deze standaard is helaas geen informatie beschikbaar. In de achterliggende jaren was dat wel telkens mogelijk.

NL GOV Assurance profile for OAuth 2.0

Waarom belangrijk?

NL GOV Assurance profile for OAuth 2.0 is een open standaard voor de beveiliging van applicaties 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 maakt hiervoor gebruik van 'tokens' die 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 stijgt gestaag 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. Exacte gebruikscijfers zijn er nog niet en ook een compliance voorziening is er nog niet. 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,

Rijkswaterstaat, Justitie, politie, KOOP, Logius, VNG en SSC-ICT met de standaard gewerkt wordt.

Relevante ontwikkeling

Afgelopen jaar is de standaard verder doorontwikkeld en is naast de "authorization code flow" ook de "client credentials flow" toegevoegd. Verder is de leesbaarheid van het document verbeterd door toepassing van de laatste Respec opmaak mogelijkheden. Deze aanpassingen zijn gedaan in samenwerking met het Kennisplatform APIs en getoetst met de deelnemers uit de werkgroep security van het platform zoals geadviseerd in de adoptieadviezen van BFS. In 2024 is een nieuwe versie van het profiel opgeleverd en de publieke consultatie gestart. Na goedkeuring door het MIDO zal deze versie worden aangemeld bij het Forum Standaardisatie.

De standaard heeft een sterke relatie met de OIDC standaard die in 2023 is toegevoegd aan de 'pas toe of leg uit'-lijst en gezamenlijk biedt deze set van standaarden nog meer mogelijkheden voor moderne vormen van authenticatie en autorisatie.

Verder zijn er verbanden tussen OAuth en de ontwikkelingen van de EU digital wallet, eDelivery, EIDAS en andere vormen van Digital Proof of Posession (DPoP) en verifiable credentials.

RPKI

Waarom belangrijk?

Resource Public Key Infrastructure (RPKI) is een standaard met als doel om zogenaamde route hijacks te voorkomen. Bij een route hijack wordt internetverkeer omgeleid naar de systemen van een niet-geautoriseerd netwerk. Een hijack kan het gevolg zijn van een simpele typefout van een netwerkbeheerder die daarmee onbedoeld internetverkeer omleidt, of van een doelgerichte aanval op de infrastructuur van het internet om bijvoorbeeld websites onbereikbaar te maken of om gegevens van internetgebruikers afhandig te maken. Deze standaard staat op de 'pas toe of leg uit'-lijst, sinds november 2019.

Feitelijk gebruik

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

	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**
webverkeer	78 %	86 %	91 %	94 %	
e-mailverkeer	75 %	87 %	90 %	93 %	

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

Een uitsplitsing van deze cijfers naar type overheid wijst het volgende uit (peildatum: medio 2024, tussen haakjes de cijfers van medio2023).

	Centrale overheid (n=1.556 resp. 1.690)	**Provincies** (n= 24)	**Water-schappen** (n= 30)	**Gemeenten** (n= 370 resp. 368)	**Gemeen-schappelijke regelingen** (n= 352 resp. 355)
webverkeer	94 % (90 %)	88 % (67 %)	93 % (93 %)	97 % (79%)	89 % (73 %)
e-mailverkeer	90 % (86 %)	95 % (76 %)	97 % (83 %)	96 % (88%)	94 % (88 %)

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 gebruik bij onder andere DigiD machtigen en eHerkenning. SAML is een internationale standaard die is ontwikkeld door de standaardenorganisatie 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 authentiseren 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.

	2018	**2019**	**2020**	**2021**	**2022**	**2023**	**2024**
eHerkenning: SAML	359	439	458	493	onbekend	559	?
DigiD: SAML	398	429	558	onbekend	onbekend	1.167	1.167
eHerkenning + DigiD	757	868	1.016	onbekend	onbekend	1.726	?

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. Een vergelijking met vorig jaar is echter niet te maken; in dat jaar zijn geen cijfers beschikbaar gekomen. 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 toegangsdiensten. 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 machtigingen 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 authentiseren. Beiden zijn nog niet op grote schaal uitgerold en hebben daarom nog geen effect op de gebruikscijfers.

In de achterliggende periode is door OBDO besloten tot een geclusterde opname van NL GOV AP OIDC en SAML.

Security.txt

Waarom belangrijk?

Elke dag vinden beveiligingsonderzoekers kwetsbaarheden in websites of IT-systemen. Vaak is niet duidelijk waar een beveiligingsonderzoeker een gevonden kwetsbaarheid kan melden en gaat daardoor mogelijk kostbare tijd verloren. Het gebruik van de security.txt standaard kan helpen dit te voorkomen. 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. De standaard staat pas kort op de 'pas toe of leg uit'-lijst, sinds 25 mei 2023.

Feitelijk gebruik

Aan Internet.nl is een test toegevoegd voor security.txt die is bedoeld als hulpmiddel voor bedrijven en andere organisaties. Als indicator voor het feitelijk gebruik van deze open standaard kijken we of het security.txt-bestand op de geteste domeinnaam aanwezig is en of de opgenomen informatie het juiste formaat heeft.

	begin 2023 (n = 2.653)	**medio 2023** (n = 2.593)	**begin 2024** (n = 2.505)	**medio 2024** (n = 2.332)	**begin 2025**
webdomeinen	24 %	37 %	47 %	50 %	

De **stijging** van het gebruik die we vorig jaar al konden noteren, zet dit jaar door.

Een uitsplitsing van deze cijfers naar type overheid wijst het volgende uit (peildatum: medio 2024, tussen haakjes de cijfers van medio 2023).

	Centrale overheid	Provincies	Water-schappen	Gemeenten	Gemeen-schappelijke regelingen
	(n=1.556)	(n= 24)	(n= 30)	(n= 370)	(n= 352)
Webdomein	52 % (43 %)	48 % (42%)	56 % (47%)	54 % (27%)	22 % (13 %)

De vergelijking tussen beide peildata wijst uit dat bij elk van de overheidscategorieën sprake is van een duidelijke stijging. Met name de grote stijging bij de gemeenten valt op. De gemeenschappelijke regelingen blijven achter bij de andere overheidscategorieën, ook al is ook daar sprake van een stijging.

Relevante ontwikkeling

SIDN heeft security.txt opgenomen in de score-card.

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.

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

Bij ruim negen op de tien e-mailservers (93%) is de STARTTLS-configuratie conform de richtlijnen van NCSC geconfigureerd; bij één op de tien moet dat nog gebeuren. De score blijft oplopen. DANE scoort met minder dan 50% laag in vergelijking met de andere standaarden die in de IV-meting zijn meegenomen. Wat daarbij opvalt is dat enige groei ontbreekt en dat eerder sprake is van een lichte terugloop. Daarmee wijkt de cijfermatige ontwikkeling met betrekking tot DANE af van het algemene beeld waarbij sprake is van beperkt maar gestaag oplopende percentages. Migratie naar de cloud is vermoedelijk de reden van de afname van DANE.

Een uitsplitsing van deze cijfers naar type overheid levert het volgende beeld op (peildatum: medio 2024, tussen haakjes de cijfers van medio vorig jaar).

	Centrale overheid (n=663)	**Provincies** (n=21)	**Water-schappen** (n=30)	**Gemeenten** (n=357)	**Gemeen-schappelijke regelingen** (n=334)
STARTTLS cf. NCSC	93 % (90%)	100 % (91%)	97 % (86%)	93 % (89%)	91 % (86%)
DANE	59 % (56%)	11 % (21%)	23 % (21%)	33 % (47%)	15 % (22%)

De verschillende categorieën overheden ontlopen elkaar weinig waar het gaat om de toepassing van STARTTLS. Bij elk van de overheidslagen is sprake van een stijging van het percentage. Bij DANE ligt dat anders. Terwijl de centrale overheid met een percentage boven de 50% relatief goed scoort, blijven de andere vier categorieën duidelijk achter; het beeld van vorig jaar herhaalt zich op dit punt. Hierbij valt op dat zowel bij provincies als gemeenten en gemeenschappelijke regelingen sprake is van een teruglopend percentage.

Relevante ontwikkeling

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

STIX & TAXII

Waarom belangrijk

STIX en TAXII zijn standaarden voor partijen die samenwerken op het gebied van cybersecurity. Door standaarden te gebruiken wordt het mogelijk om sneller en gemakkelijker informatie te delen over cyberdreigingen om zodoende de juiste maatregelen te kunnen nemen om computersystemen 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

Er is (nog) geen objectieve meetmethode voorhanden om het gebruik van STIX en TAXII inzichtelijk te maken. Op de markt voor cybersecurity-software is wel een beweging zichtbaar dat nieuwe producten steeds meer bij deze standaarden aansluiten. Dat zijn met name uitwisselingsdiensten van cybersecurity-informatie en geïntegreerde "security orchestration, automation and response-platformen" (SOAR-tooling). Deze systemen gebruiken de standaarden steeds vaker als opslag- en uitwisselingsformaat en anders hebben ze tenminste connectoren die daarmee kunnen uitwisselen.

