Inventarisatie gebruiksgegevens 2023 door BFS

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. Het 'pas toe of leg uit'-regime is gericht op aanbestedingen, voor een completer beeld van de adoptie is het feitelijk gebruik dus interessant.

Net als vorig jaar is dit deelonderzoek dit jaar uitgevoerd door de accountmanagers van het Bureau Forum Standaardisatie (BFS). Helaas is het niet altijd even eenvoudig om (voor alle open standaarden) vast te stellen in welke mate die feitelijk door overheden gebruikt worden. De accountmanagers van BFS hebben hiervoor contact opgenomen met beheerders van standaarden en sommige specifiek voor de standaard relevante voorzieningen. In vergelijking met vorig jaar zijn twee standaarden van de lijst verdwenen: COINS en OWMS. Daar staat tegenover dat er een nieuwe standaard aan de lijst is toegevoegd: security.txt (datum van besluit: 25 mei 2023).

Voor een aantal standaarden uit het domein Veilig Internet zijn de gebruiksgegevens afkomstig uit het halfjaarlijkse onderzoek naar internet-veiligheids-standaarden (zie meting medio 2023, nog te publiceren). De peildatum van deze meest recente IV-meting is juli 2023.

Over het gebruik van de volgende vier standaarden is dit jaar geen (actuele) informatie beschikbaar: Ades Baseline Profiles, EML_NL, E-Portfolio NL NEN 2035 en NL LOM.

B4.1. 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 nieuwe standaard security.txt is overigens geen informatie te vinden in de binnenkort te verschijnen rapportage 'Meting informatieveiligheidsstandaarden overheid medio 2023'. Reden daarvan is dat met betrekking tot deze standaard nog geen streefbeeldafspraak is gemaakt.

In de meest recente meting (juli 2023) zijn 5.352 domeinnamen getoetst. In de meting begin 2023 waren dit er nog 2.654. Dit is een forse groei en de verwachting is dat deze groei de komende tijd verder gaat doorzetten. De groei dit jaar 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 juli-meting in een 'afgeleide' meting die is gebaseerd op de

steekproef die in januari 2023 is gebruikt. Zodoende is er een goede basis om de beide peilmomenten uit 2023 met elkaar te vergelijken. De steekproef die afgelopen januari is gehanteerd, verschilt vrijwel niet van de steekproef uit 2022. Om die reden wordt ook de meting uit 2022 in het gepresenteerde tijdsperspectief meegenomen.

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 2.661 domeinen van de overheid[1].

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	medio 2024	begin 2025
DMARC policy	72 %	79 %	81 %			

[1] Bij de meting 2022 lag dit aantal op 2.584 domeinen. Dit is de best mogelijk beschikbare basis om te vergelijken.

DKIM	82 %	84 %	85 %
SPF Policy	87 %	87 %	87 %

Het gebruik van anti-phishing standaarden ligt bij de hier gepresenteerde standaarden medio 2023 grofweg rond de 85% (voorjaar vorig jaar: ongeveer 80%). We zien dus **een stijging** ten opzichte van de monitor-rapportage van vorig jaar. DMARC is net als vorig jaar een relatieve achterblijver (81%), ook al is de relatieve winst ten opzichte van vorig jaar bij die standaard het grootst. Dat betekent voor nu dat voor 19% 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 2023 naar type overheid laat een volgend beeld zien (tussen haakjes de score van voorjaar 2022).

	Centrale overheid (n=1.869)	Provincies (n=24)	Water-schappen (n=30)	Gemeenten (n=363)	Gemeen-schappelijke regelingen (n=375)
DMARC policy	84 % (74%)	71 % (68%)	90 % (87%)	90 % (86%)	57 % (48%)
DKIM	83 % (78%)	92 % (82%)	100 % (97%)	99 % (99%)	85 % (82%)
SPF Policy	85 % (86%)	88 % (77%)	97 % (93%)	96 % (95%)	86 % (84%)

In dit overzicht valt op dat vrijwel overal hogere percentages worden genoteerd als de meest recente score van dit jaar (medio 2023) wordt vergeleken met die van het voorjaar vorig jaar (uit de monitor 2022). 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 2.600 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 = 2.600[2])	begin 2024	medio 2024	begin 2025
web-domein	89 %	90 %	91 %			
mailserver-domein	57 %	56 %	63 %			

Bij webdomeinen is sprake van een hoge score (91%), voor mailserverdomeinen ligt dit beduidend lager (63%). In de IV-meting wordt over dit laatste opgemerkt dat gebruik wordt gemaakt van clouddiensten voor e-mailverkeer, die de standaarden DNSSEC (en ook DANE) over het algemeen niet ondersteunen. Een soortgelijke opmerking is in de monitor 2022 ook gemaakt. In vergelijking met het voorjaar 2022 is sprake van een **geringe stijging**.

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.

	Centrale overheid (n=1.808 resp. 1.869)	Provincies (n=24 voor beide)	Water-schappen (n=30 voor beide)	Gemeenten (n=363 voor beide)	Gemeen-schappelijke regelingen (n=368 resp. 375)
web-domein	91 % (89%)	92 % (95%)	97 % (100%)	99 % (99%)	83 % (80%)
mailserver-domein	77 % (66%)	33 % (28%)	30 % (40%)	52 % (57%)	38 % (39%)

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 77% duidelijker hoger dan de rest. Gemeenten komen met een score van 52% nog het dichtst bij. De andere drie categorieën scoren duidelijk onder-gemiddeld. De eerdere opmerking hierboven met betrekking cloud-dienstverleners voor email-verkeer is hierbij een factor van belang ter verklaring van de lage scores.

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

HTTPS & HSTS en TLS

Waarom belangrijk ?

HTTPS & HSTS en ook TLS zorgen samen voor beveiligde verbindingen met websites, met als doel de veilige uitwisseling van gegevens tussen een webserver en client (vaak een webbrowser). Dit maakt het voor cybercriminelen moeilijker om verkeer om te leiden naar valse websites en om de inhoud van webverkeer te onderscheppen.
HTTPS zorgt voor het gebruik van HTTP over een met TLS beveiligde verbinding. Dit betekent dat het webverkeer door middel een certificaat wordt versleuteld.
HSTS zorgt ervoor dat een webbrowser, na het eerste contact over HTTPS, bij 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 2.653 respectievelijk 2.593 webdomeinen van de overheid[3].

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

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 sprake van een **lichte stijging** ten opzichte van de meting uit 2022. 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 2023, tussen haakjes de cijfers van vorig jaar).

Centrale overheid	Provincies	Water-schappen	Gemeenten	Gemeen-schappelijke regelingen
(n=1.808)	(n=24)	(n=30)	(n=363)	(n=368)

[3] Dit bestand biedt de best mogelijke vergelijking met het aantal domeinen van vorig jaar: 2.558.

HTTPS doorv.	93 % (91%)	92 % (82%)	100% (100%)	99 % (99%)	91 % (92%)
HSTS	81 % (75%)	88 % (91%)	93 % (93%)	97 % (97%)	58 % (52%)
TLS cf. NCSC	78 % (72%)	92 % (95%)	97 % (97%)	90 % (94%)	72 % (66%)

De centrale overheid – met verreweg de grootste groep webdomeinen – laat een score zien die vrijwel overeenkomt met het overall beeld[4]. Op elk van de drie standaarden is daar sprake van licht hogere percentages.

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

Relevante ontwikkelingen

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

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 2.653 respectievelijk 2.593 webdomeinen en 2.710 respectievelijk 2.661 domeinen voor e-mailverkeer van de overheid.

IPv6	voorjaar 2022	begin 2023 (n = 2.653 resp. 2.710)	medio 2023	begin 2024	medio 2024	begin 2025

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

			(n = 2.593 resp. 2.661[5])
webverkeer	70 %	72 %	75 %
e-mailverkeer	50 %	54 %	56 %

De adoptie van IPv6 voor e-mailverkeer ligt in deze meting met 56% net boven de helft (vorig jaar: 50%). De score voor webverkeer is beter, met 75% adoptiegraad (vorig jaar: 70%). Voor beide deel-metingen geldt dat sprake is van een **geringe maar continue stijging**.

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

	Centrale overheid (n=1.808 resp. 1.869)	Provincies (n=24 voor beide)	Water-schappen (n=30 voor beide)	Gemeenten (n=363 voor beide)	Gemeen-schappelijke regelingen (n=368 resp. 375)
webverkeer	75 % (68%)	75 % (82%)	93 % (97%)	94 % (94%)	55 % (49%)
emailverkeer	58 % (52%)	62 % (72%)	53 % (43%)	70 % (64%)	38 % (33%)

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 stijging. Bij de provincies is juist sprake van lagere percentages ten opzichte van 2022. 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 stijging.

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

Waarom belangrijk ?

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

De NEN-ISO/IEC 27002-standaard is een best practice van beveiligingsmaatregelen ('controls') om informatiebeveiligingsrisico's aan te pakken met betrekking tot vertrouwelijkheid, integriteit

[5] Dit biedt de beste basis voor een vergelijking met vorig jaar..

en beschikbaarheid van de informatievoorziening. De standaard kan gezien worden als een nadere specificatie van NEN-ISO/IEC 27001. ISO 27002 geeft richtlijnen en principes voor het initiëren, implementeren, onderhouden en verbeteren van informatiebeveiliging binnen een organisatie.

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

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

De Nederlandse overheid heeft haar eigen kaders voor informatiebeveiliging die zijn afgeleid van de 27001- en 27002-normen. Tot 2019 hadden alle bestuurslagen een eigen baseline, de BIR (Rijk), BIG (gemeenten), IBI (provincies) en BIWA (waterschappen). Deze baselines zijn (met uitzondering van de BIR2017) voor een groot deel nog gebaseerd op de ISO-normering uit 2005 en lopen achter op de actuele ISO-normen. De BIO is gebaseerd op de actuele, internationale standaard voor informatiebeveiliging (NEN-ISO/IEC 27001 en NEN-ISO/IEC 27002) en heeft risicomanagement als uitgangspunt. Alle overheidslagen hebben zichzelf verplicht de BIO toe te passen. Forum Standaardisatie heeft medio 2018 reeds geadviseerd om actief op adoptie van de BIO in te zetten, en de voortgang te monitoren. In reactie daarop heeft de werkgroep BIO aangegeven dat iedere overheidslaag zelf zal monitoren wat de voortgang is van de implementatie van de BIO. Vanaf 1 januari 2019 is de Baseline Informatiebeveiliging Overheid (BIO) van kracht. De BIO vervangt de bestaande baselines voor Rijk, Gemeenten, Waterschappen en Provincies.*Feitelijk gebruik*

Voor de Monitor 2023 zijn door de verschillende overheidslagen geen kwantitatieve gegevens over het gebruik van hun beveiligingsbaselines aangeleverd. Verantwoording over de beveiliging vindt in beginsel plaats aan de eigen controlerende organen.

Rijksoverheid

In de vorige monitor-rapportage stond dat CIO Rijk meldt dat de opvolger van de BIR2017, de BIO 1.04, op 11-2-2020 is gepubliceerd in de staatcourant en geldt voor alle overheidslagen. In 2020 hebben de departementen in de jaarlijkse CISO-gesprekken gemeld dat BIO 1.04 is of wordt geïmplementeerd. Een aantal departementen heeft ervoor gekozen om de BIO 1.04 in eigen departement specifieke baselines op te nemen. De departementen hebben aangegeven dat de initiële implementatie van de BIO 1.04 risicogericht is afgerond en dat via de PDCA-cyclus de implementatie actueel wordt gehouden. De BIO wordt momenteel geëvalueerd en de Rijksoverheid doet mee aan de evaluatie. Toepassing van de BIO is inmiddels dus onderdeel van de PDCA-cyclus.

