

Antwoorden op de zeven vragen van het IAK

***Ter onderbouwing van
het voorstel tot verplichting van het gebruik van open standaarden
in de wet voor de Generieke Digitale Infrastructuur***

Laatste versie: 23 maart 2016,

Aan: de werkgroep en de toetsgroep Wgdi

Van: Arnold Reinders, Frank Heijligers, Harry Wever, Stephan Klaassen (BZK)
Kristel Wattel (EZ)
Ludwig Oberendorff en Désirée Castillo Gosker (BFS)

Versiebeheer 1.4 (toetsgroep)

Vraag 1: aanleidingInleiding: GDI en open standaarden

Als een Navajo indiaan en een Achterhoeker met elkaar spreken zullen ze elkaar niet verstaan. Zo is het ook met informatieverwerkende systemen: als het ene systeem uitsluitend XML spreekt en het ander alleen JSON verstaat, hebben ze een probleem. Alleen als wordt afgesproken welke taal beide systemen met elkaar zullen spreken kunnen ze elkaar verstaan, dit noemen we standaardiseren. Standaardiseren gaat echter verder: het gaat niet alleen over die twee systemen, maar over alle relevante systemen die met elkaar moeten spreken. Dit stuk gaat over de noodzaak dat ICT-systemen elkaar verstaan. De argumentatie daartoe is opgebouwd uit vier stappen:

- I. ICT gedijt niet zonder standaarden. De oplossing is standaarden te gebruiken;
- II. Sommige standaarden hebben ongewenste bijeffecten, zoals leveranciersafhankelijkheid, hoge kosten en gebrek aan marktwerking. De oplossing is gelegen in het gebruiken van *open* standaarden. Dit is daarom ook staand kabinetsbeleid;
- III. Sommige open standaarden worden onvoldoende toegepast of er bestaan keuzemogelijkheden. Dit heeft gevolgen voor de beveiliging, kosten en marktwerking. De oplossing hiervan is gelegen in sterker bevorderen van open standaarden en is mede aanleiding geweest voor het opstellen van de pas-toe-of-leg-uit lijst;
- IV. Voor sommige standaarden is bevorderen van gebruik niet voldoende. De gevolgen daarvan kunnen ernstig zijn: de rechtszekerheid van de burger kan gevaar lopen, betrouwbaarheid en veiligheid van gegevens kunnen in het geding zijn, de kosten hoog en de marktwerking te gering. De oplossing hiervoor is gelegen, na afweging, in wetgeving.

Punt IV is het onderwerp van dit IAK. Soms zal worden teruggегреpen op de ervaringen van de voorafgaande punten.

I. ICT gedijt niet zonder standaarden

De Generieke Digitale Infrastructuur (GDI) is het digitale wegennet, inclusief verkeersregels waarbinnen overheidscommunicatie zich begeeft als het over organisatiegrenzen heen en weer gaat. Het digitale verkeer kan zich richting andere bestuursorganen begeven of van en naar burgers en bedrijven. Digitale overheidscommunicatie moet veilig zijn, betaalbaar en moet een vertaling bevatten van oude waarborgen naar de digitale wereld. Denk bij het laatste bijvoorbeeld aan het briefgeheim. Kortom: overheidscommunicatie via de GDI moet goed werken en passen in de open samenleving die we voorstaan. Een noodzakelijke randvoorwaarde daarvoor is dat de ICT-systemen van samenwerkende bestuursorganen elkaar kunnen verstaan en probleemloos op elkaar aansluiten, ook al zijn hun ICT-systemen afkomstig van verschillende leveranciers. Daarom zijn standaarden noodzakelijk.

Standaarden zijn afspraken, vastgelegd in een specificatiedocument, en beschrijven hoe gegevens eruit zien, wat ze betekenen en hoe ze kunnen worden uitgewisseld. Door standaarden te gebruiken begrijpen partijen hoe gegevens moeten worden gelezen en geïnterpreteerd. Zonder gebruik van die standaarden is gegevensuitwisseling niet mogelijk. Net zoals bij de fysieke infrastructuur is het essentieel om duidelijk te hebben aan welke afspraken de aanbieders en gebruikers van de digitale infrastructuur zich moeten houden. Zo is het voor de veiligheid en de efficiënte doorstroming op straat van belang dat mensen rechts rijden, stoppen bij rood licht en weer gaan rijden bij groen licht. Zonder deze afspraken loopt het verkeer vast en gebeuren er ongelukken. Zonder afspraken loopt het digitale verkeer ook vast, is het verkeer onveilig en kost deelnemen aan het verkeer onnodig veel geld¹. Echter standaardiseren zonder meer levert nieuwe problemen op: de belangrijkste zijn leveranciersafhankelijkheid en gebrek aan kostenbeheersing. Daarom heeft de Nederlandse overheid in 2007 besloten om een op *Open Standaarden* gericht beleid te voeren².

II. Open standaarden vermijden een aantal bijeffecten van standaarden

Open standaarden zijn standaarden die vrij te gebruiken zijn, waarvan de specificaties vrij opvraagbaar zijn (eventueel tegen een redelijke vergoeding³) en die ontwikkeld en beheerd worden op een open en toegankelijke manier. Open standaarden worden vrij van licentierechten toegepast en gebruikt. Door deze kenmerken zorgen open standaarden voor meer keuzevrijheid en daarmee minder afhankelijkheid van leveranciers. Om deze redenen is sinds 2007 het gebruik van open standaarden staand kabinetsbeleid.

Het belang van open standaarden wordt al sinds 2002 consequent benadrukt door de politiek. In 2002 werd kamerbreed de motie Vendrik aangenomen, met onder andere als doel om vanaf 2006 alleen nog maar met open standaarden te werken⁴. Omdat sommige bestuursorganen nog altijd met gesloten standaarden werken dringt de Tweede Kamer in 2007 aan om het gebruik van open standaarden te versnellen. In 2007 heeft het kabinet het actieplan NOIV vastgesteld⁵, en sinds 2008 geldt voor bestuursorganen een 'pas toe of leg uit' regime⁶. In 2011 concludeerde de Algemene Rekenkamer⁷ dat het open standaardenbeleid te vrijblijvend is. Dat constateert ook de parlementaire onderzoekcommissie ICT (de commissie Elias) in oktober 2014 in haar eindrapportage, en

¹ Zie bijlage E voor voorbeelden.

² *Kamerstukken II 2007/08*, 26643, nr. 98.

³ Voor het gebruik van een open standaard mogen geen licentiekosten worden gevraagd. Hierop wordt getoetst bij plaatsing op de lijst. Wél mag voor de beschikbaarstelling van de specificaties een redelijke vergoeding gevraagd worden die in verhouding moet staan voor de gemaakte kosten. De kosten mogen niet te hoog zijn want mogen niet leiden tot onacceptabele belemmeringen. Het bedrag hiervoor is niet exact te noemen.

⁴ *Kamerstukken II 2002/03*, 28600 XIII, nr. 30.

⁵ *Kamerstukken II 2007/08*, 26643, nr. 98.

⁶ de Rijksinstructie (2008), Rijksbegrotingsvoorschriften, iNUP-Resultaatafspraak 20, de Richtlijnen commissie BBV, en een verlengingsafspraken in het Nationaal Beraad. Zie Bijlage D.

⁷ Open standaarden en opensourcesoftware bij de rijksoverheid, 15 maart 2011

beveelt daarom aan dat de overheid voortaan daadwerkelijk toeziet op naleving van haar pas-toe-of-leg-uit beleid rondom open standaarden⁸.

Begin 2015 werd bij de behandeling van de Kabinetsreactie op het eindrapport de motie Oosenbrug/Gesthuizen⁹ ingediend die de regering verzoekt om ervoor te zorgen dat voor eind 2015 bij alle aanbestedingen correct wordt omgegaan met de relevante open standaarden. De Kamer dringt in november 2015 in de Motie Oosenbrug/Veldman ook specifiek aan op toepassing van open standaarden bij gemeenten¹⁰. Het kabinet heeft de motie Oosenbrug/Gesthuizen overgenomen en verwijst meermaals naar haar plannen voor een wet^{11 12 13}. Zie verder bijlage A.

III. Open standaarden bevorderen via de pas-toe-of-leg-uit lijst

Open standaarden die voor overheden relevant zijn en bijdragen aan een goede informatie-uitwisseling, komen na toetsing door het Forum Standaardisatie op de pas-toe-of-leg-uit lijst. Plaatsing op deze lijst betekent onder meer twee dingen. Ten eerste dat de relevante standaarden op deze lijst door bestuursorganen uitgevraagd moeten worden in aanbestedingen van ten minste € 50.000 of meer (pas-toe). Wegens zwaarwegende reden kan hiervan worden afgeweken, mits gemotiveerd in het jaarverslag (leg-uit). Deze verplichting volgt in eerste instantie uit de Instructie Rijksdienst inzake aanschaf ICT-diensten en ICT-producten¹⁴. Via verschillende bestuursakkoorden strekt deze verplichting echter verder dan de Rijksoverheid en is deze verplichting van toepassing op alle bestuursorganen als ZBO's, provincies, gemeenten en waterschappen¹⁵.

Ten tweede betekent plaatsing op de pas-toe-of-leg-uit lijst een oproep aan alle bestuursorganen in Nederland om de voor hen relevante open standaarden te gaan gebruiken. In 2010 maakten de leden van het College Standaardisatie de afspraak dat het bestuursorgaan dat zij vertegenwoordigen zelf de relevante standaarden zo spoedig mogelijk zou gaan gebruiken en dat zij ook buiten hun eigen bestuursorgaan het gebruik van de standaard zouden bevorderen.¹⁶ Het effect hiervan, van de Rijksinstructie, en de afspraken over de overheidsbrede werking, is beperkt. Uit diverse metingen¹⁷ blijkt dat het

⁸ Tweede Kamer, vergaderjaar 2014-2015, 33 326, nr. 5, p. 21

⁹ Tweede Kamer, vergaderjaar 2014-2015, 33 326, nr. 21

¹⁰ Tweede Kamer, vergaderjaar 2015-2016, 34 300 VII, nr. 36

¹¹ Tweede Kamer, vergaderjaar 2014-2015, 33 326, nr. 13, p. 15

¹² <https://zoek.officielebekendmakingen.nl/ah-tk-20142015-906.pdf>: "Door bepaalde open standaarden bij wet te kunnen aanwijzen, kunnen alle overheden worden verplicht om deze standaarden te gebruiken."

¹³ Tweede Kamer, vergaderjaar 2015-2016, 26 643, nr. 389, p.9

¹⁴ Besluit van de Staatssecretaris van Economische Zaken van 8 november 2008, nr. WJZ/8157380, tot vaststelling Instructie rijksdienst inzake aanschaf ICT-diensten en ICT-producten, <https://zoek.officielebekendmakingen.nl/stcrt-2008-837.html>

¹⁵ Zie bijlage C (Besluit Nationaal Beraad Digicommissaris 18 mei 2015).

¹⁶ Besluit van het College Standaardisatie over de betekenis van de plaatsing van open standaarden op de pas-toe-of-leg-uit lijst, oktober 2010

<https://www.forumstandaardisatie.nl/sites/default/files/CS/2010/1117/CS-20101117.02F-Forumadvies-betekenis-lijst.pdf>

¹⁷ Monitor Open Standaarden Beleid 2015 (zie Bijlage F), dezelfde Monitor over de jaren 2014, 2013, 2012 en de Dissertatie Paapst 2012, de 1-meting informatieveiligheidsstandaarden. Uit de *Derde voortgangsrapportage Nederland Open in Verbinding*

adoptietempo van de standaarden laag is, en dat er maar sporadisch wordt uitgelegd waarom niet wordt toegepast.