Om zicht te geven op het feitelijke gebruik moeten we kijken naar de organisaties die cybersecurity-informatie verwerken met onderscheid tussen de coördinerende instanties en de daarbij aangesloten organisaties.

Nationaal niveau

Het Nationaal Cyber Security Center (NCSC) heeft als taak om Nederland weerbaar te maken tegen cyberdreigingen. Op dit moment werkt het NCSC vooral voor de Rijkoverheid en vitale sectoren van de industrie maar die doelgroepen worden de komende tijd uitgebreid naar andere sectoren. Het NCSC maakt voor zijn dienstverlening onder meer gebruik van het Nationaal Detectie Netwerk (NDN) dat zich richt op het onderling delen van dreigings- en incidentinformatie. Bij deze informatie-uitwisseling wordt onder meer de TAXII standaard gebruikt en bij de analyse van cybersecurity-gegevens wordt de STIX standaard gebruikt.

Veel Rijksoverheidsorganisaties maken voor hun informatievoorziening en hun informatiebeveiliging gebruik van shared service organisaties (zoals SSC-ICT, DICTU, DUO, JIO, en SSC Campus). Deze shared service organisaties hebben SOC-afdelingen (Security Operations Center) waar de monitoring, detectie en afhandeling van informatiebeveiligingsincidenten is belegd. Het zijn vooral deze SOC's die gebruikers zijn van de cybersecurity tools waar de STIX en TAXII standaarden op van toepassing zijn. Momenteel is de Rijksoverheid druk doende om alle organisaties aan te sluiten op een SOC. Grotere organisaties als de Politie en de Belastingdienst hebben een eigen SOC maar de meeste organisaties binnen de Rijksoverheid sluiten aan via het SOC van hun shared service organisatie.

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 (165 van de 207) aangesloten bij het NDN waarvan 101 organisaties zijn aangesloten via de sensor van een shared service organisatie. Dat geeft een dekkingsgraad geeft van 80%. In **absolute getallen** is het aantal aangesloten organisaties bij het NDN in vergelijking met vorig jaar **nauwelijks gewijzigd.** De **dekkingsgraad is beperkt toegenomen**, van 77% naar 80%. Dit is een teken dat de inzet van sensoren bij de bescherming tegen cyberdreigingen een grote mate van dekking bereikt heeft.

Het gebruik van de standaarden is met name van belang voor deze shared service organisaties. Deze organisaties hebben SOC (security operation centers) en CERT (computer emergency response teams) afdelingen die cyber-incidenten detecteren en oplossen voor

de aangesloten organisaties. Er zijn ook gespecialiseerde securitybedrijven die SOC- of CERT-diensten aanbieden. De systemen die SOC's en CERT's gebruiken zijn onder meer SIEM-systemen (Security information and event management), TIP-systemen (Threat intelligence platformen), XDR-systemen (Extended detection and response) en SOAR-tooling (Security orchestration, automation and response). Deze systemen bieden voorzieningen om cyber-incidenten te detecteren en te analyseren en om opvolgingshandelingen te ondersteunen en te automatiseren. Bij de verwerving van zulke systemen is het raadzaam om de standaarden op te nemen in het programma van eisen om daarmee de interoperabiliteit en de mogelijkheden voor de uitwisseling van cybersecurity-informatie te waarborgen.

Gemeentelijk niveau

In de vorige monitor is onder 'relevante ontwikkeling' gemeld dat er op het toenmalige peilmoment een nieuwe aanbesteding voor Monitoring en Response werd gepubliceerd. In het programma van eisen bij deze aanbesteding werd ook het gebruik van de STIX en TAXII standaarden uitgevraagd. Inmiddels is deze aanbesteding afgerond. Daarover het volgende.

Binnen de Nederlandse gemeenten krijgt Monitoring en Response steeds meer aandacht. Dit mede door de recent succesvol afgeronde aanbesteding voor de inkoop van M&R diensten, waarbij er raamcontracten gesloten zijn met 6 M&R leveranciers(MSSP's). Ook de uitwisseling van dreigingsinformatie speelt hierin een belangrijke rol. Vanuit de aanbesteding/raamcontracten is een samenwerking tussen de leveranciers met de IBD CERT opgestart. Een belangrijke component van deze samenwerking is de bi-directionele uitwisseling van dreigingsinformatie. Op deze wijze maken de gemeenten via de M&R leveranciers actiever gebruik van de dreigingsinformatie en neemt daarmee het gebruik van de STIX en TAXII standaarden toe. Het feit of gemeenten wel of geen kennis en capaciteiten hebben voor het gebruik van de standaarden (binnen het TI proces) is daarmee niet relevant meer. Het NCSC blijft een belangrijke bron voor dreigingsinformatie, maar ook de M&R leveranciers worden hier aan toegevoegd en vormen daarmee belangrijke bronnen voor de IBD en de Nederlandse gemeenten.

Begin dit jaar zijn de eerste minicompetities opgestart en die vinden nu doorlopend plaats. Daarmee groeit het gebruik van de M&R diensten binnen gemeenten en dus ook het actief gebruik van dreigingsinformatie, uitgewisseld op basis van de STIX en TAXII standaard. Over de snelheid van deze groei kan op dit moment geen indicatie worden afgegeven.

Relevante ontwikkeling

De belangrijkste ontwikkeling met betrekking tot deze standaarden is dat er nieuwe versies zijn die STIX 1.2.1 en TAXII 1.1.1 vervangen. De actuele versies die al sinds 2021 zijn vastgesteld zijn STIX 2.1 en TAXII 2.1. De oude standaarden in de pas-toe-of-leg-uit lijst worden in bestaande toepassingen nog wel gebruikt. Ook veel NDN aansluitingen zijn nog gebaseerd op STIX/TAXII versies 1.x maar voor nieuwe toepassingen wordt het gebruik afgeraden. Voorafgaand aan de actuele versie zijn nog 2.0 versies gepubliceerd maar die bevatten praktische onvolkomenheden die in de actuele 2.1 versies zijn gecorrigeerd. STIX 2.1 en TAXII 2.1 zijn dan ook de aanbevolen standaarden. De nieuwe versies omvatten een veel groter aantal informatiesoorten met niet alleen dreigingen, kwetsbaarheden en incidenten maar

ook doelstellingen, motieven, aanvalspatronen, verdedigingstactieken en beschermingsmaatregelen.

Specificatiedocumenten:

https://oasis-open.github.io/cti-documentation/resources.html#stix-21-specification

Een tweede belangrijke ontwikkeling is de grote uitbreiding van de soorten diensten en applicaties waarin deze standaarden worden toegepast. De standaarden werden voorheen voornamelijk toegepast in threat intelligence platformen (TIP) en security incident and event monitoring systemen (SIEM) voor het analyseren en delen van cybersecurity informatie tussen samenwerkende IT-dienstverleners en de beveiligingsafdelingen van grote organisaties. De standaarden zorgden daarbij voor de uitwisselbaarheid van de informatie.

In de afgelopen jaren is cybersecurity een dienstverleningssector op zich geworden met vele gespecialiseerde toepassingen en diensten. De integraties en de aansluiting op relevante informatiestromen worden daarbij verzorgd door managed security service providers (MSSP). Op de achtergrond maken deze cybersecurity-bedrijven nog steeds gebruik van standaarden waaronder ook STIX en TAXII. Overheidsorganisaties die gebruik maken van cybersecurity-diensten hoeven de standaarden niet direct zelf toe te passen maar het is nog steeds nuttig om je dienstverlener te vragen om dat te doen.

WPA2 Enterprise

Over deze standaard is helaas geen informatie beschikbaar. In de achterliggende jaren was dat wel telkens mogelijk.

Domein openbaar en toegankelijk

Ades Baseline Profiles

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

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 kunnen 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

Tot twee jaar terug 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[3].

Inmiddels is een Dashboard DigiToegankelijk ontwikkeld en operationeel en in beheer bij Logius. Het dashboard, gelanceerd in maart 2023, geeft een totaalbeeld van de toegankelijkheidsstatus van alle websites en apps van overheidsorganisaties. Het Dashboard was bij de start uitsluitend gebaseerd op informatie uit het register van toegankelijkheidsverklaringen. Een paar maanden later (juni 2023) is een inventarisatiecampagne gestart om ook zicht te krijgen op de websites en apps waarvoor nog geen verklaring was aangemaakt. Bij de vorige monitor open standaarden is gebruik gemaakt van informatie uit dit dashboard. Op de peildatum 8 september 2023 was de Nederlandse overheid verantwoordelijk voor 7.639 websites en mobiele apps en inmiddels is dit aantal gestegen tot 9.017 (peildatum 22 augustus 2024). Dit zijn echter momentopnamen.

