Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Aanbiedingsformulier Overheidsbreed Beleidsoverleg Digitaal Overheid

1. Korte titel	Standaardisatie: Monitor open standaarden 2022
2. Datum behandeling	OBDO 30 maart 2023 (SO OBDO 14 maart 2023)
3. Aard van de behandeling: *(dubbelklikken op vakje en 'ingeschakeld' aanvinken)*	☐ Scrum ☐ Hamerstuk ☒ Ter besluitvorming ☒ Ter bespreking ☐ Ter kennisname ☐ Anders: …….
4. Eerder behandeld in:	☒ PGDI ☒ DOD ☐ IDO ☐ MT- DO ☐ MT- DS ☐ MFG ☐ Werkagenda ☒ Anders: Forum Standaardisatie ☐ Niet Uitkomst behandeling in bovenstaand gremium: ☒ Overeenstemming *(geen toelichting vereist)* ☐ Geen overeenstemming
5. Voorgeschiedenis / context *6. Samenvatting/ toelichting*	Duiding en maatregelen op basis van de Monitor open standaarden 2022 Bijlagen: a. Monitor Open Standaarden 2022 (bijlage als link) b. Duiding en maatregelen monitor Open standaarden 2022 Forum Standaardisatie duidt de resultaten van de Monitor Open Standaarden 2022 als volgt: ook in 2022 is nog steeds te weinig toepassing van open standaarden in openbare aanbestedingen en is geen uitleg te zien in jaarverslagen hierover. In overheidsbrede voorzieningen gaat de toepassing van de relevante open standaarden wél goed. In ieder geval is meer focus nodig op standaarden voor web

	en e-mailbeveiliging en voor IPv6. De resultaten van de laatste meting naar het gebruik van deze standaarden kwamen al aan de orde in de vergadering van het OBDO op 1 december van 2022. De rest van de onderzoeksgegevens is nieuw. Het Forum stelt aan het OBDO voor de onderstaande vijf maatregelen te nemen, die aansluiten op de adviezen die het Forum al in december 2022 gaf naar aanleiding van de laatste meting van het gebruik van de informatieveiligheidstandaarden. Deze voorstellen zijn eerder dit jaar naar aanleiding van de Monitor van 2021 ook gedaan en zijn voor een belangrijk deel een herhaling hiervan. 1. @ OBDO: zorg dat de resultaten van de Monitor Open Standaarden 2022 en de Meting Informatieveiligheidstandaarden meer en beter gecommuniceerd worden met de achterban. Communiceer over het belang van open standaarden naar aanleiding van de resultaten van de Monitor Open Standaarden en de IV-meting in uw organisatie. Doe dat minimaal één keer per jaar. Voor de veiligheidsstandaarden minimaal twee keer per jaar. NIEUW: Maak hiertoe ook de besluiten van het OBDO zélf openbaar. In ieder geval wat betreft de besluitvorming over standaarden. Achterblijvers betwijfelen vaak de (mate van) verplichting en missen voldoende toegang tot bewijs wat er is afgesproken in het OBDO. Daarnaast past openbaarmaking in de geest van de Wet Open Overheid. 2. @ CIO Rijk en @ koepelorganisaties: communiceer de resultaten van de Monitor Open Standaarden 2022 en de Meting Informatieveiligheidstandaarden via de lijn van CIO's en CISO's en roep op tot verbetering. 3. @ CIO Rijk en @ koepelorganisaties: onderzoek in 2023 hoe CIO Rijk en koepelorganisaties de naleving van 'pas toe of leg uit' voor open standaarden verder kunnen stimuleren/ faciliteren en wat hiertoe overheidsbreed via het OBDO gedaan kan worden. NB: Deze derde maatregel is in lijn met de afspraak die gemaakt is op 1 december 2022 naar aanleiding van de bespreking van de IV-meting van voorjaar 2022. Toen is in het OBDO al afgesproken dat CIO-Rijk (trekker) in samenwerking met VNG, Manifestgroep en BZK/Digitale Overheid een ('licht') plan van aanpak zal opstellen, waarmee collectief door het OBDO op adoptie bij achterblijvers kan worden gestuurd. 4. Verweef de aandacht voor open standaarden in reeds bestaande kaders. 5. Zie toe op uitleg in het jaarverslag als 'pas toe of leg uit'- standaarden niet worden toegepast. De kracht zit in de herhaling en in een meervoudige, gelaagde aanpak: de hiergenoemde – deels ook al naar aanleiding van eerdere monitoren voorgelegde – maatregelen zijn aanvullend op eerder genoemde besluiten. Zo heeft het OBDO in december 2022 naar aanleiding van de Meting Informatieveiligheidstandaarden besloten dat CIO-Rijk een concept Plan van Aanpak opstelt waarmee het OBDO gaat sturen om bij de achterblijvers de adoptie van deze standaarden (waarvoor streefbeeldafspraken met inmiddels verlopen uiterlijke implementatiedata gelden) op orde te krijgen en dit plan voor een volgende OBDO-vergadering te agenderen.

