



# Notitie

FORUM STANDAARDISATIE 8 december 2021

Agendapunt 4C1

Duiding en maatregelen monitor open standaarden 2021

Nummer: FS 20211208.4C1

Aan: Forum Standaardisatie

Van: Bureau Forum Standaardisatie

Datum: 25 november 2021

Versie: 1.0

Bijlagen: FS-20211208.4C2-Monitor-Open-standaarden-2021-v1.0

## Ter besluit

### **Het Forum Standaardisatie wordt gevraagd om:**

- In te stemmen met de duiding van de Monitor, inclusief het advies over de voorgestelde maatregelen, ter doorgeleiding aan het OBDO.

## Duiding

Meer interoperabiliteit & leveranciersafhankelijkheid, veiligheid, toegankelijkheid en datakwaliteit vraagt om meer bewuste, bestuurlijke inzet van open standaarden. Uit de laatste cijfers van de Monitor open standaarden van 2021 blijkt dat het gebruik van de open standaarden van de 'pas toe of leg uit'-lijst weliswaar toeneemt, maar erg langzaam. Te langzaam volgens het Forum Standaardisatie. Er is meer bestuurlijke inzet nodig.

## Noodzaak van bestuurlijke aandacht

Open standaarden zorgen voor interoperabiliteit: voor de vloeiende uitwisseling van vindbare, toegankelijke en begrijpelijke gegevens. Bovendien beperkt hun toepassing de afhankelijkheid van afzonderlijke leveranciers per systeem, helpen ze een vrij speelveld te scheppen. De historisch gegroeide afhankelijkheid van gesloten systemen (zonder die open standaarden) of van hun leveranciers is een belangrijke hindernis voor vernieuwing van oudere systemen én voor een open speelveld bij aanbestedingen. Dat leidt tot hogere kosten en tot risico's in veiligheid en beschikbaarheid: data-diefstal en gijzeling van de systemen van organisaties doordat hackers de bedrijfsvoering stil leggen komen regelmatig in het nieuws.

Inzet van open standaarden helpt hierbij. Dat is niet altijd eenvoudig, maar het feit dat verschillende overheden wél de afgesproken norm halen laat zien, dat naleving van de

standaarden wel degelijk mogelijk is. Mits daar consequent op wordt gestuurd in het beheer en de aanbesteding van ICT.

Uit gesprekken is gebleken dat afzonderlijke inkopers of goedwillende projectleiders de oude patronen niet altijd kunnen doorbreken, waardoor de open standaarden in de praktijk te vaak worden gepasseerd. Dus zijn bestuurders nu aan zet. Zowel interbestuurlijk (met andere organisaties) als intern (binnen de eigen organisatie).

Bij de Monitor 2016 is al gerapporteerd dat het voldoen aan sommige standaarden alleen kan als alle schakels in de keten meewerken. Anders kunnen meerdere voorzieningen niet voldoen aan de standaard, doordat één partij verstek laat gaan. Deze keer wijst het Forum erop dat die noodzakelijke afstemming ook binnen elke eigen organisatie geldt. Met name binnen grotere organisaties blijkt het lastig om hiervoor alle disciplines tijdig, blijvend en vruchtbaar bij elkaar te brengen. Tenminste de afdelingen voor beleid, praktijk, ICT en Inkoop hebben elkaar nodig voor een goede aanbesteding, vaak met nog andere disciplines. Wanneer het bestuur zo'n integrale aanpak niet actief nastreeft, dan komt die van onderop slechts moeizaam of niet tot stand. Interviews voor de monitor met de 'eenzame' trekker (projectleider of inkoper) getuigen hiervan. Rugdekking uit de bestuurlijke top om de standaarden prioriteit te geven wordt dan gemist, terwijl de naleving niet zou mogen afhangen van hun individuele of persoonlijke inzet.

Het verzuim om deze afspraken uit te voeren wringt ook met het beginsel, dat burgers en bedrijven erop mogen vertrouwen dat de overheid zich aan zijn eigen afspraken houdt. Denk aan leveranciers die zien dat de uitvraag van open standaarden wel met de mond wordt beleden, maar dat er als het erop aankomt toch wordt gekozen voor aanbiedingen van concullega's die de standaarden niet (allemaal) ondersteunen. Die ongeloofwaardigheid tast opdrachtrelaties aan.

## Voorbeelden van achterstanden: beveiliging en IPv6-adressen

Vorig jaar heeft het Forum Standaardisatie met klem gewaarschuwd voor beveiligingsrisico's rond het nalaten van de verplichte e-mailstandaarden. Bij vijf daarvan (die tegen phishing) ligt de toepassing nu wel op 94% of hoger. Vier andere blijven echter nog steeds steken op 55%-74%, met kwetsbaarheid voor kwaadwillende inbreuken als gevolg. Het resultaat daarvan komt regelmatig in het nieuws.