IV. Sommige standaarden zijn zo belangrijk dat niet toepassen geen optie meer is

In het regeerakkoord staat dat burgers en bedrijven uiterlijk in 2017 zaken die ze met de overheid doen digitaal kunnen afhandelen. Deze digitale dienstverlening van de overheid aan burgers en bedrijven moet veilig, betrouwbaar en efficiënt verlopen.

Vanuit dat perspectief is voor sommige standaarden 'bevorderen' alleen niet voldoende. De gevolgen zijn te ernstig. De beveiliging kan in gevaar komen waardoor er kan worden gefraudeerd, gegevens op straat komen te liggen, de overheid burgers en bedrijven telkens moet lastig vallen met dezelfde vragen of stelselmatig teveel blijft betalen voor ICT. In deze gevallen is het afwachten van een eventuele aanbesteding van boven de 50.000 euro voor een product of dienst niet aan de orde: het bestuursorgaan moet zelf aan de slag gaan. Het niet toepassen van open standaarden is hier niet gerechtvaardigd.

Dit ziet het kabinet ook zo: In de kabinetsreactie¹⁸ op het rapport van de onderzoekscommissie Elias wordt voor open standaarden verwezen naar het wetsvoorstel voor de wet GDI. In december 2015 schrijft de Minister van BZK namens het Kabinet aan de Kamer in een brief over de uitgangspunten van wetgeving over de GDI dat het voor een eenduidige toegang van burgers en bedrijven tot overheidsinformatie, en voor een betere en betrouwbare samenwerking en informatie-uitwisseling tussen overheden noodzakelijk is dat bestuursorganen gebruik maken van open standaarden¹⁹. Dat is, behalve uniformering voor burgers en bedrijven, ook van groot belang voor interoperabiliteit van de overheid, het garanderen van communicatie tussen ICT-systemen, de betrouwbaarheid en veiligheid van de systemen en gegevens, en het doelmatiger functioneren van de overheid²⁰.

Vraag 2: wie zijn de betrokkenen?

- Betrokken bij de *totstandkoming* van het artikel:
Ministerie van Economische Zaken, ministerie van Binnenlandse Zaken en Koninkrijksrelaties en het Forum Standaardisatie

(Kamerstukken II 2011/12, 26 643, nr. 217, blg-144855) bleek dat slechts in 40 procent van de aanbestedingen open standaarden worden uitgevraagd. Van de overige zestig procent werd in de jaarverslagen de toepassing van *leg uit* niet teruggevonden. Uit onderzoek onder 1114 onderwijsinstellingen blijkt volgens Stichting ICTU dat met namen bij kleinere instellingen in het primair en voorbereidend onderwijs een achterstand bij het implementeren van open standaarden (Rapport Meting Open Standaardenbeleid Onderwijs, Kamerstukken II 2013/14, 26 643 nr.295, blg-269959).

¹⁸ Tweede Kamer, vergaderjaar 2014-2015, 33 326, nr. 13, p. 15

¹⁹ Tweede Kamer, vergaderjaar 2015-2016, 26 643, nr. 373, p.5-6: "Voorts moeten bestuursorganen dezelfde standaarden gaan gebruiken voor het publiceren en onderling uitwisselen van deze informatie Gebruikmaking van de afgesproken standaarden zorgt voor een betere en betrouwbare samenwerking en informatie-uitwisseling tussen overheden, en dat is noodzakelijk voor het naar burgers en bedrijven kwalitatief kunnen ontsluiten van informatie van de gehele overheid."

²⁰ Tweede Kamer, vergaderjaar 2015-2016, 26 643, nr. 373, p.7

- Betrokken in de zin van *normadressaten*:
Alle bestuursorganen
- Betrokken in de zin van wie ondervinden de *gevolgen* van het voorstel?
Bestuursorganen en burgers en bedrijven die digitaal in contact staan met de overheid.

Vraag 3: wat is het probleem?

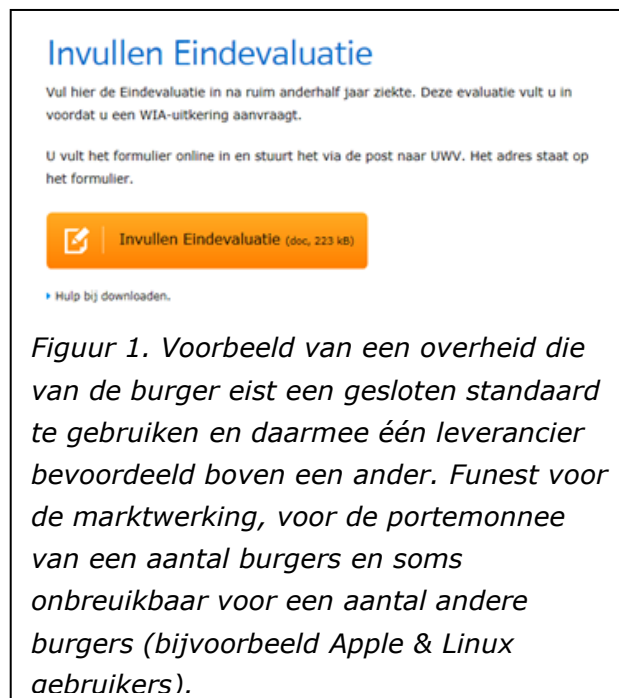
De Nederlandse overheid streeft met informatie-uitwisseling en informatieverstrekking een aantal belangrijke maatschappelijk baten na:

1. rechtszekerheid in de communicatie tussen bestuursorganen onderling, en tussen bestuursorganen, burgers en bedrijven;
2. een veilige en betrouwbare gegevensuitwisseling tussen bestuursorganen onderling en tussen bestuursorganen, burger en bedrijven;
3. lagere kosten voor gegevensuitwisseling;
4. leveranciersonafhankelijkheid.

Door het onvoldoende toepassen van open standaarden van de pas-toe-of-leg-uit lijst in de communicatie tussen bestuursorganen en maatschappij, alsmede tussen bestuursorganen onderling, ontstaan de volgende problemen:

1. Onvoldoende rechtszekerheid in de communicatie met bestuursorganen

Vanuit het oogpunt van rechtszekerheid is het nodig dat burgers en bedrijven weten wanneer communicatie met de overheid slaagt. Het moet bijvoorbeeld duidelijk zijn met welke documentformaten de overheid in ieder geval overweg kan, zodat bijvoorbeeld het indienen van een bezwaarschrift of een aanvraag van een beschikking probleemloos verloopt. Als een burger of bedrijf met een bestuursorgaan communiceert volgens bepaalde afspraken mag deze laatste zich er niet op beroepen de communicatie niet "begrepen" te hebben. Verder moeten besluiten van de overheid op een manier worden kenbaar gemaakt dat eenieder daar kennis van kan nemen.



2. Digitaal verkeer is minder veilig dan mogelijk

In verband met het in het regeerakkoord opgenomen streven dat burgers en ondernemers in 2017 zaken met de overheid digitaal kunnen afhandelen, dient in de Algemene Wet Bestuursrecht te worden geregeld dat bestuursorganen de elektronische weg openstellen. De uitwisseling van informatie langs de elektronische weg dient veilig te zijn, te meer omdat aan de berichten rechtsgevolgen kunnen zijn verbonden. Het gebruik van verschillende standaarden zorgt dat meer koppelvlakken noodzakelijk hetgeen weer leidt tot een verhoogd risico op fouten. Elk koppelvlak dient gebouwd of gekocht te worden en dient vervolgens te worden beheerd. De kans op fouten, variërend van systemen die niet werken tot systemen die de verkeerde beslissingen nemen, neemt hiermee toe en de integriteit van gegevens en van systemen die ze gebruiken neemt af.

Sommige open standaarden zijn dermate belangrijk voor het functioneren van de digitale overheid dat afwijkingen of het niet toepassen ervan het functioneren van de digitale overheid en daarmee het functioneren van de overheid als geheel in gevaar brengt. Veiligheidsstandaarden vallen in deze categorie.

Fraude zoals 'phishing' komt regelmatig voor. Er is een sterke toename in valse e-mails die in naam van onder andere de overheid worden geschreven en verstuurd²¹. Het is voor zowel burgers als bedrijven steeds moeilijker om te ontdekken of een e-mail met een verwijzing naar een website daadwerkelijk van een bestuursorgaan afkomstig is. Indien inloggegevens in handen vallen van criminelen, kan dit de burger veel geld kosten of zijn gegevens misbruikt worden voor bijvoorbeeld ID-fraude.

Door bepaalde beveiligingsstandaarden niet toe te passen kan onevenredig veel schade worden toegebracht aan de belangen van burgers, bedrijven of andere bestuursorganen (zie ook bijlage E). Wat daarbij ook een rol speelt is dat een aantal standaarden pas werken als ze aan beide kanten worden toegepast. Als voor beveiliging wordt besloten dat een bepaalde standaard wordt toegepast, bijvoorbeeld SAML, en één organisatie besluit om deze standaard niet toe te passen dan worden het alle bestuursorganen die met deze organisatie communiceren onmogelijk gemaakt om deze standaard toe te passen, althans in de

²¹ <https://www.waarschuwingsdienst.nl/Risicos/Actuele+dreigingen/Softwarelekken/WD-2014-007+Waarschuwing+phishing-e-mail+uit+naam+van+het+Centraal+Justitieel+Incassobureau+CJIB+in+omloop.html>
<https://www.waarschuwingsdienst.nl/Risicos/Actuele+dreigingen/Virussen+en+wormen/WD-2013-014+Sterke+toename+in+nep+incasso+e-mails.html>. Grote toename 'valse e-mails' bij Fraudehelpdesk (7 februari 2016)
<http://nos.nl/l/2085484>, Sterke stijging in nep-mails (7 januari 2016) <http://www.crimesite.nl/sterke-stijging-in-melding-nep-mails/>, Nepmails uit naam van DG Belastingdienst (19 januari 2016) <http://www.nu.nl/internet/4200310/man-opgepakt-versturen-nepmails-naam-belastingdienst.html>, Criminelen misbruiken overheid in phishingmails <http://www.volkskrant.nl/tech/criminelen-misbruiken-webwinkels-en-overheid-in-phishingsmails~a4057348/>, CJIB krijgt veel meldingen van phishing <http://www.bnr.nl/nieuws/132478-1509/cjib-krijgt-veel-meldingen-van-phishing>, Belastingdienst waarschuwt voor phishingmail, <http://www.nu.nl/internet/4101462/belastingdienst-waarschuwt-phishingmail.html>, Hogeschool InHolland waarschuwt voor phishingmails <http://www.nu.nl/binnenland/4144795/waarschuwing-phishingmail-inholland.html>, Overheid veel vaker doelwit van cyberaanvallen, <http://www.volkskrant.nl/tech/overheid-veel-vaker-doelwit-van-cyberaanvallen~a4119366/>

communicatie met die ene organisatie. Eén zwakke broeder infecteert alle eraan gerelateerde sterke broeders. Standaardisatie werkt alleen als iedereen de standaard toepast.

3. Door niet te standaardiseren worden potentiële kostenbesparingen niet gerealiseerd

Wanneer een bestuursorgaan niet ontvankelijk is voor communicatie door middel van een bepaalde standaard, zijn andere bestuursorganen gedwongen ook de standaard te gebruiken die dat bestuursorgaan wel hanteert. Dat leidt tot kosten bij deze partijen die vaak niet opwegen tegen de investering die dat orgaan moet doen voor gebruik van die specifieke open standaard. In de business case naar de potentiële besparingen van de voorzieningen voor het stelsel van basisregistraties kwam naar voren dat bij standaardisatie op de Digikoppeling standaard, meer dan €78 miljoen²² op jaarbasis kan worden bespaard. Hierbij gaat het uitsluitend om kosten die alle bestuursorganen dienen te maken om te kunnen communiceren met andere bestuursorganen.