[3] Monitor toegankelijkheid 2021. Websites en mobiele applicaties van Nederlandse overheidsinstellingen, November 2021, Stichting Accessibility. Opdrachtgever hierbij is Logius.

Een volgende stap in het monitoren van de digitoegankelijkheid is gezet met het verschijnen van een eerste jaarmonitor digitoegankelijkheid 2023. Deze monitor biedt inzicht in de ontwikkeling van digitoegankelijkheid bij de overheid over opeenvolgende jaren en zal minimaal een keer per jaar een update krijgen. Onderstaande beeld is ontleend aan deze Jaarmonitor Digitale Toegankelijkheid 2023 (https://monitor.digitoegankelijk.nl/jaarmonitor/)[4]. De hier gepresenteerde cijfers zijn daar te vinden achter de pagina 'geclusterde cijfers'.

		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	607	301	327	(540)	1.329
	'22 > '23	+ 12%	+ 1%	-/- 7%	+ 129%		+ 15%
Provincies	2021	11	25	28	77		141
	2022	11	43	64	84		202
	2023	13	88	79	80	(257)	260
	'22 > '23	+ 18%	+ 105%	+ 23%	-/- 5%		+ 29%
Waterschappen	2021	3	31	15	4		53
	2022	1	42	12	5		60
	2023	3	43	12	18	(122)	76
	'22 > '23	+ 200%	+ 2%	=	+ 260%		+ 27%
Gemeenten	2021	141	429	520	470		1.560
	2022	210	572	504	518		1.804
	2023	279	736	791	1.123	(2.574)	2.929
	'22 > '23	+ 33%	+ 29%	+ 57%	+ 117%		+ 62%
Totaal	2021	241	979	920	685		2.825
	2022	306	1.260	904	750		3.220
	2023	389	1.474	1.183	1.548	(3.493)	4.594
	'22 > '23	+ 27%	+ 17%	+ 31%	+ 106%		+ 43%

Naar aanleiding van een inventarisatiecampagne (juni 2023) zijn in de tweede helft van dat jaar veel websites en apps zonder toegankelijkheidsverklaring toegevoegd aan het dashboard met status E. Voor deze websites en apps is nog geen toegankelijkheidsverklaring gemaakt. Met deze toevoeging van status E is het aantal overheids-websites en -apps dat in beeld is bij het dashboard in 2023 met 43% toegenomen. De verwachting is dat veel van deze websites en apps in de loop van 2024 met status A, B, C of D zullen worden toegevoegd aan het dashboard.

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 elke status A, B, C en D geldt dat in 2023 sprake is van een stijging, variërend van 17% (status B) tot 106% (status D);

[4] Bron voor deze jaarmonitor is het eerder gememoreerde dashboard.

- het aantal websites en apps dat voldoet aan de wettelijke verplichting (status A, B of C) is in 2023 gegroeid met 23%;
- het aantal websites dat volledig voldoet aan de toegankelijkheidseisen (status A) is in 2023 met 27% gestegen;
- genoemde stijgingen zijn terug te vinden bij elk van de te onderscheiden typen overheidsorganisaties.

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 ge-updatet;
- 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 Proof of Concept (PoC) voor 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. Hopelijk is die PoC eind dit jaar gereed. Indien succesvol wordt dat in 2025 doorontwikkeld tot een volwaardige omgeving;

- Met betrekking tot de publicatietool NLdoc, gericht op het omzetten van ontoegankelijke documenten naar toegankelijke HTML: doel is om eind dit jaar een API te kunnen aanbieden. In 2025 wordt, bij voldoende budget, verder gewerkt aan een platform.

ODF en PDF

Over deze standaard is helaas geen informatie beschikbaar. In de achterliggende jaren was dat wel telkens mogelijk.

SKOS

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 60 begrippenlijsten van bijna alleen overheden. Het thesaurusplatform is volledig gebaseerd op de 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 - 2023. De inhoud en opzet van de enquête in 2024 is onveranderd. Daarmee zijn de antwoorden te vergelijken met de uitkomsten van de enquêtes van voorgaande jaren.

In totaal is de enquête 46 keer ingevuld waaruit 39 unieke organisaties (en/ of programma's) zijn af te leiden. In vergelijking met vorig jaar is sprake van een hogere respons. Van de 39 unieke organisaties of programma's geeft 62% (24 organisaties) aan een begrippenlijst, woordenboek of taxonomie op het internet te publiceren. Dit is nagenoeg gelijk ten opzichte van 2023 (toen 61%). Dit zijn in principe organisaties die in aanmerking komen voor de verplichting van SKOS. Als wordt ingezoomd op deze 24 organisaties die kwalificeren voor een verplichting van SKOS, dan zien we het volgende:

- 19 daarvan gebruiken SKOS (79%). Dat is een lichte daling in vergelijking tot het gebruik van vorig jaar (toen 84%).
- Over deze 19 gebruikers van SKOS nog het volgende:
  - er zijn geen organisaties die alleen van SKOS gebruik maken
  - 12 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.
  - 13 van de 19 organisaties (68%) 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.

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 **lichte 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, waterschappen en programma's 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.
- 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 en we zien toenemend gebruik van de combinatie van SKOS en SHACL.

- 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.
- een aantal respondenten gebruikt de nieuwe Nederlandse 'Standaard voor Beschrijven van Begrippen' (NL-SBB), zowel voor publiceren van begrippenlijst op internet als voor interne bedrijfsprocessen. 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 2024 heeft na 2023 voor de tweede 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 39 unieke organisaties of programma's geeft 64% (25 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. 18 organisaties gebruiken hierbij linked data standaarden, waarvan 14 organisaties ook SKOS (56%). 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 is met of zonder SKOS toe te passen. NL-SBB is inmiddels in beheer bij Geonovum, en werkgroep en Geonovum hebben gezamenlijk NL-SBB aangemeld om te verplichten aan de overheid via plaatsing op de 'Pas toe of leg uit'-lijst van Forum Standaardisatie.

Het publiceren van linked data, en van (SKOS) kennissystemen in het bijzonder, vereist specialistische kennis over semantiek en standaarden. 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 kiezen 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, Ministerie van Financiën, Politie, Belastingdienst, DUO, RWS, RDW, de erfgoedsector en de onderwijssector zijn voorbeelden van adoptie van linked data bij de Nederlandse overheid. Programma's zoals Federatief Datastelsel kunnen baat hebben bij omarmen van SKOS en linked data standaarden. De opkomst van Artificial Intelligence en incidenten zoals de Toeslagenaffaire zorgt voor een roep om een transparantere overheid. "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.

In 2023 zijn SKOS en aanpalende linked data standaarden op de lijst open standaarden van Forum Standaardisatie geëvalueerd. Het Evaluatieonderzoek bevestigt de toegevoegde waarde van SKOS voor de digitale overheid en ziet dat linked data meer en meer relevant worden. Binnen de overheid groeit (de wens naar) het aantal begrippenkaders, zowel vanuit informatievoorziening als vanuit semantische standaardisatie. Het Evaluatieonderzoek bevestigt de meerwaarde om linked data standaarden te combineren in één cluster op de lijst open standaarden.

Domein uitwisselingsfundament

OpenAPI Specification

Algemeen

Open API Specification (OAS) is een standaard voor de documentatie van Application Programming Interfaces (API's). 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

In de monitor 2020 is voor het laatst gerapporteerd over deze standaard OAS 3.0. Toen werd opgemerkt dat het ministerie van BZK in 2019 in samenwerking met VNG Realisatie het portal https://developer.overheid.nl/ had opgezet. Een volwaardige meting kon toen nog niet worden gepresenteerd op basis van dit platform. Inmiddels kan dit wel. De opgave van 2023 is beschouwd als een (hernieuwde) nul-meting.

Inmiddels zijn 107 REST API's geregistreerd (peildatum augustus 2024). Ten opzichte van de 103 REST API's van de peildatum september 2023 is dit een lichte stijging. Deze 107 REST API's komen vanuit alle lagen van de overheid: gemeenten, provincies, ministeries, uitvoeringsorganisaties, Zbo's en stichtingen. In dit kader zijn alleen de specifieke REST API's geteld die zijn gekenmerkt als OData, REST/JSON & REST/XML. Dit aangezien deze REST API's ook beschikken over de vereiste OAS 3.0 Specificatie en als zodanig ook te raadplegen zijn op developer.overheid.nl.

Relevante ontwikkeling

Afgelopen jaar is OAS3.1 aangemeld voor opname op de lijst van het Forum. Ook is gestart aan de ontwikkelingen van OAS4.

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 standaarden en open source.

Feitelijk gebruik

Het aantal API's is gegroeid ten opzichte van vorig jaar (circa 116). Hiervan betreft 92% REST API's. Het aantal organisaties dat API's aanbiedt is met 2 gegroeid met naar in totaal 26 (bron: developer.overheid.nl.).

