Werkagenda Waardengedreven Digitaliseren en Open Standaarden

Versie 19 januari 2023

Inleiding

Standaarden zijn geen doel op zich, maar een middel om maatschappelijke doelen te bereiken. Een set maatschappelijke doelen is opgenomen in het Regeerakkoord en de Kabinetsdoelstellingen, en is verder uitgewerkt in de hoofdlijnenbrieven, de Werkagenda Waardengedreven Digitaliseren van de Staatsecretaris Koninkrijksrelaties en Digitalisering en de Strategie Digitale Economie van de Minister van Economische Zaken en Klimaat.

In deze notitie wordt in hoofdlijnen concreet gemaakt op welke wijze de open standaarden van de 'pas toe of leg uit'-lijst en de verdere werkzaamheden van het Forum Standaardisatie in het werkplan 2023, bijdragen aan deze maatschappelijke doelen en beleidslijnen uit de Werkagenda Waardengedreven Digitaliseren. [*PM: Over de Strategie Digitale Economie is een separate notitie*.]
(Werkplan2023#1.2)

1. Iedereen kan meedoen in het digitale tijdperk

1.2 Toegankelijke dienstverlening

Ter verbetering van de gebruiksvriendelijkheid, begrijpelijkheid en digitale toegankelijkheid van publieke dienstverlening is een aantal standaarden verplicht, volgens het 'pas toe of leg uit' principe. Daarnaast zijn er aanvullende acties in het werkplan opgenomen:

Verbetering met behulp van 'pas toe of leg uit' standaarden

Voor de overdracht van informatie, zoals bij onderzoeksrapporten en infographics, is het belangrijk dat de opmaak behouden blijft, onafhankelijk welke hardware of software (van eender welke leverancier) mensen willen gebruiken. Daar zijn documentstandaarden voor opgenomen op de lijst.

Voor mensen met een visuele beperking, of voor wie structuur belangrijk is, zijn daarnaast digitoegankelijkheids standaarden opgenomen. Op deze wijze wordt overheidsinformatie ook voor hen meer begrijpelijk.

Hoe dan?

Informatie en documenten op overheidswebsites die volgens de digitoegankelijkheidsnorm zijn ingericht, zijn beter leesbaar (contrast), beter voorleesbaar en werken beter met brailleleesregels. Digitoegankelijk (de Nederlandse naam voor EN 301 549 met WCAG 2.1) staat op de lijst.

Om ervoor te zorgen dat een overheidsdocument of rapport er op een iPad hetzelfde uitziet als op een PC, een Android tablet of een Linux computer zijn open PDF standaarden op de lijst opgenomen.

Aanvullende acties in werkplan FS 2023

Om ervoor te zorgen dat overheidswebsites en mail gebruiksvriendelijk zijn, werken we aan de herkenbaarheid van overheids internet domeinen en domeinnamen (Regie op Internetdomeinen, Register Internetdomeinen Overheid, en 1-overheids-subdomeinnaamextensie) zodat er minder verwarring optreed of een site of een e-mail van de overheid is, of privaat. Daarnaast helpen we mee aan de harmonisering van de gebruiksinteractie op overheidswebsites (NL Design System).
[Werkplan2023#1.5]

1.3 Impact online desinformatie verminderen

Om desinformatie en fake-news te voorkomen, is het belangrijk dat de authenticiteit van informatie gegarandeerd is. Dat geldt helemaal voor overheidsinformatie. Er moet gewaarborgd zijn dat een website of een e-mail daadwerkelijk van een overheidsorganisatie is, en dat de informatie niet veranderd is. Diverse informatieveiligheidstandaarden op de lijst dragen daaraan bij.

Verbetering met behulp van 'pas toe of leg uit' standaarden

Een set website standaarden op de lijst voorkomt dat kwaadwillende een overheidsdomeinnaam kunnen misbruiken om valse informatie te verspreiden. Een andere set e-mail standaarden voorkomt dat een overheids e-mail adres als afzender misbruikt wordt. Deze standaarden voorkomen eveneens dat de web- of e-mail communicatie onderweg veranderd wordt.