	Eerder op 7 april besloot het OBDO dat in de overzichten van de Metingen Informatieveiligheidstandaarden voortaan ook een naming&shaming-volgorde zal worden gehanteerd en dat een gesprek met de Audit Dienst Rijk (ADR) zal plaatsvinden. Naar aanleiding van de laatste Meting Informatieveiligheidstandaarden zijn eind november 2022 Kamervragen aan de Minister van JenV en aan de Staatssecretaris BZK gesteld. De Staatssecretaris BZK geeft in antwoord aan dat ze *"het onacceptabel [vindt] dat overheden dit niet op orde hebben en per brief, via de koepelorganisaties, alle overheden [zal] oproepen zo snel mogelijk de standaarden te implementeren."* Daarnaast meldt ze: *"Ook zijn veel organisaties afhankelijk van hun externe leverancier. Zo biedt de meest gebruikte cloudmail-provider van de overheid default geen IPv6 en geen DANE. […] De implementatie van deze standaarden is door Microsoft steeds in tijd opgeschoven. SLM [(Strategisch Leveranciers Management Rijksoverheid)] en Forum Standaardisatie hebben Microsoft opnieuw gewezen op de verplichting voor de Nederlandse Overheid deze standaard toe te passen en hebben Microsoft gevraagd de huidige ultieme invoerdatum van juli 2023 hoe dan ook te garanderen. Het blijft belangrijk dat overheden hun leverancier aanspreken op tekortkomingen en zo nodig overstappen naar een leverancier die de standaard wel goed ondersteunt."*
7. Beslispunten/ discussiepunten	Monitor open standaarden 2022 en notitie duiding en maatregelen Het OBDO stemt in met: o de duiding die het Forum Standaardisatie geeft aan de Monitor Open Standaarden 2022 en de maatregelen die het Forum op basis hiervan voorstelt (zie hierboven onder 3), waaronder het voorstel de besluiten van het OBDO openbaar te maken, in ieder geval voor wat betreft de besluitvorming over standaarden.
8. Contactgegevens	Inhoud: 2. Monitor Open Standaarden 2022, Désirée Castillo Gosker (adviseur) [06-52504226] Proces: Joram Verspaget (bureausecretaris) [06-52845592]

Notitie

Monitor Open Standaarden 2022

Duiding en maatregelen

Aan:	OBDO
Van:	Forum Standaardisatie
Datum:	23 februari 2023
Versie:	1.0
Bijlage:	Monitor Open Standaarden 2022

Ter bespreking en besluitvorming

Het OBDO wordt gevraagd om:

- in te stemmen met de duiding van de Monitor Open Standaarden 2022 en met de voorgestelde maatregelen, waaronder het openbaar maken van de besluiten van het OBDO

Duiding

De ambitie om publieke waarden te borgen in de digitale wereld kunnen overheidsorganisaties niet waarmaken zonder daarvoor óók de standaarden van de 'pas toe of leg uit'- lijst toe te passen. Interoperabiliteit, leveranciersonafhankelijkheid, digitale soevereiniteit, innovatie, inclusie, veiligheid, vindbare en toegankelijke data, allemaal redenen om de publieke ruimte in de digitale wereld te verbeteren en om de standaarden die hiervoor zijn ook daadwerkelijk in te zetten. Daarom monitort Forum Standaardisatie jaarlijks het gebruik van de standaarden met de status 'pas toe of leg uit'.