Recente ontwikkelingen (Europese regelgeving, Open Data Act en DSA) tonen dat organisaties contact zoeken met de beheerorganisatie en developer.overheid.nl met vragen over API's, de API regels en hoe de API's (intern) te testen in hun CI/CD straat.

Om inzicht te krijgen in de kwaliteit van deze API's is een applicatie gebouwd op basis waarvan kan worden nagegaan in hoeverre de geregistreerde API's voldoen aan de API Design Rules. Deze applicatie voert controles uit op basis van de 7 Design Rules die daadwerkelijk meetbaar zijn. Het huidige beeld van de kwaliteit in de vorm van de API Design Rule score is als volgt is als volgt:

- 26 API's voldoen aan geen van de API Design Rules
- 46 API's voldoen aan 1 API Design Rule
- 2 API's voldoen aan 2 API Design Rules
- 9 API's voldoen aan 3 API Design Rules
- 4 API's voldoen aan 4 API Design Rules
- 18 API's voldoen aan 5 API Design Rules
- 4 API's voldoen aan 6 API Design Rules
- 7 API's voldoen aan alle 7 API Design Rules

Afgelopen jaar is de applicatie aangepast met specifiekere controles op de 7 design rules. Dit heeft als effect gehad dat de overall scores licht zijn gedaald. Door de specifieke controles zijn echter de metingen zuiverder en kunnen API aanbieders duidelijker voldoen aan de regels. Dit effect is ook zichtbaar. De organisaties die initiatief hebben genomen om

aan de rules te voldoen slagen hier ook beter in. Het aantal API's wat aan 5 of meer rules voldoet is gestegen van 16 naar 29.

Ook zijn in de applicatie nieuwe testsets toegevoegd. Zo is er een testset voor transport security met 2 TLS tests en een testset met 4 tests in het kader van API metagegevens.

Van de Secure connections using TLS testset zijn de scores als volgt:

- 9 API's geven aan dat de testset niet van toepassing is
- 7 API's voldoen aan 0 van de tests
- 10 API's voldoen aan 1 van de 2 tests
- 90 API's voldoen aan 2 van de 2 tests.

Van de API metagegevens testset zijn de scores als volgt

- 1 API voldoen aan 0 van de tests
- 21 API's voldoen aan 1 van de 4 tests
- 19 API's voldoen aan 2 van de 4 tests
- 46 API's voldoen aan 3 van de 4 tests
- 29 API's voldoen aan 4 van de 4 tests

Relevante ontwikkeling

Afgelopen jaar is de REST-API-Design Rules standaard door de beheerder (Logius) verder doorontwikkeld in samenwerking met alle spelers van het Kennisplatform API's. Formele besluiten zijn genomen in het, conform de governance (op basis van BOMOS) ingestelde, Technische Overleg & de MIDO. De definitieve 2.0 van de standaard sluit beter aan bij de testset op Developer.overheid, de modulaire opbouw van de NL API Strategie, de doorontwikkeling van de Digikoppeling en het NL-OAUTH-Profiel. De nieuwe versie van de standaard is in 2024 aangemeld voor opname op de 'pas toe of leg uit' lijst ter vervanging van de eerdere versie. Ook is uitstekend beheer aangevraagd om in de toekomst sneller kleine wijzigingen en verbeteringen in de standaard door te kunnen voeren. De standaard zal in ontwikkeling blijven en vormt met de 2 andere API standaarden de kern van het Kennisplatform API's.

Digikoppeling

Algemeen

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

- Synchroon 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.

Feitelijk gebruik

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

Digikoppeling	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 %[5]		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[6]		98%	75%	59%	95%[7]
Zomer 2019 Najaar 2020		60%	100%	100%	100%	90%[2]
Najaar 2020		65%	100%	100%	100%	91%
Zomer 2021		65%[8]	100%	100%	100%	91%
Zomer 2022		65%	100%	100%	100%	91%
Zomer 2023		69%[9]	100%	100%	100%	92%
Zomer 2024		69%	100%	100%	100%	92%

Bron: opgave beheerorganisatie Logius

[5] 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.

[6] 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%

[7] Hierin zijn voor 2018 alleen de aantallen voor gemeenten, provincies en waterschappen opgenomen

[8] 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.

[9] Relatieve dekking binnen de groep gemeenschappelijke regelingen is toegenomen.

Deze stabilisatie 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 bijvoorbeeld voor Gemeenschappelijke regelingen en Adviescollege's.

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 wordt het profiel uitgebreid met afspraken met betrekking tot Signing en Encryptie.
2. Het Digikoppeling ebMS2 profiel zal worden uitgefaseerd en worden vervangen door een Digikoppeling ebMS3/AS4 profiel direct gebaseerd op eDelivery. Dit profiel en het bijbehorend migratie traject wordt de komende tijd verder ontwikkeld (en besluitvorming hierover zal plaatsvinden binnen de MIDO governance).

Geo-Standaarden

Waarom belangrijk?

Het geheel van Geo-standaarden is een van de drie stelselstandaarden 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 Nederlandse profielen op WMS en WFS (t.z.t. te vervangen door de OGC API standaarden)
- 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.

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 geodatasets 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 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 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.

In de monitors van 2020, 2021 en 2022 is aangegeven dat PDOK elk jaar aanzienlijke groeicijfers laat zien. Sinds 2023 is er een dalende trend (bron: PDOK factsheet 2022) en deze zet zich door in 2024 met een daling van 29,1 miljard hits naar 22,2 miljard. Door de overgang van PDOK naar de cloud zijn er cijfers ontdubbeld en er wordt een nieuwe rekenmethodiek gehanteerd, waarbijf foutieve bevragingen en uitgefaseerde hits niet meer worden meegeteld. Dit maakt vergelijken met eerdere jaren lastig. De overgang naar de cloud is nu afgerond waardoor de cijfers vanaf volgend jaar weer beter vergelijkbaar zijn.
Het aantal datasets is ook gedaald, van 235 naar 214, maar het aantal services is gestegen van 605 naar 642. De daling in datasets is te verklaren uit het samenvoegen van datasets en overgang naar de cloud, en 1 dataset is daadwerkelijk uitgefaseerd.
Voor het eerst kunnen we ook de jaarcijfers over OGC API Tiles en OGC API Features bekijken. Er zijn nog niet zoveel datasets via deze nieuwe standaarden ontsloten als via WMS/WMST/WFS. Het gebruik van Features is stijgend noch dalend in de loop van het jaar. Bij Tiles zie je wel een duidelijke stijging in de loop van 2023, van bijna 400.000 hits in Q1 naar 2,3 miljoen in Q4. Er is 1 dataset via OGC API Features ontsloten en 5 datasets via OGC API Tiles.

Samenvattend: het aantal hits op PDOK 2023 is 22,2 miljard waarvan 2.1 miljard WMS, ruim 212 miljoen WFS, 3 miljard WMTS, 9.4 miljoen OGC API Features en ruim 140 miljoen OGC API Tiles.

Het aantal hits op het Nationaal Georegister (NGR) laat nog steeds een stijgende lijn zien: van 23,2 in 2022 naar 26,6 miljoen.

Relevante ontwikkeling

In 2024 verwachten we de (hopelijk positieve) afronding van de procedure 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. Voor de Geo-module van de NL API strategie is het de intentie dat die gebundeld met de andere generieke API standaarden (i.e. de API strategie) aangemeld wordt vanuit Logius.

StUF

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.

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 veel pakketsoftware op de markt of dit komt binnenkort op de markt. De adoptie voor StUF ZKN en StUF BG neemt nog steeds toe in oplossingen. Voor beide geldt wel een toename van aantal leveranciers dat deze StUF standaarden meeneemt in haar software producten.

Onderstaande tabel geeft een beeld van de adoptie van de twee StUF onderdelen (StUF-BG en StUF-ZKN) door de ICT-markt.

	Totaal		**StUF-BG**		**StUF-ZKN**	
Aantal leveranciers	312	(299)	81	(72)	74	(58)
Aantal softwareproducten (incl. versies)	3883	(2961)	1464	(1201)	899	(738)
wv. beschikbaar/in gebruik	1733	(1447)	413	(368)	268	(226)
wv. gepland/in ontwikkeling	105	(91)	46	(50)	22	(26)

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 is gestegen (overall een stijging van 4%). Dit komt onder andere doordat het gebruik van de softwarecatalogus niet meer van een convenant afhankelijk is. Daarnaast is er een toename te zien van het aantal pakketten ten opzichte van 2023. 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 2023.

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.

Er zijn geen wijzigingen doorgevoerd in StUF koppelvlakken. Trendmatig zien we over de gehele breedte deze periode een stabiel aantal tests door leveranciers voor alle StUF-standaarden. Voor de in de tabel genoemde twee specifieke StUF koppelingen zien we stabiel aantal tests.