Als aanvulling hierop het volgende. CIO Rijk meldt dat het gebruik van de BIO 1.04 (met als basis ISO27001 en 27002) binnen de Rijksoverheid goed gaat. Dit wordt via de CISO-gesprekken, de IB-beelden en de rode draden analyse daarop gemonitord. Daarnaast is er een jaarlijks onderzoek door de Audit Dienst Rijk naar informatiebeveiliging en doet de Algemenere Rekenkamer ook onderzoek. Kleine stijging: er wordt al jaren gestuurd op het voldoen aan de BIO.

Provincies

Alle provincies zijn bezig met het implementeren van de BIO en doen dat in combinatie met de ambitie om ISO 27001 certificeerbaar te worden voor één of meerdere processen.

In 2023 zijn drie provincies ISO 27001 gecertificeerd. In 2022 was één provincie ISO 27001 en BIO gecertificeerd. Dit is gerealiseerd door de BIO als extra normenkader aan de 27001-certificering toe te voegen. Het is onbekend hoeveel provincies in 2023 nog bezig zijn met een ISO 27001-cerficerertraject. [6]

Daarnaast zullen alle provincies op basis van risicoanalyses het juiste BBN niveau bepalen en daar de juiste maatregelen voor implementeren.

In de 2e helft 2021 hebben alle provincies een audit ondergaan, door dezelfde auditor. Op basis van deze auditresultaten hebben de provincies hun aanpak voor de komende periode bepaald om de certificeerbaarheid te realiseren.

Waterschappen[7]

Terugblikkend is de BIO bestuurlijk vastgesteld in de Ledenvergadering van 12 oktober 2018 van de Unie van Waterschappen. De BIO is daarmee vanaf 1 januari 2020 van toepassing.

Waterschappen zijn bezig met de volwaardige implementatie van de BIO; zij gebruiken alle de BIO als normenkader voor informatiebeveiliging. Deze is aangevuld met de IEC62443, specifiek voor procesautomatisering.

Naast de individuele verbeteracties wordt in gezamenlijkheid gewerkt aan het verhogen van de digitale weersrand van zowel de sector, als ook die van ketenpartners. In onderlinge samenwerking wordt onder meer gewerkt aan de ontwikkeling van een sectormethodiek van risicoanalyses, een CyberSecurity Implementatie Richtlijn (CSIR) en een ketenanalyse methodiek. Voortgang van de individuele en sectorale voortgang is dit jaar door een onafhankelijke partij beoordeeld. De resultaten van deze audit zijn zowel op individueel, als ook op sectoraal niveau, door de auditor voorzien van aanbevelingen. Waterschappen werken zowel sectoraal als

[6] Vanuit de hoek van de provincies is dit jaar geen reactie ontvangen. De tekst betreft de 'oude' tekst uit de vorige monitor-rapportage waarbij enkel het aantal provincies met certificering is geüpdatet en geeft mogelijk geen volledig actueel beeld.

[7] De tekst met betrekking tot de waterschappen is afkomstig uit de vorige monitor-rapportage en is nog steeds actueel dus behoeft geen bijstelling (bron: waterschapshuis).

individueel aan het verhogen van de digitale weerbaarheid. In 2024 zal opnieuw een sector brede audit uitgevoerd worden.

Gemeenten

Implementatie van de BIO is een doorlopend proces van plannen, uitvoeren, controleren en bijstellen. Gemeenten leggen jaarlijks concreet verantwoording af aan hun hoogste politieke orgaan, de eigen gemeenteraad, over de implementatie van de BIO middels ENSIA (de Eenduidige Normatiek Single Information Audit). Daarmee hanteert 100% van de gemeenten de BIO als normenkader. De koepel van gemeenten VNG heeft in de individuele resultaten geen inzicht, want VNG heeft geen toezichthoudende taken.

Overview over bovenstaande vier bestuurslagen

Het geheel van overheidslagen overziend wordt de vraag in welke mate een en ander inmiddels conform BIO is ingericht weinig concreet beantwoord. De passages die betrekking hebben op de verschillende overheidslagen beperken zich voornamelijk tot een procedurele insteek, waaruit blijkt dat men ermee bezig is. Een vergelijking met de stand van zaken vorig jaar is dan ook niet goed te maken.

Relevante ontwikkeling

In navolging van de vernieuwde ISO normering zal de BIO van versie 1.0.4zv naar 2.0 gaan. Er wordt op dit moment gewerkt aan de BIO2.0, deze wordt naar verwachting eind 2024 van kracht. Op 1 juni 2023 is een BIO2.0-opmaat handreiking gepubliceerd, deze is ingedeeld in lijn met ISO/IEC 27002:2022 en bevat actualisaties van een aantal maatregelen.

NL GOV Assurance

Waarom belangrijk?

NL GOV Assurance profile for Auth 2.0 is een open standaard voor de beveiliging van applicaties die gegevens uitwisselen met behulp van REST APIs. Met OAuth 2.0 kunnen gebruikers een website of webapplicatie autoriseren om hun persoonlijke gegevens via een REST 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 OAuth2.0 standaard is een aanscherping van de generieke invulling door het iGov profiel in de eindeloze mogelijkheden die OAuth2.0 biedt. Dit profiel is dan ook van groot belang bij het correct en veilig inrichten en toepassen van Oauth. Maatschappelijk helpt dit de aanbieders en afnemers van APIs om op een eenduidige en veilige manier zich te 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, API DR en het Digikoppeling REST profiel. Exacte gebruikscijfers zijn er 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.

Relevante ontwikkeling

Afgelopen jaar is de standaard 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.

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 dit 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 de Meting Informatieveiligheidstandaarden begin en medio 2023.

	begin 2023 (n = 2.653 resp. 2.710)	medio 2023 (n = 2.593 resp. 2.661)	begin 2024	medio 2024	begin 2025
webverkeer	78 %	86 %			
e-mailverkeer	75 %	87 %			

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

	Centrale overheid (n=1808)	Provincies (n= 24)	Water-schappen (n= 30)	Gemeenten (n= 363)	Gemeen-schappelijke regelingen (n= 368)
webverkeer	90 % (84 %)	67 % (36 %)	93 % (60 %)	79 % (69%)	73 % (65 %)
e-mailverkeer	86 % (81 %)	76 % (33 %)	83 % (53 %)	88 % (71 %)	88 % (72 %)

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.

Aanvullend hierop is voor de beantwoording van de eerste twee vragen gekeken naar routes naar IP adressen welke worden aangekondigd door een reeks overheidsnetwerken. Kanttekening daarbij is wel dat er geen uitputtende lijst is met overheidsnetwerken of IP adressen. Van de onderzochte overheidsnetwerken[8] zijn 236 van de 245 route aankondigingen (96%) ondertekend met een geldige Route Origin Authorization (ROA).

Voor de derde vraag met betrekking tot validatie, de zogenaamde Route Origin Validation (ROV), is gekeken naar beschikbare data uit de APNIC Labs Measurements. Het aantal data hiervoor is beperkt. Ongeldige IPv4 adres aankondigingen worden bij 8 van de 9 netwerken praktisch volledig gefilterd, echter is bij 14 netwerken geen (7) dan wel zeer beperkte (7) data beschikbaar, waardoor hier niets over is de zeggen. Voor ongeldige IPv6 adres aankondigingen

[8] Er is gekeken naar de overheidsnetwerken van SSC-ICT, Ministerie van Economische Zaken / DICTU, Belastingdienst, Defensie, Dienst Uitvoering Onderwijs (DUO), Ministerie van Financiën, Politie Nederland, Ministerie van Justitie, Logius, Dienst Wegverkeer (RDW), Ministerie van IenW / RWS, UWV, Gemeente Den Haag, Gemeente Zaanstad, Gemeente Amsterdam, Gemeente Maastricht, Gemeente Rotterdam, Gemeente Schiedam, Gemeente De Fryske Marren, Gemeente Heerlen (voor regio gemeenten), Gemeente Geldrop-Mierlo, Kadaster, Sociale Verzekeringsbank en VNG.

is op één netwerk met zekerheid te zeggen dat deze wordt gefilterd, voor de overige netwerken zijn geen of te weinig data beschikbaar.

De conclusie is dat de IP-adres aankondigingen veel worden ondertekend (ROA), en dat dit groeiende is. Echter is er te weinig data beschikbaar om de ontwikkeling van validatie (ROV) te kunnen duiden.

Relevante ontwikkeling

In augustus 2022 heeft NCSC-NL in een RPKI-test in Internet.nl ingebouwd. In de websitetest en e-mailtest wordt gekeken of voor alle IPv4 en IPv6 routes een ROA wordt gepubliceerd. Zodoende heeft er in december 2022 een nulmeting kunnen plaatsvinden en heeft Forum Standaardisatie het advies aan het OBDO gedaan om voor RPKI een streefbeeld te formuleren. In mei 2023 is er een streefbeeld voor RPKI vastgesteld dat deze voor het einde van 2024 moet worden geïmplementeerd. In de drie Rijkbrede connectiviteitsaanbestedingen CDR2023 van Rijkswaterstaat is RPKI meegenomen als vereiste.

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’ lijs 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

eHerkenning: SAML	359	439	458	493	onbekend	559
DigiD: SAML	398	429	558	onbekend	onbekend	1.167
eHerkenning + DigiD	757	868	1.016	onbekend	onbekend	1.726

Bron: navraag bij de beheerders van eHerkenning en DigiD bij Logius (peildatum: voorjaar 2023).

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.

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.

Er loopt momenteel een toetsingsprocedure voor NL GOV AP OIDC dat is aangemeld door Logius. Naar verwachting zal OBDO na de zomer besluiten 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 = 2653)	medio 2023 (n = 2593)	begin 2024	medio 2024	begin 2025
webdomeinen	24 %	37 %			

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

	Centrale overheid (n=1808)	Provincies (n= 24)	Water-schappen (n= 30)	Gemeenten (n= 363)	Gemeen-schappelijke regelingen (n= 368)
webdomein	43 % (31 %)	42 % (0 %)	47 % (7 %)	27 % (8%)	13 % (8 %)

Bij de eerste meting begin 2023 laat Rijk een relatief hoge score zien. De verklaring hiervoor is dat zij een aantal platforms hebben met daaronder een flink aantal domeinen waar standaard de doorverwijzing van security.txt naar het centrale bestand van de NCSC is ingeregeld. In de tussenliggende periode tussen beide metingen is sprake van **groei** en wordt het onderlinge verschil tussen de overheidslagen minder groot.

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 1.502 respectievelijk 1.470 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	medio 2024	begin 2025
STARTTLS cf. NCSC	81 %	84 %	89 %			
DANE	46 %	46 %	44 %			

Bij negen op de tien e-mailservers (89%) 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 enige **groei ontbreekt**. Daarmee wijkt de cijfermatige ontwikkeling met betrekking tot DANE 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 (Microsoft Exchange Online heeft nog geen DANE, komt wel in Q2-3 2024).

Een uitsplitsing van deze cijfers naar type overheid levert het volgende beeld op (peildatum: medio 2023, tussen haakjes de cijfers van vorig jaar).

	Centrale overheid (n=710)	Provincies (n=21)	Water-schappen (n=30)	Gemeenten (n=358)	Gemeen-schappelijke regelingen (n=351)
STARTTLS cf. NCSC	90 % (80%)	91 % (81%)	86 % (79%)	89 % (86%)	86 % (80%)
DANE	56 % (55%)	21 % (19%)	21 % (24%)	47 % (53%)	22 % (25%)

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 en de gemeenten met een

percentage rond de 50% relatief goed scoren, blijven de andere drie categorieën duidelijk achter; het beeld van vorig jaar herhaalt zich op dit punt.