Ook in 2022 richtte het onderzoek zich op drie onderdelen:

1. De vraag naar open standaarden in openbare aanbestedingen en de uitleg in de jaarverslagen.
2. Het gebruik in voorzieningen van de Generieke Digitale Infrastructuur.
3. Overige gebruiksinformatie, waaronder de halfjaarlijkse IV-meting van de standaarden waarvoor streefbeelden zijn afgesproken in het OBDO.

Forum Standaardisatie duidt de resultaten van de Monitor Open Standaarden 2022 als volgt:

Ook in 2022 nog steeds te weinig toepassing van open standaarden in openbare aanbestedingen en geen uitleg in jaarverslagen.

Het resultaat van de Monitor Open Standaarden van 2022 laat – als het gaat om aanbestedingen en jaarverslagen gaat- hetzelfde beeld zien als in voorgaande jaren. Uit het onderzoek naar de

vraag om de relevante open standaarden in aanbestedingen blijft het gebruik rond de 50% schommelen. Dat betekent, is een standaard relevant – en heel vaak betreft dit een veiligheidsstandaard- dan is de kans circa 50% dat de standaard ook daadwerkelijk gevraagd wordt in een publieke aanbesteding. Dat is te weinig, vooral gelet op de heersende veiligheidsrisico's.

Ook het onderzoek naar jaarverslagen levert het zelfde beeld op als in voorgaande jaren. Organisaties verantwoorden zich niet in het jaarverslag als zij standaarden niet toepassen, terwijl dat wel had gemoeten Dat betekent niet alleen dat het 'pas toe of leg uit'- beleid hier slecht wordt nageleefd, maar dat geldt ook voor de rijksbegrotingsvoorschriften op dit punt (voor zover het rijksorganisaties betreft).

Het Forum Standaardisatie vat deze resultaten op als een aanwijzing voor nog te onvolwassen ICT-opdrachtgeverschap in de publieke sector in het algemeen en bij overheidsorganisaties in het bijzonder. Daarnaast dat bestuurlijke sturing en toezicht op het gebruik van open standaarden ontbreekt en/of de werkvloer nog onvoldoende bereikt als het gaat om aanbestedingen.
Het zou helpen als besluiten van het OBDO openbaar gepubliceerd worden.
Daarnaast wordt uit het aanbestedingenonderzoek duidelijk dat dat organisaties in de loop der jaren steeds meer cloudoplossingen inzetten. Voor zover die oplossingen de open standaarden (nog) niet volgen, belemmert dat de adoptie. Daarnaast brengen cloudoplossingen nieuwe uitdagingen met zich mee, rond behoud van data, en exit-strategie.

Toch zijn er ook in 2022 weer enkele uitstekende aanbestedingen te vinden als het gaat om het correct vragen om open standaarden. Die zullen later als goede voorbeelden op de website van het Forum Standaardisatie gepubliceerd worden bij de uitstekende aanbestedingen van 2021 en 2020:

De best scorende aanbestedingen (Monitor 2021) | Forum Standaardisatie

De best scorende aanbestedingen van 2020 | Forum Standaardisatie

In overheidsbrede voorzieningen gaat het wél goed.

Beheerders van voorzieningen van de Generieke Digitale Infrastructuur laten een zonniger beeld zien. Hier is de toepassing van de relevante open standaarden wél goed vooruit gegaan in de loop der jaren en is inmiddels behoorlijk op peil. De voorzieningen die in 2022 onderzocht zijn, laten een percentage zien van 81%. Dat wil zeggen; is een standaard relevant voor een voorziening dan wordt die in 81 % van de gevallen ook daadwerkelijk toegepast. Daar komt bij, dat voor de nog ontbrekende standaarden vaak plannen bestaan om de ontbrekende standaarden alsnog toe te passen. Dat stemt optimistisch.