Wat de business case ook laat zien is dat de baten exponentieel afnemen naarmate er meer registraties afhaken. Als bijvoorbeeld slechts 6 van de 13 basisregistraties standaardiseren op de standaard Digikoppeling dan zijn de baten niet, zoals verwacht, 36 miljoen²³ doch 11 miljoen euro. Dit voorbeeld laat zien dat het niet meedoen van slechts enkele bestuursorganen, de anderen onevenredig op kosten jagen. Standaardisatie werkt alleen als iedereen meedoet.

4. Niet open standaardiseren levert meer leveranciersafhankelijkheid voor de bestuursorganen op

Cruciaal bij standaardiseren is dat de standaard niet in handen is van een bepaalde leverancier die kan eisen dat bepaalde software wordt aangeschaft om de informatie te lezen dan wel exorbitante eisen (zoals kosten) stelt aan het gebruik van die standaard. Dit betekent dat men de kosten voor het gebruiken van de standaard niet onder controle heeft.

Het is niet altijd in het belang van de leverancier om open standaarden aan te bieden, of hun ICT-product eraan aan te passen.

Hierdoor wordt de overheid meer afhankelijk van een specifieke leverancier, omdat overstappen van de ene naar een andere leverancier lastiger is. Dit komt doordat die leverancier die specifieke standaard niet kent of gebruikt of omdat applicaties dan wel koppelvlakken aangepast dienen te worden. Maar afhankelijkheid van een leverancier geldt ook voor burgers en bedrijven. Zij mogen in hun communicatie met de overheid niet verplicht worden dit te doen via software/programma's van één of een beperkte groep

²² Verfijning en herijking kostenbatenanalyse voor investeringen in gemeenschappelijke voorzieningen in het stelsel van basisregistraties. PWC, 23 februari 2010

²³ Bij een lineaire relatie zou dit zes dertiende van 78 miljoen zijn

softwareleveranciers.²⁴ Dat software beschikbaar is, zonder dat daarvoor betaald moet worden, is niet genoeg. Het is immers de vraag hoe lang dat het geval is.

Vraag 4: wat is het doel van het wetsvoorstel?

Voor de bovengenoemde 4 maatschappelijke baten streeft de overheid de volgende doelen na:

1. Rechtszekerheid in de communicatie tussen bestuursorganen en burgers en bedrijven

Burgers mogen erop vertrouwen dat als zij volgens bepaalde afspraken communiceren met een bestuursorgaan, dat deze laatste er zich niet op kan beroepen dat deze het 'niet begrepen heeft' omdat er niet werd gecommuniceerd in de specifieke standaard van het bestuursorgaan, omgekeerd mogen ze verwachten dat het bestuursorgaan met hen dusdanig communiceert dat zij geen extra software behoeven aan te schaffen. De overheid behoeft niet van nul uit te gaan: zij mag verwachten dat als de burger een internetaansluiting heeft ook over een tekstverwerker beschikt. Ze mag echter geen uitspraak doen over welk merk tekstverwerker de burger dient aan te schaffen, wel weer over de open standaard die de tekstverwerker ook dient te *kunnen* leveren.

2. Een veilige communicatie tussen bestuursorganen onderling en tussen bestuursorganen, burger en bedrijven

Resultaten komen niet zomaar op straat te liggen en bestuursorganen doen alle moeite om hun data niet te laten 'kapen' door criminele organisaties. Met de open standaarden TLS, DNSSEC, DKIM/SPF, DMARC kan fraude zoals 'phishing' worden bestreden.²⁵ (zie verder bijlage E).

3. Lagere kosten

De overheid als geheel bespaart kosten doordat bestuursorganen in verschillende ketens met elkaar samen kunnen werken, en elkaars gegevens kunnen hergebruiken²⁶ zonder burgers en bedrijven met dezelfde uitvragen lastig te vallen (principe van eenmalige uitvraag en meervoudig gebruik).

²⁴ Uit het rapport 'Meting Open Standaardenbeleid Onderwijs' (*Kamerstukken II* 2013/14, 26 643 nr. 295, blg-269959, p. 5.) blijkt dat veel instellingen knelpunten ervaren met betrekking tot de afhankelijkheid van leveranciers.

²⁵ DomainKeys Identified Mail Signatures (DKIM) koppelt een e-mail aan een domeinnaam met behulp van een digitale handtekening. Het stelt de ontvanger - of een internetserviceprovider - in staat om te bepalen welke domeinnaam (en daarmee welke achterliggende organisatie) verantwoordelijk is voor het zenden van de e-mail. Daardoor kunnen spam- en phishing-mails beter worden gefilterd.

²⁶ Vanzelfsprekend alleen wanneer daarvoor een wettelijke grondslag is. Standaardisatie ziet op de technische herbruikbaarheid.

De verplichting om de jaarrekening bij de Kamer van Koophandel via SBR (Standard Business Reporting) te deponeren levert 68,2 miljoen op jaarbasis op²⁷ en heeft geleid tot de verplichting om de standaard XBRL te gebruiken.

Zoals al in de inleiding betoogd: samenwerking in ketens vereist standaardisatie, staand overheidsbeleid daarbij is standaardisatie op *open standaarden*.

4. Leveranciersafhankelijkheid

De overheid gedraagt zich als een waardig hoeder van belastinggeld en zorgt ervoor niet meer dan strikt noodzakelijk is afhankelijk van leveranciers. Open standaarden bevorderen de marktwerking en verhinderen dat de leverancier een monopoliepositie verwerft, dit heeft een positieve impact op de kosten. Met open standaarden hebben bestuursorganen een exit-strategie, en kunnen hun gegevens zonodig meenemen naar een andere leverancier.

Vraag 5: rechtvaardiging van het overheidsingrijpen

Gegevensuitwisseling vindt plaats binnen bestuurslagen, maar ook tussen bestuurlagen. Standaardisatie daarmee ook. Binnen een bestuurlaag vindt reeds de nodige afstemming plaats, tussen bestuurslagen is dat veel lastiger.

De overheid stuurt via allerlei afspraken op verhoging van de kwaliteit van de eigen bedrijfsvoering om de in de aanleiding genoemde problemen I t/m III aan te pakken. Het belang dat in het geding is bij problemen die hierboven staan benoemd, is zodanig dat verder ingrijpen gerechtvaardigd is. Het ingrijpen van de overheid bij het maken van afspraken over het gebruik van bepaalde open standaarden is proportioneel omdat het:

- de rechtszekerheid bevordert;
- persoonsgegevens veilig stelt;
- kosten bespaart;
- bestuursorganen meer leveranciersafhankelijkheid biedt.

Voor welke standaarden dit proportioneel is, is de vraag die in de volgende paragraaf wordt beantwoord.

Vraag 6: wat is het beste instrument?

In het verleden is een groot aantal instrumenten²⁸ toegepast om het gebruik van de open standaarden te vergroten, met name: communicatie, Actieplan NOiV, instructie rijksdienst inzake de aanschaf van ICT-diensten en ICT-producten, waarmee het gebruik van open standaarden van de pas-toe-of-leg-uit lijst wordt voorgeschreven bij ICT-aanbestedingen van tenminste 50.000 euro. En verder de bestuursakkoorden voor gemeenten, waterschappen en provincies die het pas-toe-of-leg-uit principe ook verplichten voor andere

²⁷ Tweede Kamer, vergaderjaar 2014–2015, 34 262, nr. 3

²⁸ Voor een nadere toelichting over ingezette instrumenten zie bijlage D.

overheden. Deze instrumenten zijn in de praktijk onvoldoende gebleken om de doelstelling ten aanzien van gebruik van open standaarden binnen de overheid te realiseren. Uit diverse metingen²⁹ blijkt dat het adoptie tempo van open standaarden laag is, en dat er in de jaarverslagen maar sporadisch wordt uitgelegd waarom een open standaard niet wordt toegepast.

Ondanks het hierboven geschetste beeld, blijft voor een groep open standaarden het pas-toe-of-leg-uit principe het meest proportionele instrument. Echter voor sommige standaarden is in sommige situaties toepassing *zonder uitzondering* nodig. Het pas-toe-of-leg-uit principe en de hierboven geschetste resultaten zijn niet voldoende om dat te realiseren. Dit doet zich voor wanneer het gebrek aan tempo bij de invoering van bepaalde open standaarden het publieke belang³⁰ schaadt, bijvoorbeeld bij de 4 genoemde maatschappelijke baten: door te tornen aan de rechtszekerheid of de veiligheid, verkwisting van geld of leveranciersafhankelijkheid.

Het regelen van ICT-standaarden via wet- en regelgeving is staande overheidspraktijk. Zo vinden we bijvoorbeeld wettelijk verplichte standaarden in de SUWI-keten³¹ (SZW), voor de elektronische burgerlijke stand³² (V&J), voor een viertal GDI³³ voorzieningen (BZK) en op verschillende andere plekken³⁴. Dit voorstel ziet toe op betreffende wet- en regelgeving voor de sector Overheid als geheel.

Voor het verplichten van een open standaard zal steeds een afweging noodzakelijk zijn ten aanzien van:

- *Proportionaliteit*. Het reduceren van kosten is een van de doelen die de overheid nastreeft. Een besparing van 5 euro door gebruik van een open standaard is geen aanleiding voor wetgeving, echter als deze 78 miljoen op jaarbasis bedraagt dan kan er reden zijn voor het afdwingen van een open standaard³⁵. Zo is niet elke open beveiligingsstandaard reden voor een wet, maar wel als daarmee fraude kan worden voorkomen, of kan worden voorkomen dat persoonsgegevens op straat komen te liggen
- *Toepassingsgebied*. De toepassing van een open standaard is noodzakelijk binnen een bepaald functioneel- en organisatorisch toepassingsgebied. Buiten die toepassingsgebieden kunnen echter nog steeds redenen van bijzonder gewicht zijn

²⁹ Monitor Open Standaarden Beleid 2015 (zie Bijlage F), dezelfde Monitor over de jaren 2014, 2013, 2012, de Dissertatie Paapst 2012, en de 1-meting informatieveiligheidsstandaarden.

³⁰ De wens om middels een wettelijke regeling organisaties te binden, en wel binnen – niet alleen de Rijksoverheid maar – de gehele overheid, komt ook naar voren bij de aanbevelingen in het proefschrift van Paapst 2013, p. 198.

³¹ SGR en SUWI-ML; wetten.overheid.nl/BWBR0013280

³² <http://wetten.overheid.nl/BWBR0036618/2015-07-01>

³³ Zie artikel 6 lid 1 <https://zoek.officielebekendmakingen.nl/stcrt-2015-37158.html>

³⁴ <https://lijsten.forumstandaardisatie.nl/lijsten/standaarden-in-wet-en-regelgeving>.

³⁵ Verwijzing naar onderzoeken of pagina van dit document waar de onderzoeken zijn vermeld.

een open standaard niet toe te passen (daar blijft daarom het bestaande pas-toe-of-leg-uit beleid geleden).

- *Invoeringstermijn*. Het invoeren van een nieuwe standaard is niet altijd een triviale zaak. In die gevallen dat de wetgever aanleiding heeft om te denken dat dit zo is, kan hij in lagere regelgeving een andere invoeringstermijn dan de standaard 6 maanden voorstellen.
- *De mate van treden in de bevoegdheid van andere ministers*. In de meeste gevallen is de bepaling van de wet een “ook” bepaling. Daarmee wordt bedoeld dat de bestuursorganen de aangewezen standaard *ook* moeten implementeren naast de al gehanteerde standaarden en dat de bevoegdheid van de vakminister niet wordt beperkt.

Veiligheid en rechtszekerheid kunnen gronden zijn bij het aanwijzen van een standaard om andere standaarden uit te sluiten voor dat toepassingsgebied. Dat kan bij lagere regelgeving worden meegenomen.

Een gemengde aanpak van verplichtende wetgeving in combinatie met de communicatie/voorlichtingsacties die reeds lopen in het kader van het pas-toe-of-leg-uit beleid, wordt ondersteund door de uitkomsten van wetenschappelijk onderzoek uit 2015³⁶.

