Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Aanbiedingsformulier Overheidsbreed Beleidsoverleg Digitaal Overheid

1. Korte titel	Standaardisatie: streefbeeldafspraak RPKI
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:	☐ PL ☐ ICM ☐ MFG ☐ MT- DO i.o. **X** Anders: Forum Standaardisatie ☐ Niet Uitkomst behandeling in bovenstaand gremium: ☒ Overeenstemming *(geen toelichting vereist)*
5. Voorgeschiedenis / context *6. Samenvatting/ toelichting*	1. Streefbeeldafspraak RPKI [bijlage 1a.] In 2019 heeft het OBDO besloten om RPKI - een fundamentele beveiligingsstandaard op het gebied van internetroutering - toe te voegen aan de 'pas toe of leg uit'-lijst op advies van het Forum Standaardisatie. Sindsdien zijn overheden verplicht de standaard uit te vragen bij aanbestedingen. Daarmee is de verwachting dat de standaard inmiddels al enige doorwerking op de overheid heeft. Implementatie van de standaard had enkele incidenten in de praktijk kunnen voorkomen. Zo werd in 2014 kortstondig een set IP-adressen van het Ministerie van Buitenlandse Zaken 'gekaapt' door een Bulgaarse partij en in 2019 Europees netwerkverkeer omgeleid via een telecombedrijf in China. Bij wijze van nulmeting wordt in bijgaande nulmeting per domeinnaam aangegeven of RPKI ondersteund wordt. De meetdatum is 31 december 2022. 77,9% van de

	2517 domeinen met een webserver heeft RPKI correct geïmplementeerd, tegenover 75,1% van de 1459 domeinen met een mailserver. Dit geeft aan dat de standaard al breed gedragen wordt binnen de overheid. Kijkende naar de top 10 grootste achterblijvende leveranciers kunnen deze percentages naar 90% toenemen, wanneer deze RPKI ook implementeren. De reeds hoge adoptiegraad, in combinatie met snelle groeimogelijkheden wanneer enkele grote leveranciers instappen, maakt dat het Forum Standaardisatie adviseert om nu een streefbeeldafspraak te maken. De individuele testresultaten per domein per ministerie zijn te vinden in een online bijlage op de website van Forum Standaardisatie: https://www.forumstandaardisatie.nl/sites/default/files/OBDO/2023/0330/1b-Bijlage-nulmeting-streefbeeldafspraak-RPKI-2022.pdf
7. Beslispunten/ discussiepunten	1. Streefbeeldafspraak RPKI Het OBDO stemt in met het maken van de streefbeeldafspraak RPKI.
8. Contactgegevens	Inhoud: Bart Knubben (adviseur) [06-21162373] Proces: Joram Verspaget (bureausecretaris) [06-52845592]

Notitie

OBDO – 30 maart 2023
Overheidsbrede streefbeeldafspraak RPKI

Nummer:	Bijlage 1A – Streefbeeldafspraak RPKI
Aan:	Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO)
Van:	Forum Standaardisatie (via strategisch vooroverleg OBDO)
Datum:	30 maart 2023
Versie:	1.0

Samenvatting

Het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) wordt door het Forum Standaardisatie verzocht om in te stemmen met een overheidsbrede streefbeeldafspraak voor RPKI. Het doel is om alle overheidswebsites en e-maildomeinen van de overheid uiterlijk eind 2024 middels RPKI te beveiligen, en bij netwerkroutering te filteren op ongeldige RPKI-records.

RPKI kan gebruikt worden om de routes die internetverkeer aflegt beter te beveiligen. Hiervoor worden digitaal ondertekende verklaringen gebruikt, welke aangeven vanaf welke oorsprong een IP-adres internetverkeer mag versturen. Deze verklaringen worden centraal opgeslagen, wat het voor gebruikers mogelijk maakt de route van internetverkeer te valideren. Hiermee beveiligt RPKI een fundamenteel onderdeel van het internet. Het OBDO heeft RPKI dan ook al in 2019 op de 'pas toe of leg uit'-lijst geplaatst van Forum Standaardisatie.

Uit de praktijk zijn er incidenten bekend waarbij Europees en Nederlands (overheids)netwerkverkeer oneigenlijk werd omgeleid via buitenlandse telecombedrijven, waaronder China. Deze incidenten hadden met RPKI voorkomen kunnen worden.