Het Forum Standaardisatie constateert dan ook dat het met het gebruik van open standaarden in generieke overheidsvoorzieningen vrij goed gaat. Het uitvoeren van het monitoronderzoek zélf, heeft daar waarschijnlijk ook een rol in gespeeld, doordat de onderzoekers regelmatig terug komen bij dezelfde groep mensen, die vaak ook het belang van het gebruik van open standaarden goed begrijpen. Het blijft ook hier wel een uitdaging om ook achterblijvende resterende procenten in te lopen.

De plannen voor de inrichting van de GDI zijn om in de toekomst minder op voorzieningen in te zetten en meer op afsprakenstelsels en standaarden. Hoewel het Forum Standaardisatie uiteraard meer inzet op standaarden toejuicht, kan het ook een risico voor verlies van centrale aanspreekpunten en daarmee structurele aandacht voor open standaarden binnen de GDI betekenen. Het is daarom extra belangrijk uitvoering te geven aan de maatregelen waar het OBDO op 7 april 2022 al mee ingestemd heeft en die hieronder zullen worden herhaald. Namelijk het structureel toewijzen van de verantwoordelijkheid en de aandacht hiervoor aan CIO's, CTO's en CISO's. Meer hierover hieronder bij de maatregelen.

Vooral meer focus nodig op standaarden voor web en e-mailbeveiliging en voor IPv6

In de Monitor Open Standaarden 2022 is de laatste meting opgenomen van de informatie veiligheidsstandaarden waar het OBDO naast het 'pas toe of leg uit'- beleid aanvullende streefbeeldafspraken voor heeft gemaakt. Naar aanleiding hiervan blijft het Forum Standaardisatie met klem waarschuwen voor beveiligingsrisico's rond het nalaten van de toepassing van verplichte web- en e-mailstandaarden en IPv6.

De IV-meting van voorjaar 2022 laat zien dat bij 53% van de internetdomeinen alle verplichte websitestandaarden correct zijn toegepast. Het gaat om belangrijke beveiligingsstandaarden voor vertrouwelijk webverkeer, en IPv6 voor duurzame bereikbaarheid van online diensten.

Bij 44% van de internetdomeinen zijn alle verplichte e-mailstandaarden correct toegepast. Hier gaat het om belangrijke beveiligingsstandaarden om e-mailvervalsing uit naam van de overheid te voorkomen en het e-mailverkeer vertrouwelijk te houden, en ook IPv6 voor duurzame bereikbaarheid van online diensten.

Met de meting zijn in totaal 2584 overheidsdomeinen gecontroleerd. Dat is een uitbreiding ten opzichte van voorgaande metingen, in de voorgaande meting zijn 559 overheidsdomeinen gecontroleerd. De 2584 overheidsdomeinen zijn slechts een deelwaarneming van alle overheidsdomeinen, het totaalportfolio heeft vele duizenden meer domeinen. De overheid heeft als geheel geen zicht op het totaalportfolio. Dit rapport toont met diverse doorsnedes inzicht in de stand van zaken per overheidscategorie en per ministerie. De mate van adoptie kan gezien worden als een indicator voor de effectiviteit van sturing op kwaliteit van de informatievoorziening.

Zeven jaar na het maken van de eerste streefbeeldafspraak, en ruim twee jaar na het maken van de laatste, is geen van de streefbeelden voor de overheid als geheel gehaald. Het ontbreekt aan effectieve sturingsmechanismen om overheidsbrede afspraken eenduidig te laten landen en nageleefd te krijgen bij achterblijvende individuele overheidsorganisaties.

Zodra de Wet Digitale Overheid van kracht wordt kunnen standaarden wettelijk worden verplicht, zoals reeds is voorgenomen met HTTPS en HSTS. Ook hier speelt dan vervolgens de vraag hoe deze verdergaande verplichtingen de operationele werkvloer bereiken, en hoe vervolgens gestuurd wordt op naleving van de verplichtingen.