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 (157 van de 203) aangesloten bij het NDN waarvan 101 organisaties zijn aangesloten via de sensor van een shared service organisatie. Dat geeft een dekkingsgraad geeft van 77%. In absolute getallen is het aantal aangesloten organisaties bij het NDN in vergelijking met vorig jaar **nauwelijks gewijzigd** en de dekkingsgraad is dan ook hetzelfde als bij de vorige rapportage. 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

De Informatiebeveiligingsdienst (IBD) van VNG Realisatie faciliteert de verspreiding van threat intelligence voor verschillende gemeenten middels het Malware Information Sharing Platform (MISP). De voornaamste bron voor het MISP platform van de IBD is het MISP platform van het NCSC. Het grootste deel van de gemeenten heeft niet de kennis en capaciteit om eigenstandig het proces van threat intelligence uit te voeren. Gemeenten kunnen vrijwillig aansluiten op het MISP platform van de IBD. De IBD stimuleert MSSP's die gemeenten bedienen om ook aan te sluiten op dit MISP platform via een aangesloten gemeente. MISP ondersteunt de open standaarden (STIX/TAXII).

Het Cyber Threat Intelligence platform (CTI platform), een onderdeel van de GGI-Veilig SIEM/SOC-dienst voor gemeenten, is in het derde kwartaal van 2021 in gebruik genomen (zie vorige monitor), maar is inmiddels weer afgebouwd. Dat heeft er helaas voor gezorgd dat de **verwachte groei** in het gebruik van de standaard is **uitgebleven**. Het is wel de verwachting dat de inzet van de standaard komend jaar weer gaat toenemen in verband met de huidige

collectieve ontwikkelingen en initiatieven voor gemeenten (zie hieronder bij 'relevante ontwikkeling)'.

Relevante ontwikkeling

In opdracht van Forum Standaardisatie zijn de open standaarden STIX en TAXII geëvalueerd (Evaluatierapport Veilig Internet, 2022). Het ontbreken van de regierol was de hoofduitkomst van het rapport. In een daarop volgende Gespreksnotitie regierol standaarden STIX TAXII in Nederland (23 december 2022) wordt het ontbreken van de sturende rol (regierol) in Nederland op de open standaarden STIX en TAXII (standaarden voor cyberdreigingsinformatie) geadresseerd. Er wordt voorgesteld het gesprek te starten met het NCSC over het nemen van de regierol door NCSC voor het stimuleren van adoptie van STIX en TAXII en voor het zijn van aanspreekpunt voor Nederlandse overheden voor deze standaarden.

Langs die weg staat er voor de ontwikkeling van het cybersecurity stelsel de komende tijd veel te gebeuren. Dat biedt voor het NCSC wellicht ook mogelijkheden om meer invulling te geven aan de coördinerende rol waar het Forum Standaardisatie om vraagt ten aanzien van de het gebruik van STIX en andere standaarden.

Ook vanuit een andere invalshoek worden de taken en de doelgroepen van het NCSC de komende tijd uitgebreid. Dat is het gevolg van de nieuwe *Network and Information Security directive* van de Europese Unie. Deze NIS-2 richtlijn wordt momenteel in Nederlandse wetgeving doorgevoerd en gaat gelden voor een veel grotere groep aan bedrijven en organisaties. Deze partijen worden verplicht om maatregelen te nemen tegen cyberdreigingen en om incidenten te melden. De richtlijn schrijft voor dat essentiële en belangrijke entiteiten met advies en bijstand worden ondersteund door een CSIRT. De ondersteuning vanuit de overheid kan verder bestaan uit informatie-uitwisseling, richtlijnen en weerbaarheid verhogende instrumenten, bijvoorbeeld voor het uitvoeren van een risicobeoordeling. Daarbij hoort ook het stimuleren van informatie-uitwisseling door het gebruik van standaarden.

Vanuit NCSC wordt aangegeven dat in de achterliggende periode nieuwe versies van beide standaarden beschikbaar zijn gekomen, het meest recent al weer even geleden een nieuwe (2.1) versie van de standaarden. Men geeft aan dat het tijd is om de pas-toe-of-leg-uit lijst aan te passen met de nieuwe versie. Een soortgelijke opmerking is ook al in de vorige monitor-rapportage gemaakt.

Vanuit de hoek van VNG Realisatie wordt hier nog aan toegevoegd dat er op het peilmoment een nieuwe aanbesteding voor Monitoring en Response is gepubliceerd. Dit is de opvolger van de GGI-Veilig SIEM/SOC dienst, welke afgelopen jaar is afgebouwd. In het programma van eisen in deze nieuwe aanbesteding is ook het gebruik van de STIX en TAXII standaarden uitgevraagd. Het is de verwachting dat dit een boost gaat geven aan het gebruik van de standaard binnen de Nederlandse gemeenten.

WPA2 Enterprise

Waarom belangrijk ?

WPA2 Enterprise maakt het mogelijk dat gebruikers automatisch en veilig toegang krijgen tot aangesloten WiFi-netwerken. Ook als deze WiFi-netwerken zich buiten de eigen organisatie bevinden. De authenticatie kan plaatsvinden op basis van bestaande identiteitsgegevens van de gebruiker. Hierdoor hoeven gebruikers niet opnieuw in te loggen. Met het gebruik van WPA2 Enterprise is ook de integriteit van de netwerkverbinding geborgd. Bij WPA2 Enterprise spelen drie partijen een rol: de 'gebruiker', de 'Identity Provider (IdP)' en de 'Service Provider (SP)'. Zodra een gebruiker contact maakt met het betreffende WiFi-punt toetst de SP (beheerder van het WiFi-punt) op basis van de inloggegevens bij de IdP (de thuisorganisatie van de gebruiker) de identiteit van de gebruiker. Na positieve verificatie van de identiteit van de gebruiker, wordt toegang verleend tot het WiFi-netwerk zonder dat aanvullende inlog noodzakelijk is. Diensten zoals govroam (een overheidsbreed wifi-netwerk), Rijk2Air (specifiek ingericht voor Rijksambtenaren) en eduroam (doelgroep: onderwijs- en onderzoek-instellingen) maken gebruik van WPA2 Enterprise. De standaard staat op de 'pas toe of leg uit' lijst sinds 2 februari 2016.

Feitelijk gebruik

Als indicator voor het feitelijk gebruik van deze open standaard wordt sinds 2016 het aantal deelnemende organisaties (peildatum begin september) geteld van govroam en eduroam. (Bron: navraag bij govroam en https://eduroam.nl/instellingen). Eduroam is er al sinds 2003 en govroam is in 2013 gelanceerd.

	2016 (sept.)	**2017** (sept.)	**2018** (sept.)	**2019** (sept.)	**2020** (juni)	**2021** (aug/sept)	**2022** (juni)	**2023** (okt)
govroam	49	132	244	307	332	337	351	366
eduroam	157 (mei)	199	215	222	231	250	254	264
samen	206	331	459	529	563	587	605	630

Uit bovenstaand overzicht blijkt dat het gebruik van WPA2 Enterprise vergeleken met vorig jaar **licht toegenomen** is (+4%).

Het aantal gekoppelde instellingen aan eduroam is hoog en zit tegen het maximum aan; de groeipotentie voor de komende periode is daarmee beperkt geworden. Het aantal gekoppelde organisaties aan govroam stijgt gestaag. Hier ligt ook nog voldoende potentie om het aantal deelnemers te laten stijgen. Bij de huidige (366) deelnemende organisaties zijn ruim 1.200 locaties aangesloten waar per werkdag in totaal gemiddeld circa 232.000 authenticaties plaatsvinden (een **toename** van +16% ten opzichte van vorig jaar).

Er was eerder een dip in het aantal authenticaties als gevolg van corona en thuiswerken. Uit de cijfers is te zien dat er minder wordt thuisgewerkt, de laatste drie maanden lag het werkdag gemiddelde op 350.000. Het aantal inlogpogingen heeft echter een grote variatie, zo lag de hoogste piek op 775.000. Enkele grote organisaties die technisch reeds aangesloten waren, zijn

pas later tot interne uitrol gekomen in termen van locaties en bereikte eindgebruikers, waardoor het aantal daadwerkelijke eindgebruikers ook is toegenomen en daarmee het aantal authenticaties. Een andere factor die meespeelt is dat steeds meer Rijksambtenaren hun dagelijks werk op locaties verrichten waar ze feitelijk de hele dag te gast zijn en er zodoende dus veel wordt geroamd.

Relevante ontwikkeling

Vanuit de stichting govroam zijn de volgende ontwikkelingen gemeld (deels een continuering van ontwikkelingen die vorig jaar al werden gesignaleerd):

- getgovroam is succesvol gelanceerd met meer dan 80 aangesloten organisaties die er gebruik van maken, en werken enkele zeer grote overheidspartijen aan de uitrol ervan. Getgovroam maakt het eenvoudig om via een app een govroam-profiel te genereren op basis van EAP-TLS, na inlog via SAML met de credentials van de thuisorganisatie, en is gebaseerd op geteduroam; Met Rijkspartijen wordt gewerkt om de authenticaties lokaal mogelijk te maken.
- op verzoek beperkt govguest (dienst voor tijdelijke veilige wifi-toegang voor bezoekers zonder govroam-account) sinds half 2022 de toegang voor gasten tot uitsluitend de wifi-netwerken van de organisatie waar zij te gast zijn, om zo het bezwaar weg te nemen dat gasten bij andere organisaties online kunnen komen;
- govVPN is gelanceerd met bijbehorende apps die ook op niet-veilige wifi-hotspots het dataverkeer van de eindgebruiker beschermt en aflevert zeer dichtbij de AMS-IX.
- stichting govroam ontsluit alle aanvullende diensten met Single Sign On door centrale koppelingen via govConext, op basis van wederom een Open Source bouwsteen van SURF, namelijk OpenConext;
- een opvallende ontwikkeling zet door waarbij stichting govroam geregeld het belang van veilige doch transparante internettoegang tracht te benadrukken, nu die geregeld door organisaties zover beperkt wordt dat roamende ambtenaren aldaar hun werk niet meer kunnen doen (omdat bijvoorbeeld VPN naar de thuisorganisatie niet meer werkt, of door 'conflicterende' videoconferencingapplicaties).
- Cloudadaptatie heeft duidelijk een grote vlucht genomen in de doelgroep: steeds vaker worden de RADIUS server(s) van de Deelnemers in de cloud geplaatst en wordt Single Sign On gekoppeld vanuit een cloud-IdP. Daarmee gepaard gaat de snelle adaptatie van mobile device management (MDM, met name vanuit de cloud) met de wens om govroam bij voorbaat te configureren via MDM.

B4.2. 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 vorig jaar is voor zicht op het feitelijk gebruik van de standaard gemaakt van metingen door de Stichting Accessibility (inmiddels onderdeel van Bartiméus): een nulmeting uit 2019 en een tweede meting in 2021[9].

Inmiddels is een Dashboard DigiToegankelijk ontwikkeld en operationeel en in beheer bij Logius. Dit dashboard geeft een totaalbeeld van de toegankelijkheidsstatus van alle websites en apps van overheidsorganisaties. Het Dashboard is gebaseerd op informatie uit het register van toegankelijkheidsverklaringen. Informatie uit dit Dashboard komt in de plaats van de uitkomst van eerdergenoemde onderzoeken.

De Nederlandse overheid is momenteel (peildatum 8 september 2023) verantwoordelijk voor (minimaal) 7.639 websites en apps. Een volledig zicht ontbreekt nog en dit aantal zal de komende periode dan ook naar verwachting flink oplopen. Men schat in dat met dit aantal van 7.639 websites en apps niet meer dan een derde van alle overheidswebsites en -apps in beeld is. De status van de toegankelijkheid van deze 7.639 websites en apps is als volgt:

- A: voldoet volledig 382
- B: voldoet gedeeltelijk 1.745
- C: eerste maatregelen zijn genomen 1.108
- D: voldoet niet 1.833
- E: geen toegankelijkheidsverklaring (eigenaar wel bekend) 2.571

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

Een vergelijking met eerdere metingen is dit jaar nog niet te maken; dat gebeurt bij een volgende monitor.

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

Het Dashboard geeft vooralsnog alleen algemene statistieken en biedt ook de mogelijkheid om digitale toegankelijkheid van individuele organisaties te bekijken. Volgens Logius wordt het Dashboard nog uitgebreid met functies om gerichtere statistieken op te vragen. Bijvoorbeeld: 'Hoe toegankelijk zijn de 10 grootste gemeenten van Nederland'? Of 'Hoe doet ministerie X het ten opzichte van het gemiddelde voor het Rijk?'.