Het voorstel tot een streefbeeldafspraak volgt uit een eerder verzoek van Forum om het gebruik van RPKI tot een hoger niveau te brengen. Ten behoeve van dit voorstel is een nulmeting uitgevoerd op Nederlandse overheidsorganisaties. Hieruit blijkt dat 77,9% van de gemeten overheidswebsites RPKI geïmplementeerd hebben. Bij e-maildomeinen ligt dit percentage op 75,1%. Ook op de markt is beweging zichtbaar, zo is RPKI onderdeel van het MANRS-initiatief, een verzameling gedragsregels over netwerkroutering waar ook Nederlandse partijen zich aan hebben gecommitteerd. Individuele meetresultaten per domeinnaam zijn terug te vinden in een online bijlage: https://www.forumstandaardisatie.nl/sites/default/files/OBDO/2023/0330/1b-Bijlage-nulmeting-streefbeeldafspraak-RPKI-2022.pdf

Eerder hebben de streefbeeldafspraken voor internetbeveiligingsstandaarden laten zien dat met een streefbeeldafspraak een adoptie-impuls kan worden gegeven. Gelet op het voorgaande is nu het juiste moment om ook voor RPKI een streefbeeldafspraak te maken. Zo kunnen ook de laatste achterblijvers gestimuleerd worden om tot adoptie over te gaan.

Daarnaast zijn er continu ontwikkelingen op het gebied van internetbeveiliging. Dit maakt dat er met enige regelmaat nieuwe streefbeeldafspraken gemaakt dienen te worden, opdat de digitale

veiligheid van de overheid op pijl blijft. De deadline van de laatste streefbeeldafspraak verliep op 31 december 2021.

Gevraagd besluit

Het OBDO wordt gevraagd om in te stemmen met het advies van het Forum Standaardisatie om:

A. Een streefbeeldafspraak te maken om op alle overheidswebsites en e-maildomeinen van de overheid uiterlijk eind 2024 de open standaard Resource Public Key Infrastructure (RPKI) toe te passen. Dit behelst voor deze diensten:
   i. Het publiceren van autoritatieve, digitaal getekende verklaringen (Route Origin Authorizations ofwel ROA's) voor de IP-adresblokken die gebruikt worden door webservers, mailservers en autoritatieve nameservers van overheden;
   ii. Het filteren op basis van gepubliceerde verklaringen door netwerksystemen van de overheid, waarbij invalide routes nooit geaccepteerd of geadverteerd mogen worden.
B. Om door Forum Standaardisatie de implementatievoortgang van de publicatiezijde (onderdeel i onder punt A) van RPKI halfjaarlijks te laten meten en daarover te rapporteren.
C. Koepels en samenwerkingsverbanden (zoals CIO-Beraad, Manifestgroep, IPO, VNG Realisatie en UVW) te verzoeken om hun achterban actief te stimuleren en zelf het goede voorbeeld te geven.

Achtergrond

RPKI is door het OBDO in 2019 toegevoegd aan de "pas toe, of leg uit"-lijst op advies van Forum Standaardisatie. De afgelopen jaren hebben overheidsorganisaties de tijd gehad om RPKI verder uit te rollen en dienen alle nieuwe systemen aan RPKI te voldoen.

Het implementeren van RPKI draagt bij aan een veiliger en betrouwbaar internet. Daarom is het van belang dat niet alleen nieuwe systemen RPKI implementeren, maar op den duur de gehele infrastructuur van de overheid RPKI implementeert. Dit betreft dus zowel het publiceren van digitale verklaringen voor IP-ranges, als het valideren van verklaringen door netwerkrouters. Forum Standaardisatie heeft daarom zelf eerder aangegeven dat een streefbeeldafspraak een goede volgende stap kan zijn.

1. Over RPKI

Nut

Resource Public Key Infrastructure (RPKI) is een open standaard met als doel om zogenaamde route hijacks te voorkomen. Bij een route hijack wordt internetverkeer omgeleid naar de systemen van een niet-geautoriseerd netwerk. Een hijack kan het gevolg zijn van een simpele typefout van een netwerkbeheerder die daarmee onbedoeld internetverkeer omleidt, of het gevolg zijn van een doelgerichte aanval op de infrastructuur van het internet om bijvoorbeeld websites onbereikbaar te maken of om gegevens van internetgebruikers afhandig te maken.[1] Een relevant voorbeeld hiervan betreft een incident waarbij een set IP-adressen van het ministerie van Buitenlandse Zaken in 2014 tijdelijk gekaapt is door een Bulgaarse partij.[2] [3] Bij een tweede voorbeeld uit 2019