Criteria

Een en ander leidt tot de volgende *criteria* voor het aanwijzen van een open standaard:

- Het betreft een open standaard van de pas-toe-of-leg-uit lijst;
- Het gaat om een bevoegdheid en bovensectorale open standaarden in het kader van de elektronische overheid en de generieke digitale infrastructuur;
- De open standaard moet van maatschappelijk belang zijn (zo relevant dat de continuïteit, veiligheid, kenbaarheid, eenduidigheid en efficiëntie van elektronische dienstverlening anders in gevaar komt);
- Er moet sprake zijn van een positieve business case (anders blijven baten liggen en onnodige kosten bestaan); de business case dient alle vier de maatschappelijke baten mee te wegen: rechtszekerheid, veiligheid, kosten en leveranciersafhankelijkheid;
- Daarnaast kan de Minister open standaarden op het gebied van informatievoorziening voorschrijven die conform internationale verdragen of Europese regelgeving verplicht zijn (bijvoorbeeld de codificatie in nationale regelgeving van de Europese toegankelijkheidsstandaard, volgende uit Europese Richtlijn).

³⁶ Florian Henning, *Living Up to Standards, Interoperability Governance and Standards Adoption in Government Information Networks*, uitgeverij Boekenplan 2015.

<http://pub.maastrichtuniversity.nl/5b21623c-8813-4873-9baf-128169ddfdb7>.

Onderbouwing van het argument dat een wettelijke dwang adoptie van standaarden kan ondersteunen in dit proefschrift : p119, p162, p164, p176, 259-263, p269.

Onderbouwing van het argument dat “harde” governance op adoptie idealiter in combinatie met soft governance moet gebeuren is o.a. te vinden op: p160, p.162, p170, p174, p175, p270.

Gezien het gewicht van het middel worden de volgende waarborgen voorgesteld:

- In lagere regelgeving wordt de specifieke verplichting geregeld. Daarin wordt het gevoelen van de Ministerraad meegenomen (inclusief het gebruikelijke voorbereidingstraject). Daarop aanvullend wordt het Nationaal Beraad - waarin alle overheden en beleid en uitvoering zijn vertegenwoordigd - om advies gevraagd. Daaraan voorafgaand wordt het - publiek/privaat samengestelde - Forum Standaardisatie om een pre-advies gevraagd, ten aanzien van de voorgenomen verandering van pas-toe-of-leg-uit naar 'verplicht'. Daarbij worden kosten/baten en proportionaliteit afgewogen.
- slechts open standaarden van de pas-toe-of-leg-uit lijst komen voor een verplichting in aanmerking. Omdat het gaat om open standaarden van de pas-toe-of-leg-uit lijst, is voor wat betreft de *kwaliteit*³⁷ van de open standaard, al een open proces doorlopen, waaronder een expertoets met alle stakeholders, openbare internetconsultatie van dat expert-advies, advies van het publiek-privaat samengestelde Forum Standaardisatie, en besluitvorming in het Nationaal Beraad.
- De open standaarden op de pas-toe-of-leg-uit lijst hebben specifieke functionele³⁸- en organisatorische toepassingsgebieden. Wanneer een open standaard van de lijst verplicht wordt, zal extra kritisch naar de afbakening daarvan gekeken worden. Er is immers geen 'leg-uit' meer mogelijk. De afbakening met toepassingsgebieden, voorkomt dat de open standaard ergens verplicht wordt waar dat - alle belangen afwegend - onwenselijk is.
- Afhankelijk van het soort open standaard dat wordt verplicht, en de urgentie, kan in lagere regelgeving desgewenst gekozen worden voor een afwijkende invoeringstermijn dan de zes maanden die er standaard voor staan. Datzelfde geldt voor een hardheidsclausule.

Vraag 7: wat zijn de gevolgen?

Wat zijn de implementatiekosten van de standaarden?

Per specifieke open standaard moeten de implementatiekosten worden ingeschat. Een gebruikelijk instrument hiervoor is de 'ex ante uitvoeringstoets'.³⁹

³⁷ Getoetst wordt o.a. de openheid van de standaard (specificaties beschikbaar, kosteloos bruikbaar), ondersteuning van de standaard door leveranciers en het bestaan van een beheerorganisatie.

³⁸ Zo zal voor een overheidsorganisatie die geen burgers of bedrijven hoeft te authenticeren, niet de verplichting gaan gelden om de authenticatiestandaard (de standaard SAML, die wordt gebruikt door DigiD en eHerkenning) te gebruiken.

³⁹ Voor wat betreft de informatieveiligheid standaarden is een eerste indicatie gemaakt van de ordegrote van de kosten inclusief bandbreedte: anti-website fraude: eenmalig €400, €700 per jaar (TLS + DNSSEC); anti-email fraude: eenmalig €2.500 tot €10.000, jaarlijks €1.250 tot EUR €5.000 (DKIM, SPF, DMARC).

Deze inschatting is tot stand gekomen na consultatie van onder andere het Platform Internet Standaarden, en - voor wat betreft TLS+DNSSEC - de impactanalyse van VNG/KING.

Welke ruimte houdt een andere minister om voor de eigen sector andere standaarden aan te wijzen?

Het artikel beoogt geen wijzigingen aan te brengen in de taken en bevoegdheden van vakministers. Zij kunnen zelf open standaarden aanwijzen voor hun eigen beleidsterrein. De minister dient *ook* de aangewezen standaard te implementeren. Echter in een aantal gevallen bestaat die vrijheid niet. In het nu actuele geval⁴⁰ van de veiligheidsstandaarden TLS en SSL 2.0 is het aanwijzen van TLS gewenst en extreem ongewenst dat bestuursorganen SSL 2.0 nog gebruiken. In dit geval zal TLS moeten worden aangewezen en het gebruik SSL 2.0 afgewezen.

Moet er een noodprocedure worden opgenomen in de wet als een aangewezen standaard toch op enig moment onveilig wordt bevonden?

Artikel 4 is mede bedoeld als die noodprocedure.

Wat is het risico van alleen standaarden verplichten/voorschrijven die 'open' zijn?

Het doel van het aanwijzen van *open* standaarden is gelegen in het voorkomen van de risico's die gepaard gaan met het gebruik van *gesloten* standaarden. Die zijn gelegen in buitensluiten van bepaalde groepen burgers en bedrijven, burgers en bedrijven kunnen confronteren met onnodige kosten en het als overheid geen controle hebben over de eigen kosten.

Geef een uitputtende opsomming van de open standaarden die – op het moment van inwerkingtreding van de Wet gdi – wettelijk moeten worden aangewezen (verplicht).

Open standaarden die meteen bij de inwerkingtreding van deze wet verplicht zouden moeten worden betreffen: de veiligheidsstandaarden DNSSEC, TLS, DKIM, DMARC en SPF. Het voldoen aan de veiligheidsstandaarden vormt hiermee een wettelijke ondergrens voor overheden om informatie met burgers en bedrijven veilig te kunnen uitwisselen en hergebruiken. Vanzelfsprekend dient ook voor deze open standaarden de hierboven beschreven procedure van advies en pre-advies te worden gevolgd.

Een andere kandidaat is de Europese toegankelijkheidsstandaard (webstandaard: de codificatieverplichting volgende uit Europese Richtlijn). Momenteel wordt voorzien dat deze open standaarden bij de inwerkingtreding van de wet nog onvoldoende zullen zijn geïmplementeerd⁴¹.

⁴⁰ <http://www.rtlnieuws.nl/nieuws/binnenland/beveiliging-tientallen-gemeentesites-lek-persoonsgegevens-niet-veilig>

⁴¹ Wanneer er op dat moment toch volledige implementatie bij overheidsorganisaties is, kan van verplichting worden afgezien.

Moeten bestuursorganen in het Caribisch deel van Nederland (BES) worden verplicht bepaalde open standaarden te gebruiken of te accepteren?

Ja. Er is geen reden waarom bestuursorganen op de Cariben met toepassingen die vallen in het functioneel en organisatorisch toepassingsgebied van een standaard die middels deze grondslag verplicht wordt, per definitie – louter op basis van hun geografische ligging - worden uitgezonderd van toepassing. Ook daar is het van belang dat bestuursorganen veilig, betrouwbaar en eenduidig digitaal communiceren, en bereikbaar zijn. Wanneer het - uit het oogpunt van proportionaliteit - onwenselijk is dat voor een bepaalde standaard op de BES eilanden middels een verplichting te regelen, kan daarvoor in lagere regelgeving een uitzondering worden opgenomen.

Voorts is van belang om het beleid ten aanzien van het gebruik van open standaarden ook op Europees niveau af te stemmen, aangezien ook vanuit Europese regelgeving het gebruik van standaarden verplicht wordt gesteld.

Moet het gehele proces om te komen tot een pas-toe-of-leg-uit lijst worden vastgelegd bij of krachtens de wet?

Het proces voor het tot stand komen van een pas-toe-of-leg-uit lijst hoeft niet te worden vastgelegd in de wet. Dit is niet proportioneel en leidt tot inflexibiliteit indien in de toekomst een ander proces nodig blijkt te zijn.

Bijlage A. Politiek belang open standaarden, moties, Kamervragen & toezeggingen*Politiek belang van open standaarden.*

Vanaf 2002 is de tendens dat de Tweede Kamer de overheid aanzet tot het gebruik van open standaarden. Toen werd de motie Vendrik, met als doel om vanaf 2006 alleen nog maar met open standaarden te werken, kamerbreed aangenomen.⁴²

Omdat sommige bestuursorganen nog altijd met gesloten standaarden werkten, hebben de Tweede Kamer en de regering op 21 maart 2007 afgesproken het gebruik van open standaarden te versnellen en werd het actieplan NOIV vastgesteld.⁴³

In 2011 heeft de Algemene Rekenkamer onderzoek gedaan naar open standaarden en open source-software bij de rijksoverheid. Hiertoe had de Tweede Kamer verzocht.⁴⁴ Dat er nog maar beperkt positieve effecten zichtbaar zijn, komt vooral doordat het open standaardenbeleid redelijk vrijblijvend is geweest. Veel bestuursorganen werken nog niet volgens de zelfopgelegde standaarden en worden hier ook niet op afgerekend.

Dat constateerde de parlementaire onderzoekcommissie ICT (de commissie Elias) in oktober 2014 ook in haar eindrapportage van het onderzoek naar het verloop van grote ICT projecten bij de overheid, en de onderzoekscommissie beval daarom aan dat de overheid voortaan daadwerkelijk toeziet op naleving van haar pas-toe-of-leg-uit beleid rondom open standaarden⁴⁵. In de kabinetsreactie⁴⁶ op het rapport wordt op dit punt verwezen naar dit voorgenomen wetgevingstraject rondom ondermeer standaarden.

De Minister van BZK antwoordde in november 2014 op Kamervragen van Oosenbrug over de toepassing van een open standaard bij gemeenten en provincies⁴⁷ dat het van groot belang is dat we sterker dan voorheen inzetten op het gebruik van deze open standaarden. "Om die reden zijn open standaarden onderdeel van het gezamenlijk wetgevingsproces van EZ, W&R en BZK waarover collega Kamp, mede namens mij, u per brief van 25 april 2014 heeft ingelicht. Door bepaalde open standaarden bij wet te kunnen aanwijzen, kunnen alle overheden worden verplicht om deze standaarden te gebruiken".

Bij de behandeling van de kabinetsreactie wordt in april 2015 de motie Oosenbrug/Gesthuizen ingediend, die de Regering verzoekt om ervoor te zorgen dat voor eind 2015 bij alle aanbestedingen correct wordt omgegaan met de relevante open standaarden. Die motie⁴⁸ wordt door Kamer en Regering overgenomen. In de motie wordt de Regering verzocht dat voor eind 2015 bij alle aanbestedingen correct wordt omgegaan met de relevante open standaarden. De Kamer dringt in november 2015 in de Motie

⁴² Kamerstukken II 2002/03, 28600 XIII, nr. 30.

