# Notitie

## FORUM STANDAARDISATIE 8 februari 2023
## Agendapunt 5A Streefbeeldafspraak RPKI

| | |
|---|---|
| Nummer: | FS-20230208.5A |
| Aan: | Forum Standaardisatie |
| Van: | Stuurgroep Open Standaarden |
| Datum: | 30 januari 2023 |
| Versie: | 1.0 |

## Samenvatting

Forum Standaardisatie wordt gevraagd om in te stemmen met het advies aan het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) om een overheidsbrede streefbeeldafspraak voor de open standaard RPKI vast te stellen. Het doel is dat alle overheidswebsites en e-maildomeinen van de overheid uiterlijk eind 2024 met RPKI beveiligd zijn, en dat netwerken van de overheid dan ook filteren op ongeldige RPKI-status.

Met RPKI (afkorting voor: Resource Public Key Infrastructure) kan de rechtmatige houder van een blok IP-adressen een digitaal ondertekende verklaring met route-autorisatie (Route Origin Authorisation; afgekort: ROA) publiceren. Een andere netwerkprovider die internetverkeer wil sturen naar een bepaalde IP-adres, kan de bijbehorende verklaring gebruiken om ongeldige (Invalid) routes te filteren. Daarmee voorkomt de netwerkprovider dat internetverkeer vanuit zijn netwerk naar ongeautoriseerde providernetwerken wordt gestuurd.

RPKI kan bepaalde zogenaamde route hijacks voorkomen. Bij een route hijack wordt internetverkeer omgeleid naar de systemen van een niet-geautoriseerd netwerk. Een relevant voorbeeld hiervan betrof een incident waarbij een set IP-adressen van het ministerie van Buitenlandse Zaken in 2014 tijdelijk gekaapt werd door een Bulgaarse partij, dat leidde tot Kamervragen.

Het OBDO heeft RPKI in 2019 op de 'pas toe of leg uit'-lijst geplaatst van Forum Standaardisatie. Het voorstel tot een streefbeeldafspraak volgt uit een eerder verzoek van Forum Standaardisatie 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 veel marktpartijen maken al gebruik van RPKI. Zo is RPKI onderdeel van het groeiende MANRS-initiatief, een verzameling gedragsregels over netwerkroutering waar ook Nederlandse partijen zich aan hebben gecommitteerd.

Eerder hebben de streefbeeldafspraken voor internetbeveiligingsstandaarden laten zien dat hiermee 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.

# Gevraagd besluit

Het Forum Standaardisatie wordt gevraagd om in te stemmen met het advies om de volgende punten ter besluitvorming aan het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) voor te leggen:

A. Maak een streefbeeldafspraak om uiterlijk eind 2024 de open standaard Resource Public Key Infrastructure (RPKI) toe te passen. Dit omvat:
   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. Laat Forum Standaardisatie de implementatievoortgang van de publicatiezijde (onderdeel i onder punt A) van RPKI halfjaarlijks meten en daarover te rapporteren in de Metingen Informatieveiligheidstandaarden.
C. Verzoek koepels en samenwerkingsverbanden (zoals CIO-Beraad, Manifestgroep, IPO, VNG Realisatie en UvW) 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 binnen afzienbare tijd de gehele infrastructuur van de overheid RPKI implementeert. Dit betreft dus zowel het publiceren van digitale verklaringen voor IP-blokken, als het valideren van verklaringen door netwerkrouters. Forum Standaardisatie heeft daarom zelf al eerder besproken dat een streefbeeldafspraak een logische volgende stap lijkt te 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 betrof een incident waarbij een set IP-adressen van het ministerie van Buitenlandse Zaken in 2014 tijdelijk gekaapt werd door een Bulgaarse partij.[2] Over dat incident werden destijds Kamervragen gesteld.[3]

[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://www.volkskrant.nl/wetenschap/ip-adressen-ministerie-gekaapt-door-bulgaren~b75ad982/
[3] https://zoek.officielebekendmakingen.nl/ah-tk-20142015-3181.html

## 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. BGP Routering valt terug op bestaande (onbeveiligde) routering als RPKI wegvalt. Er is geen onderbreking van de routering wanneer RPKI-data niet beschikbaar is.

RPKI Route Origin Validation is gestandaardiseerd in RFC 6811.[4] Bij implementatie kan gebruik gemaakt worden van de operationele ervaring zoals beschreven in sectie 5 van RFC 7115[5], en in het hoofdstuk "validating routes" van het RPKI-documentatieproject geschreven door leden van de Internet-gemeenschap.[6]

De streefbeeldafspraak betekent dat partijen die namens overheden IP-adressen beheren ROA's moeren 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.

## 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.[7] 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.[8] De adoptie van MANRS wordt op Europees niveau gemeten via de EU Internet Standards Deployment Monitoring Website.[9] Het Bureau Forum Standaardisatie neemt MANRS in procedure als proof of concept voor 'andersoortige standaarden' op de lijst aanbevolen standaarden.