Maatregelen en adviezen

Gelet op bovenstaande duiding adviseert Forum Standaardisatie aan het OBDO:

1) @ OBDO: zorg dat de resultaten van de Monitor en de IV meting meer en beter gecommuniceerd worden met de achterban.

   Communiceer over het belang van open standaarden naar aanleiding van de resultaten van de Monitor Open Standaarden en de IV-meting in uw organisatie. Doe dat minimaal één keer per jaar. Voor de veiligheidsstandaarden minimaal twee keer per jaar.

   NIEUW: Maak hiertoe ook de besluiten van het OBDO openbaar, ten minste die besluiten die genomen zijn naar aanleiding van de adviezen van het Forum Standaardisatie.

   Achterblijvers betwijfelen vaak de verplichting en missen voldoende toegang tot bewijs wat er is afgesproken in het OBDO. Daarnaast past openbaarmaking in de geest van de Wet Open Overheid.

2) @ CIO rijk en @ koepelorganisaties: communiceer de resultaten van de monitor open standaarden 2022 en de IV-meting via de lijn van CIO's en CISO's met de achterban en roep op tot verbetering.

3) @ CIO rijk en @ koepelorganisaties: onderzoek in 2023 hoe CIO rijk en koepelorganisaties de naleving van 'pas toe of leg uit' voor open standaarden verder kunnen stimuleren/ faciliteren en wat hiertoe overheidsbreed via het OBDO gedaan kan worden.

Bij voorbeeld door ook na te gaan welke (delen van de) adviezen overheidsbreed via de OBDO-lijn opgepakt zouden moeten worden (bijvoorbeeld via de lijn van de Architectuurraad).

NB: Deze derde maatregel is in lijn met de afspraak die gemaakt is op 1 december 2022 naar aanleiding van de bespreking van de IV-meting van voorjaar 2022. Toen is in het OBDO al afgesproken dat CIO-Rijk (trekker) in samenwerking met VNG, Manifestgroep en BZK/Digitale Overheid een ('licht') plan van aanpak zal opstellen, waarmee collectief door het OBDO op adoptie bij achterblijvers kan worden gestuurd.

4) Verweef de aandacht voor open standaarden in reeds bestaande kaders

De aandacht voor verplichte open standaarden moet structureel in bestaande kaders verweven zijn en het onderwerp belegd bij de functies van CIO, CISO en CTO.
a. Kaders rond i-Control & ICT-kwaliteitsaspecten (CIO's)
b. Informatiebeveiliging (BIO) en bedrijfsvoering (CISO's)
c. Aanschaf en inkoop (gebruik de Beslisboom Open Standaarden)
d. Architectuurkaders (zoals NORA, en Enterprise Architectuur Rijk)

5) Zie toe op uitleg in het jaarverslag als 'pas toe of leg uit'- standaarden niet worden toegepast.

@OBDO, zie toe op correct uitleggen met een zwaarwegende reden in het jaarverslag bij het achterwege laten van relevante standaarden. In ieder geval als de organisatie onderwerp van onderzoek is geweest in de Monitor Open Standaarden en de IV-meting, zoals voor het Rijk is dit geregeld in de toelichting op de bedrijfsvoeringsparagraaf van de Rijksbegrotingsvoorschriften.

De kracht zit in de herhaling:

Het OBDO heeft op 1 december 2022 besloten dat CIO-Rijk een concept Plan van Aanpak opstelt, waarmee het OBDO gaat sturen om de adoptie bij de achterblijvers bij de streefbeeldafspraken op orde te krijgen. Eerder op 7 april 2022, besloot het OBDO dat daartoe in de meetoverzichten ook een naming & shaming volgorde zal worden gehanteerd, en een gesprek met de ADR zal plaatsvinden. De hiergenoemde – deels ook al naar aanleiding van eerdere monitoren voorgelegde – maatregelen zijn hierop aanvullend.