[1] https://www.computable.nl/artikel/opinie/infrastructuur/6526971/1509029/de-on-veiligheid-van-de-routetabel.html, https://tweakers.net/nieuws/131133/phishingcampagne-gericht-op-myetherwallet-heeft-13000-euro-opgeleverd.html, https://rpki.readthedocs.io/en/latest/rpki/resources.html#examples-of-bgp-hijacks
[2] https://zoek.officielebekendmakingen.nl/ah-tk-20142015-3181.html
[3] https://www.volkskrant.nl/wetenschap/ip-adressen-ministerie-gekaapt-door-bulgaren~b75ad982/

werd een groot deel van het Europese netwerkverkeer kortstondig doorgeleid via een Chinese telecomprovider.[4]

Werking

Met RPKI kan de rechtmatige houder van een blok IP-adressen een autoritatieve, digitaal getekende verklaring publiceren met betrekking tot de intenties van de routering vanaf haar netwerk. Deze verklaringen, genaamd Route Origin Authorisations (ROA's), kunnen andere netwerkbeheerders cryptografisch valideren en vervolgens gebruiken om filters in te stellen. Hiermee filteren routers routes uit die in strijd zijn met de voor de betreffende IP-adressen gepubliceerde ROA's.

RPKI vraagt dus om actie vanuit twee partijen. Ten eerste moet de houder van de IP-adressen ROA's publiceren. Ten tweede moet de partij die via Border Gateway Protocol (BGP) routes ontvangt van andere netwerken filteren op basis van alle wereldwijd gepubliceerde ROA's, waarbij invalide routes nooit geaccepteerd of geadverteerd mogen worden. Partijen die namens overheden IP-adressen publiceren moeten dus conform voorgaande ROA's publiceren. Verder moeten partijen die aan overheden netwerkdiensten aanbieden genoemde filtering toepassen. Overheden die deze diensten zelf uitvoeren en beheren moeten deze acties uiteraard zelf uitvoeren. BGP Routering valt terug op bestaande (onbeveiligde) routering als RPKI wegvalt. Er is geen onderbreking van de routering te verwachten wanneer RPKI-data niet beschikbaar is.

RPKI Route Origin Validation is gestandaardiseerd in RFC 6811.[5] Bij implementatie kan gebruik gemaakt worden van de operationele ervaring zoals beschreven in sectie 5 van RFC 7115[6], en in het hoofdstuk "validating routes" van het RPKI-documentatieproject geschreven door leden van de Internet-gemeenschap.[7]

Marktontwikkelingen

Op de markt wordt de meerwaarde van RPKI voor de stabiliteit van het internet ingezien. Dit is terug te zien in het feit dat RPKI onderdeel is van het Mutually Agreed Norms for Routing Security (MANRS)-initiatief.[8] Binnen dit initiatief committeren organisaties, zoals internetproviders, zich aan een set van gedragsregels betreffende internetroutering. Deze gedragsregels kunnen standaarden, best practices en onderlinge afspraken beslaan. RPKI is een van de standaarden die via MANRS wordt aanbevolen.

Ook Nederlandse partijen zijn bij het MANRS-initiatief aangesloten, zoals Stichting Internet Domeinregistratie Nederland (SIDN), SURF en KPN.[9] Naar verwachting neemt Forum Standaardisatie MANRS in procedure als proof of concept voor 'andersoortige standaarden' op de lijst aanbevolen standaarden. De Internet Society heeft aangegeven MANRS aan te melden in het kader van deze proof of concept.

Wereldwijd is op het moment van schrijven ongeveer 40% van alle gepubliceerde routes voorzien van ROA-records.[10] Binnen Nederland blijkt ruim 80% van alle domeinnamen volledig beschermd door middel van ROA-records.[11]

2. RPKI bij de overheid

Pas toe of leg uit

Het OBDO heeft RPKI in 2019 op de 'pas toe of leg uit'-lijst geplaatst. Dit betekent dat overheidsorganisaties verplicht zijn RPKI op te nemen in aanbestedingen voor die nieuwe

[4] https://www.manrs.org/2019/06/large-european-routing-leak-sends-traffic-through-china-telecom/
[5] RFC 6811 https://tools.ietf.org/html/rfc6811 | BGP Prefix Origin Validation
[6] RFC 7115, sectie 5: https://tools.ietf.org/html/rfc7115#section-5
[7] Validating Routes: https://rpki.readthedocs.io/en/latest/rpki/using-rpki-data.html#validating-route
[8] https://www.manrs.org/
[9] https://www.manrs.org/netops/participants/
[10] https://roa-stats.manrs.org/
[11] https://stats.sidnlabs.nl/nl/web.html#secure%20routing%20(rpki)