Hoe dan?

Zonder extra maatregelen is het kinderlijk eenvoudig om namens een ander (e-mail adres) een mail te versturen. Dat komt omdat het e-mail protocol in de jaren '80 van de vorige eeuw is ontworpen nagenoeg zonder beveiligingsmaatregelen. Zo kan - zonder de toepassing van nadere standaarden - binnen enkele seconden een mail namens bijvoorbeeld de minister-president of Jaap van Dissel gestuurd worden, en komt deze ook nog bij de ontvanger aan. De aanvullende e-mailbeveiliging standaarden die dit voorkomen, werken net zoals de echtheidskenmerken in bankbiljetten. Een vals bankbiljet is herkenbaar omdat bijvoorbeeld het watermerk ontbreekt. Dat wordt zelden opgemerkt door consumenten, maar wel bij supermarkten of banken. De valse bankbiljetten worden dan uit de roulatie gehaald.

Voornoemde anti phishing standaarden werken net zo. In elke legitieme e-mail zit (onder de motorkap) een onvervalsbaar echtheidskenmerk verstopt. Wanneer dit ontbreekt, houden internetserviceproviders deze e-mails tegen, voordat ze de ontvanger bereiken.

Het gaat hierbij o.a. om de standaarden TLS+HSTS (voor websites) en DKIM+SPF+DMARC (voor e-mail) die op de 'pas toe of leg uit'-lijst staan.

Aanvullende acties in werkplan FS 2023

Gelet op het belang van deze informatieveiligheidstandaarden zijn in het OBDO, naast de 'pas toe of leg uit' verplichting bij aanschaf van ICT, nadere gebruiksafspraken gemaakt. Eind 2019 zouden deze standaarden bij elke overheidswebsite en e-mail zijn geïmplementeerd. Dat blijkt in 2022 bij een groot deel (ongeveer de helft) nog niet het geval. In het werkplan 2023 van het Forum, hebben die acties prioriteit die de adoptie bij achterblijvende overheidsorganisaties

verder aanjagen.
(Werkplan2023#3.2)

2. Iedereen kan de digitale wereld vertrouwen

2.1 Publieke waarden borgen

Publieke waarden zijn ook essentieel in de digitale wereld. Concentratie van marktmacht is een actueel gevaar, omdat platformen een essentieel onderdeel vormen van ons digitale leven, maar zich niet altijd publiek verantwoord gedragen. Daarom worden (publieke) veilige alternatieven gemaakt, die interoperabel zijn met andere diensten en ze worden open-source ontwikkeld als 'digital commons'. Daarnaast steunt Nederland interoperabiliteit van bedrijven, omdat dit marktmacht tegengaat.

Verbetering met behulp van 'pas toe of leg uit' standaarden

Het gebruik van open standaarden helpt bij het tegengaan van deze concentratie van marktmacht, omdat deze open standaarden van de 'pas toe of let uit lijst' gratis bruikbaar zijn voor alle bedrijven, overheden en burgers, ze vendor-lockin helpen voorkomen, ze data uitwisselbaar en portabel maken, en systemen van verschillende leveranciers interoperabel maken.

Hoe dan?

Omdat de open standaarden vrij bruikbaar zijn, kunnen alle leveranciers ze kosteloos gebruiken, en gelden er geen intellectuele eigendomsbeperkingen. Dat heeft als voordeel dat systemen van verschillende leveranciers kunnen samenwerken, dat je niet gebonden bent aan systemen en software van één bepaalde leverancier, dat data vanuit het systeem van de ene leverancier kan worden overgezet naar dat van een andere (exit-strategie), en toetreding tot de markt laagdrempeliger wordt voor nieuwe toetreders.