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 website-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 te eisen als zij nieuwe ICT-systemen of -diensten

[4] RFC 6811 https://tools.ietf.org/html/rfc6811 | BGP Prefix Origin Validation
[5] RFC 7115, sectie 5: https://tools.ietf.org/html/rfc7115#section-5
[6] Validating Routes: https://rpki.readthedocs.io/en/latest/rpki/using-rpki-data.html#validating-route
[7] https://www.manrs.org/
[8] https://www.manrs.org/netops/participants/
[9] https://ec.europa.eu/internet-standards/manrs.html
[10] https://roa-stats.manrs.org/
[11] https://stats.sidnlabs.nl/nl/web.html#secure%20routing%20(rpki)

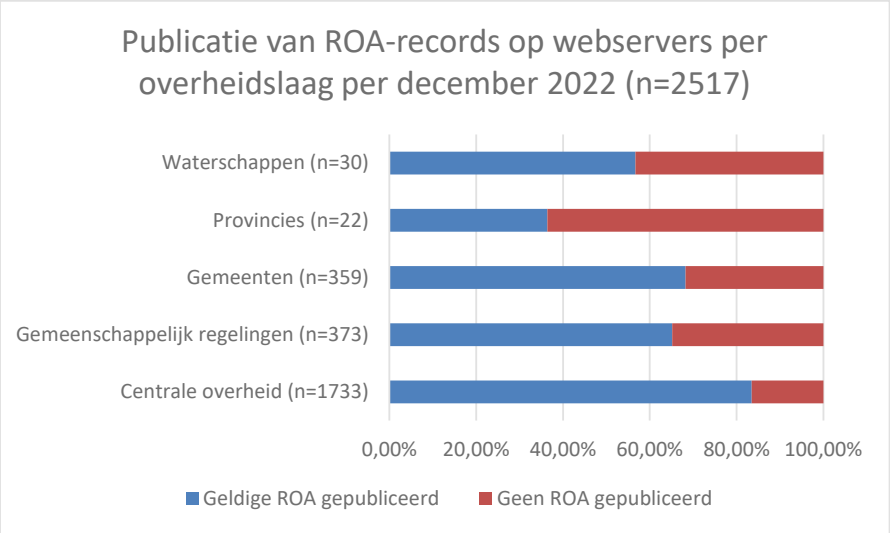
waarvoor deze standaard relevant is aanschaffen. Er bestaat nog geen verplichting om RPKI op alle ICT-systemen of -diensten ook daadwerkelijk te gebruiken. De geadviseerde streefbeeldafspraak zorgt daar wel voor en sluit aan bij de ambitie over RPKI die Forum Standaardisatie in de vergadering van 9 juni 2021 heeft uitgesproken.[12]

Het belang van veilige routering wordt ook in de Basline Informatiebeveiliging Overheid onderschreven. Zo staat in maatregel 14.1.3 het volgende (onderstreping toegevoegd): *"Transacties van toepassingen beschermen: Informatie die deel uitmaakt van transacties van toepassingen behoort te worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen."*[13]

## Statistieken

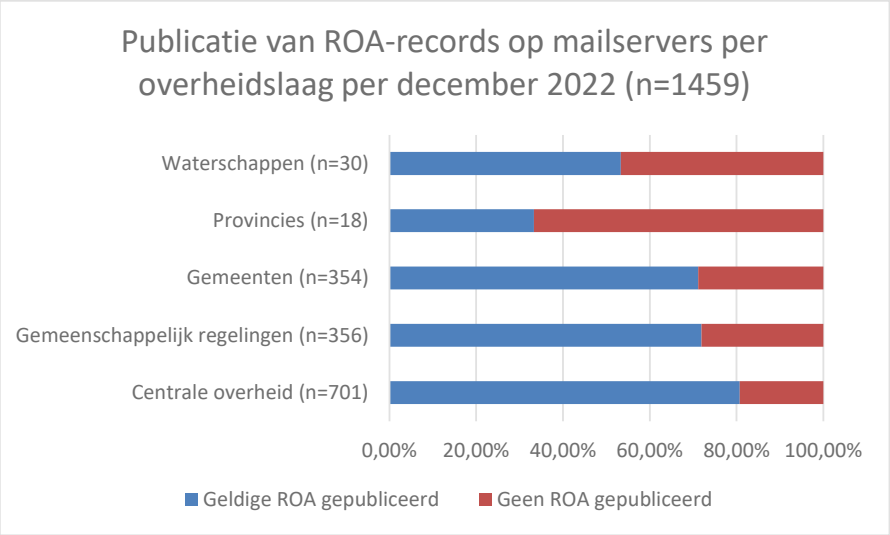
De publicatiekant van RPKI kan sinds augustus 2022 worden gemeten met de testtool Internet.nl. In december 2022 is een meting uitgevoerd op de ongeveer 2500 domeinnamenvan de overheid die deel uitmaken van de Meting Informatieveiligheidstandaarden.[14] Deze set domeinnamen is samengesteld uit het Websiteregister Rijksoverheid en het Register van Overheidsorganisaties.[15] In deze meting wordt 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://bio-overheid.nl/
[14] https://forumstandaardisatie.nl/nieuws/bredere-aanpak-meting-informatieveiligheidstandaarden-legt-achterblijvers-bloot
[15] 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 website.

De over het algemeen reeds 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.

De meting beperkt zich tot het publiceren van ROA-records. Voor RPKI is het ook noodzakelijk dat internetverkeer gefilterd wordt wanneer er een RPKI-status 'ongeldig' optreedt. Om hier inzicht in te krijgen, is de afgelopen jaren een uitvraag onder een aantal grote overheidsorganisaties (zoals de Belastingdienst, de Politie, de VNG, SSC ICT, Logius en de ministeries van Defensie en Justitie en veiligheid) 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.[16]

# 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

[16] Monitor Open standaarden 2022, https://www.forumstandaardisatie.nl/sites/default/files/FS/2022/1207/FS-20221207.4A2-Monitor-Open-standaarden-2022.pdf

aangevuld met aanvullende streefbeeldafspraken door het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO), de opvolger van het Nationaal Beraad.

Bij de evaluatie van de eerste streefbeeldafspraak[17] 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.[18]

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

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