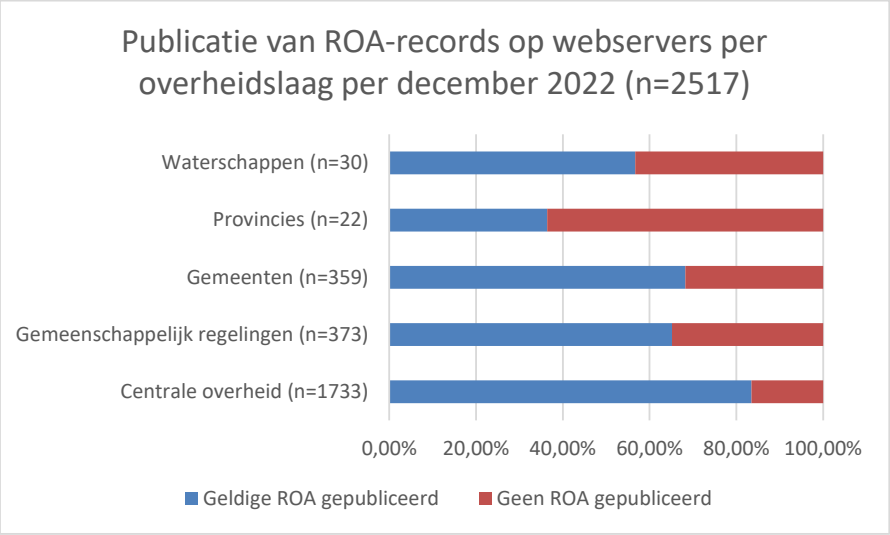
systemen waar deze standaard relevant is. Er bestaat nog geen verplichting om bestaande systemen aan te passen, zodat zij RPKI ondersteunen.

Een streefbeeldafspraak sluit aan bij de ambitie over RPKI die Forum Standaardisatie in de vergadering van 9 juni 2021 heeft uitgesproken.[12]

Statistieken

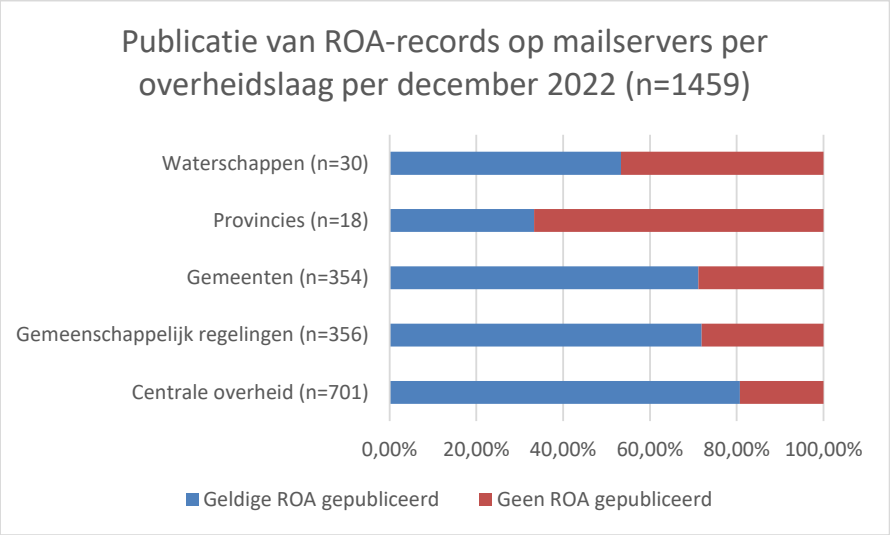
RPKI maakt sinds augustus 2022 onderdeel uit van testtool Internet.nl. In december 2022 is een meting uitgevoerd op de ongeveer 2500 domeinnamen die deel uitmaken van de Meting Informatieveiligheidstandaarden.[13] Deze set domeinnamen is samengesteld uit het Websiteregister Rijksoverheid en de lijst van overheidsorganisaties.[14] In deze meting wordt alleen gecontroleerd of voor ieder IP-adres een geldige ROA is gepubliceerd. Tijdens de meting werden geen ongeldige ROA's gedetecteerd. Dit betekent dat alle overheidsorganisaties die reeds RPKI hebben geïmplementeerd, dit op een correcte wijze hebben gedaan.