Ter illustratie kan het voorbeeld van de open standaard Bluetooth worden genoemd. Waarmee systemen van een veelheid van leveranciers interoperabel zijn: op een bluetooth speaker kan zowel een PC, als Linux als MacOS als Android als iPhone worden aangesloten. Gebruikers kunnen ook tussen die systemen switchen. Nieuwe speaker leveranciers kunnen toetreden tot de markt zonder dat ze worden uitgesloten van de standaard, of ervoor moeten betalen.

Dit in tegenstelling tot speakers met de gesloten Airplay standaard, waarmee alleen Apple apparatuur kan communiceren. Nieuwe toetreders tot de markt kunnen worden uitgesloten of moeten voor gebruik betalen.

Welke acties uit het Werkplan FS 2023?

Eind 2022 is het Bureau van het Forum Standaardisatie nauw betrokken bij het publiek alternatief voor (o.a.) Twitter in de vorm van het initiatief om een Nederlandse publieke Mastodon server op te zetten.

Extra Kans

Open Standaarden expliciet standaard onderdeel laten worden van het "Verplicht keurmerk" en het "Ïnterbestuurlijk normen- en begippenkader voor publieke waarden bij digitalisering", in de 5 Digital Commons (werkagenda pagina 20 en 21).

2.4 Versterken cybersecurity

De overheid loopt achter wat betreft digitale weerbaarheid, vanwege het ontbreken van basismaatregelen (Cybersecurity Beeld 2022) en is een interessant doelwit is voor kwaadwillenden (statelijk en crimineel). Als onderdeel van deze brede maatschappelijke opgave heeft de overheid als taak het goede voorbeeld te geven en op een veilige manier met gegevens van burgers om te gaan.

Verbetering met behulp van 'pas toe of leg uit' standaarden

Een set informatieveiligheid standaarden op de lijst helpt phishing via e-mail en websites voorkomen, voorkomt dat criminelen of statelijke actoren web- en emailverkeer meelezen, toegang hebben tot persoonsgegevens in de backoffice en basisregistraties, of dat internetverkeer wordt gekaapt en omgeleid. Daarnaast maken ze de snelle uitwisseling van cyber-dreigingsinformatie mogelijk.

Hoe dan?

Phishing
Criminelen proberen bij mensen geld, wachtwoorden, of andere persoonsgegevens buit te maken (phishing), door zich voor te doen als een andere partij (spoofing). Vaak doen ze zich voor als overheidsorganisatie. Hun modus-operandus is om mensen met een valse e-mail te verleiden een valse website te bezoeken. Op die website wordt dan gevraagd naar persoonsgegevens, zoals wachtwoorden, of om geld over te maken of software te installeren (zoals ransomware). Sommige vormen van phishing zijn specifiek gericht op medewerkers van organisaties (CEO-fraude). De criminelen gebruiken eenvoudig kopieerbare kenmerken van bonafide sites en e-mail, zoals logo's en huisstijl, om zich zo echt mogelijk voor te doen. Organisaties kunnen zich tegen dit misbruik wapenen, door – net zoals bij het watermerk in papier geld – niet kopieerbare echtheidskenmerken toe te voegen aan hun websites en e-mail.
Bij websites gebeurt dat met name met informatieveiligheid standaarden als 'het slotje'. Bij e-mail gebeurt dat met informatieveiligheid standaarden, waarmee internetserviceproviders vervalste mails onderscheppen voordat ze bij eindgebruikers terecht komen. Deze echtheidskenmerken waarborgen dat de inhoud van een website bij het website adres hoort (de zogeheten domeinnaam, bijvoorbeeld www.toeslagen.nl) , en de inhoud van de e-mail bij het afzenderadres hoort (bijvoorbeeld: incasso@cjib.nl). Een crimineel kan deze echtheidskenmerken niet kopiëren.