⁴³ Kamerstukken II 2007/08, 26643, nr. 98.

⁴⁴ Kamerstukken II 2009/10, 26643, nr. 156. Motie van het lid Gerkens c.s.

⁴⁵ Tweede Kamer, vergaderjaar 2014-2015, 33 326, nr. 5, p. 21

⁴⁶ Tweede Kamer, vergaderjaar 2014-2015, 33 326, nr. 13, p. 15

⁴⁷ <https://zoek.officielebekendmakingen.nl/ah-tk-20142015-906.pdf>

⁴⁸ Tweede Kamer, vergaderjaar 2014-2015, 33 326, nr. 21

Oosenbrug/Veldman ook specifiek aan op toepassing van open standaarden bij gemeenten door de minister van BZK te verzoeken daarover in overleg te treden met VNG⁴⁹.

De Tweede Kamer dringt dus consequent aan, op het slagvaardiger en minder vrijblijvend doorzetten van het open standaarden beleid.

In december 2015 schrijft de Minister van BZK namens het Kabinet aan de Kamer in een brief over de uitgangspunten van wetgeving over de GDI⁵⁰ dat het voor een eenduidige toegang van burgers en bedrijven tot overheidsinformatie, en voor een betere en betrouwbare samenwerking en informatie-uitwisseling tussen overheden noodzakelijk is dat overheden gebruik maken standaarden⁵¹. *Dat is, behalve uniformering voor burgers en bedrijven, ook van groot belang voor interoperabiliteit van de overheid, het garanderen van communicatie tussen (ICT-)systemen, de betrouwbaarheid en veiligheid van de systemen en gegevens, en het doelmatiger functioneren van de overheid*⁵². Deze argumenten worden herhaald in de brief van de Minister voor Wonen en Rijksdienst aan de Kamer⁵³ en in het Digiprogramma 2016-2017 van de Digicommissaris waarin standaardisatie als een speerpunt wordt genoemd⁵⁴.

Met deze artikelen in het wetsvoorstel wordt tegemoet gekomen aan bovenstaande wensen van de Kamer en de gedane toezeggingen.

⁴⁹ Tweede Kamer, vergaderjaar 2015-2016, 34 300 VII, nr. 36

⁵⁰ Tweede Kamer, vergaderjaar 2015-2016, 26 643, nr. 373

⁵¹ Tweede Kamer, vergaderjaar 2015-2016, 26 643, nr. 373, p.5-6: "Voorts moeten bestuursorganen dezelfde standaarden gaan gebruiken voor het publiceren en onderling uitwisselen van deze informatie Gebruikmaking van de afgesproken standaarden zorgt voor een betere en betrouwbare samenwerking en informatie-uitwisseling tussen overheden, en dat is noodzakelijk voor het naar burgers en bedrijven kwalitatief kunnen ontsluiten van informatie van de gehele overheid."

⁵² Tweede Kamer, vergaderjaar 2015-2016, 26 643, nr. 373, p.7

⁵³ Tweede Kamer, vergaderjaar 2015-2016, 26 643, nr. 389, p.9

⁵⁴ [Link naar definitieve versie Digiprogramma 2016-2017]

Bijlage B. definitie van Open Standaarden

Open standaarden zijn standaarden die voldoen aan de definitie van de Europese Commissie (programma IDABC⁵⁵):

- De standaard is goedgekeurd en zal worden gehandhaafd door een non-profit organisatie, en de lopende ontwikkeling gebeurt op basis van een open besluitvormingsprocedure die toegankelijk is voor alle belanghebbende partijen (consensus of meerderheidsbeschikking enz.
- De standaard is gepubliceerd en over het specificatiedocument van de standaard kan vrijelijk worden beschikt of het is te verkrijgen tegen een nominale bijdrage. Het moet voor een ieder mogelijk zijn om het te kopiëren, beschikbaar te stellen en te gebruiken om niet of tegen een nominale prijs;
- Het intellectueel eigendom – m.b.t. mogelijk aanwezige patenten – van (delen) van de standaard is onherroepelijk ter beschikking gesteld op een “royalty-free” basis;
- Er zijn geen beperkingen omtrent het hergebruik van de standaard.

⁵⁵ Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens;
<http://ec.europa.eu/idabc/>.

Bijlage C. Procedure en criteria voor plaatsing op de pas-toe-of-leg-uit lijst*Stap 1: Aanmelding en intake: wordt de standaard in behandeling genomen?*

Iedereen kan een standaard aanmelden met steun van een bestuursorgaan. Het in behandeling nemen van de standaard is een besluit dat genomen wordt op basis de volgende drie criteria:

- Is de standaard toepasbaar voor elektronische gegevensuitwisseling tussen en met (semi-) bestuursorganen?
- Draagt de standaard binnen het beoogde opnamegebied substantieel bij aan de interoperabiliteit van de (semi-)overheid?
- Is de standaard niet reeds wettelijke verplicht?

Stap 2: Experttoetsing en openbare consultatie.

Een standaard die in behandeling is genomen wordt vervolgens getoetst door experts, gebruikers van de vanuit de overheid, leveranciers en andere kennispartners. Zij beoordelen de standaard op de volgende vier hoofdpunten:

- Toegevoegde waarde: Wegen de interoperabiliteitswinst en andere adoptievoordelen van de standaard, overheidsbreed en maatschappelijk op tegen de risico's en de nadelen?
- Open standaardisatieproces: Zijn de ontwikkeling en het beheer van de standaard zijn een open, onafhankelijke, toegankelijke, inzichtelijke, zorgvuldige en duurzame wijze ingericht?
- Draagvlak: Hebben aanbieders en gebruikers voldoende positieve ervaring met de standaard en er zijn voldoende leveranciers van de standaard?
- Opname bevordert adoptie: Is opname op de lijst een geschikt middel om de adoptie van de standaard te bevorderen?

Uit deze toetsing volgt een expertverslag voor de openbare consultatie voor een periode van ten minste vier weken. De reacties worden gepubliceerd. Een samenvatting van de reacties wordt met het expertadvies voorgelegd aan het Forum Standaardisatie.

Stap 3: Vaststelling door Forum en Nationaal Beraad.

Op basis van het expertadvies, de reacties uit de openbare consultatie en eigen inzichten, brengt het Forum een advies uit aan het Nationaal Beraad over het al dan niet toekennen van de status pas-toe-of-leg-uit. Het Nationaal Beraad stelt op basis het advies van het Forum vast of de standaard de status pas-toe-of-leg-uit uiteindelijk krijgt.

Bijlage D. Instrumentarium

In 2002 is een uitgebreid communicatieprogramma gestart over de toepassing van open standaarden (OSOSS). Dit programma heeft tot onvoldoende beweging geleid voor de toepassing van open standaarden. Naar aanleiding daarvan hebben de Tweede Kamer en de regering op 21 maart 2007 afgesproken het gebruik van open standaarden te versnellen en werd het actieplan NOIV vastgesteld⁵⁶.

Om de toepassing van bepaalde open standaarden meer kracht bij te zetten, heeft de Rijksdienst zich middels een Rijksinstructie⁵⁷ verplicht, om bij de aanschaf van een ICT-dienst of ICT-product van 50.000 euro of meer, te kiezen voor een dienst of product dat gebruik maakt van de open standaarden van de pas-toe-of-leg-uit lijst van het Forum Standaardisatie. Deze Rijksinstructie is genotificeerd door de Europese Commissie en is in oktober 2008 gepubliceerd in de Staatscourant. Voorts zijn de Rijksbegrotingsvoorschriften (RBV) van kracht geworden. In aanvulling op de Rijksinstructie is hierin vastgelegd dat Rijksoverheden in de bedrijfsvoeringsparagraaf van hun jaarverslag expliciet verantwoording afleggen over de mate van naleving van 'pas toe of leg uit'.

N.a.v. de motie Oosenbrug en Gesthuizen, die in april 2015 is aangenomen in de Tweede Kamer, waarin de regering wordt verzocht ervoor te zorgen dat voor eind 2015 bij alle aanbestedingen correct wordt omgegaan met de relevante open standaarden, is de communicatie over het gebruik van open standaarden bij aanbestedingen opgevoerd. In de toelichting bij de ARBIT zal worden verwezen naar het pas-toe-of-leg-uit regime.

Voor gemeenten, waterschappen en provincies:

Bestuurlijke afspraak in het Nationaal Beraad van 18 mei 2015 om de overheidsbrede 'pas toe of leg uit' afspraak – ondermeer vastgelegd in de bestuursakkoorden (zie hieronder) te verlengen tot eind 2017. Overheidsbrede implementatieagenda voor dienstverlening en e-overheid (i-NUP), mei 2011. In het i-NUP zijn resultaatverplichtingen afgesproken waaraan rijk en gemeenten in 2015 moeten voldoen. Standaardisatie komt terug in resultaatverplichting 20: "Gemeenten maken gebruik van de open standaarden zoals vastgesteld door het College Standaardisatie en werken hierbij volgens het principe pas-toe-of-leg-uit" Gemeenten hebben zich hieraan gecommitteerd middels paragraaf 7.7 Elektronische Overheid in de Bestuursafspraken 2011-201558. In het Nationaal Beraad – waarin alle overheden zijn vertegenwoordigd – van 18 mei 2015 is deze afspraak verlengd tot eind december 2017.

- Gemeentelijke agenda informatiebeleid (@genda 2015), mei 2011
- Bestuursakkoord rijk en gemeenten, juni 2007

⁵⁶ Kamerstukken II 2007/08, 26643, nr. 98.

⁵⁷ Besluit van de Staatssecretaris van Economische Zaken van 8 november 2008, nr. WJZ / 8157380, tot vaststelling Instructie rijksdienst inzake aanschaf ICT-diensten en ICT-producten.

⁵⁸ Kamerstukken II 2010-11, 32749 nr. 1 (bijlage).

- Bestuursakkoord rijk en provincies, juni 2008
- Uitvoeringsagenda NOiV , 5 juni 2008
- Akkoord NUP, 1 december 2008

Verder ook:

Besluit begroting en verantwoording provincies en gemeenten (BBV):

De commissie BBV heeft in haar richtlijnen opgenomen dat provincies en gemeenten in de paragraaf bedrijfsvoering van hun jaarverslag verantwoording afleggen over het gebruik van open standaarden. Deze commissie heeft als taak zorg te dragen voor een eenduidige uitvoering en toepassing van het Besluit begroting en verantwoording provincies en gemeenten.

Bijlage E. Voorbeelden

1. Rechtszekerheid

Communicatie van overheid naar burgers en bedrijven

Besluiten van de overheid (openbaar dan wel specifiek) moeten dusdanig kenbaar worden gemaakt dat burgers en bedrijven er met behoud van informatie (inclusief opmaak), kennis van kunnen nemen.

Wanneer voor het kenbaar maken gesloten standaarden gebruikt worden, dan is informatie alleen goed zichtbaar wanneer van specifieke software van een bepaalde leverancier gebruik wordt gemaakt (zie voorbeeld 1). De overheid drijft burgers en bedrijven dan in handen van zo'n leverancier. Momenteel wordt nog teveel informatie van de overheid middels gesloten standaarden gecommuniceerd. Dat is tevens onwenselijk uit het oogpunt van oneerlijke concurrentie ('staatssteun'), en uit het oogpunt van toegankelijkheid voor ontvangers die slechtziend, blind of doof zijn, of bijvoorbeeld kleurenblind of dyslectisch.

Communicatie van burgers en bedrijven naar de overheid

Verder moet het duidelijk zijn met welke documentformaten de overheid in ieder geval overweg kan, zodat bijvoorbeeld het indienen van een bezwaarschrift of een aanvraag van een beschikking probleemloos verloopt. Als een burger of bedrijf met een bestuursorgaan communiceert volgens bepaalde afspraken mag deze laatste zich er niet op beroepen de communicatie niet "begrepen" te hebben. Ook hier is het van belang dat de overheid middels een open standaard bereikbaar is⁵⁹, zodat ze burgers en bedrijven niet in handen van een enkele leverancier drijft. Momenteel vereist de overheid nog teveel dat burgers en bedrijven met haar communiceren via een bepaalde leverancier (zie voorbeeld 2+3). Dat leidt ook tot Kamervragen⁶⁰.