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

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.

Deze transitie is een doorlopend proces en de verwachting is dat de StUF standaarden voorlopig nog wel in gebruik zullen blijven.

Er wordt momenteel (zomer 2024) een evaluatie van StUF uitgevoerd; deze wordt naar verwachting eind 2024 opgeleverd.

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 op de Europese Norm EN16931 voor toepassing in Nederland. 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

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 verstuurde 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 enorme groei doorgemaakt in 2023. Waar het aantal verstuurde 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 38.569 in de Peppol Directory gestegen. Dit is een stijging van 17% t.o.v. 2022 (vorig jaar: 83% stjging);
- het aantal endpoints dat documenttype SI-UBL 2.0 invoice ondersteunt, groeide naar 37.945. Een stijging van 18% t.o.v. 2022 (vorig jaar een stijging van 87%);
- het aantal endpoints dat documenttype SI-UBL 2.0 creditnote ondersteunt, groeide naar 37.043. Een stijging van 18% t.o.v. 2022 (vorig jaar een stijging van 135%).

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 2023 is wederom een stijging te zien in het aantal ontvangen e-facturen. Het totaal aantal e-facturen bedroeg 1.920.023, dat is 82% van de totale facturenstroom. Het percentage e-facturen steeg met 1,8% t.o.v. 2022. (bron: Jaarrapportage bedrijfsvoering Rijk 2023).
- Ten opzichte van 2022 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 2023 (1.208.789) is gestegen met 79% ten opzichte van het jaar daarvoor.
- Ten opzichte van 2022 is een flinke stijging van 45% in het aantal ontvangen facturen te zien via het Rijksoverheid Peppol Accesspoint (vorig jaar een forse stijging van 134%).

Mede op basis van bovenstaande gegevens is de mening van de normcommissie e-Facturatie dat het gebruik van NLCIUS **sterk** is **toegenomen**. 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.

Relevante ontwikkeling

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 2024 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.

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-XML en voor de factuur ook UBL. Deze standaarden specificeren voor de Nederlandse uitzendbranche welke gegevenselementen verplicht en welke optioneel zijn bij de uitwisseling van informatie. Deze gegevenselementen worden vervolgens afgebeeld op de gegevens in de HR-XML 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), software-leveranciers 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):

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.

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 nieuwe leden en een doelgroep aangeboord, namelijk organisaties die zich bezighouden met planning. Introductie van deze standaarden heeft bovendien voor meer naamsbekendheid en daarmee meer adoptie van de SETU standaarden gezorgd.

Relevante ontwikkeling

In 2023 is de SETU Standard for Planning and Scheduling versie 1.0 gereleased. In het najaar van 2023 zijn de eerste partijen 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 wordt 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 en wordt het in de toekomst voor partijen mogelijk om zelf nieuwe koppelvlakken te ontwikkelen op basis van de SETU-taal.

In het kader van community management is er in 2023 voorbereidend werk gedaan om een nieuwe SETU-werkgroep op te starten: werkgroep Adoptie & Communicatie. Deze werkgroep gaat zich vanaf 2024 specifiek richten op een grotere bekendheid van de SETU onder de verschillende partijen.

In 2024 is er een aantal ontwikkelingen gaande die impact hebben op de adoptie van de SETU. Nieuwe wetgeving rondom de inlenersbeloning en de wet toelating terbeschikkingstelling bieden mogelijkheden tot updates en nieuwe koppelvlakken binnen de standaard.

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 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 (MIG: Message Implementation Guidelines).

De standaard staat op de 'pas toe of leg uit' lijst sinds 15 april 2014.

Feitelijk gebruik

Met als focus de overheidssector is het WDO Datamodel niet alleen van nut voor de Douane maar ook voor andere overheidsinstellingen die betrokken zijn bij grensoverschrijdend verkeer zoals Rijkswaterstaat, de Havenautoriteiten, de Koninklijke Marechaussee en het Ministerie van I & W. Voor de Douane wordt de standaard met name toegepast voor goederenstromen, maar daarnaast biedt het WDO Datamodel zoals eerder al opgemerkt ook informatie over personen (voor bijvoorbeeld de Marechaussee) en informatie over vervoermiddelen (voor bijvoorbeeld Rijkswaterstaat).

De Douane (beheerder van de standaard) meldt dat het WDO Datamodel momenteel in Nederland gebruikt wordt voor 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.

- 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.
- Nederlandse Voedsel- en Warenautoriteit (NVWA) Veterinair en Fytosanitair. Dit betreft 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.
- 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 zg. ERMIS pakket, waarin een module voor Transit is opgenomen. Dit pakket werkt echter op basis van de door de EU gedefinieerde berichtstandaarden, welke niet identiek zijn aan de WDO datamodel standaard. Gebruik van het WDO datamodel voor het externe domein (B2G en G2B) was wel mogelijk maar zou teveel werk (conversies) met zich meebrengen.

- Als we de opgave van de berichtenstromen als indicator gebruiken voor het gebruik van het WDO Datamodel, dan kan worden geconcludeerd dat per saldo sprake is van een af**name van het gebruik**. Net als in voorgaande jaren ontbreken verdere 'harde' gegevens over het feitelijk gebruik. Een goede vergelijking met het gebruik vorig jaar gebaseerd op basis van dergelijke hard cijfermateriaal is daarom niet te maken. In zijn algemeenheid kan worden gesteld dat in Nederland de meeste partijen die de standaard zouden moeten gebruiken zijn aangesloten. De adoptiegraad is hoog, vooral vanwege het feit dat de Douane het model gebruikt in hun Maritime Single Window (MWS). Het gebruik van de standaard is daar vanzelfsprekend.

  Relevante ontwikkeling

  Binnen Nederland is de Kustwacht aan het aansluiten bij het WDO Datamodel. Eén van de Nederlandse overheidspartijen voor wie het WDO Datamodel mogelijk van toepassing lijkt, maar die het niet gebruiken, is de landbouw, en dan meer specifiek de NVWA. Hiervoor zijn recent een aantal belangrijke gesprekken geweest met onder meer die NVWA. Toen alles klaar leek te staan voor adoptie van deze groep werd er echter geen prioriteit gegeven aan de stap naar het WDO datamodel, waardoor landbouw nu nog steeds geen gebruik maakt van de standaard. De Douane onderneemt op dit moment geen verdere acties voor het werven van nieuwe gebruikers.

  Andere relevante ontwikkelingen spelen vooral op Europese schaal.

Zo ontwikkelt de EU een European Maritime Single Window Environment (EUMSW)-omgeving die ook in de basis is gebaseerd op het WDO Datamodel, zij het via het International Maritime Organization datamodel (IMO). Daarnaast lijkt het EUMSW zich te gaan richten op het eerder genoemde MMT, dat vooral betrekking heeft op havenprocessen. De IMO en de WCO stemmen ontwikkelingen onderling af, om tegenstrijdigheden te vermijden. De EUMSW kan gezien worden als een regionale specialisatie van het IMO Datamodel. Het IMO heeft een focus op vrachtverkeer; het EUMSW kijkt ook naar personen en bijvoorbeeld vergunningen. De scope is daarmee dus niet helemaal hetzelfde.

Implementatie van het EUMSW heeft naar verwachting vooral impact aan de ´markt-zijde' van het MSW. Het hangt af van de keuze die gemaakt wordt bij implementatie, of dit vooral tot aanpassingen leidt door het centrale MSW of door individuele marktpartijen.

Verder ontwikkelt de EU een nieuw raamwerk voor douane-informatie, het EUCDM. De EU is lid van de WCO, en stelt daar wijzigingen voor op basis van hun wensen om deze twee modellen op elkaar afgestemd te houden. Net als het WCO heeft dit model een focus op douane-gegevens.

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

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 al een aantal jaren 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.

	Realisatie 2019	Realisatie 2020	Realisatie 2021	Realisatie 2022	Realisatie 2023	Realisatie 2024 t/m april
Belastingdienst						
Aangifte IB + VPB	16.558.025	15.568.706	15.846.758	15.546.416	17.219.117	7.809.723
Aangifte OB + Intercomm.	5.429.106	5.890.273	6.379.104	7.288.250	7.960.681	3.526.726
Toeslagen	1.325.719	1.279.414	1.355.471	1.617.206	1.978.644	741.297
Erfbelasting+ Schenkbelasting	4.073	16.115	31.496	41.012	52.176	22.585
Uitsluitend Zakelijk Gebruik	1.143	924	854	796	312	144
KvK – Reporting Services (SBR)						
Jaarrekeningen	1.020.450	886.373	889.466	962.503	943.625	261.961
DUO – Reporting Services (SBR)						
Jaarrekeningen	1.953	1.942	1.963	3.989	5.015	108
SBR Wonen - Reporting Services (SBR)						
DPI (prognose informatie)	1.112	1.194	898	1.051	1.163	210
DVI (verantwoordingsinformatie)	1.363	1.370	1.745	1.704	1.744	7
SBR Wonen Jaarrekening	1.364	1.242	1.226	1.417	1.185	6

Een vergelijking van de cijfers over de (volledige) jaren 2019 tot en met 2023 lijkt erop te duiden dat de adoptie van SBR en daarmee XBRL binnen Nederland stabiel is.