Het gaat hierbij om dezelfde standaarden van de 'pas toe of leg uit'-lijst die helpen desinformatie en fake-news te voorkomen.

Privacy
E-mail berichten worden standaard onversleuteld over internet verstuurd, omdat het e-mail protocol zelf niet in versleuteling voorziet. Daardoor kunnen derden gedurende het transport over het internet meelezen of scannen op sleutelwoorden. Met behulp van een set open 'pas toe of leg uit'-standaarden wordt het transport tussen e-mail servers alsnog versleuteld, zodat onbevoegden de e-mails niet mee kunnen lezen (STARTLS+DANE].
Een andere set standaarden ziet op de versleuteling van het *website* verkeer, zodat niet kan worden meegekeken wanneer een burger een overheidswebsite bezoekt (TLS+HSTS).
Verder wordt met de standaarden voorkomen dat de bewegwijzering op internet wordt omgezet, zodat je bij een bepaalde domeinnaam (zoals digid.nl) ook inderdaad bij een overheidsserver terechtkomt (DNSSEC), of die voorkomen dat de hele routering van internet verkeer naar een ander land wordt omgezet (rPKI). Ook in de backoffice helpen de standaarden voorkomen dat gegevens van burgers (bijvoorbeeld die in de basisregistraties) bij criminelen of vreemde statelijk actoren terecht komen (Digikoppeling).

Deze informatieveiligheid standaarden zijn ook onderdeel van de Baseline Informatiebeveiliging Overheid (BIO), waaronder de tool inkoopeisen cybersecurity overheid (ICO) en basisbeveiliging.nl

Cyberdreigingsinformatie
Informatiebeveiliging is een kat- en muisspel tussen ICT-ers/informatiebeveiligers en hackers. De veilige ICT-omgeving van vandaag, kan morgen nieuw ontdekte kwetsbaarheden blijken te bevatten. Daarom is de snelle uitwisseling van informatie over kwetsbaarheden en dreigingen essentieel, zodat gaten tijdig kunnen worden gedicht en inbraak voorkomen. Met de standaard STIX+TAXII kunnen cyber dreigingen internationaal efficiënt en snel publiek en privaat worden gedeeld.

Aanvullende acties in werkplan FS 2023

Naast de eerdergenoemde acties om de streefbeeldafspraken alsnog te behalen, wordt in samenwerking met andere (koepels van) overheden (zoals Strategisch Leveranciers Management Rijk) in gesprek gegaan met leveranciers die aan meerdere overheden leveren en bepaalde standaarden nog niet ondersteunen, om deze leveranciers te verzoeken om ondersteuning, en daarbij te wijzen op beschikbare how to's en te vragen om een concrete planning. Zo wordt ondermeer bij Microsoft aangedrongen op ondersteuning van DANE, conform eerdere toezegging. (Werkplan2023#3.2.2)

3. Iedereen heeft regie op het digitale leven

3.1 Regie op eigen gegevens

Elke burger moet zijn eigen gegevens bij de overheid en bedrijven zoveel mogelijk kunnen inzien, corrigeren en hergebruiken. Bovendien moet de burger zelf kunnen bepalen met wie hij/zij deze gegevens deelt zonder dat er iemand over je schouders mee kijkt. De overheid moet de kaders stellen om regie op gegevens te hebben en moet zelf het goede voorbeeld geven.

Verbetering met behulp van ‘pas toe of leg uit’ standaarden

Bij de technische vormgeving van deze regie door de burger zijn diverse standaarden van de lijst essentieel. Deze standaarden maken duidelijk hoe en welke informatie bij de overheid kan worden opgehaald (via de API’s), en betrouwbaar kan worden verzonden en uitgewisseld.

Hoe dan?