Middel

Door gebruik te maken van open in plaats van gesloten standaarden kunnen bovengenoemde problemen worden bestreden. Met het oog daarop⁶¹ is de open standaard pdf/a in verschillende regelgeving reeds verplicht⁶², en wordt hij gebruikt bij officiële publicaties op Overheid.nl⁶³. De standaard is open, en wordt door verschillende software van verschillende leveranciers ondersteund⁶⁴. Burgers en bedrijven kunnen uit meerdere software en leveranciers kiezen, zonder dat er informatie (incl. opmaak) verloren raakt.

⁵⁹ De overheidsorganisatie kan daarnaast overigens besluiten om ook via een aantal gesloten standaarden bereikbaar te zijn.

⁶⁰ <https://zoek.officielebekendmakingen.nl/ah-tk-20152016-151.html>

⁶¹ En daarnaast ook met het oog op archivering http://wetten.overheid.nl/BWBR0027041/2014-01-01#Hoofdstuk3_Paragraaf2_Artikel26

⁶² <http://wetten.overheid.nl/zoeken/zoekresultaat/rs/2,3,4/titelf/1/tekst/-q-pdf-s-a-q-/>

⁶³ Bekendmakingen zijn daar beschikbaar in meerdere open formaten PDF/A, ODT, XML, HTML, mede op basis van wettelijke verplichting (Bekendmakingsregeling).

⁶⁴ Dat kan omdat voor het gebruik van de open standaard geen licentiekosten moeten worden betaald, en de specificaties beschikbaar zijn.

Het mes snijdt aan meerdere kanten, want de standaard is ook beter toegankelijk voor ontvangers met een beperking.

Voorbeeld 1) waarbij de toegepaste publicatie standaard gesloten is. En waarbij informatie – zonder software van die specifieke leverancier – ontbreekt.

In de bijlage-viewer op de iPad (figuur 2) ontbreekt paginanummering, een voetnoot, de juiste paragraafnummering en de goede opmaak. Zo ook in de Good-Reader app die de overheid meelevert voor de iPad. Pas na aanschaf van Word (@80euro per jaar) wordt duidelijk dat er voetnoten zijn, wat de juiste paragraafnummering en paginanummering is etc (figuur 3).



1.5. Betrokkenheid van leraren en schoolleiders

Het grootste deel van de samenwerkingsverbanden geeft aan dat zij leraren en schoolleiders hebben betrokken en geïnformeerd. Vrijwel alle schoolleiders zijn geactiveerd om in gesprek te gaan met hun personeel en ruim driekwart van de schoolleiders is volgens de samenwerkingsverbanden in gesprek gegaan met ouders van leerlingen met een lgf (80% in het po en 77% in het vo). Waar samenwerkingsverbanden 'nee' antwoorden op deze vragen, geven zij aan dat dit de verantwoordelijkheid is van de besturen of dat de gesprekken op korte termijn gevoerd worden. Ook geven sommige samenwerkingsverbanden aan dat gesprekken met ouders door ambulant begeleiders worden gevoerd en dat de schoolleider hier niet bij betrokken is.

In vergelijking met de meting van november 2013 zijn op meer plekken afspraken gemaakt over personele gevolgen. Dit laat zien dat de plannen van de samenwerkingsverbanden steeds concreter worden.

Volgens de samenwerkingsverbanden zijn leraren in de afgelopen periode meer betrokken geraakt bij passend onderwijs. Samenwerkingsverbanden hebben bijvoorbeeld bijeenkomsten georganiseerd, een website ingericht en nieuwsbrieven verstuurd. De vraag is of deze activiteiten ertoe geleid hebben dat leraren en schoolleiders zich ook daadwerkelijk voorbereid voelen.

Monitor over voorbereiding van leraren en schoolleiders

In de eerste helft van februari is daarom onder leraren en schoolleiders gepeild in welke mate zij zich geïnformeerd voelen over passend onderwijs. 1369 locatiedirecteuren en 5.200 onderwijspersoneelsleden vullen een vragenlijst in. Deze respons is voldoende om in een groot deel van de samenwerkingsverbanden een beeld van de huidige situatie te vormen. De belangrijkste uitkomsten zijn als volgt:

- Van het onderwijspersoneel vindt 49% (po) en 37% (vo) zichzelf goed op de hoogte van wat er op de eigen school verandert het komende schooljaar door de invoering van passend onderwijs. Er zijn echter grote verschillen tussen functiecategorieën: schoolleiders en zorgcoördinatoren (79% goed) zijn het beste op de hoogte (75-89% goed). Leraren in basis- (50%), speciaal (55%) en vooral voortgezet onderwijs (36%) zijn duidelijk minder op de hoogte.
- Wat betreft de veranderingen voor de eigen situatie is ongeveer de helft van de respondenten in het po en ruim een derde in het vo goed op de hoogte. Schoolleiders (82% goed) en zorgcoördinatoren (79% goed) zijn het beste op de hoogte. Leraren in het speciaal (37%), basis- (33%), en voortgezet onderwijs (25%) zijn duidelijk minder op de hoogte.
- Een grote meerderheid van het personeel in regulier basis- en voortgezet onderwijs verwacht geen of weinig veranderingen voor de school en zichzelf als gevolg van de invoering van passend onderwijs. In het speciaal onderwijs worden meer veranderingen verwacht: ongeveer de helft van de schoolleiders, leraren en ambulant begeleiders in het speciaal onderwijs en speciaal basis onderwijs verwacht veel veranderingen. Er is nauwelijks verband tussen hoeveel veranderingen men verwacht en hoe goed men op de hoogte is.

Hoewel samenwerkingsverbanden aangeven al veel gedaan te hebben, kan op basis van deze monitor onder onderwijspersoneel geconcludeerd worden dat met name leraren zich nog niet voldoende geïnformeerd voelen. Dat komt overeen met de ervaringen van de Aob, die op basis van bezoeken aan 200 scholen concludeert dat leraren meer duidelijkheid nodig hebben vanuit de eigen schoolleiding. Dit betekent dat samenwerkingsverbanden en scholen nog een extra inspanning moeten doen om leraren voldoende te informeren. Datzelfde geldt overigens ook voor ouders (zie paragraaf 2.6).

Samenwerkingsverbanden hebben hun plannen nu rond. Schooldirecteuren, zorgcoördinatoren en intern begeleiders voelen zich nu geïnformeerd over wat er voor hen verandert. Nu de plannen

Figuur 2. document in bijlage viewer van de standaard mail app op de iPad



2.5. Betrokkenheid van leraren en schoolleiders

Het grootste deel van de samenwerkingsverbanden geeft aan dat zij leraren en schoolleiders hebben betrokken en geïnformeerd. Vrijwel alle schoolleiders zijn geactiveerd om in gesprek te gaan met hun personeel en ruim driekwart van de schoolleiders is volgens de samenwerkingsverbanden in gesprek gegaan met ouders van leerlingen met een *laf* (80% in het po en 77% in het vo). Waar samenwerkingsverbanden 'nee' antwoorden op deze vragen, geven zij aan dat dit de verantwoordelijkheid is van de besturen of dat de gesprekken op korte termijn gevoerd worden. Ook geven sommige samenwerkingsverbanden aan dat gesprekken met ouders door ambulant begeleiders worden gevoerd en dat de schoolleider hier niet bij betrokken is.

In vergelijking met de meting van november 2013 zijn op meer plekken afspraken gemaakt over personele gevolgen. Dit laat zien dat de plannen van de samenwerkingsverbanden steeds concreter worden.

Volgens de samenwerkingsverbanden zijn leraren in de afgelopen periode meer betrokken geraakt bij passend onderwijs. Samenwerkingsverbanden hebben bijvoorbeeld bijeenkomsten georganiseerd, een website ingericht en nieuwsbrieven verstuurd. De vraag is of deze activiteiten ertoe geleid hebben dat leraren en schoolleiders zich ook daadwerkelijk voorbereid voelen.

Monitor over voorbereiding van leraren en schoolleiders

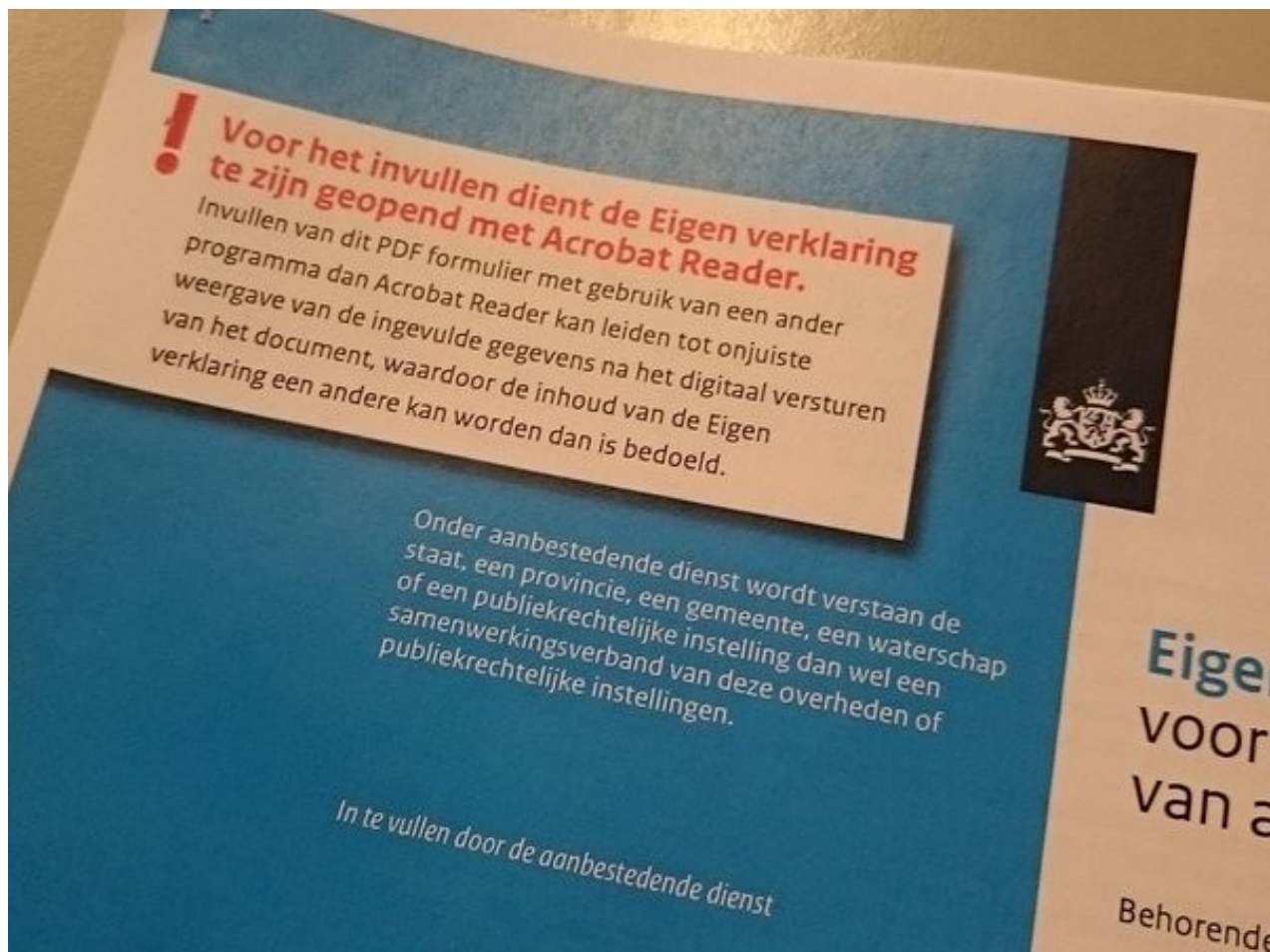
In de eerste helft van februari is daarom onder leraren en schoolleiders gepeild in welke mate zij zich geïnformeerd voelen over passend onderwijs.³ 1369 locatiedirecteuren en 5.200 onderwijspersoneelsleden vulden een vragenlijst in. Deze respons is voldoende om in een groot deel van de samenwerkingsverbanden een beeld van de huidige situatie te vormen. De belangrijkste uitkomsten zijn als volgt:

- Van het onderwijspersoneel vindt 49% (po) en 37% (vo) zichzelf goed op de hoogte van wat er op de eigen school verandert het komende schooljaar door de invoering van passend onderwijs. Er zijn echter grote verschillen tussen *functiecategorieën*: schoolleiders en zorgcoördinatoren, intern en ambulant begeleiders zijn het beste op de hoogte (75-89% goed). Leraren in basis- (50%), speciaal (55%) en vooral voortgezet onderwijs (36%) zijn duidelijk minder op de hoogte.
- Wat betreft de veranderingen voor de eigen situatie is ongeveer de helft van de respondenten in het po en ruim een derde in het vo goed op de hoogte. Schoolleiders (82% goed) en zorgcoördinatoren (79% goed) zijn het beste op de hoogte. Leraren in het speciaal (37%), basis- (33%), en voortgezet onderwijs (25%) zijn duidelijk minder op de hoogte.
- Een grote meerderheid van het personeel in regulier basis- en voortgezet onderwijs verwacht geen of weinig veranderingen voor de school en zichzelf als gevolg van de invoering van

³ Zie voor het volledige rapport de Monitor voorbereiding passend onderwijs, meting 1 (februari 2014). Dit rapport is samen met deze voortgangsrapportage conform toezegging aan de Eerste en Tweede Kamer toegezonden.

Figuur 3. document in Word app iPad (voetnoot zichtbaar, correcte opmaak incl. pagina en pagraaf nummers)

Voorbeeld 2) waarbij het voorgeschreven formaat leidt tot specifieke software met bijbehorende leverancier⁶⁵.



Figuur 4. De overheid eist expliciet een gesloten standaard van de gebruiker.

⁶⁵ <https://www.rijksoverheid.nl/documenten/formulieren/2013/03/22/eigen-verklaring-aanbestedingsprocedure-aanbestedende-diensten>

2. Veiligheid en betrouwbaarheid

Probleem

Er is een sterke toename in valse e-mails, die in naam van o.a. de overheid worden geschreven (zie de links verderop). Deze mails zijn moeilijk van echte mails te onderscheiden, en ze verwijzen dikwijls naar – nauwelijks van echt te onderscheiden – valse websites waar gegevens worden afgevangen. Daardoor komen belangrijke (bijvoorbeeld inlog-) gegevens in handen van criminelen en loopt het vertrouwen van burgers en bedrijven in de (digitale) overheid gevaar.

Analogie

Er is een sterke analogie met de bestaande fysieke geldinfrastructuur. Zowel qua probleem, als qua oplossing.

Sinds het ontstaan van bankbiljetten worden deze vervalst. Omdat het ondoenlijk is de vervalsingen zélf te voorkomen, stopt men echtheidskenmerken in échte bankbiljetten. Het watermerk is daarvan een voorbeeld. Op deze wijze kunnen mensen de echte biljetten van de valse onderscheiden. Dat kunnen de 'eindgebruikers' zijn (consumenten), maar veel vals geld wordt – na controle van de echtheidskenmerken – uit de roulatie gehaald bij 'grootgebruikers' als supermarktketens en banken zelf.

Het is essentieel dat alle échte bankbiljetten dat echtheidskenmerk voeren, anders is het ontbreken ervan geen sluitende indicatie van vervalsing. *Nota bene: dit is een voorbeeld van de onevenredige afname van het nut van een standaard wanneer een aantal partijen niet meedoen (dat geldt ook voor rechts rijden in het verkeer, hoe meer spookrijders, hoe verschrikkelijker de afname van het nut).*

Verder wordt op deze wijze wordt niet aan de wortel voorkomen dat er vals geld gedrukt wordt. Maar het wordt natuurlijk wél onaantrekkelijker om vals geld te drukken (er 'trappen wel veel minder mensen in').

Dat geldt ook voor het terugdringen van het phishing probleem. Zoals gezegd maakt een typische phishing-aanval vaak gebruik van zowel een '*niet van echt te onderscheiden e-mail*', die verwijst naar een '*niet van echt te onderscheiden website*' waar de vertrouwelijke gegevens (zoals inlogcodes) worden afgevangen. Net zoals bij geld draagt de toevoeging van echtheidskenmerken (ook wel authenticiteitskenmerken) bij aan het terugdringen. Zowel in websites als in e-mail kunnen echtheidskenmerken worden gestopt. De banken doen dat bij internet bankieren (o.a. let op het adres van de website, en let op het 'slotje' in de browser), en ze doen dat consequent. Zo weet de klant waar hij op moet⁶⁶ letten, en waar hij vanuit mag gaan. Banken doen dat in toenemende mate ook met hun e-mail. Klanten moeten letten op het afzenderadres, maar meer nog kunnen internetserviceproviders de mails tegenhouden voordat ze eindgebruikers bereiken (analoog

⁶⁶ Sinds enige tijd is in de algemene voorwaarden van banken de bewijslast zelfs omgedraaid. Een klant moet aannemelijk maken dat hij op de echtheidskenmerken heeft gecontroleerd.

aan de supermarkten en banken in het geld-voorbeeld). De onderliggende techniek werkt met behulp van standaarden.

De overheid kan hierin een voorbeeld nemen aan de banken en de onderliggende standaarden consequent gaan gebruiken. Gelet op de urgentie van het probleem, én de onevenredige afname van het nut wanneer een aantal overheidsorganisaties niet meedoen, licht daarvoor een verplichting voor de hand.

De onderliggende standaarden tegen website fraude zijn TLS en DNSSEC, en tegen e-mail fraude de standaarden DKIM, SPF en DMARC. Hieronder een paar schermvoorbeelden van het effect van de toepassing van DKIM.

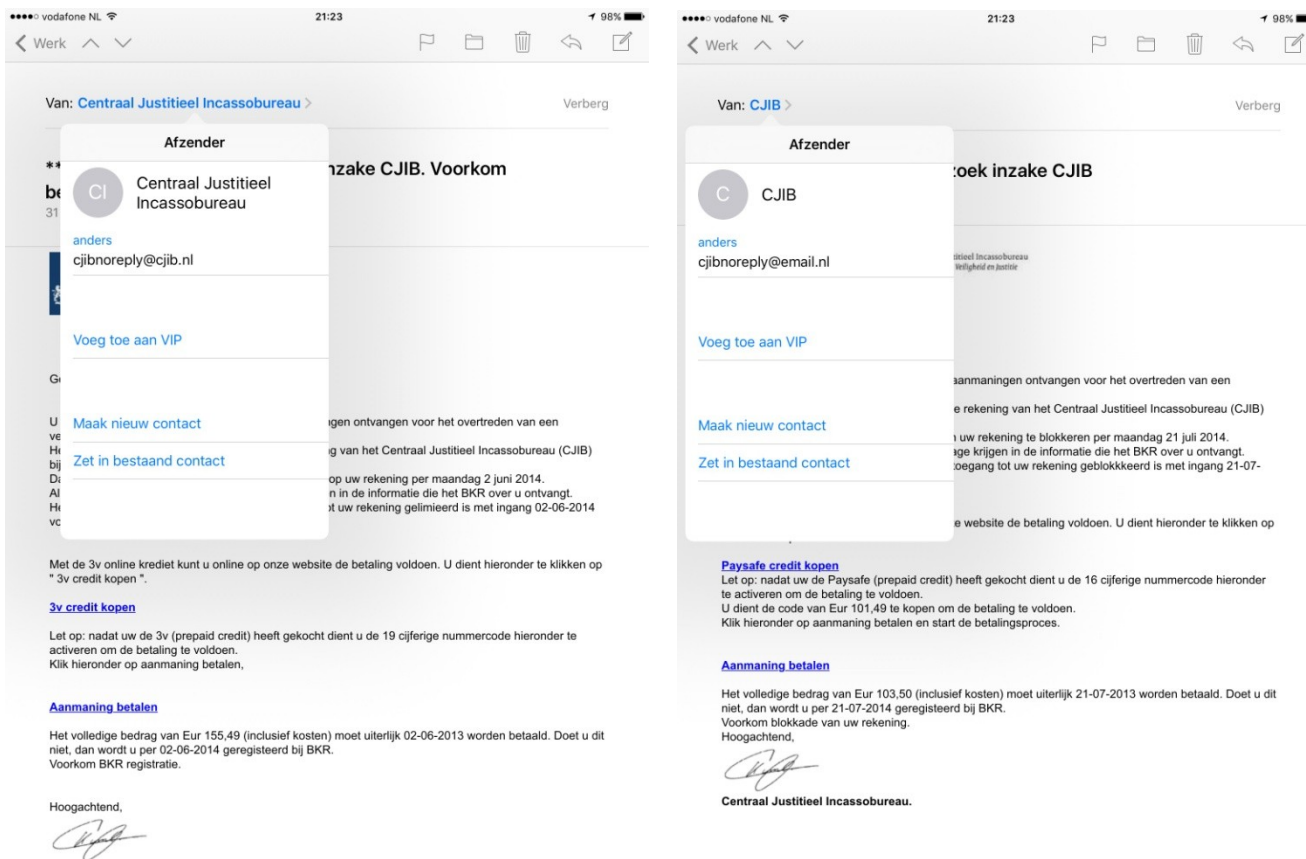
Een recent voorbeeld van de meerwaarde de internationaal breed gebruikte standaard TLS betreft een kwetsbaarheid bij gemeenten⁶⁷. TLS is een echtheidskenmerk, je kunt eraan zien of een website authentiek is. Daarnaast zorgt TLS ervoor dat de communicatie tussen (overheids)website en burger/bedrijf versleuteld is, zodat niemand kan meeluisteren of de informatie kan manipuleren.