In oktober 2022 is een motie aangenomen (Strolenberg en de Kort) waarin aan de de regering wordt gevraagd zo spoedig mogelijk in haar aanbestedingen voor nieuwe websites en apps van de overheid de toegankelijkheidseisen, genoemd in het Tijdelijk besluit digitale toegankelijkheid, op te nemen. Tevens wordt gevraagd aan de regering om zich in te spannen dat zo spoedig mogelijk alle huidige, ontoegankelijke websites en apps van de overheid voldoen aan de gestelde toegankelijkheidseisen. Staatsecretaris van Huffelen heeft deze motie overgenomen.

ODF en PDF

Waarom belangrijk ?

PDF is een format voor de uitwisseling van documenten die bedoeld zijn om op te slaan of af te drukken, en waarvan de pagina opmaak vastligt. Het uitgangspunt van PDF is dat gebruikers documenten kunnen uitwisselen, opslaan en afdrukken, onafhankelijk van de omgeving waarin ze zijn aangemaakt. Een PDF-document ziet er op alle apparaten en in alle omgevingen hetzelfde uit. PDF is minder geschikt voor het publiceren van online informatie die veel op mobiele apparaten wordt bekeken. De door ISO gestandaardiseerde PDF/A en PDF 1.7 varianten staan op de 'pas toe of leg uit' lijst sinds 18 november 2009. Het verplichtende karakter van een plaats op de 'pas toe of leg uit' lijst draagt eraan bij dat het aandeel bestanden op overheidswebsites dat voldoet aan de PDF-standaarden langzaam maar zeker toeneemt.

ODF is een applicatie- en leveranciers-onafhankelijke open standaard voor de uitwisseling van bewerkbare documenten. ODF is duurzaam toegankelijk: in de toekomst blijven ODF-bestanden leesbaar en bewerkbaar, ongeacht de kantoor-applicaties die op dat moment al dan niet

worden ondersteund. Dankzij deze structuur kunnen zoekmachines ODF-bestanden goed indexeren en vinden. Alle gangbare kantoorapplicaties kunnen ODF-bestanden lezen en schrijven. Het gebruik van het standaardformaat ODF staat los van het al dan niet gebruiken van open source kantoorapplicaties. ODF staat op de 'pas toe of leg uit' lijst sinds 15 juni 2012. Het blijft zinvol om ODF op de 'pas toe of leg uit' lijst te handhaven. Als ODF van de 'pas toe of leg uit' lijst zou verdwijnen, dan hebben organisaties geen dwingende reden meer om ODF uit te vragen in hun aanbestedingen. Daarmee kan de leveranciersafhankelijkheid toenemen, ook voor burgers en bedrijven die met de overheid willen communiceren.

Feitelijk gebruik

De resultaten van de meting laten zien dat de trends te opzichte van voorgaande jaren onveranderd blijven. Nog steeds zijn veruit de meeste documenten op overheidswebsites van het type PDF, voldoet ongeveer de helft van deze PDF bestanden aan open ISO standaarden, en is slechts een klein percentage ervan digitaal toegankelijk. Voor de publicatie van bewerkbare documenten wordt nog altijd overweldigend veel vaker een Microsoft Office format gebruikt dan het open format ODF. In deze paragraaf worden deze trends onderbouwd met de resultaten van de meting die in mei 2023 werd uitgevoerd.

De meting is gedaan op basis van een steekproef bij overheidsorganisaties die vallen binnen het organisatorisch werkingsgebied van de pas-toe-of-leg-uit lijst. De steekproef bestaat uit een totaal van 97 organisaties uit verschillende delen van de overheid:

- 30 veel bezochte websites van de Rijksoverheid (volgens Communicatie Rijk).
- De 30 grootste gemeenten plus VNG.
- De 12 provincies plus IPO.
- De 21 waterschappen plus UVW en waterschappen.nl.

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

De meting is dit jaar door dezelfde organisatie en op dezelfde manier uitgevoerd als in 2021 en 2022. Voor het tellen van documenten op websites gebruiken wij net als in de twee voorgaande jaren Google search (https://www.google.com). Door de aard van commerciële zoekmachines moet rekening worden gehouden met een zekere meetfout. Zoekmachines vinden niet noodzakelijk alle documenten op een website. Anderzijds kunnen de zoekresultaten door *caching* (lokale kopieën) op de zoekmachine referenties bevatten naar documenten die al niet

meer geldig zijn. Dit is een nadeel van de huidige meetmethode maar vooralsnog is er nog geen werkbaar alternatief voor[10].

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

	Top 30 overheid	**G30 gemeenten**	**Provincies**	**Water-schappen**
Aantal gevonden PDF	299.141 (396.552, 312.540)	184.663 (220.320, 183370)	143.945 (135.457, 150451)	15.885 (19.126, 19.711)
Aantal gevonden ODF	839 (876, 952)	54 (5, 15)	164 (127, 181)	1 (0, 3)
Aantal gevonden MS Office	14.649 (16.060, 14.523)	9.324 (10.241, 17928)	13.155 (9.150, 10886)	165 (278, 348)
Percentage PDF van alle gevonden documenten	95,08% (95,90%, 95.28%)	95,17% (95,56%, 91.09%)	91,53% (93,59%, 93,15%)	98,97% (98,57%, 98.25%)
Percentage ODF van de gevonden bewerkbare documenten	5% (5%, 6%)	<1% (<1%, <1%)	1% (1%, 2%)	1% (0%, 1%)
Percentage ISO PDF	54% (33%, 35%)	55% (55%, 45%)	31% (31%, 33%)	61% (52%, 67%)
Percentage digitaal toegankelijke PDF	8% (0%, 23%)	4% (7%, 7%)	8% (0%, 17%)	0% (0%, 0%)

De belangrijkste observaties naar aanleiding van dit overzicht:

- In 2023 vonden wij over het geheel genomen 18% minder documenten op websites van overheden dan in 2022. Bij het Rijk nam het aantal PDF bestanden relatief het meeste af. Alleen bij de provincies nam het aantal documenten juist licht toe.
- PDF blijft veruit het meest gebruikte format voor de publicatie van documenten. Over alle gemeten websites heeft 94% van de documenten een PDF format. Dat is vergelijkbaar met de percentages die wij in voorgaande jaren vonden.
- De aantallen PDF bestanden die wij op overheidswebsites vinden, verschillen enorm. Op overheid.nl staan veruit de meeste PDF bestanden in vergelijking met de andere onderzochte overheidswebsites. Dit is geen verrassing omdat overheid.nl alle wetten en veel openbare overheidsinformatie publiceert. Overheid.nl biedt dezelfde wetteksten overigens ook in andere formats aan, waaronder HTM, zodat de gebruiker het meest geschikte format kan kiezen. Aan de andere kan van de schaal zijn er ook overheidswebsites waar nauwelijks PDF bestanden op te vinden zijn, zoals kadaster.nl, werkenbijdefensie.nl en rijkshuisstijl.nl
- Van de steekproef van 97 PDF bestanden (1 per onderzochte organisatie) voldeed 54% aan de ISO standaard PDF 1.7 of PDF/A op de 'pas toe of leg uit'-lijst. Dat is meer dan in 2022 (toen 46%). Van alle overheden doen de waterschappen het relatief het beste.

[10] De inzet van een eigen '*crawler*' bleek in voorgaande jaren nog grotere problemen met zich mee te brengen. Een *crawler* moet zorgvuldig afgesteld worden, kost veel rekentijd en kan een website zwaar belasten. Afhankelijk van de afstelling ziet een *crawler* vaak belangrijke aantallen documenten op een website over het hoofd. Dit bleek geen passende oplossing in voorgaande jaren.

- Van de steekproef van 97 PDF bestanden van na 2018 is slechts 5% digitaal toegankelijk. Dit is wel meer dan de 2% in 2022. Wel moeten wij hierbij aantekenen dat de steekproef de uitkomst bepaalt. De steekproef heeft ieder jaar dezelfde omvang van 97 bestanden maar bestaat ieder jaar uit een verschillende verzameling willekeurig gekozen documenten. Het kan dus zijn dat we per toeval meer, dan wel minder digitaal toegankelijke documenten treffen. Desondanks laat het resultaat duidelijk zien dat het aantal digitaal toegankelijke PDF bestanden op overheidswebsites erg laag is.
- Ongeveer 12% van de onderzochte overheidswebsites publiceert geen of vrijwel geen informatie meer in PDF. Dit aantal is iets meer dan in 2022 en 2021. Het vermijden van PDF bestanden heeft vaak een positief effect voor de digitale toegankelijkheid van de website. De Rijksoverheid blijft hierin een voorloper: 27% van de 30 grootste websites van de Rijksoverheid hebben (vrijwel) geen PDF's meer. Een aantal organisaties hanteert een HTML-first beleid, wat de digitale toegankelijkheid ten goede komt. Voorbeelden hiervan zijn de SVB, het Kadaster, Geonovum, de gemeenten Eindhoven en Tilburg, de provincie Fryslân en de websites werkenbijdefensie.nl, crisis.nl (NCTV) en consuwijzer.nl (ACM).
- ODF vormt slechts 3% van de bewerkbare documenten op alle onderzochte websites. Dat is gelijk aan vorig jaar.

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

- Het **aantal documenten** op websites van de overheid lijkt **afgenomen** ten opzichte van vorig jaar, zelfs als we de (aanzienlijke) meetfout in aanmerking nemen die zoekmachines veroorzaken. Een verklaring hiervoor kan zijn, dat steeds meer overheden besluiten om informatie niet meer in PDF bestanden aan te bieden in verband met digitale toegankelijkheid en de toenemende mobiele toegang tot websites (basis: Wet Digitale Overheid). Wel is de vraag hoe de Wet open overheid deze trend gaat beïnvloeden, omdat deze wet overheden juist aanzet tot proactief publiceren van documenten[11].
- Ongeveer de helft (46%) van de PDF bestanden uit de steekproef op overheidswebsites voldoet aan de **open standaarden PDF 1.7 en PDF/A** op de 'pas toe of leg uit' lijst. Dat is gelijk aan het percentage van vorige jaren. Er blijft dus **geen stijgende of dalende trend** waarneembaar.
- **Digitale toegankelijkheid** van PDF bestanden op overheidswebsites blijft een knelpunt. Slechts 5% van de recente (van 2019 of jonger) PDF bestanden uit de steekproef bleek digitaal toegankelijk. Onlangs een lichte stijging van het aantal digitaal toegankelijke bestanden in de steekproef blijft de **trend hetzelfde als voorgaande jaren**. Wel zien wij dat steeds meer organisaties kiezen voor HTML-first publicatiebeleid, waarbij er geen nieuwe PDF bestanden meer op de website komen. Dit komt de digitale toegankelijkheid van de websites meestal ten goede.

[11] Hier is derhalve sprake van een krachtenspel van twee wetten die op dit aspect tegen elkaar in werken.

- Ook dit jaar moeten we concluderen dat **ODF** veel te weinig wordt toegepast waar dat verplicht is. Dit is een **voortzetting van de trend van eerdere jaren**.

Relevante ontwikkeling

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

PDF/A en PDF 1.7 worden beheerd door ISO. Deze internationale organisatie heeft geen specifieke ambities om het gebruik van PDF bij de Nederlandse overheid te stimuleren. Dit geldt ook voor de NEN die de ISO specificaties beschikbaar stelt. De PDF Association stimuleert het gebruik van PDF/A en PDF 1.7 en heeft een Benelux Chapter met een contact in Nederland (https://www.pdfa.org/local-contacts/?highlight=benelux%20chapter). De PDF Association en in het bijzonder de Benelux Chapter worden gedragen door leveranciers van producten gerelateerd aan PDF. De stimulering en ondersteuning van PDF/A en PDF 1.7 vanuit de PDF Association is daarom nauw verweven met het commerciële aanbod.