Overheidsgegevens over een burger, die deze wil uitwisselen met andere partijen, moet op een eenduidige en geharmoniseerde manier beschikbaar worden gesteld. Zodat apps of dienstverleners die burgers daarbij ondersteunen, niet bij elke gegevensbron opnieuw het wiel hoeven uitvinden. Daarom is de manier waarop die informatie (via API’s) wordt aangeboden geharmoniseerd (OAS, de Open Api Specificatie).

De uitwisseling van deze gegevens kan slechts plaatsvinden met geautoriseerde organisaties, servers en software. Daarnaast mag deze informatie ook onderweg niet in vreemde handen vallen. De digikoppeling standaard zorgt voor authenticatie van partijen die gegevens opvragen en aanbieden, en voor versleuteling onderweg.

Welke acties uit het Werkplan FS 2023?

Om mensen meer regie op hun gegevens te geven, wordt ondermeer een afsprakenstelsel gemaakt en een referentiearchitectuur Regie op Gegevens gemaakt. Het Forum Standaardisatie adviseert welke open standaarden (deels van de 'pas toe of leg uit'-lijst) daar onderdeel van uit zouden moeten maken, om de publieke waarden te waarborgen, en ook aan te kunnen blijven sluiten op internationale ontwikkelingen, zoals die in Europa.
(Werkplan2023#1.3)

3.2 Hoogwaardig identiteitsstelsel waaronder inlogmiddelen en een wallet

De maatschappelijke opgaves rond het digitale identiteitsstelsel liggen op het gebied van het makkelijker, betrouwbaarder en privacy vriendelijker maken van het digitaal zaken doen. Het is belangrijk dat digitale authenticatiemiddelen voldoende betrouwbaar zijn, voor de gegevens waartoe zij toegang geven. Daarnaast is het belangrijk dat er verschillende alternatieven bestaan en er internationale interoperabiliteit is, zodat er bijvoorbeeld ook van paneuropese diensten gebruik gemaakt kan worden in een andere EU-lidstaat.

Verbetering met behulp van 'pas toe of leg uit' standaarden

Om ervoor te zorgen dat meerdere alternatieve authenticatiemiddelen (ook uit andere lidstaten) ingezet kunnen worden bij verschillende digitale dienstverleners zijn afspraken nodig in de vorm van technische standaarden.

Hoe dan?

De technische interactie tussen burger, elektronische dienstverlener en (leveranciers van) authenticatiemiddelen vindt plaats in een afsprakenstelsel. Om ervoor te zorgen dat deze verschillende diensten en authenticatiemiddelen naadloos met elkaar samen kunnen werken (en er geen dialecten ontstaan) wordt gewerkt met de standaard Open ID-connect (OIDC), die aansluit op het Europese eID stelsel (EIDAS). Een profiel van OIDC is momenteel in procedure voor opname op de 'pas toe of leg uit'-lijst.

Welke acties uit het Werkplan FS 2023?

In de handreiking betrouwbaarheidsniveau's van het Forum Standaardisatie werd beschreven op welk betrouwbaarheidsniveau de elektronische identificatie van gebruikers bij bepaalde elektronische dienstverlening plaats zou moeten vinden. Een groot deel daarvan is gebruik als basis voor een Algemene Maatregel van Bestuur (AMvB) over het eID stelsel, onder de Wet digitale overheid (Wdo). De handreiking zal daarop geupdate worden. (Werkplan2023#1.4)

4. Een digitale overheid die waardengedreven en open werkt voor iedereen

4.1 Verbeteren informatiehuishouding voor openbaarheid van bestuur

Nederlandse overheidsorganisaties moeten open zijn: handelingen en besluiten moeten transparant, beargumenteerd en vindbaar zijn, zonder twijfels over juistheid of echtheid. Een gelijkwaardiger informatiepositie van burgers en organisaties helpt hen de overheid ter verantwoording te roepen en om belangen te behartigen, en draagt bij aan efficiëntie en effectiviteit.