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.

Relevante ontwikkeling

Momenteel wordt er wetgeving voorbereid die grote rechtspersonen vanaf boekjaar 2025 verplicht hun jaarrekeningen in Inline XBRL te deponeren. Hiervoor wordt het huidige SBR-afsprakenstelsel aangepast. Inline XBRL is gekozen omdat de Europese Corporate Sustainability Reporting Directive (CSRD) voorschrijft dat ESG-informatie (Environmental, Social en Governance) vanaf 1 januari 2026 in Inline XBRL moet worden opgenomen in het bestuursverslag van een grote rechtspersoon. Omdat het bestuursverslag onderdeel is van het jaarverslag, is besloten om het hele jaarverslag, waaronder dus ook de jaarrekening, in

Inline XBRL op te stellen. Het grote voordeel van Inline XBRL is dat de informatie zowel leesbaar is voor mensen als dat het geautomatiseerd kan worden verwerkt.

Het afgelopen jaar is de SBR Governance aangepast op verzoek van de deelnemers. De SBR Governance kent nu een Strategisch en Tactisch Beraad met vertegenwoordigers van verschillende private en publieke domeinen. Het operationele werk, zoals het opstellen van wijzigingsvoorstellen voor het SBR-afsprakenstelsel, wordt uitgevoerd door gespecialiseerde taakgroepen.

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 nieuwe bron (Wiki XL):

- bezoeken 30.573 (+ 44% t.o.v. 2022)
- paginaweergaven[10] 115.433 (+ 14% t.o.v. 2022)
- downloads 4.025 (+ 7% t.o.v. 2022)
- uitgaande links[11] 1.414 (- 28% t.o.v. 2022)

[10] Geslaagd verzoek om een bepaalde webpagina te tonen.

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

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'.

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 stellen[12].

GWSW

Waarom belangrijk ?

Riolering is een essentiële maatschappelijke voorziening en het beheer ervan een sleuteltaak 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)[13];

[12] Bron: Jaarverslag 2023 Informatiehuis Water

[13] PDOK is het landelijke platform voor het ontsluiten van geodatasets van Nederlandse overheden.

- 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.gwsw.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 modelleringssoftware de voorgeschreven GWSW-formaten kunnen uitwisselen;
- 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.

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 aangeven 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 wordt op dit moment gewerkt aan het uitbreiden van de Basisregistratie Ondergrond met data over de milieu-hygiënische kwaliteit van de bodem (BRO fase II). Bij de standaardisatie van de milieukwaliteit (inclusief PFAS) is het uitgangspunt dat SIKB0101 als basis dient voor de ontwikkeling van IMBRO/IMBRO-A standaard. Waar nodig worden aanpassingen in de standaard worden doorgevoerd. Allereerst wordt de catalogus voor IMBRO/A, de archiefgegevens, gerealiseerd, zodat bestaande data kunnen worden aangeleverd. Hierna volgt de catalogus voor IMBRO voor de nieuwe data. IMBRO/A is naar verwachting medio 2024 operationeel.
Hiernaast wordt gewerkt aan het uitbreiden van de standaard ten behoeve van uitwisseling van onderzoeksgegevens over asbest in bodem.

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 voorbereidingen van de herbouw zijn 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.

Domein bouwen en wonen

IFC

Waarom belangrijk?

IFC is een gestandaardiseerde, digitale beschrijving van assets in de bouw- en infrasector, ontwikkeld door buildingSMART International. In Nederland wordt de standaard ondersteund door buildingSMART Nederland. IFC is een open internationale standaard (ISO 16739-1:2018)die de uitwisseling van leveranciers-neutrale en bruikbare informatie tussen verschillende softwareplatforms en interfaces mogelijk maakt. De standaard is specifiek gericht op BIM-informatie (Building Information Modeling) en maakt het mogelijk om gedetailleerde 3D-modellen van bouwwerken inclusief bijbehorende gegevens en relaties digitaal vast te leggen en uit te wisselen. Het maatschappelijk nut van de IFC-standaard ligt in de verbeterde samenwerking en communicatie tussen verschillende stakeholders in de bouwsector, wat resulteert in duurzamere, veiligere en efficiëntere bouwprojecten. Dit draagt bij aan een betere leefomgeving en een duurzamere samenleving.

Het gebruik van de IFC-standaard is van groot belang omdat het:

- de efficiëntie verbetert. Door uniforme data-uitwisseling tussen verschillende partijen in de bouwsector worden processen gestroomlijnd en fouten verminderd;
- kosten bespaart. Minder fouten en efficiëntere samenwerking leiden tot lagere projectkosten;
- duurzaamheid bevordert. Betere planning en uitvoering dragen bij aan duurzamere bouwprojecten;
- wetgeving ondersteunt. Dit faciliteert automatische controles op naleving van bouwregelgeving.

De IFC-standaard staat op de ‘pas-toe-of-leg-uit’-lijst sinds november 2011. Opname van de IFC-standaard op de ‘pas toe of leg uit’-lijst stimuleert overheidsorganisaties om deze standaard te gebruiken (bredere adoptie), wat de consistentie en interoperabiliteit in de sector ten goede komt.

Feitelijk gebruik

Er zijn lang geen gegevens geweest over het feitelijk gebruik van de IFC-standaard bij overheden. Daarin is verandering gekomen met het verschijnen in de zomer van 2021van een 1e Nationale BIM monitor. Deze rapportage is in de monitor open standaarden 2022 (over 2021) gepresenteerd als een 0-meting. Vorig jaar waren geen nieuwe cijfers beschikbaar; er wordt eens in de twee jaar gemeten. Dit jaar zijn er wel nieuwe cijfers. Deze meting werd uitgevoerd onder 600 respondenten, waaronder 80 overheidsorganisaties.

Uit de Nationale BIM Monitor 2023 blijkt het volgende:

- bekendheid met IFC: 25% (stijging van 3% ten opzichte van 2022);
- gebruik van IFC: 8% (stijging van 2% ten opzichte van 2022).

Net als bij de nulmeting is vooralsnog sprake van lage scores op kennis en gebruik van deze standaard, het **gebruik is beperkt**. Tegelijkertijd zien we wel een **lichte stijging**, zowel als het gaat om de bekendheid als om het gebruik ten opzichte van de vorige meting.

Relevante ontwikkeling

Een belangrijke mijlpaal in 2023 is dat IFC4 nu officieel is erkend als een ISO-standaard (ISO 16739-1:2018). Deze nieuwe versie van de standaard biedt verbeterde functionaliteiten, uitgebreidere mogelijkheden voor data-uitwisseling en betere ondersteuning voor complexe infrastructuurprojecten. De erkenning als ISO-standaard versterkt de positie van IFC4 als de toonaangevende standaard voor BIM-informatie in de bouw- en infrasector.

In 2023 heeft de gemeente Amsterdam een pilotproject uitgevoerd waarbij IFC-modellen werden geïntegreerd met AI-gestuurde analysetools. Deze tools analyseerden grote hoeveelheden bouwdata om potentiële constructiefouten te identificeren voordat ze zich voordeden, wat resulteerde in een vermindering van bouwfouten met 15%.

Bouwbedrijf Heijmans heeft in 2023 IFC-modellen gebruikt om de duurzaamheidsprestaties van hun nieuwe woonprojecten te evalueren. Met deze verhoogde focus op duurzaamheid door gegevens over energieverbruik en materiaalgebruik te analyseren, kon Heijmans ontwerpen optimaliseren om de CO2-uitstoot van hun projecten met 10% te verminderen.

De luchthaven Schiphol heeft digitale tweelingen (Digital Twins) van haar terminals gecreëerd met behulp van IFC-gegevens. Deze digitale replica's worden gebruikt om de operationele efficiëntie te verbeteren door real-time monitoring van passagiersstromen en onderhoudsbehoeften, wat heeft geleid tot een verbeterde klanttevredenheid en een reductie van onderhoudskosten met 12%.

Rijkswaterstaat heeft de Nationale BIM Basis ILS (Informatie Leverings Specificatie) toegepast in een groot infrastructureel project, waarbij IFC-modellen werden gebruikt om alle projectinformatie te standaardiseren. Dit zorgde voor een soepele samenwerking tussen verschillende partijen, zoals ontwerpers, aannemers en toezichthouders, en verminderde de tijd die nodig was voor informatie-uitwisseling met 25%.