De meting bestaat uit een websitetest en een mailtest. De websitetest kijkt naar de adressen van de webserver en bijhorende nameservers. In deze test bleken 2517 domeinnamen een webserver te serveren, waarvan 77,9% RPKI correct geïmplementeerd heeft. De mailtest kijkt naar de adressen van de mailserver, de nameservers van het domein en de nameservers van de mailserver. Binnen de set domeinnamen waren er 1459 met een gekoppelde mailserver, waarvan 75,1% RPKI correct geïmplementeerd had. De resultaten van deze tests zijn in onderstaande grafieken per overheidsorganisatie uitgesplitst.



Uit de websitetest is op te maken dat de centrale overheid voorloopt op de adoptie van RPKI en al een hoge adoptiegraad (83%) heeft bereikt. De provincies blijken daarentegen het meest achter te lopen met adoptie (36%).

[12] https://www.forumstandaardisatie.nl/vergaderingen/2021/fs-20210929-1b-verslag-forum-standaardisatie-9-juni-2021
[13] https://forumstandaardisatie.nl/nieuws/bredere-aanpak-meting-informatieveiligheidstandaarden-legt-achterblijvers-bloot
[14] https://websiteregisterrijksoverheid.nl en https://organisaties.overheid.nl



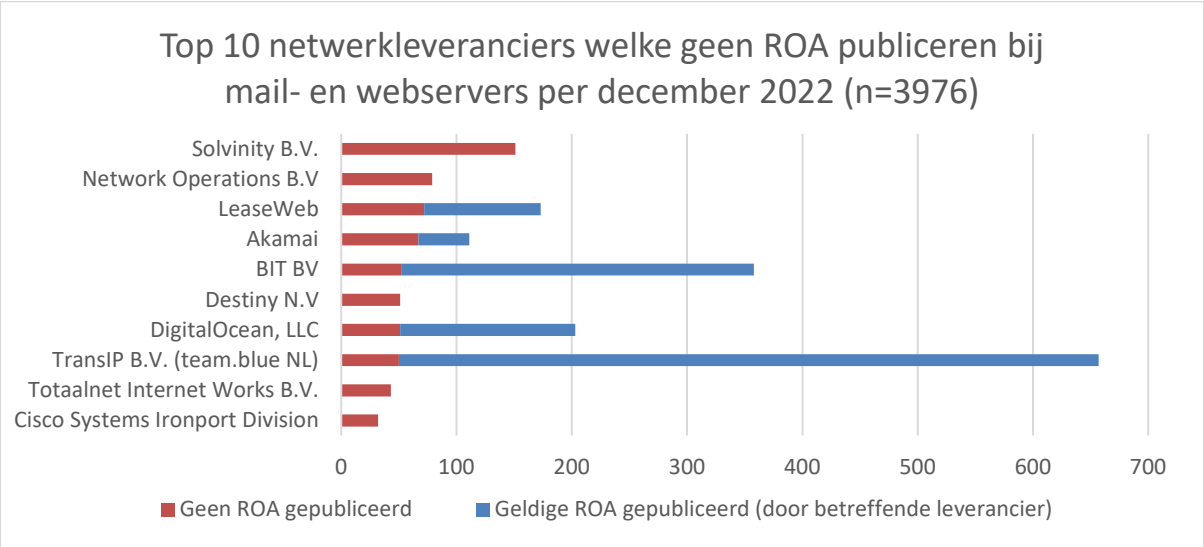
In de resultaten van de mailtest is een vergelijkbaar beeld te zien. Opvallend is dat de centrale overheid marginaal slechter scoort (81%) dan in de websitetest, terwijl de andere overheidslagen marginaal beter scoren dan in de mailtest.

De over het algemeen hoge adoptie laat zien dat de tijd nu rijp is om een extra impuls aan de achterblijvers te geven middels het maken van een streefbeeldafspraak. In een online bijlage kan ook de resultaten per gemeten domeinnaam ingezien worden, opdat overheidsonderdelen kunnen inzien waar er nog actie benodigd is.[15]

De meting beperkt zich tot het publiceren van ROA-records. Voor RPKI is het ook noodzakelijk dat internetverkeer gefilterd wordt op ongeldige records. Om hier inzicht in te krijgen, is de afgelopen jaren een uitvraag aan overheidsorganisaties gedaan in het kader van de Monitor Open Standaarden. In de laatste uitvraag, in 2022, bleek dat uit zes respondenten twee organisaties RPKI-validatie toepasten. Twee andere organisaties gaven aan dit op hun interne planning te hebben staan.