Het Nationaal Archief stimuleert het gebruik van PDF/A voor duurzame toegankelijke toepassingen. Bij het Nationaal Archief kunnen overheidsorganisaties terecht voor advies en ondersteuning bij het gebruik van PDF/A.

Er bestaat inmiddels een nieuwe standaard PDF 2.0 bestaat, die gratis beschikbaar is via de PDF Association. Hiermee onderscheidt PDF 2.0 zich van PDF 1.7 en PDF/A, waarvoor nog betaald moet worden bij NEN-ISO. Geen enkele organisatie heeft PDF 2.0 echter nog aangemeld voor de 'pas toe of leg uit' lijst. Dit kan komen omdat er nog relatief weinig software ondersteuning bestaat voor PDF 2.0 bestanden.

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 voor het vergelijken en interpreteren van data uit verschillende systemen. 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. De standaard 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 52 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 vrijwel gelijk aan de steekproef bij de metingen van 2019 - 2022. De inhoud en opzet van de enquête in 2023 is nagenoeg onveranderd. Daarmee zijn de antwoorden te vergelijken met de uitkomsten van de enquêtes van voorgaande jaren.

In totaal is de enquête 38 keer ingevuld waaruit 31 unieke organisaties zijn af te leiden. In vergelijking met vorig jaar is sprake van een lagere respons. Van de 31 unieke organisaties geeft 61% (19 organisaties) aan een begrippenlijst, woordenboek of taxonomie op het internet te publiceren. Dit is een lichte stijging ten opzichte van 2022 (toen 57%). Dit zijn in principe organisaties die in aanmerking komen voor de verplichting van SKOS. Als wordt ingezoomd op deze 19 organisaties die kwalificeren voor een verplichting van SKOS, dan zien we het volgende:

- 16 daarvan gebruiken SKOS (84%). Dat is een lichte stijging in vergelijking tot het gebruik van vorig jaar (toen 72%).
- Over deze 16 gebruikers van SKOS nog het volgende:
  - 2 organisaties maken alleen gebruik van SKOS
  - 7 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. SKOS en OWL zijn ook goed in combinatie te gebruiken.
- 2 van de 16 organisaties gebruiken SKOS niet maar deze organisaties gebruiken wel OWL.

- 8 van de 16 organisaties (50%) 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 stijging in het gebruik** van SKOS t.o.v. vorig jaar. Een belangrijke bijbehorende conclusie is ook: daar waar deze open standaarden (SKOS maar als alternatief ook OWL) 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 bij het uitwisselen van gegevens over grenzen van organisatie en/ of domein heen toenemende aandacht hebben voor het vastleggen en het harmoniseren van begrippen.

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 SKOS en linked data toepassen. Uit de respons van decentrale overheden komt een beeld naar voren dat zij geen begrippenlijst, woordenboek of taxonomie op internet publiceren, met de waterschappen als positieve uitzondering.
- 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.
- Bijna de helft van organisaties die SKOS gebruiken, gebruikt ook de OWL-standaard. De toepassingsgebieden van SKOS en OWL overlappen deels, waarbij OWL de 'zwaardere' standaard is die bij formelere kennissystemen wordt ingezet. Dit suggereert dat ook SKOS wordt toegepast in grotere, serieuze linked data projecten. De deze keer uitgezette 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.

SKOS heeft een 'pas toe of leg uit'-verplichting voor publiceren van begrippenlijst **op internet**. De enquête van 2023 heeft voor het eerst 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 31 unieke organisaties geeft 58% (18 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. 9 organisaties gebruiken hierbij linked data standaarden,

waarvan 7 organisaties ook SKOS (39%). Organisaties die linked data standaarden gebruiken voor interne bedrijfsprocessen, gebruiken 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 en hulp. Onder auspiciën van PLDN is een werkgroep actief voor het opstellen van een Nederlandse 'Standaard voor Beschrijven van Begrippen' (werknaam: SBB). SBB is in zekere zin te zien als een Nederlands profiel op SKOS, hoewel SBB ook zonder SKOS is toe te passen. De werkgroep heeft de intentie SBB aan te melden voor de lijst open standaarden 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. Kadaster, de erfgoedsector en de onderwijssector zetten al een aantal jaar achtereen grote stappen. In 2022 heeft Ministerie van Financiën de miljoenennota en de achterliggende processen via linked data ontsloten. Deze inzet van Ministerie van Financiën is een stap voorwaarts in adoptie van linked data; de stap wordt gezien als een voorbeeldfunctie, en kan op navolging rekenen.

Forum Standaardisatie en PLDN overleggen over de meerwaarde om linked data standaarden te combineren in één cluster op de lijst open standaarden. Dit naar analogie van de Geo-standaarden of Digikoppeling op de 'pas toe of leg uit'-lijst en die ook uit afzonderlijke, autonome standaarden bestaan. De linked data community geeft het signaal af dat 'pas toe of leg uit'-verplichting van SKOS bijdraagt aan de adoptie van SKOS (en van aanpalende linked data standaarden). In 2023 worden SKOS en aanpalende linked data standaarden geëvalueerd. Een van de aandachtspunten in de evaluatie is de vraag naar de meerwaarde van linked data standaarden als cluster op de lijst open standaarden. De evaluatie wordt eind 2023 opgeleverd.

B4.3. 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.

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. Een vergelijking met de score van 3 jaar terug is echter niet mogelijk. De opgave van dit jaar beschouwen we om die reden als een (hernieuwde) nul-meting. Onderstaande gegevens dienen als referentiekader voor eventuele vervolgmetingen. Gegeven het feit dat sprake is van een nulmeting is over een ontwikkeling van het gebruik van OAS 3.0 in dit stadium nog niets te zeggen.

Inmiddels zijn meer dan 100 REST API's geregistreerd (103, peildatum september 2023). Deze komen vanuit alle lagen van de overheid: gemeenten, provincies, ministeries, uitvoeringsorganisaties, Zbo's en en stichtingen.

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 tool 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:

- 13 API's voldoen aan geen van de API Design Rules
- 37 API's voldoen aan 1 API Design Rule
- 12 API's voldoen aan 2 API Design Rules
- 10 API's voldoen aan 3 API Design Rules
- 8 API's voldoen aan 4 API Design Rules
- 9 API's voldoen aan 5 API Design Rules
- 2 API's voldoen aan 6 API Design Rules
- 5 API's voldoen aan alle 7 API Design Rules

Het team van developer.overheid.nl zoekt actief contact met de API leveranciers om de API regels uit te leggen en te helpen om de score beter te maken.

Relevante ontwikkeling

Afgelopen jaar zijn er vele API's ontwikkeld die gebruik maken van deze standaard. Denk hierbij aan de API's van HaalCentraal, de SDG, CBS, Kadaster, KNMI en vele andere.

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 de 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.

Feitelijk gebruik

Het aantal API's is gelijk gebleven ten opzichte van vorig jaar (circa 100). Hiervan betreft 75% REST API's. Het aantal organisaties dat API's aanbiedt is met 5 gegroeid met naar in totaal 24 (bron: developer.overheid.nl.).

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

Relevante ontwikkelingen

Afgelopen jaar is de REST-API-DR 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 conceptversie 2.0 van de standaard is in een laatste afstemmingsfase en 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. Ook is aandacht besteed aan de aansluiting van de standaard bij de eDelivery ontwikkelingen en de ontwikkelingen bij VNG inzake de opzet van de FSC standaard.

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

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 %[12]		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[13]		98%	75%	59%	95%[14]
Zomer 2019 Najaar 2020		60%	100%	100%	100%	90%[2]
Najaar 2020		65%	100%	100%	100%	91%

[12] 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.

[13] 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%

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

Zomer 2021		65%[15]	100%	100%	100%	91%
Zomer 2022		65%	100%	100%	100%	91%
Zomer 2023		69%[16]	100%	100%	100%	92%

Bron: opgave beheerorganisatie Logius

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

Dit is niet per definitie slecht nieuws. In de categorieën gemeenten, provincies en waterschappen is de dekking sinds 2019 volledig te noemen. Voor de categorie Rijk en uitvoeringsorganisaties geldt dat niet voor alle onderdelen Digikoppeling relevant is zoals bv voor Gemeenschappelijke regelingen en 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. In April 2022 heeft het OBDO de toevoeging van een RESTful API-profiel aan Digikoppeling goedgekeurd en naar aanleiding hiervan is een nieuwe versie van de Digikoppeling standaard uitgebracht. Dankzij dit nieuwe profiel is het nu ook mogelijk om binnen het toepassingsgebied van Digikoppeling API's toe te passen conform de Restful API Design Rules (eveneens een 'pas toe of leg uit' -standaard). Het RESTful API-profiel is doorontwikkeld en wordt bijvoorbeeld uitgebreid met afspraken met betrekking tot signing en encryptie.

[15] 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.

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

2. De Digikoppeling architectuur is hierbij ook aangepast. Enerzijds om het nieuwe RESTful API-profiel op te kunnen nemen in de Digikoppeling standaard. Anderzijds om de harde koppeling tussen het type bevraging en de specifieke Digikoppeling koppelvlakken los te laten. In de nieuwe architectuur worden verschillende transactiepatronen beschreven en wordt weergegeven hoe dit met de verschillende koppelvlakken kan worden ingevuld.

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 laatste drie monitors is aangegeven dat PDOK elk jaar aanzienlijke groeicijfers laat zien. De meest actuele beschikbare gegevens laten een wat ander beeld zien (bron: PDOK factsheet 2022). Voor verschillende variabelen ziet de ontwikkeling er als volgt uit:

- aan de afnamekant is er een daling van 36,4 miljard hits op PDOK over 2021 naar 29,1 miljard hits over 2022, een daling van 20%;
- aan de aanbodzijde is het aantal datasets licht gedaald van 239 (2021) naar 235, een daling van 1,7%;
- het aantal services is gedaald van 747 in 2021 naar 605 in 2022, ook een afname (-19%);
- het aantal hits op het Nationaal Georegister (NGR) is daarentegen wel gestegen: 21,2 miljoen in 2021 tegen 23,2 in 2022 (+9,4%).

Het geheel overziend is sprake van een opvallende **afname van het gebruik, behalve in het aantal raadplegingen van het NGR.** De afname van het aantal hits is te verklaren uit de overgang van PDOK naar de cloud, waardoor de cijfers ontdubbeld zijn; tevens wordt een nieuwe rekenmethode gehanteerd. Het aantal datasets is gedaald doordat data-aanbieders simpelweg iets minder datasets via PDOK verkiezen aan te bieden, bijvoorbeeld om kosten te reduceren. De daling van het aantal services volgt uit de overgang naar de cloud en de vermindering van het aantal datasets. Aan het stijgende aantal raadplegingen van NGR kunnen we zien dat de vraag naar geo-data nog onverminderd aanwezig is.

Relevante ontwikkeling

In 2023 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, model gedreven ontwikkeling;
- 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 10 miljoen 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.

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	299	(276)	72	(67)	58	(55)
Aantal softwareproducten (incl. versies)	2961	(3632)	1201	(1420)	738	(501)
wv. beschikbaar/in gebruik	1447	(1590)	368	(460)	226	(187)
wv. gepland/in ontwikkeling	91	(109)	50	(60)	26	(16)

Peildatum april 2023 (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 8%). Dit komt onder andere doordat het gebruik van de softwarecatalogus niet meer van een convenant afhankelijk is. Ondanks meer leveranciers is het aantal softwarepakketten gedaald met 18%.

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

neemt weer toe, uitgedrukt in oplossingen in de zin van: softwareproducten. Vorig jaar was op dit punt nog sprake van een flinke daling, deze is met de stijging van nu weer (meer dan) volledig teruggedraaid. Voor StUF BG neemt de adoptie in tegenstelling tot vorig jaar af. De bewegingen bij StUF BG en StUF ZKN zijn zodoende elkaars spiegelbeeld. Voor beide geldt wel een toename van aantal leveranciers dat deze StUF standaarden meeneemt in haar software producten. Vorig jaar was op dit punt voor beide nog sprake van een daling, deze is met de stijging dit jaar gedeeltelijk gecorrigeerd. 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.