In Den Haag wordt IFC gebruikt voor geautomatiseerde veiligheidsinspecties van nieuwe bouwprojecten. Door veiligheidsprotocollen in het IFC-model te integreren, kunnen inspecteurs automatisch controleren op naleving van veiligheidsnormen tijdens elke fase van de bouw, wat heeft geleid tot een vermindering van veiligheidsincidenten met 30%.

De stad Eindhoven heeft IFC-modellen geïntegreerd in haar smart city-platform. Dit platform koppelt gegevens over gebouwen en infrastructuur aan stadsbrede systemen voor energiebeheer en milieumonitoring. Hierdoor kan de stad energie-efficiëntie verbeteren en luchtkwaliteit in real-time monitoren, wat heeft bijgedragen aan een reductie van stedelijke CO2-uitstoot met 8%.

NLCS

Waarom belangrijk?

Organisaties hanteren vaak een eigen tekenstandaard voor digitale tekeningen. Hiermee geeft een organisatie een eigen signatuur af. Maar het belemmert ook de uitwisseling en het hergebruik van tekeningen waardoor deze vaak opnieuw moeten worden getekend. NLCS zorgt voor meer eenheid in het tekenwerk. NLCS is een tekenstandaard voor het maken van 2D-ontwerptekening en gaat uit van objectgericht werken. Alle informatie in een tekening wordt gekoppeld aan objecten die in lagen worden geordend. Gebruikers kunnen hiervoor een standaard objectenbibliotheek gebruiken die met de NLCS wordt meegeleverd. NLCS staat op de 'pas toe of leg uit' lijst sinds mei 2018.

Door een plaats op de 'pas toe of leg uit'-lijst is NLCS een breder geadopteerde standaard geworden. De markt gebruikt de standaard en ziet ook het groeipotentieel van de standaard. Door de hogere adoptiegraad worden meer inkomsten gegenereerd door middel van een vrijwillige beheerbijdrage vanuit de gebruikers, welke ingezet wordt voor het beheer maar met name ook voor de doorontwikkeling van de standaard binnen de kaders van DSGO en het Bestuursakkoord 2027 vanuit digiGO. NLCS wordt ook ingezet om ontwikkelingen rond maatschappelijke opgaves zoals de energietransitie, circulariteit, duurzaamheid, CO2-reductie enz. beter inzichtelijk te krijgen.

Feitelijk gebruik

Er zijn op dit moment (zomer 2024) vele honderden organisaties die de NLCS Standaard gebruiken. Het grootste deel daarvan betreft de private sector en 230 organisaties betreft de publieke sector, dit zijn vaak de opdrachtgevers . Het feitelijk gebruik door overheidsorganisaties, uitgedrukt in het aantal gebruikers van CAD software met NLCS, ziet er als volgt uit.

Type overheid	2020	2021	2022	2023
Gemeenten	138	138	158	..
Waterschappen	15	8	13	..
Provincies	10	11	11	..
Rijksoverheid	5	5	2	..
Netbeheerders	5	5	19	..
Kennisinstellingen	6	6	6	..
Totaal	179	173	209	230

In vergelijking met voorgaande jaren is sprake van een ***geringe toename*** van het gebruik. De verklaring voor deze stijging is het feit dat de standaard meer volwassen is geworden waarmee het gebruik is toegenomen. Er wordt met doorontwikkelingen van de 3 pijlers (Stedelijk spoor, Netbeheer en Openbare Ruimte) van de standaard ingespeeld op vragen die leven in de markt. Door het integreren van deze ontwikkelingen in de standaard, worden

weer meer gebruikers bereikt en neemt het gebruik toe. Ook het aantal leveranciers zal waarschijnlijk toenemen als gevolg van de uitbreiding naar de energiesector.

In het afgelopen jaar is het aantal organisaties dat een vrijwillige bijdrage levert vergroot naar ongeveer 120 organisatie die een bijdrage aan de ontwikkeling van de standaard. Echter, de methodiek waarbij de vrijwillige bijdrage wordt geïncasseerd is niet toekomstbestendig en zal op korte termijn aangepast moeten worden. Door de transitie van BIM Loket naar digiGO wordt een professionaliseringsslag gemaakt waarbij een gestructureerd proces wordt ingericht met betrekking tot het contact met organisaties voor een te leveren bijdrage aan de ontwikkeling van de standaard. In 2024 wordt nagedacht om de inning van de vrijwillige bijdrage in samenwerking met de ICT leveranciers uit te voeren.

De trend om tekenwerk uit te besteden heeft ook dit jaar weer verdere stappen gezet. Net als vorig jaar wordt ook nu geconstateerd dat in de gemeentelijke markt niet alle organisaties beschikken over een civieltechnische afdeling en/of medewerkers met vakinhoudelijke kennis. Deze gemeenten laten zich voor de ontwerp-werkzaamheden conform NLCS volledig ontzorgen door marktpartijen (opdrachtnemers). Deze gemeenten voldoen dus indirect wel aan de 'pas toe of leg uit' norm, maar zullen niet beschikken over eigen software oplossingen. Verder is het gebruik van de standaard bij beheerders van ondergrondse infrastructuur nog een stuk lager dan zou kunnen. Diverse organisaties gebruiken nog eigen laagindelingen. Dat is wel aan het veranderen en zal nog een stuk sneller gaan wanneer NLCS geschikt wordt gemaakt voor deze sector.

De verwachting is dat de aankomende jaren een significante groei zal ontstaan omdat meerdere sectoren op dit moment willen aansluiten op de NLCS standaard, dit zijn:

- de energiesector
- de waterleidingbedrijven
- gasbedrijven
- bedrijven die zich bezig houden met de ondergrondse bekabeling
- stedelijk spoor vervoerders

Relevante ontwikkeling

DigiGO heeft in 2024 het afsprakenstelsel voor de bouwsector gelanceerd. Dit betreft een afsprakenstelsel om op een gestandaardiseerde manier gegevens uit te wisselen. Dit afsprakenstelsel is gebaseerd op open standaarden. In de aankomende jaren zal er beleid ontwikkeld worden om het tekenwerk op deze gestandaardiseerde manier te delen met andere organisaties in de bouwsector, de lokale overheden en de landelijke overheden.

In 2024 is de release 5.1 op de markt gebracht. Deze release is ook middels linkeddata beschikbaar gesteld. Eind 2024 zal er een volgende release op de markt worden gebracht, daarin zit o.a. regulier onderhoud van vele 10-tallen RFC's, aansluiting van de energiesector, koppeling met de standaarden uit de openbare ruimte en de standaardisatie van de Nederlandse verkeersborden.

De opdrachtgevers die de NLCS standaard willen gebruiken in de energiesector hebben behoefte aan verdere certificering van software leveranciers. Dit traject zal in 2024 worden gestart en de verwachting is dat dit in 2025 realiteit zal worden.

Met het uitbreiden van de tekenstandaard uit andere sectoren zal het aantal gebruikers sterk groeien. Er is een verwachting dat het aantal ICT leveranciers zal verdubbelen.

Er is steeds meer vraag om 2D en 3D tekenwerk op elkaar aan te laten sluiten.

Er is steeds meer vraag om de afspraken die van toepassing zijn in de NLCS Standaard te gebruiken als basis voor de planning en begroting voor de volgende fasen in het bouwproces.

In 2023 zijn er grote stappen gemaakt om het beheer te professionaliseren. Zo heeft een technische migratie plaatsgevonden van de SQL database naar een linkeddata database, zijn er 10-tallen knelpunten opgelost en is het functioneel en technisch beheer geprofessionaliseerd.

VISI

Waarom belangrijk?

"Ik wil aantoonbare en traceerbare communicatie tussen participanten in de verschillende disciplines in de bouw voor alle fasen van een object/project (initiatie t/m sloop)". Dat is volgens gebruikers van de VISI standaard de essentie. Communicatie is essentieel voor het functioneren van organisaties. Afspraken tussen opdrachtgevers aannemers, architecten, klanten en toeleveranciers komen immers tot stand door te communiceren. Hetzelfde geldt voor de acceptatie van geleverde resultaten.

De VISI standaard zet deze 'communicatieve acties' ten behoeve van besluitvorming centraal en richt zich op het digitaal organiseren en vastleggen van communicatie tussen partijen in elke fase van de bouw en onderhoud aan het gebouw. De VISI-standaard biedt daartoe een methodiek en format voor het beschrijven van verantwoordelijkheden, interacties, en proces workflow tussen actoren in bouwend Nederland.

Met behulp van VISI worden contractuele en bedrijfsprocessen in de vorm van workflow gedigitaliseerd en digitaal uitvoerbaar in gecertificeerde applicaties. Daarmee is vastgelegd wanneer (proces), wie (rol), wat (informatie), aan wie (rol) aanlevert of mag accorderen. Door het uitwisselen van VISI berichten (digitale formulieren) wordt stapsgewijs elk proces uitgevoerd. Hierbij kan gedacht worden aan het geven van opdrachten, het aanleveren van tijdschema's, ontwerpen of plannen, het opleveren van resultaten en het melden van afwijkingen of wijzigingen.