[15] https://www.forumstandaardisatie.nl/sites/default/files/OBDO/2023/0330/1b-Bijlage-nulmeting-streefbeeldafspraak-RPKI-2022.pdf

Uit onderzoek naar de betrokken netwerkleveranciers blijkt dat het aantal verschillende leveranciers beperkt is. Bij de web- en mailtest zijn 231 netwerkleveranciers gevonden, waarvan 122 volledig voldoen aan de standaard, 61 gedeeltelijk voldoen en 48 niet voldoen. De top 10 leveranciers welke geen ROA-records publiceren, veroorzaken 59% van de falende RPKI-validatie op mail- en webservers. Wanneer er bij een mail- of webserver geen ROA wordt gepubliceerd komt dit gemiddeld door 1,2 netwerkleverancier. De top 10 is benaderd met de vragen wanneer RPKI volledig wordt geïmplementeerd en wat de oorzaak is dat RPKI nog niet volledig is geïmplementeerd.



3. Achtergrond streefbeeldafspraken

Sinds 2015 biedt het Platform Internetstandaarden de mogelijkheid om via de website Internet.nl domeinen te toetsen op het gebruik van een aantal moderne internetstandaarden, waaronder een aantal informatieveiligheidstandaarden, die op de 'pas toe of leg uit'-lijst van Forum Standaardisatie staan. In datzelfde jaar is Forum Standaardisatie gestart om met behulp van Internet.nl een halfjaarlijkse meting van de adoptiegraad van informatieveiligheidsstandaarden voor overheidsdomeinen (web en e-mail) uit te voeren.

Die metingen hebben ertoe geleid dat het Nationaal Beraad in februari 2016 de ambitie uitsprak deze standaarden versneld te willen adopteren. Dit betekent concreet dat voor deze standaarden niet het tempo van 'pas toe of leg uit' wordt gevolgd (d.w.z. wachten op een volgend investeringsmoment en dan de standaarden implementeren), maar dat actief wordt ingezet op implementatie van de standaarden op de kortere termijn.

Onderdeel van deze afspraak is dat Forum Standaardisatie de voortgang van de adoptie meet en inzichtelijk maakt. De halfjaarlijkse Meting Informatieveiligheidstandaarden is ook onderdeel van de jaarlijkse Monitor Open Standaarden. De eerste streefbeeldafspraak is eind 2017 afgelopen. Begin 2018 is een eindmeting voor deze afspraak gepubliceerd. Ondanks een grote stijging was volledige adoptie nog niet bereikt. Daarom zijn deze afspraken in april 2018 herbevestigd en aangevuld met aanvullende streefbeeldafspraken door het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO), de opvolger van het Nationaal Beraad.

Bij een evaluatie van de eerste streefbeeldafspraak[16] werd geconcludeerd dat de streefbeeldafspraak van het Nationaal Beraad over de adoptie van informatieveiligheidstandaarden voor eind 2017 een succes is geweest. Met deze afspraak werd beoogd om een grote stimulans te geven aan de adoptie van deze standaarden, en dat is ook feitelijk terug te zien in de resultaten. Het succes van deze afspraak is toe schrijven aan een aantal punten die meer algemeen geformuleerd kunnen worden:

- De afspraak speelt een informerende rol. Het maakt duidelijk aan organisaties wat er moet gebeuren en wanneer dit gedaan moet zijn, en dat geeft richting aan de adoptie.
- De afspraak speelt een dwingende rol. Organisaties worden aangesproken wanneer ze niet voldoen aan de gemaakte afspraak.
- De afspraak speelt een ondersteunende rol. Organisaties zoals Forum Standaardisatie die adoptie stimuleren kunnen in contact met organisaties verwijzen naar de gemaakte afspraken.

Ook bij de latere streefbeeldafspraken is de groei in adoptie van de standaarden duidelijk terug te zien in de metingen.[17]

[16] Oplegnotitie adoptie open standaarden https://www.forumstandaardisatie.nl/sites/bfs/files/proceedings/FS%20180314.4A%20Evaluatie%20en%20vervolg%20streefbeeldafspraak%20IV-standaarden.pdf

[17] https://forumstandaardisatie.nl/metingen/informatieveiligheidstandaarden