Los van veiligheid loopt ook de gewone bereikbaarheid gevaar, omdat de oude IPv4-adressen opraken. De bereikbaarheid via nieuwe IPv6-adressen (dat is één van de standaarden) groeide wel van 64% naar 79% voor websites en van 17% naar 40% voor email, maar het OBDO-streefbeeld van 100% in 2021 is nog niet in zicht. Dat brengt dus de feitelijke bereikbaarheid van de overheid via internet in gevaar. Ook hiervoor zijn de bestuurders aan zet, om prioriteit aan vernieuwing van hun IT-systemen te geven.

Bij het verschijnen van deze nieuwe Monitor merkt het Forum Standaardisatie op dat de beslissende invloed ligt bij bestuurders van publieke organisaties zelf. Het ligt voor de hand dat de CIO, de CISO of andere portefeuillehouder ICT in elke overheidsorganisatie deze handschoen opneemt. Die heeft immers zeggenschap over de kwaliteitskaders, en kent de uitvoerders/opdrachtgevers in de eigen organisatie. De rol van het Forum is prikkelen, helpen en informeren; dus niet regelen, uitvoeren, bewaken of handhaven.

De onderzoekers van de monitor hebben het gebruik van de standaarden in 2020 besproken met inkopers en met beheerders van overheidsbrede voorzieningen. Daaruit bleek helaas een aanzienlijke kennisachterstand. Na 15 jaar "pas toe of leg uit"- beleid leven er toch nog diverse misverstanden over de toepassing van de open standaarden. Bijvoorbeeld dat iedere organisatie alsnog zelf zou mogen afwegen of ze de standaarden gaat toepassen. Of dat die "leg uit" bij afwijking niet op schrift in het jaarverslag zou hoeven, maar ook achteraf (uit het hoofd) kan worden geconstrueerd. Met de volgende maatregelen stelt het Forum Standaardisatie voor om hier verandering in te brengen.

## Maatregelen

Gelet op bovenstaande overwegingen adviseert Forum Standaardisatie aan bestuurders van het OBDO:

- 1) Het is van belang de resultaten van de monitor open standaarden en de IV-meting in uw organisatie en achterban terug te leggen, met het oog op adoptie bij de achterblijvers<sup>1</sup>.  
Er zijn goede ervaringen met het bespreken van de meerwaarde voor maatschappij en organisatie in departementale en koepelgremia. Het Forum Standaardisatie helpt graag bij een op maat gesneden bespreking, aan de hand van voor dat gremium relevante meetresultaten.
- 2) Het is daarbij goed om de verplichte open standaarden te verweven in bestaande kaders, zoals
  - 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).

De ervaring leert dat met een dergelijke aanpak veel winst behaald kan worden. Zo heeft VWS een methode rond domeinnaamregie (op orde krijgen van web- en emaildomeinen) ontwikkeld, jaagt de Nationale Politie de adoptie van de iv-standaarden bij haar ketenpartners aan, en heeft CIO-BZK opdracht gegeven voor een BZK-breed project rond haar domeinnamen. Daarnaast heeft HIS het Forum Standaardisatie een aantal keer gevraagd om mee te denken over relevante standaarden in het Programma van Eisen bij grote verwervingen. Bij gemeenten zijn de standaarden meegenomen in de GIBIT & modelovereenkomsten. Verder leidt verweving in de BIO ertoe dat duidelijk is wat de standaarden aan informatieveiligheid bijdragen, en wordt 'stapeling van kaders' voorkomen. De toepassing van de standaarden draait dan mee in bestaande plan-&control-cyclus.

Deze aanpak is echter nog niet overal doorgevoerd. Om die reden wordt voorgesteld de sturing op de toepassing van standaarden via CIO's en ICT-opdrachtgeverschap (de kaderstellende vraagkant) te versterken. Dat kan bijvoorbeeld door open standaarden op te nemen in toetskaders. Om dit te realiseren kan gebruik worden gemaakt en geleerd van bovengenoemde en andere bestaande goede ervaringen ('good practices').

- 3) Extra aandacht te genereren voor de achterblijvende adoptie van open standaarden, door een vraaggestuurd onderzoek op dat punt aan te vragen bij de Rekenkamer.

---

<sup>1</sup> Dat sluit aan bij de taak uit het instellingsbesluit OBDO art 4 lid 2.