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 2022.

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. Dat geldt ook voor de in de tabel genoemde twee specifieke StUF standaarden.

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[17]. In verband daarmee worden er API standaarden ontwikkeld als alternatief voor de StUF standaarden. Ook wordt gestuurd op het vervangen van de StUF standaarden in het gemeentelijke IT landschap. 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.

B4.4. Domein economie en werk

[17] *Bron: https://www.gemmaonline.nl/index.php/Ontwikkelagenda_API-standaarden*

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 en bevordering van het gebruik van NLCIUS is belegd bij het Standaardisatieplatform e-factureren (STPE) waarin twee partijen samenwerken: NEN en TNO. Het initiatief wordt ondersteund door het Ministerie van Economische Zaken en Klimaat vanwege het maatschappelijke belang. De belangrijkste gebruikersgroepen zijn aangesloten bij het STPE: softwareleveranciers van financiële pakketten, PEPPOL-service providers, leveranciers van telecommunicatie en IT, en overheden: het Rijk, provincies en gemeenten. Deze gebruikersgroepen leveren ook hun bijdrage aan het Nationaal Multi-belanghebbenden Forum e_Procurement (NMBF).

Het STPE 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. Dat 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 met 40% gestegen t.o.v. 2021 (ter vergelijking: vorig jaar een stijging van 38%);
- het aantal ontvangen e-facturen in het NLCIUS-formaat (2.582.600) via het Peppol-netwerk is met 109% gestegen t.o.v. 2021 (ter vergelijking: vorig jaar een stijging met 6%).

Het aantal ontvangen e-facturen in het NLCIUS-formaat heeft derhalve een enorme groei doorgemaakt in 2022. 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 de gegevens van Ionite blijkt het volgende:
- het aantal endpoints in Nederland is naar 32.904 in de Peppol Directory gestegen. Dit is een stijging van 83% t.o.v. 2021 (vorig jaar: 34% stjjging);
- het aantal endpoints dat documenttype SI-UBL 2.0 invoice ondersteunt, groeide naar 32.135. Een stijging van 87% t.o.v. 2021 (vorig jaar een stijging van 37%);
- het aantal endpoints dat documenttype SI-UBL 2.0 creditnote ondersteunt, groeide naar 31.488. Een stijging van 135% t.o.v. 2021 (vorig jaar een stijging van 118%).

Ook de gegevens van Ionite bevestigen de eerdergenoemde verdere stijging van de adoptie van de NLCIUS.

Tot slot blijkt uit gegevens van Logius het volgende:
- In 2022 is wederom een stijging te zien in het aantal ontvangen e-facturen. Het totaal aantal e-facturen bedroeg 1.721.693, dat is 80% van de totale facturenstroom. Het percentage e-facturen steeg met 4,4% t.o.v. 2021. (bron: Jaarrapportage bedrijfsvoering Rijk 2022).
- Ten opzichte van 2021 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 2022 (681.467) is gestegen met 55% ten opzichte van het jaar daarvoor.
- Ten opzichte van 2021 is een enorme stijging van 134% in het aantal ontvangen facturen te zien via het Rijksoverheid Peppol Accesspoint (vorig jaar een relatief lichte stijging van 14%).

Mede op basis van bovenstaande gegevens is de mening van het STPE 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 2021 zijn het STPE en NPa gestart om de samenwerking te intensiveren. Het vormen van een gezamenlijk toekomstbeeld is gestrand, maar heeft wel vorm gekregen voor de werkgroepen waar inhoudelijke kwesties inmiddels goed met elkaar worden afgestemd. Zo is de NLCIUS en Peppol BIS v3 dichter naar elkaar toegebracht waarbij TNO de verschillen op een visuele wijze laat zien in het semantic treehouse. Daarbij ondergaat het semantic treehouse een verbeteringsslag die mede met de visuele weergave van het factuurlandschap op de website van het STPE in eerste helft van 2023 beschikbaar zal komen.

Het STPE heeft in 2022 een bijdrage geleverd aan het Europese amendement en het elektronische 'bonnetje' (e-Receipt). De Nederlandse bijdrage was om tegen het amendement te stemmen. Het uiteindelijke resultaat na stemming was dat het amendement afgekeurd is. Een

opmerkelijk resultaat aangezien heel veel landen een positieve stem hebben uitgebracht, maar toch op basis van gewogen resultaat de grens van 65% niet haalt. Ook het e-Receipt-voorstel is afgekeurd na stemming. Een pas op de plaats, maar het STPE blijft de verdere ontwikkelingen van de Europese Norm als van de Europese e-Receipt standaard nauwgezet volgen.

Daarnaast is het STPE actief rondom de ontwikkelingen van VAT in the Digital Age en zal hieraan gaan bijdragen.

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. 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. Uit de cijfers blijkt dat er grote verschillen bestaan tussen de implementatie van de diverse berichten in de standaard. Zo worden de factuur (Invoice) en urenbrief (Timecard) op veel grotere schaal geadopteerd dan de overige berichten, die aan het begin van het proces toegepast dienen te worden.

In 2022 was er een daling van 8% van het totaal aantal uren in de uitzendbranche (Bron: Jaarcijfers uitzendbranche 2022)[18]. Veel van de SETU-standaarden zijn direct of indirect gekoppeld aan het aantal uren, bijvoorbeeld de Timecard, waarop de uren worden geregistreerd. Op basis van deze generieke cijfers over de uitzendbranche zou kunnen worden ingeschat dat er sprake is van een **lichte daling** van het gebruik van de SETU-standaarden. Daar staat echter tegenover dat de Stichting SETU een nieuwe participant en een nieuwe abonnee heeft verwelkomd in 2022, wat de adoptie van de SETU-standaarden verhoogt. Wellicht is dat terug te zien in een volgende monitor.

Relevante ontwikkeling

In 2022 is er gewerkt aan een nieuwe standaard voor het uitwisselen van planningsgegevens tussen inleners en uitzenders: De SETU Standard for Planning and Scheduling. Deze zal naar verwachting in de loop van 2023 in versie 1.0 beschikbaar komen.

Daarnaast heeft de SETU in 2022 verder gewerkt aan het formuleren van haar nieuwe strategie. De SETU wil haar koers aanpassen aan ontwikkelingen sinds de oprichting van SETU in 2007, zoals de veranderende rol van uitzendorganisaties, de complexiteit van de back-offices, (toekomstige) wijzigingen in wet- en regelgeving en digitaliseringstrends. Hiermee verbreedt de SETU haar scope. Naar verwachting zal de nieuwe strategie in de eerste helft van 2023 voorgelegd worden aan het bestuur.

Community management is en blijft een belangrijk onderwerp voor de SETU. In 2021 is gestart met het organiseren van webinars, niet alleen voor huidige leden van de SETU, maar voor alle

[18] Jaarcijfers uitzendbranche 2022 - ABU

geïnteresseerden. Hiermee is de SETU in contact gekomen met een bredere achterban en dit heeft ook in 2022 geleid tot nieuwe leden.

De verwachting is dat deze initiatieven leiden tot toename van de bruikbaarheid en het gebruik van de standaarden. Met name de nieuwe SETU Standard for Planning and Scheduling kan nieuwe gebruikers aantrekken, die zich specifiek bezig houden met personeelsplanning.

WDO Datamodel

Waarom belangrijk ?

Het WDO Datamodel (WDO: Wereld Douane Organisatie) 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 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 veel 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 vaak een eigen standaard voorschrijven, ook binnen de Europese Unie. Door het gebruik van het WDO Datamodel kunnen de diverse overheids-organisaties dezelfde taal spreken en eenvoudig informatie uitwisselen. Voor de administratie van import en export bevat het WDO Datamodel zogenaamde ‘informatiepakketten’ voor gegevensuitwisseling. 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 betreft het gebruik van de standaard de 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 gebruikt wordt voor de volgende bericht- en aangiftestromen voor wat betreft Nederland:

- Single Window: dit betreft WCO 46 berichten (vorig jaar: 22 binnenkomende en 15 uitgaande berichttypes. Gebruikers: Douane, Rijkswaterstaat en overige grensbewaking);
- Douane aangifte (DMS): dit betreft 3 WCO berichten (vorig jaar: 2 binnenkomende en 1 uitgaand berichttypen met de Douane als gebruiker);
- Douane eCommerce (DECO): dit betreft 3 WCO berichten (vorig jaar: 2 binnenkomende en 1 uitgaand berichttypen, met de Douane als gebruiker);
- Control bericht: 1 WCO bericht (vorig jaar ook);
- De MIG voor ICS2-PNI 1.0; dit betreft 4 WCO berichten (vorig jaar: 1 binnenkomend en 1 uitgaand berichttype, gebaseerd op het WDO Datamodel 3.8.1);
- Dit jaar toegevoegd: Douane Vervoersaangifte (DVA) met 3 WCO-berichten.

Als we de opgave van de berichtenstromen als indicator gebruiken voor het gebruik van het WDO Datamodel, dan kan worden geconcludeerd dat sprake is van een **toename 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 hardcijfermateriaal 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 Windo 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.

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 t/m april**
Belastingdienst					
Aangifte IB + VPB	16.558.025	15.568.706	15.846.758	15.546.416	7.707.110

Aangifte OB + Intercomm. prestaties	5.429.106	5.890.273	6.379.104	7.288.250	3.461.705
Toeslagen	1.325.719	1.279.414	1.355.471	1.617.206	696.832
Erfbelasting + Schenkbelasting	4.073	16.115	31.496	41.012	25.184
Uitsluitend Zakelijk Gebruik Bestelauto	1.143	924	854	796	91
KvK – Reporting Services (SBR)					
Jaarrekeningen	1.020.450	886.373	889.466	962.503	236.559
DUO – Reporting Services (SBR)					
Jaarrekeningen	1.953	1.942	1.963	3.989	561
SBR Wonen - Reporting Services (SBR)					
DPI (prognose informatie)	1.112	1.194	898	1.051	278
DVI (verantwoordingsinformatie)	1.363	1.370	1.745	1.704	13
SBR Wonen Jaarrekening	1.364	1.242	1.226	1.417	10

Een vergelijking van de cijfers over de (volledige) jaren 2019, 2020, 2021 en 2022 lijkt erop te duiden dat de adoptie van SBR en daarmee XBRL binnen Nederland per saldo **toeneemt**; waar op de meeste onderdelen sprake is van een stijging, is op een enkel onderdeel sprake van een (lichte) daling.

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

Om het deponeren van de jaarrekening door grote rechtspersonen via SBR per 1 januari 2025 te realiseren worden voorbereidingen getroffen. Hierdoor zal ook de mogelijkheid worden gecreëerd om rapportages in het Inline XBRL formaat te deponeren. Want effecten-uitgevende instellingen in de Europese Unie moeten de jaarlijkse financiële verantwoording opstellen op basis van het door de ESMA vastgestelde Europees uniform elektronisch verslaggevingsformaat (ESEF). ESEF behelst dat een jaarverantwoording openbaar moet worden opgemaakt in het XHTML-formaat waarbij Inline XBRL wordt toegepast. Alle overige ondernemingen in Nederland krijgen de mogelijkheid om ook in het Inline XBRL formaat te gaan rapporteren.

In november 2022 nam de Europese Unie de Corporate Sustainability Reporting Directive (CSRD) aan. De richtlijn zal vanaf 2024 steeds meer grote bedrijven verplichten hun impact van hun activiteiten op mens en milieu te rapporteren. De CSRD-richtlijn staat centraal in de Green Deal van de Europese Unie en is bedoeld om een einde te maken aan 'greenwashing' en te zorgen voor meer transparantie over en de basis leggen voor standaarden voor duurzaamheidsrapportages op mondiaal niveau. Voor deze duurzaamheidsrapportages zal Inline XBRL moeten worden toegepast. En er zal gebruik worden gemaakt van een taxonomie

waarin de definities van de te rapporteren gegevens zijn vastgelegd. Bedrijven moeten zich nu al voorbereiden op de richtlijn, zodat ze een jaar voor de startdatum kunnen beginnen met het verzamelen van de nodige data en het inrichten van de governance-structuur.