Verbetering met behulp van 'pas toe of leg uit' standaarden

Om een adequate informatiehuishouding mogelijk te maken wordt erop ingezet dat "de overheidsinformatie duurzaam toegankelijk is voor openbaarmaking via uniforme en open standaarden (…)". Een set daarvan staat op de 'pas toe of leg uit'-lijst.

Hoe dan?

Iedereen moet kennis kunnen nemen van onderzoeken, overwegingen en besluiten van de overheid. Zoals eerder gezegd moet dat kunnen ongeacht van welk merk je software of hardware gebruikt, en ongeacht een eventuele lichamelijke beperking (de open standaarden pdf en WCAG, zie paragraaf 1.2).

Daarnaast is belangrijk dat de beweegredenen achter het handelen van de overheid duidelijk zijn. Aangezien overheidshandelen wordt gelegitimeerd door wet- en regelgeving, is het belangrijk dat de inhoud daarvan duidelijk is, evenals de verhouding tussen verschillende wet- en regelgeving en rechterlijke uitspraken daarover. Een set standaarden zorgt er voor eenduidige benamingen en verwijzingen van wet en regelgeving (BWB, JDCR) en relevante verwijzingen naar rechterlijke uitspraken (ECLI).

Verder moet de overheid zich telkens kunnen verantwoorden, bijvoorbeeld financieel, maar ook over verkiezingsuitslagen. Daar staan respectievelijk de standaarden XBRL en EML voor op de lijst.

Welke acties uit het Werkplan FS 2023?

Om de begrijpelijkheid en de (ict) uitvoerbaarheid en de onderlinge verhoudingen van wet- en regelgeving te verbeteren, wordt samen met uitvoeringsorganisaties en departementen de samenloop van wet- en regelgeving in een aantal praktijkcases geanalyseerd. Ondermeer om ongewenste samenloop inzichtelijk te maken. Daarbij helpt het Forum meer aan harmonisatie en afstemming van semantische begrippen (waar mogelijk) en uitvoeringsprocessen, en stimuleert tegelijkertijd multidisciplinaire iteratieve samenwerking tussen onder meer wetgevingsjuristen, beleid en (ICT)uitvoering. (Werkplan2023#1.1.1.)

4.2 Verbeteren gegevenshuishouding voor burgers en organisaties

Welke acties uit het Werkplan FS 2023?

De informatiehuishouding van overheids internetdomeinen is niet op orde, en overheidsorganisaties hebben onvoldoende zicht op hun overheids internet domein portfolio. Geschat wordt dat er meer dan 40.000 overheid internetdomeinnamen zijn, waardoor zowel burgers en bedrijven als overheidsorganisaties door de bomen het bos niet meer zien. Op basis van bestaande best-practices van onder andere VWS en AZ/DPC heeft het Forum een handreiking opgesteld, die ze helpt uit te rollen (Werkplan2023#1.1.1.).

Extra Kans

Het Forum kan helpen met het verbeteren van het delen van data tussen overheden en (semi-) publieke organisaties waaronder het federatief datastelsel en het toekomstbeeld Stelsel van Basisregistraties. Onder andere door afspraken over standaarden & nieuwe standaarden (of nieuwe versies van standaarden) op de 'pas toe of leg uit lijst'.

4.3 Versterken ICT-organisatie en -systemen van het Rijk

Acties uit het Werkplan FS 2023 & Extra Kans

Open standaarden vormen een essentieel onderdeel van “goed opdrachtgeverschap bij de Rijksoverheid voor IV-/IT-diensten en het faciliteren van innovatief inkoopbeleid waarin moderne eisen en wensen (bijvoorbeeld met betrekking tot Europese digitale soeveiniteit, standaarden en harmonisering, openheid/open source, etc.) stevig verankerd worden.”
Door het gebruik van open standaarden kan leveranciersafhankelijkheid worden beperkt (exit strategie) en digitale soevereiniteit worden gewaarborgd (data portabiliteit).
(Werkplan 2023#3.5.)