Door het samenwerken in VISI ontstaat voor elke deelnemende organisatie een dossier van afspraken en communicatie daartoe. Elke organisatie heeft daarbij vrije marktkeuze in VISI leverancier, waardoor iedereen in eigen software kan werken. Hierdoor hoeven organisaties niet meer in elkaars systeem in te loggen of in een centraal systeem te werken. Bij een geschil

heeft elke partij dezelfde informatie en is het meteen duidelijk hoe de samenwerking is verlopen. VISI zorgt in elke deelnemende applicatie voor een audit trail.

Het doel van VISI is om de transparantie en traceerbaarheid van het bouwproces te vergroten en hiermee de kwaliteit en efficiency te verhogen en de doorlooptijd te verkorten. Als conclusie van de recente herijking van de VISI standaard hebben alle betrokken organisaties (overheid en markt) gesteld dat daarin de VISI standaard nog steeds relevant en actueel is.

VISI staat op de pas-toe-of-leg-uit-lijst sinds 9 december 2014.

Feitelijk gebruik

Organisaties kunnen VISI gecertificeerde software inkopen bij een viertal software-leveranciers, of hebben de mogelijkheid om deze zelf in eigen applicaties in te bouwen. In een VISI project zitten doorgaans 2 of meerdere organisaties. Elke organisatie binnen een project kan voor een andere leverancier kiezen.

Om een VISI applicatie een toepassing te geven is een VISI raamwerk nodig. Dit definieert de verantwoordelijkheden, interacties, en proces workflow tussen de actoren in een project en kan dus gebaseerd zijn op elke type samenwerkingsvorm of contract. VISI raamwerken kunnen onafhankelijk van een softwareleverancier worden opgesteld door (advies)organisaties en worden ingelezen in de software. Momenteel zijn er 7 organisaties die VISI raamwerken bouwen voor organisaties.

In achterliggende jaren zijn door de beheerorganisatie gegevens over het gebruik van de standaard bij overheidsorganisaties aangeleverd, dit jaar ontbreken dergelijke cijfers. Van de kant van de beheerorganisatie wordt wel gemeld dat het gebruik van de VISI standaard **stabiel** is. Het gebruik van de VISI Standaard in de GWW sector is hoog en de naamsbekendheid is eveneens hoog. Het gebruik van de VISI standaard in de woningbouw is minimaal, er is één grote gemeente die de VISI standaard in de woningbouw gaat toepassen. De verwachting is dat dit verdere opvolging zal krijgen bij andere grote gemeentes. De VISI standaard is voornamelijk interessant bij bouwprojecten van 50.000 euro en hoger én waarbij er sprake is van een langere doorlooptijd. Het gebruik van de VISI standaard is afhankelijk van de conjunctuur in de bouwsector.

Relevante ontwikkeling

Er zijn een paar belangrijke ontwikkelingen die relevant zijn om te vermelden.

- Het aantal toepassingsgebieden groeit. Naast het bouwproces wordt de VISI standaard ook gebruikt bij beheer van gebouwen.
- Naast de traditionele bouwsector wordt de VISI standaard ook gebruikt bij de aanleg van windmolenparken, havens, afvalverwerkingsbedrijven en groenvoorzieningen bij gemeenten. De VISI Standaard heeft een ISO norm. Op dit moment wordt de VISI standaard besproken in Europese Standaardisatie organisaties. Wellicht zorgt dit ervoor dat de VISI standaard ook in de EU gebruikt gaat worden.

Domein bestuur en recht

BWB, ECLI en JCDR
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 oplossingsrichtingen worden onderzocht. Daarbij wordt ook gekeken naar de STOP-standaard (Standaard Officiële Publicaties) die in het kader van het Digitaal Stelsel Omgevingswet is ontwikkeld. STOP is gebaseerd op de Akoma Ntoso-standaard van OASIS. Ook wordt gekeken naar mogelijke implementatie van de European Legislation Identifier (ELI). Op korte termijn wordt echter geen uitfasering verwacht van de BWB standaard. Hiervan wordt al melding gemaakt sinds de Monitor Open Standaarden 2020. Er zijn momenteel geen concrete plannen voor vervanging, al wordt er wel nog steeds naar de genoemde alternatieven gekeken.

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

Waarschijnlijk zal een nieuwe, in het kader van BWB te ontwikkelen standaard ook toepasbaar zijn op 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. De Europese Commissie is nu bezig met de (verplichte) implementatie. De voortgang is vertraagd, mede als gevolg van de recente coronacrisis.

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

In LiDO, linkeddata.overheid.nl komt de toepassing van alle drie de juridische standaarden samen. LiDO is een databank met miljoenen hyperlinks, waarmee iemand snel inzicht kan krijgen in de verbanden tussen nationale en Europese regelgeving, uitspraken van Nederlandse en Europese rechters, parlementaire documenten en officiële bekendmakingen. De bezoekers zijn (her)gebruikers van juridische overheidsdata. Hierbij gaat het om overheid (centraal en decentraal), uitgevers van juridische informatie, content integrators, uitvoeringsorganisaties, studenten en rechtswetenschappers van universiteiten en hogescholen.

Het gebruik van LiDO wordt sinds de Monitor Open standaarden 2018 aangemerkt als een graadmeter voor het gebruik van de standaarden BWB, JCDR en ECLI samen.
Deze meetmethode bleek niet het gewenste inzicht te bieden in het daadwerkelijk gebruik van de Juriconnect standaarden. Gezocht is naar een methodiek die beter inzicht verschaft. 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 en de Tweede Kamerverkiezing van 22 november 2023. 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. Aangezien de vermoedelijke datum van inwerkingtreding van de WPV nu 01-07-2025 is, blijft de EML_NL standaard voorlopig nog op de 'pas toe of leg uit'-lijst staan.

Domein onderwijs en cultuur

E-Portfolio NL NEN 2035

Waarom belangrijk?

Door de invoering van competentiegericht leren en toenemende interesse in het gebruik van e-portfolio's is het van belang een afspraak te hebben voor het uitwisselen van e-portfolio-gegevens. Met E-portfolio NL kunnen de competenties van een individu worden bijgehouden. Het voordeel van deze standaard is dat de student/lerende medewerker zijn profiel mee kan nemen naar verschillende organisaties. E-portfolio NL (beheerorganisatie: NEN) is een toepassingsprofiel voor studenten en werknemers bij Nederlandse organisaties, van de internationale IMS ePortfolio specificatie. De standaard staat op de 'pas toe of leg uit' lijst sinds mei 2010.

Feitelijk gebruik

Volgens de gegevens van NEN is de standaard in 2023 6 keer aangeschaft via de NEN-website en 2 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.

De score van 2022 was 4 keer aangeschaft en respectievelijk 12 keer ingezien. Geen van de hier bedoelde gebruikers van de standaard is werkzaam bij een publieke organisatie.

Relevante ontwikkeling

Er hebben in de afgelopen jaren geen nieuwe ontwikkelingen plaatsgevonden. Wel heeft de herziene versie van de internationale standaard ISO/IEC 20013 uit 2020 dezelfde reikwijdte als NEN 2035 uit 2014. Deze standaarden bevatten geen tegenstrijdigheden. Over het algemeen heeft het gebruik van een internationale standaard de voorkeur boven een nationale en de ervaring leert dat, wanneer een internationale standaard gepubliceerd is deze gewoonlijk het gebruik van de nationale standaard minimaliseert omdat partijen voor de internationale standaard kiezen. In het geval van de e-portfolio standaarden is dat echter niet het geval: ISO/IEC 20013 is in 2023 één keer ingezien via NEN Connect.

Ondanks het beperkte gebruik van NEN 2035 en een afname in het totaal aantal gebruikers, geven partijen aan geen noodzaak te zien om over te schakelen naar een andere (internationale) standaard. Uit gesprekken blijkt dat partijen NEN 2035 bruikbaarder vinden dan het internationale alternatief, aangezien NEN 2035 de Nederlandse specificatie van een Europese afspraak (e-portfolio) betreft en specifiek gericht is op de Nederlandse markt.

Er wordt voorgesteld om NEN 2035 op de lijst te laten staan en deze breder onder de aandacht te brengen. NEN zal hiervoor artikelen publiceren in haar eigen nieuwsbrieven en op de website, en daarnaast samenwerking zoeken met organisaties die publicaties voor de onderwijssector aanbieden.

NL LOM

Over deze standaard is helaas geen informatie beschikbaar. In de achterliggende jaren was dat wel telkens mogelijk.

De standaard staat op de nominatie om afgevoerd te worden van de ‘pas toe of leg uit’-lijst. In de vorige monitor-rapportage is dit al nadrukkelijk als optie benoemd. Om die reden is dit jaar (2023) niet bevraagd.