Links met voorbeelden van toename in valse mails/valse sites

- Grote toename 'valse e-mails' bij Fraudehelpdesk (7 februari 2016)
<http://nos.nl/l/2085484>
- Sterke stijging in nep-mails (7 januari 2016)
<http://www.crimesite.nl/sterke-stijging-in-melding-nep-mails/>
- Nepmails uit naam van DG Belastingdienst (19 januari 2016)
<http://www.nu.nl/internet/4200310/man-opgepakt-versturen-nepmails-naam-belastingdienst.html>
"De 23-jarige Almeerder maakte vermoedelijk deel uit van een grotere organisatie die mails uit naam van de directeur-generaal van de Belastingdienst verstuurde."
- Criminelen misbruiken overheid in phishingmails
<http://www.volkskrant.nl/tech/criminelen-misbruiken-webwinkels-en-overheid-in-phishingsmails~a4057348/>
- CJIB krijgt veel meldingen van phishing
<http://www.bnr.nl/nieuws/132478-1509/cjib-krijgt-veel-meldingen-van-phishing>
- Belastingdienst waarschuwt voor phishingmail
<http://www.nu.nl/internet/4101462/belastingdienst-waarschuwt-phishingmail.html>
- Hogeschool InHolland waarschuwt voor phishingmails
<http://www.nu.nl/binnenland/4144795/waarschuwing-phishingmail-inholland.html>
- Overheid veel vaker doelwit van cyberaanvallen
<http://www.volkskrant.nl/tech/overheid-veel-vaker-doelwit-van-cyberaanvallen~a4119366/>

⁶⁷ 4 maart 2016: <http://www.rtlnieuws.nl/nieuws/binnenland/beveiliging-tientallen-gemeentesites-lek-persoonsgegevens-niet-veilig>

- Waarschuwing valse CJIB e-mails door Waarschuwingdienst (overheid)
<https://www.waarschuwingdienst.nl/Risicos/Actuele+dreigingen/Softwarelekken/WD-2014-007+Waarschuwing+phishing-e-mail+uit+naam+van+het+Centraal+Justitieel+Incassobureau+CJIB+in+omloop.html>
- Waarschuwingdienst: Sterke toename in nep incasso e-mails
<https://www.waarschuwingdienst.nl/Risicos/Actuele+dreigingen/Virussen+en+wormen/WD-2013-014+Sterke+toename+in+nep+incasso+e-mails.html>



Figuur 5. Voorbeeld van een valse CJIB mail voordat ze DKIM gebruikten (links, let op de afzender @cjb.nl) en een voorbeeld van een valse CJIB nadat ze DKIM gebruiken (rechts, let op de afzender @email.nl)

3. Kostenbesparing

Wanneer een bestuursorgaan niet ontvankelijk is voor communicatie door middel van een bepaalde standaard, zijn andere bestuursorganen gedwongen ook de standaard te gebruiken die dat bestuursorgaan wel hanteert. Dat leidt tot kosten bij deze partijen die vaak niet opwegen tegen de investering die dat orgaan moet doen voor gebruik van die specifieke open standaard. In het kosten-/batenonderzoek naar de potentiële besparingen van de voorzieningen voor het stelsel van basisregistraties kwam naar voren dat bij

standaardisatie op de Digikoppeling standaard, meer dan €78 miljoen⁶⁸ op jaarbasis kan worden bespaard. Hierbij gaat het uitsluitend om kosten die alle bestuursorganen dienen te maken om te kunnen communiceren met andere bestuursorganen.

Wat dit onderzoek ook laat zien is dat de baten exponentieel afnemen naarmate meer organisaties niet meedoen aan het standaardisatieproces. Zo is in het bovenstaande onderzoek tevens berekend wat de impact is als slechts 5 dan wel 6 basisregistraties wel meedoen. Uitgaand van 13 basisregistraties zou men bij een lineaire relatie verwachten dat de besparingen zouden afnemen tot 30 resp. 36 miljoen euro, nog steeds een respectabele besparing. Echter, de besparingen zijn slechts 7,4 resp 11 miljoen euro. Dit bevestigt nog eens het beeld dat standaardisatie pas echt effectief is als iedereen meewerkt: als maar één organisatie niet meer meewerkt dan berokkent deze onevenredig veel schade.

De verplichting om de jaarrekening bij de Kamer van Koophandel via SBR te deponeren levert 68,2 miljoen op jaarbasis op⁶⁹ en heeft geleid tot de verplichting om SBR te gebruiken.

Een ander voorbeeld van kostenbesparingen betreft de Administratieve Lastenreductie van burgers en bedrijven wanneer overheden hen niet telkens hoeven te vragen naar de bekende weg. Dat kan alleen als overheden de haar bekende gegevens onderling – met behoud van kwaliteit en betekenis – uitwisselen. Dat kan alleen als ze daarvoor dezelfde standaarden gebruiken.

4. Leveranciersafhankelijkheid

In het rapport "Mogelijkheden om de afhankelijkheid van ICT-leveranciers te verminderen" van Berenschot, Rand en VKA⁷⁰ wordt geconcludeerd dat open standaarden een probaat middel zijn voor het verminderen van afhankelijkheden van leveranciers. Er is tevens een wisselwerking met de mogelijkheid over te kunnen stappen (exit-strategie: het beperken negatieve gevolgen van exit, doordat bijvoorbeeld gegevens of koppelvlakken - omdat ze in een open formaat zijn ontsloten - nog steeds bruikbaar zijn).

⁶⁸ Verfijning en herijking kostenbatenanalyse voor investeringen in gemeenschappelijke voorzieningen in het stelsel van basisregistraties. PWC, 23 februari 2010

⁶⁹ Tweede Kamer, vergaderjaar 2014–2015, 34 262, nr. 3

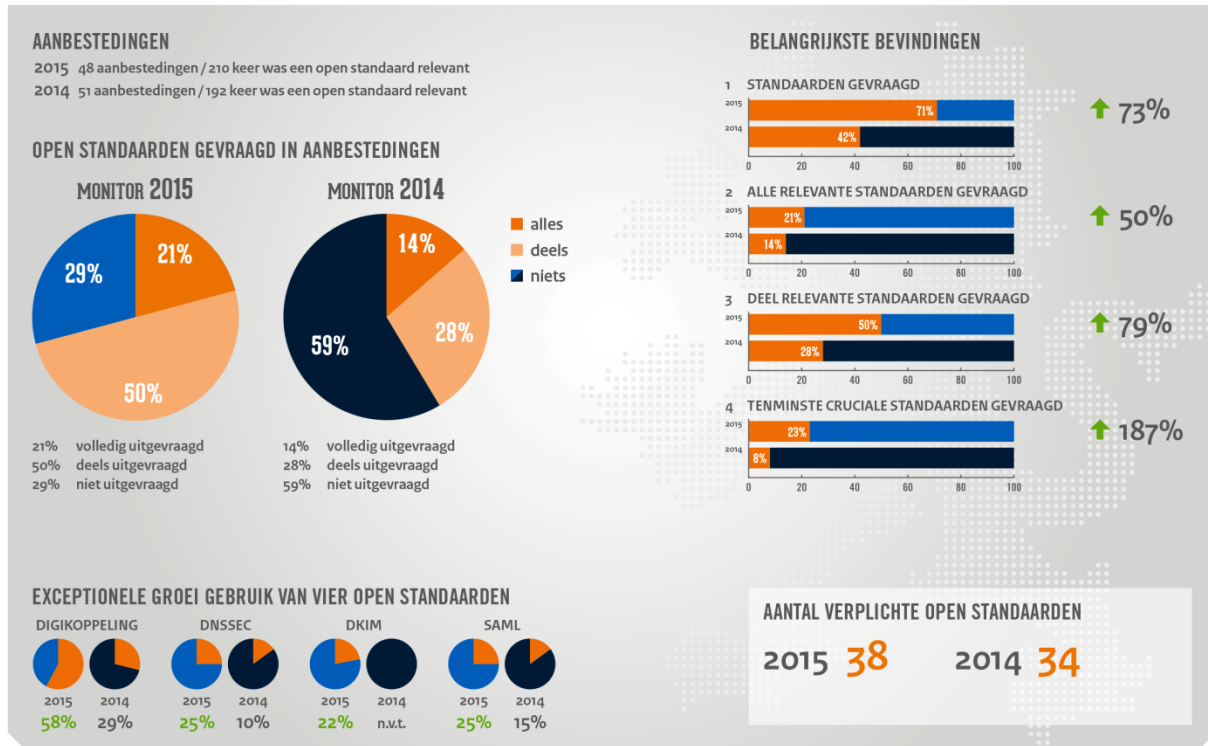
⁷⁰ Bijlage bij Tweede Kamer, vergaderjaar 2015–2016, 26643, nr. 394.

Bijlage F. Beperkt adoptietempo huidige middelen

OPEN STANDAARDENBELEID

AANBESTEDINGEN 2015

METING JULI 2014 - JUNI 2015



Figuur 6. De uitvraag naar open standaarden in de monitor van 2015.

De monitor 2015 laat een verbetering zien in de uitvraag van de pas-toe-of-leg-uit standaarden in aanbestedingen. Toch wordt nog in 79% niet om alle relevante standaarden gevraagd. Dat was in 2014 en voorgaande jaren nog beperkter.

Daarover wordt zelden uitgelegd in de verantwoordingen, terwijl dat wel zou moeten conform de Rijksbegrotingsvoorschriften⁷¹.

Deze beperkte uitvraag, gekoppeld aan de lage frequentie van aanbestedingen, leidt tot een laag adoptie-tempo. Voor sommige standaarden is dat onaanvaardbaar.

In de zomer van 2015 is de adoptie van de hiergenoemde informatieveiligheidsstandaarden in ca. 150 domeinnamen van bestuursorganen in en rondom het Nationaal Beraad gemeten (figuur 8). Eind december is nogmaals gemeten. De groei is daarna geëxtrapoleerd naar

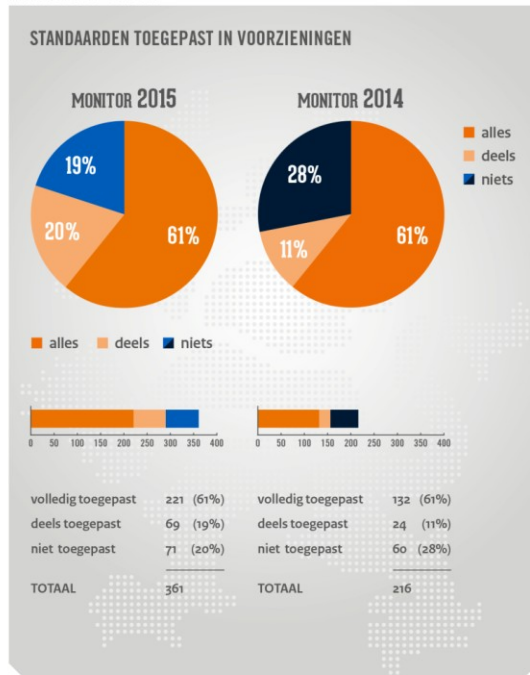
⁷¹ In de Rijksbegrotingsvoorschriften (RBV) is hierin dat Rijksoverheden in de bedrijfsvoeringsparagraaf van hun jaarverslag expliciet verantwoording afleggen over de mate van naleving van 'pas toe of leg uit'.

eind 2017. Zelfs over 2 jaar (b)lijken de standaarden dan – bij deze bestuursorganen - nog lang niet overal waar nodig te worden gebruikt. Dat is hoogst onwenselijk.

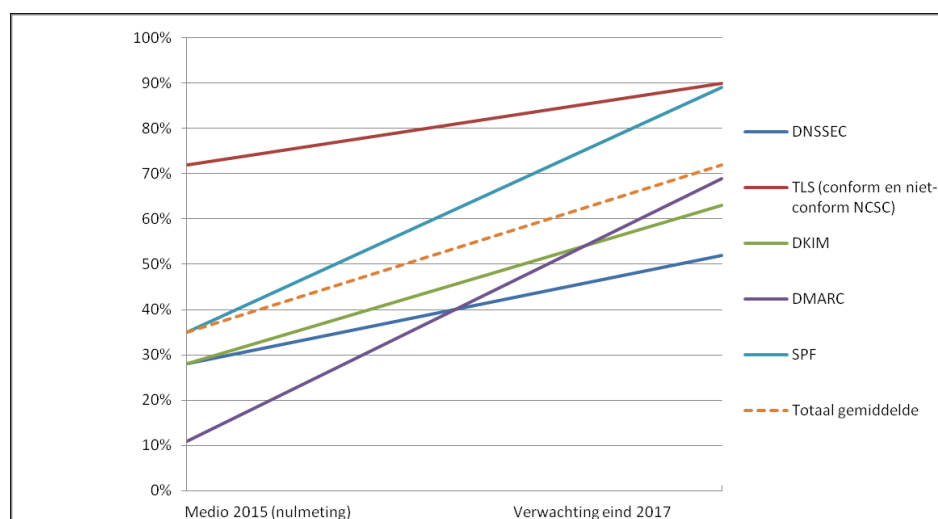
OPEN STANDAARDENBELEID

CENTRALE VOORZIENINGEN 2015

METING JULI 2014 - JUNI 2015



Figuur 7. Ook in de GDI-voorzieningen zijn nog niet alle relevante standaarden geadopteerd.



Figuur 8. Groei van de adoptie van beveiligingsstandaarden.