Deze maatregelen vullen ook de volgende meer specifieke vier adviezen aan, die eerder in december 2022 naar aanleiding van de laatste IV-meting zijn gegeven en hier in het kader van de Monitor Open Standaarden 2022 worden herhaald.

Advies 1: Onderzoek welke sturingsmechanismen kunnen worden ingezet om overheidsbrede architectuurafspraken en kwaliteitseisen (beleid) – bijvoorbeeld in de vorm van gemeenschappelijke standaarden en streefbeeldafspraken – effectief te laten landen in de uitvoering bij de individuele overheidsorganisaties (implementatie).

Toelichting:
Positieve uitschieters binnen overheidscategorieën en tussen ministeries zijn vaak te verklaren vanuit proactieve sturing (regie) op de toepassing van standaarden, bijvoorbeeld vanuit een CIO- of CISO-office (voorbeelden: CIO BZK en CISO VWS).

Advies 2: Organiseer regie op internetdomeinen binnen ministeries en individuele overheidsorganisaties. Jaag dit initieel project- of programmamatig aan, en borg dit vervolgens in de lijnorganisatie.

> Toelichting:
> Proactieve sturing op de omvang en kwaliteitsaspecten van het internetdomeinportfolio is noodzakelijk om risico's voor zowel organisaties als burgers te kunnen beheersen. Als handreiking heeft Forum Standaardisatie vijf basisprincipes voor regie op internetdomeinen op een rij gezet. Voor de Rijksoverheid heeft het Rijksprogramma voor Duurzaam Digitale Informatiehuishouding (RDDI), in samenwerking met Forum Standaardisatie, in 2021 de Handreiking Beheer Internetdomeinen Rijksoverheid gepubliceerd.

Advies 3: Verken of het centrale dienstverleningsconcept rond DNS-beheer van de rijksoverheid (let op: dit gaat over DNS incl. domeinnaamregistratie, niet over het eventueel invoeren van één domeinnaamextensie) ook kan worden ingezet bij decentrale overheden, bijvoorbeeld door samenwerkingsverbanden.

> Het komt regelmatig voor dat websites of e-maildiensten decentraal ingekocht worden, terwijl er centrale (overheids)dienstverlening bestaat waarmee dezelfde diensten efficiënter geleverd kunnen worden. Dat geldt soms zelfs binnen organisaties.
> Met regie op internetdomeinen kan er beter op gestuurd worden dat centrale dienstverlening ook wordt benut.
>
> Toelichting:
> (Gedeeltelijke) centralisering van dienstverlening heeft veelal een positief effect op de toepassing van standaarden. Wanneer een gemeenschappelijke dienstverlener een standaard consequent toepast heeft dit een hefboomeffect. Dit is zichtbaar bij diverse dienstverleningsconcepten; bijvoorbeeld de centrale registrarrol die de Dienst Publiek en Communicatie (AZ/DPC) vervult voor de Rijksoverheid, maar ook bij gemeenschappelijke dienstverleners voor web en e-maildiensten, zoals SSC-ICT, DICTU en diverse regionale dienstverleners.

Advies 4: Zorg ervoor dat naleving van IT-kwaliteitseisen – waaronder ondersteuning van verplichte open standaarden – onderdeel zijn van het leveranciersmanagement van individuele overheidsorganisaties. Vraag leveranciers periodiek naar de planning voor ondersteuning van standaarden. Overweeg om over te stappen als een leverancier onvoldoende meebeweegt.

Extra aandachtspunt daarbij is dat overheden hun e-mailvoorzieningen steeds vaker uit aan clouddienstverleners. Een aantal van dit soort dienstverleners ondersteunen niet alle verplichte standaarden. Conform het open standaardenbeleid zou formeel moeten worden gekozen voor dienstverlening die de standaarden wel ondersteunt. Indien hiervan is afgeweken is het belangrijk dat overheden hun dienstverleners alsnog blijven vragen om ondersteuning van verplichte standaarden. Diverse dienstverleners geven in informele gesprekken aan dat een gebrek aan klantvraag een reden is om niet te investeren in ondersteuning van de voor overheid verplichte standaarden.