De afspraken binnen de publiek-private SBR Governance worden momenteel tegen het licht gehouden in relatie tot de huidige eisen en wensen. In afstemming met de deelnemers wordt een concreet voorstel voorbereid voor aanpassing van de huidige SBR Governance.

Internationaal wordt de XBRL standaard breed gebruikt door financiële toezichthouders zoals de Europese Centrale Bank (ECB) maar ook nationale partijen zoals de SEC (USA) en de ESMA (EU).

Tot slot: organisaties moeten zelf kennishouder zijn of gaan worden met betrekking tot XBRL. Logius overweegt om de ondersteuning van organisaties op dit gebied af te bouwen. Voor de adoptie van XBRL is dit een risico.

B4.5. Domein schoon water en beschermde bodem

Aquo-standaard

Waarom belangrijk ?

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

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

Feitelijk gebruik

Het gebruik van de Aquo-standaard binnen het waterbeheer is groot. Zo hebben de waterbeheerders (waterschappen, de provincies en Rijkswaterstaat) 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. Vanuit het IHW geeft men aan dat deze nieuwe geïntegreerde omgeving veelvuldig wordt gebruikt, in de maanden daarna en ook in het jaar 2022. Het onderstaande inzicht van het gebruik in 2022 is gebaseerd op deze nieuwe bron (Wiki XL):

- Aquo wiki bezoekers 21.213 (+ 34% t.o.v.2021)
- Pageviews[19] 89.990 (+ 14% t.o.v. 2021)
- Downloads 3.764 (+ 28% t.o.v. 2021)
- Outlinks[20] 1.976 (+ 77% t.o.v. 2021)

Deze cijfers wijzen op een **toename van het gebruik** in de periode 2022 ten opzichte van 2021.

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: 154 (vorig jaar: 184)
  - aantal gemelde incidenten: 149 (vorig jaar: 135).
- aantal waterbeheerders dat een wijzigingsvoorstel indient / een incident meldt:
  - betrokken instanties bij wijzigingsvoorstellen: 29 (vorig jaar: 33)
  - betrokken instanties bij melden incident: 46 (vorig jaar: 47)

Relevante ontwikkeling

De Aquo-standaard wordt beheerd en onderhouden op basis van de wensen van gebruikers; zij dienen hiervoor wijzigingsvoorstellen in. En ook door nieuwe wet- en regelgeving en (inter)nationale ontwikkelingen is het nodig de Aquo-standaard regelmatig bij te werken. Het Aquo-team van het Informatiehuis Water beoordeelt of wijzigingsvoorstellen passen binnen de standaard. Expertgroepen en technische werkgroepen, waarin gebruikers zijn vertegenwoordigd, helpen en adviseren daarbij1

Het Aquo-team streeft voortdurend naar optimalisatie van de toegankelijkheid van de standaard via de Aquo Wiki. In 2022 zijn hiervoor de volgende acties uitgevoerd:

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

[20] Hyperlinks die verwijzen naar andere (externe) websites (o.a. Aquo-sharepoint, ihw, Sikb).

- In de Aquo Wiki zijn domeinwaarden aan begrippen gekoppeld. Eind 2022 was deze actie gevorderd t/m de letter P, in 2023 ronden we dit af. Door deze koppeling wordt het zoeken naar de definitie van een domeinwaarde eenvoudiger en bereiden we de Aquo-standaard voor op de doorontwikkeling tot een ontologie.
- In januari 2022 is een compleet herziene versie van de praktijkrichtlijn Aquo Begrippen opgeleverd. In dit document wordt de opbouw van de begrippen in de Aquo Wiki toegelicht. Dit biedt gebruikers en beheerders inzicht in hoe de begrippen in de Aquo-standaard worden beheerd en gebruikt.

(Geo-)Standaardisatie is een internationaal proces. Veranderingen in standaarden en modellen op internationaal en Europees niveau werken door op nationaal niveau. De Aquo-standaard sluit hierop aan. De vraagstukken die binnen de watersector opgelost moeten worden, staan namelijk niet op zichzelf. Ze hebben een relatie met andere omgevingen en, daardoor, ook met andere standaarden. Aansluiting bij internationale en nationale referentiestandaarden zorgen ervoor dat met de Aquo-standaard een integrale werkwijze en maximale gegevensuitwisseling mogelijk is. BOMOS is een Beheer- en OntwikkelModel voor Open Standaarden. Van origine is het beheer van de Aquostandaard gebaseerd op het BOMOS-model. Het BOMOS-model wordt beheerd door Logius dat in 2022 het beheer weer actief heeft opgepakt. Het Aquo-team neemt deel aan de klankbordgroep die betrokken is bij de ontwikkeling van een nieuwe versie van het BOMOS-model. Zo brengen wij onze ervaring met het beheer van een Open Standaard in en leren we gelijktijdig van andere standaardbeheerders hoe we elementen van BOMOS nog meer in Aquo kunnen toepassen.

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 2022 hebben 185 gemeenten rioleringsdatasets op het landelijke dataplatform met rioleringsdatasets geplaatst. Een jaar daarvoor, eind 2021, waren dat nog 160 gemeenten. De **gestage groei** (net als vorig jaar) is toe te schrijven aan het volgende:

- in 2022 zijn beheerapplicaties het GWSW beter gaan ondersteunen waardoor gemeenten in staat zijn het GWSW zelf toe te passen;
- steeds meer gemeenten willen hun rioleringsdata open publiceren via Publieke Dienstverlening Op de Kaart (PDOK)[21];
- andere (software-)toepassingen gaan zich op GWSW-conforme rioleringsdata baseren (rechtstreeks, via het GWSW-platform van Stichting RIONED en zeker ook via PDOK) waardoor meer gemeenten gemotiveerd worden het GWSW zelf ook te gaan toepassen;
- 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).

Verder mag in het kader van het realiseren van de randvoorwaarden voor het gebruik van GWSW het volgende niet onvermeld blijven:
- alle bestekken voor rioolreiniging en –inspectie schrijven het RibX uitwisselformaat voor;
- en uit de jaarlijkse GWSW applicatietoets blijkt dat de meerderheid van de rioleringsbeheerpakketten, alle inspectiesoftware en alle modelleringssoftware de voorgeschreven GWSW-formaten kunnen uitwisselen.

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.

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

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

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, Het Waterschapshuis, 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 voor wat betreft het aantal gebruikers uit de overheidssector niet groot meer bij SIKB0101.

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 milieuhygiënische kwaliteit van de bodem (BRO fase II). Uitgangspunt hierbij is dat gebruikt wordt gemaakt van SIKB0101 volgens de PTOLU-

principes. Waar nodig zullen 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.

Ten aanzien van SIKB0102 werkt de Rijksdienst voor het Culturele Erfgoed aan een grote verbeterslag op het Archeologisch Basis Register (ABR). Mede daarom en op verzoek van de gebruikers, is besloten het model de komende jaren zoveel mogelijk te bevriezen, om hiermee meer ruimte te creëren voor brede implementatie.

B4.6. Domein bouwen en wonen

IFC

Waarom belangrijk ?

IFC is een gestandaardiseerde, digitale beschrijving van assets in de bouw- en infrasector en wordt ontwikkeld door de internationale organisatie buildingSMART. In Nederland wordt de standaard ondersteund door de lokale buildingSMART organisatie. Het is een open, internationale standaard (ISO 16739-1:2018) en bevordert uitwisseling van leveranciers-neutrale en bruikbare informatie tussen hardware-apparaten, softwareplatforms, en interfaces voor veel verschillende use cases. IFC is een standaard voor zowel semantische afspraken als voor dataformats en richt zich specifiek op BIM-informatie over bouwwerken. De standaard maakt het mogelijk om een driedimensionaal geometrisch model van een bouwwerk digitaal vast te leggen, inclusief de gegevens van de daarin ondergebrachte elementen en hun onderlinge relaties. Deze beschrijving kan vervolgens in IFC formaat uitgewisseld worden tussen partijen die betrokken zijn bij de ontwikkeling, vergunning-verlening, beheer en onderhoud van een gebouw. Zo verloopt de informatie-uitwisseling tussen overheden onderling en tussen overheden en vergunning-aanvragers of bouw-ondernemers efficiënter. Dit is bijvoorbeeld nuttig bij het verlenen van bouwvergunningen en bij de ontwikkeling en het ontwerpen van gebouwen. De IFC-standaard staat op de ‘pas-toe-of-leg-uit’-lijst sinds november 2011.

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 vorige monitor open standaarden gepresenteerd als een 0-meting en die gegevens vormen ook nu de basis. Omdat er eens in de twee jaar wordt gemeten, is er nu nog geen vervolgmeting met actuelere gegevens beschikbaar. Onderstaande sores zijn derhalve dezelfde als vorig jaar. Bij een volgende meting (2023) zal moeten blijken hoe een en ander zich ontwikkelt.

De BIM monitor is gebaseerd op een enquête onder de belangrijkste deelsectoren uit de Nederlandse bouwkolom, waaronder ook de opdrachtgevers. Onder de 577 respondenten

bevinden zich 76 overheidsorganisaties, alle in de rol van opdrachtgever. Uit de monitor kunnen enkele uitspraken worden gedestilleerd over de categorie van 150 opdrachtgevers. Over de subcategorie 'overheden' daarbinnen is niet afzonderlijk gerapporteerd.

Over de categorie opdrachtgevers kan in relatie tot IFC het volgende worden vastgesteld:
- bekendheid met IFC: 22 %
- gebruik van IFC: 6 %.

Vooralsnog is sprake van lage scores op kennis en gebruik van deze standaard bij de genoemde deelsector, het **gebruik is beperkt**. Dit beeld sluit aan bij de opbrengst van het in augustus 2021 verschenen Evaluatierapport Bouwstandaarden, uitgevoerd in opdracht van Bureau Forum Standaardisatie. Enkele conclusies uit die evaluatie luiden als volgt:
- het aantal IFC-experts werkzaam bij de overheid is erg beperkt;
- experts geven unaniem aan dat IFC op de 'Pas toe of leg uit'-lijst hoort, ondanks de beperkte kennis en toepassing binnen overheidspartijen;
- de bekendheid van IFC binnen de overheid is nog beperkt; hier is nog veel werk te verzetten.

Relevante ontwikkeling[22]

In 2019 en 2020 is aangetoond in een door TNO samen met het ministerie van BZK ontwikkelde Proof of Concept dat geautomatiseerde checks op wet- en regelgeving op basis van IFC mogelijk is.

Inmiddels is de gemeente Rotterdam gestart met een pilot voor automatische vergunning-controleservice waarbij IFC als uitwisselformaat is gekozen en gekoppeld wordt aan gebouwgegevens. Met behulp van de ifc OWL-ontologie kan men IFC-gegevens beschikbaar stellen zodat gebouwgegevens eenvoudig kunnen worden gekoppeld aan materiaalgegevens, GIS-gegevens, gegevens van productfabrikanten, sensorgegevens, classificatieschema's, sociale gegevens, enzovoort. Het resultaat is een web van gekoppelde gebouwdata dat grote kansen biedt voor databeheer en -uitwisseling in de bouwsector en daarbuiten. Deze ontwikkeling bevindt zich weliswaar nog in de ontwikkelfase, maar kan in de toekomst een grote impact kan hebben in het kader van de Wet Kwaliteitsborging.

Naast deze ontwikkeling wordt IFC4.3 momenteel verder ontwikkeld als uitbreiding voor de beschrijving van infrastructuurwerken binnen de domeinen Spoorwegen, Wegen, Havens en Waterwegen, met inbegrip van de elementen die in die domeinen gemeenschappelijk zijn. Naar verwachting wordt ook deze standaard op niet al te lange termijn door ISO erkend als standaard.

[22] Deze passage is ongewijzigd gebleven.

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 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 digiAkkoord 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

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
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

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 4 pijlers (Stedelijk spoor, Netbeheer, Openbare Ruimte en Data Inwinning) 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.

Van de 209 organisaties leveren er 55 ook een bijdrage aan de ontwikkeling van de standaard. Deze bijdrage aan ontwikkeling is gelijk aan vorig jaar; ook toen 55 organisaties. 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.

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.

Relevante ontwikkeling

Op 17 juni 2022 is NLCS 5.0 gelanceerd, de langverwachte opvolger van NLCS 4.2. In deze versie is een mapping tussen NLCS met zowel BGT als GWSW opgenomen. Door opname van deze mappings in de database van de NLCS zijn de mappings echt in de NLCS verankerd, waarmee het importeren van BGT/GWSW datasets vanuit verschillende softwarepakketten nu een uniform resultaat opleveren.

Vanuit de markt is er al langer vraag naar uitbreiding van de NLCS voor zowel stedelijk spoor als netbeheer. Binnen de NLCS waren deze groepen slechts beperkt ingericht. Na een inventarisatie binnen de stedelijk spoor en netbeheerbedrijven, staat 2022 in het teken van het uitwerken van de betreffende hoofdgroepen binnen de NLCS. Er zijn afspraken gemaakt met leveranciers om naast de NLCS 5.0 te kunnen werken met testversies van de diverse uitbreidingen. Deze worden als "losse test modules" toegevoegd aan de NLCS-database. Hiermee wordt in een iteratief proces gekomen tot een verdere ontwikkeling van de standaard wat uiteindelijk definitief opgenomen wordt in een toekomstige versie van de NLCS. Zo is deze toekomstige versie geschikt bevonden door de stedelijk spoorbedrijven en netbeheerders waarna de uitbreiding breed uitgedragen kan worden naar alle gebruikers. Met deze uitbreiding is de verwachting dat we meer stedelijk spoorbedrijven en netbeheerders als gebruikers van de NLCS kunnen toevoegen.

Met NLCS 5.0 is een eerste basis gelegd voor de verdere uitbreiding van de NLCS en de aansluiting op informatiemodellen zoals IMBOR, IMKL, GWSW. De vraag naar een koppeling tussen CAD en GIS wordt vanuit de markt steeds luider. Er wordt gewerkt aan een werkbaar principe waarbij het mogelijk wordt om met de CAD-applicatie de objecten te definiëren vanuit het datamodel (OTL) inclusief de kenmerken (attributen) en deze vervolgens middels een geschikte tooling als NLCS-objecten te tekenen. Het doel is om aanvullende kenmerken als data aan de NLCS-objecten te koppelen, zodat hier vervolgens een dataset uit gegenereerd kan worden voor onder andere Assetmanagement. Op het moment dat er een werkbaar principe is kan dit voor de verschillende werkpakketten/ontwikkelingen binnen de NLCS worden ingezet. Deze werkpakketten zijn cruciaal in de opmaat van de NLCS naar een BIM 'Level 2' standaard. Een volgende stap die door opname van IMBOR in een volgende versie van de NLCS wordt

bewerkstelligd is dat tijdens de ontwerpfase van een object, de informatie zo rijkelijk mogelijk, gestandaardiseerd en eenduidig beschikbaar komt voor levenscyclus van een object (Ontwerp-Aanleg-Registratie-Beheer-Ontwerp). Hierdoor gaat de NLCS een belangrijke rol spelen in de uitwisseling van gegevens volgens ISO-19650. De NLCS gaat dienen als input voor de (Basis) ILS (Infra).

Wij gaan ook voor het werkpakket NLCS – RAW bestekken op dit principe verder investeren. Al 15 jaar doet de markt pogingen om CAD- en RAW-programma's met elkaar te verbinden. Eerder bleek dit niet opportuun, onder andere door het ontbreken van een standaard voor CAD-tekeningen en een sterk verzuilde bedrijfscultuur. Inmiddels zijn de benodigde standaarden beschikbaar en groeit het besef dat je met digitalisering deze werkzaamheden efficiënter uit kunt voeren. Zaak is de verzuiling in de branche te doorbreken, door standaarden in samenhang te zetten. Met als uiteindelijk doel integrale digitale samenwerking tussen tekenaars, bestekschrijvers, calculators en beheerders.

Dat er nog geen samenhangend geheel is, is een gemiste kans als je bedenkt dat circa 80 procent van de werkzaamheden in de buitenruimte tot stand komt op basis van NLCS-tekeningen en een RAW-contract. Met de huidige werkmethode is het doorvoeren van wijzigingen in het ontwerp een arbeidsintensieve, handmatige en foutgevoelige exercitie. En dat lijdt uiteindelijk weer tot discussies over meer- en minderwerk door tegenstrijdigheden tussen tekeningen en het contract.

Ook voor het werkpakket Nationaal dataportaal wegverkeer wordt de link tussen CAD en GIS gezocht. Vanuit de brede informatiebehoefte voor mobiliteit werkt het Ministerie van IenW aan het oprichten van een netwerkregistratie voor wegen zodat publieke en private gebruikers kunnen beschikken over digitale informatie over de verkeerskundige inrichting van het wegennetwerk.

Naast de werkpakketten met betrekking tot CAD en GIS is ook het werkpakket Inmetingen (landmeetkundig) verwerken op basis van NLCS direct in de keten relevant. Steeds meer opdrachtgevers eisen dat de ingewonnen meetgegevens direct ingezet kunnen worden in het project. Leveranciers van apparatuur voor data-inwinning sluiten steeds meer aan op de (inter)nationale ontwikkelingen met betrekking tot data-standaarden. Dit is echter nog niet goed geland binnen gebouwde omgeving waar de NLCS een steeds belangrijke en prominente rol speelt. Het doel is om afspraken te maken en te verankeren in de NLCS zodat ingewonnen data direct, conform NLCS, toegepast kunnen worden in de levenscyclus van assets/objecten in de gebouwde omgeving[23].

[23] Bovenstaande passages onder 'relevante ontwikkeling' zijn identiek aan die van vorig jaar. De hier beschreven ontwikkelingen zijn nog steeds van toepassing en zijn nog niet doorgevoerd. Dit is niet iets wat "snel" doorgevoerd gaat worden. Ook het jaarplan 2023 is hierop gebaseerd maar is eigenlijk een meerjarenplan en zal dus nog langer als relevante ontwikkeling gezien kunnen worden.

Daarnaast krijgt de standaard een fundamentelere inbedding voor BV Nederland tot 2030 door de ondertekening van het digiAkkoord door stakeholders. Met deze ondertekening worden stakeholders en brancheverenigingen nadrukkelijker betrokken om ruchtbaarheid te geven aan de toepassing van openstandaarden. Hieruit is het overzicht van informatiestandaarden in de bouwsector (https://www.bimloket.nl/ictstandaarden/) een eerste vrucht.

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. 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.

Met betrekking tot het gebruik van de standaard vanuit de overheidshoek worden de volgende gegevens door de beheerorganisatie aangeleverd:

- overheidsorganisaties: 119 (115, +3%)
- individuele gebruikers bij overheden 6002 (5129, +17%)
- overheidsprojecten 6528 (5222, +25%)

(Peildatum: zomer 2023. Tussen haakjes staan de aangeleverde gegevens voor de monitor van vorig jaar door de beheer organisaties.)

De beheerorganisatie geeft aan dat sprake is van een **lichte toename van het gebruik**. Op elk van de drie variabelen in bovenstaand overzichtje is sprake van een stijging.

Zowel het aantal gebruikers als het aantal projecten is gestegen, ondanks dat het aantal organisaties maar licht is gestegen. Deze stijging is als volgt te verklaren:

- projecten schrijven steeds vaker voor dat VISI actief / online moet blijven, ook tijdens de garantie- en onderhoudstermijn;
- organisaties kiezen steeds vaker voor het toepassen van VISI, voorafgaand aan de uitvoeringsfase, denk aan ontwerp- en voorbereidingsfase. Dat doet met name het aantal projecten en gebruikers toenemen;
- organisaties besluiten steeds vaker om projecten langer actief te houden als online archief, ten behoeven van de toegankelijkheid en traceerbaarheid van de online communicatie en informatie.
- omdat mensen vaak meerdere projecten doen is de stijging in gebruikers lager dan de stijging in het aantal projecten;
- aantal overheidsorganisaties verkiest gebruik van software boven de toepassing van een Open Standaard;
- onbekendheid van (vooral) lagere overheidsorganisaties met (de verplichting van) Open Standaarden;
- negatieve invloed van stikstofmaatregelen op aantal projecten;
- werkzaamheden worden steeds vaker ondergebracht in “raamovereenkomsten”. Dat heeft gevolgen voor het aantal projecten;
- huidige projecten hebben door de regel een langere looptijd. Dat voorkomt ook het starten van nieuwe projecten;

- overheid werkt steeds meer op regiebasis, waardoor er veel capaciteit (gebruikers) wordt gevraagd van de aannemerij en minder van de overheidsorganisatie;
- overheidsorganisaties zijn selectiever in het toevoegen van gebruikers op hun projecten.

Relevante ontwikkeling

Twee nieuwe toepassingsgebieden zijn hier relevant. Op de eerste plaats de twee sectoren Bouw & Utiliteit en de installatiebranche. Hier is de toepassing van VISI nog erg beperkt. Langzaam komen er steeds meer toepassingen voor nieuwbouw en renovatie van woningbouw. Het blijft moeilijk om de toegevoegde waarde van VISI in deze sector uit te leggen, doordat :

- De relatief grote aantal kleine projecten met veel kleine specialistische bedrijven bemoeilijken een goede implementatie van VISI omdat het voor de individuele bedrijven niet direct zichtbaar is wat het oplevert,
- Het digitalisering van het werk is meer gericht op het assembleren van componenten, elementen en artikelen dan op het optimaliseren van werkprocessen, waardoor VISI buiten de focus van de sector valt,
- Er zijn geen grote opdrachtgevers in de B&U die het gebruik van VISI kunnen 'doordrukken'
- De behoefte aan 'compliance' is minder groot bij het grote deel van particuliere marktpartijen, dan bij de overheidspartijen die de GWW sector domineren

Ten tweede de energiesector. In deze sector vindt VISI steeds meer aftrek. Door de grote druk vanwege de energietransitie op de energiesector om projecten versneld uit te voeren, zien we in het tweede deel van 2021 al een forse stijging van de hoeveelheid projecten bij de verschillende gebruikers in de energiesector. Een trend die zich in 2022 heeft doorgezet.

Ook de volgende aspecten dragen bij aan zicht op relevante ontwikkelingen:

- Een toenemend besef van en behoefte aan "out-of-the-box" oplossingen (i.p.v. maatwerk);
- meer aandacht voor applicatierationalisatie bij organisaties;
- aanscherping van aanbestedingsdrempels- en richtlijnen;
- Wet open overheid (Woo) vraagt om betere vastlegging, betrouwbaarheid en terugvindbaarheid van afspraken en communicatie;
- veranderende administratieve voorwaarden binnen (overheids)projecten;
- demografische ontwikkeling van het werkveld i.r.t. "digivaardigheid" van medewerkers;
- promotie en toepassing van de Open Standaard buiten de GWW;
- versnelling in release cyclus van de Open Standaard.

B4.7. 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.

Feitelijk 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. Het gebruik lag vorig jaar behoorlijk lager (periode juni 2021 – mei 2022) dan in het jaar daarvoor:

- 2.352.160 bezoekers >> bijna 200.000 per maand
- 4.597.363 page-views >> bijna 400.000 per maand

Omdat tussentijds de meetmethode is aangepast, kon vorig jaar geen uitspraak worden gedaan over de ontwikkeling van het gebruik. Dit jaar zijn geen nieuwe cijfers beschikbaar.

EML_NL

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

B4.8. Domein onderwijs en cultuur

E-Portfolio NL NEN 2035

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

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.